September 2015
White Paper

The Use of Information Technology in Risk Management

Author

Tom Patterson, CPA
Complex Solutions Executive
IBM Corporation

Executive Summary:

These days, executives recognize enterprise risk management (ERM) as a much-needed core competency that helps organizations deliver and increase stakeholder value over time. Because ERM is viewed as an essential tool for helping management continually create, sustain, and deliver value, an ERM program is then only as effective as the people, processes, and technologies the program uses. As executives increase their focus on risk management as an emerging core competency, many also see the need for better data and information, so their organizations can take action on an ever-evolving inventory of risks. One challenge risk managers face, however, is risk data scattered across the organization and not shared across business unit silos. Equally challenging is that many risk management functions lack the tools they need to capture and use risk information more effectively. So, to be truly effective, risk management teams must facilitate and encourage the capture, analysis, and delivery of current and forward-looking (predictive or directive) risk information. Predictive risk information can give management a leg-up in making better informed decisions and help them take actions that produce more reliable outcomes. Leading organizations realize risk management is fundamental to good organizational governance because managing risks effectively requires management to connect and align the organization's assets, people, activities, and goals, and it does that by focusing attention on the achievability of the organization's important objectives.

> An Ernst & Young study concluded: "Effectively harnessing technology to support risk management is the greatest weakness or opportunity for most organizations."

Yet, many ERM programs also fall short when it comes to having skilled "risk aware" resources, analytical processes, and tools. Many risk programs can also do a better job identifying, collecting, and analyzing risk data and preparing to respond to risk scenarios, as evidenced in root cause analyses done after the occurrence of an unexpected loss event. But, the good news is that evolutions in computing and risk technology, and related developments in new technologies that exploit Big Data, analytics, mobile applications, cloud computing, enterprise resource planning (ERP), and governance, risk, and compliance (GRC) systems, are also

important for risk management. These technical advancements offer risk managers and those in management or outside the organization engaged in improving existing risk management programs with better abilities for enhancing risk management effectiveness.

This report was written for risk professionals and CPAs engaged in operating, managing, and evaluating the effectiveness of risk management functions and their investments in risk information technology (IT). This report contains general information on current trends in technology tools (those becoming more visible to risk managers) and covers simple and more sophisticated risk applications and explains how they can be useful in enhancing the maturity of risk management overall. Finally, this report compliments a recently released AICPA publication, *Enterprise Risk Management: A Practical Guide to Implementation and Assessment*.

The Evolving Use of IT

Almost all organizations these days would say they are critically dependent on IT as the enabler of their continued success. This is especially true if one considers the potential impacts from a data breach or network outage, as demonstrated recently in the Sony attack and data theft. As IT and related technologies continue to evolve, organizations see more uses for leveraging technology to do the following:

- More accurately and securely connect, communicate, and process business transactions with customers, suppliers, and other stakeholders
- Support human resources management and talent attraction and sustainment
- Handle detailed logistics activities across globally-integrated business operations or supply-chain processes
- Support execution of business strategies and objectives and assign the accountability for execution and achievement of these strategies and objectives with key managers

IT also supports and underlies other business-related activities, such as scientific and quantitative research, financial modeling applications for asset-trading firms, and the monitoring of assets and asset values, investment positions, and contractual liabilities. IT tools are also used to support enterprise-wide GRC activities, such as inventorying the entity's risks, control activities, and control testing and monitoring required by market and regulatory authorities. Such tools can be very simple applications that operate on one personal computer connected to the Internet or intranet, or they can be very sophisticated. However, when one considers the breadth of technology options available today, it is encouraging to realize that continuing evolutions in IT will provide risk managers and CPAs many opportunities to continue to add value to the discipline of risk management.

One interesting recent development in the evolution of IT is the introduction of viable cognitive computing applications, which represent a giant leap in computing capabilities from traditional, highly programmed applications. This evolution is the next step in computing that originally began with large computational machines that calculated complex mathematical problems, which then evolved into programmable computers that executed millions of pre-defined commands to solve more complex problems. The theoretical next step in the evolution of computing has been described as "artificial intelligence," in which computers are able to ingest and organize massive amounts of facts and data points and be programmed to apply natural language programming and complex algorithms to self-learn, apply logical thinking, and apply knowledge to problem solving. One interesting development in this regard was the introduction of the IBM Watson computer on the U.S. television show *Jeopardy*. As a test to see whether a computer could ingest massive amounts of data, and after some time in preparation, the Watson computer beat the top two all-time Jeopardy champions, proving that this next evolution of natural language computing applied to massively large, big data repositories can have very practical applications to real world problems. Although this paper is not about this emerging shift in computing technology, the application of this game-changing technology to risk management will also fundamentally transform the risk technology used in the future.

ERM

Generally accepted risk management principles and standards articulate that an effective risk management program is one that operates in an organization in which the governing board and executives formally accept responsibility for managing enterprise risks, and in doing so, agree to adhere to generally accepted risk management standards. Standards such as the Committee of Sponsoring Organizations' (COSO) ERM

Framework (COSO ERM) and the International Standards Organization's ISO31000 are considered acceptable ERM frameworks and recognize the connection between good governance and effective risk management. These standards also prescribe that to be effective, an ERM program should integrate "risk informed" or "risk aware" decision making into an entity's formal governance structures and processes. So, an effective risk program should provide management with an enhanced ability to continually capture, evaluate, analyze, and respond to risks arising from changing internal operations, external markets, or regulations. Not managing these changes effectively can produce financial losses, negative publicity, and affect the achievement of the organization's objectives or mission. Therefore, effective risk programs consider, evaluate, and provide input to an organization's planning and performance measuring and support the evaluation of potentially negative events and their impacts from changes to an organization's established risk appetite and tolerance-setting processes. ERM framework standards, such as COSO ERM, also note that information and communication are essential framework components, but more importantly, feedback tools.

Having timely information is key to an effective ERM program. Immediately knowing a key supplier has experienced significant disruptions to a raw materials supply chain, for example, allows customers to invoke supply chain resiliency plans to quickly secure replacement materials elsewhere. Without that timely information, a supplier's disruption might also disrupt its customer's manufacturing processes. Because of such scenarios, management must continually monitor internal operations, suppliers, related parties, counter-parties, and customers to look for changing circumstances that must be addressed to reduce the risk of loss. Because having timely information is so critical, some businesses now actively monitor social media content (for example, Yelp) to collect timely insights on customer service, product quality, or service delivery issues. In this example, widely and immediately available social media content provides valuable insights into the public's perceptions of the business' products and services, which helps the business avoid reputational damage by providing management tools that can quickly address service and product quality issues before they cause serious brand or franchise damage.

Risk information is key to delivering an effective ERM program, and information about emerging, yet critical, new risk events and causal factors are key to effective risk management processes. These days, many ERM programs maintain an inventory or listing of the organization's critical enterprise-wide risks. Moreover, from a technological perspective, these risk inventories can be fairly well managed with spreadsheets, tables, or, in more sophisticated situations, using commercially available "off the shelf" ERM or GRC software. Risk managers in many organizations use these tools to capture, categorize, organize, evaluate, track, and prioritize the organization's inventory of risks. Many of these systems come pre-configured and can be further configured to apply risk prioritization schemas to risk inventories. Because risk prioritization helps management focus attention on the most critical risks, then a risk inventory generally captures data about the following:

- The types and categories of risk (that is, human resources, financial, market, operational, counter-party, regulatory, and so on)
- The probability of occurrence for a specific risk loss event
- The potential impact and severity of the most probable risk events, including the potential for loss of life or asset values and the potential costs required to recover from a loss event or loss scenario
- The strength of the organization's risk management process and related risk mitigation and control activities (that is, the ability and readiness of the organization to react and respond to risk loss events and optimize potential recovery costs)
- The names of the individuals responsible and accountable for monitoring and managing each critical risk

There are other potential data points that can be captured in a risk inventory, but generally speaking, the preceding list is a good starting point for an evaluation of potential risk technologies. Yet, before one decides to evaluate an investment in risk technology or a technology-enabled risk system, it will be helpful to answer questions about additional risk data and information needs that may be missing from an organization's existing risk-tracking tools. Some of these questions include the following:

- What data from current operations or the markets where we operate do we need, and if we had that data, would it help us do a better job identifying emerging critical risks?

- What risks, risk scenarios, or stress tests should we evaluate, and for which of these should we prepare a response?
- What additional data do we need to perform this type of "what if" analysis more accurately?
- Can we enhance risk management effectiveness using other nontraditional risk data points, for example, with data from external data and information providers?
- If we invest, how much should we spend given our risk profile and past experience with financial significant risk loss events?

When considering whether to make investments in new or updated risk technology, it's also important to note that many organizations already have large and extensive databases currently in production, and many IT departments are actively engaged in integrating these better with existing applications to extract more value from IT investments. Many databases contain risk data points that can also be extracted, "mined," or ingested by more powerful computing platforms to deliver even more organizational value over time. Tools that chief information officers (CIOs) of organizations now use to help facilitate such efforts include electronic data warehouses (EDWs), "Big Data," business intelligence (BI) applications, and information analytical technologies. These tools can be complimented with powerful data extraction, transformation, and loading (ETL) technologies that provide greater latitude in extracting value from hard-to-locate and parse data files. Though risk managers may not initially be the intended beneficiaries of such data integration investments, many organizations are, nonetheless, using these tools for that purpose.

Big Data is a term frequently used these days to describe massive amounts of structured (that is, numeric data, such as financial amounts and values) and unstructured, yet digital, data sets (that is, textual data in free forms or data that is visually graphical), many of which are too large or complex for traditional database management applications. To enhance the usability of Big Data, the latest generation of Big Data analytic tools provides features that provide users with the ability to consume and analyze very large and diversely structured and formatted data sets. These tools may also perform incredibly complex problem solving by using powerful "parallel-processing" computing platforms. Parallel processing allows an application to break down and separate very complex and computationally intensive calculations into even smaller sub-tasks. This is done using multiple, interconnected virtual machine processors, so the job of parsing and comparing very large data sets can be performed faster and more efficiently than with many of today's single-use personal computer operating systems based computing platforms.

With the integration of technologies like Big Data analytics, cloud computing, GRC and ERM applications, and parallel-processing platforms, in the near future, risk managers will be able to gain even greater advantages from capturing, extracting, transforming, and using legacy databases to perform risk assessments, stress tests, and risk scenario analyses. Although not easy nor cheap to implement and manage, these current IT evolutions will become less costly over time and have a huge impact on the way organizations track and manage risks.

Future risk applications using this technology can further enhance risk management when integrated with workflow process and business "rule logic" software. Business rules systems can be pre-programmed to seek out and capture emerging risk data within transaction execution systems and present these data points to management in more consumable formats. As future Big Data-enabled technologies become even more integrated into an organization's existing operational monitoring and reporting processes, management will be able to more objectively measure and rationally explain the actual events that affect the organization's current operating results or might affect future performance.

Nowadays, data about changing economic conditions and markets is instantaneously available to most organizations via real-time data feeds. Business news service providers, such as Thompson Reuters, BlackRock, Bloomberg, Dow Jones, and the Wall Street Journal, all offer up-to-the-minute information on the changing values of financial assets and markets. Such data feeds can also be exploited to support mature ERM programs and risk-monitoring processes, and the impact of these information services on equity trading and capital markets participants can be seen. Many global organizations are becoming more globally integrated and operate very complex business processes across borders. Such organizations execute transactions and evaluate and take actions in nanoseconds when real-time changes in market conditions occur. Many of the newer breed of Big Data-oriented, "analytics-based" BI systems already support intelligent decision making, transaction

processing, and the visualization of data, all useful tools for monitoring risks and operational performance. As these applications become less expensive and more widely available, many organizations may still struggle to integrate them with existing "legacy" applications or do so across historically "siloed" functions, databases, and processes.

Therefore, it's sometimes necessary to modernize an organization's IT infrastructure before risk managers attempt to use new technologies to capture, synthesize, process, and use real-time data from different data sources and in different data formats. Transforming IT to embrace these technologies may be required before risk managers can also embrace future evolutions in risk management technologies. Furthermore, investments required to fully integrate and unleash trapped organizational data from legacy stand-alone databases may be hard to come by even in the most technically sophisticated and well-funded IT organizations, especially in organizations not known for investing in recently evolved information technologies.

In line with that, risk management executives can find the task of attempting to connect diverse data bases challenging without executive support and a clear, concise project plan that defines the risk program's requirements in terms of people, processes, and technology, and more specifically, financial resource requirements, architectures, data flows, and quantifiable risk management needs. Yet, as organizations continue to build their enterprise content, enterprise data management, and EDW capabilities, they will also find it important and extremely valuable to implement strong data governance, master data management practices, and the use of a risk taxonomy (see section that follows) to define risk management terms and risk data elements in technical terms, so risk-related data elements can be defined, identified, captured, processed, and analyzed.

Because many ERM programs may be immature or small because the organizations they support do not require much sophistication, from a cost-benefit perspective, such risk programs can greatly benefit from less complex and less expensive office automation tools, such as Microsoft Excel, PowerPoint, and SharePoint. These tools are used extensively in large, medium, and smaller organizations for risk tracking and reporting purposes. These tools can help a risk management program

- capture and evaluate the impacts and potential of identified enterprise risks;
- define, communicate, track, and monitor risk appetite and risk tolerance levels within the organization;
- assign ownership for executing ongoing risk monitoring and internal control activities; and
- report an organization's ongoing risk management effectiveness.

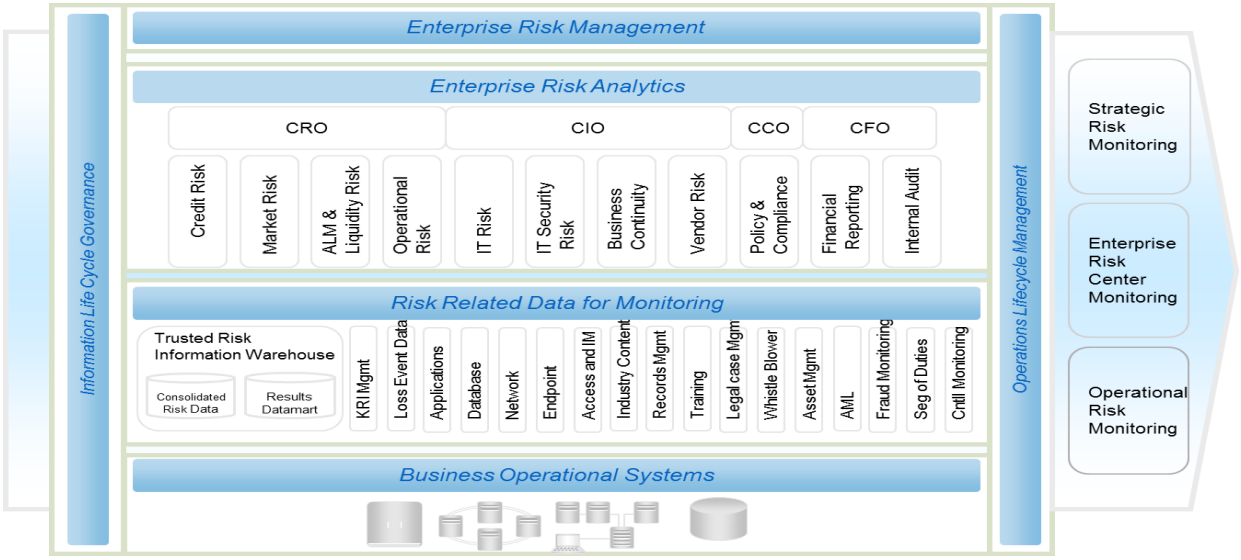
Stand-alone or network-based "off-the-shelf" GRC systems are also widely available to help risk managers capture and report on an organization's corporate and legal structures, create and apply a risk taxonomy, and evaluate risks and related risk-mitigating control activities and their performance over time. These tools also support ongoing evaluations and a fundamental requirement of a generally accepted risk framework, and they help risk managers evaluate potential impacts to an ERM program's coverage from organizational changes. GRC systems offer the ability to collect, capture, and report data about assets and people resources to help organizations define and monitor risk and control performance, establish risk accountability, and help track compliance with internal codes of conduct or regulations. GRC tools also help in defining an organization's risk framework. For readers interested in learning more about GRC and risk analytic systems, organizations such as Forrester Research, Gartner, IDC, and Chartis Research, issue research reports that analyze and compare leading market tools available for purchase.

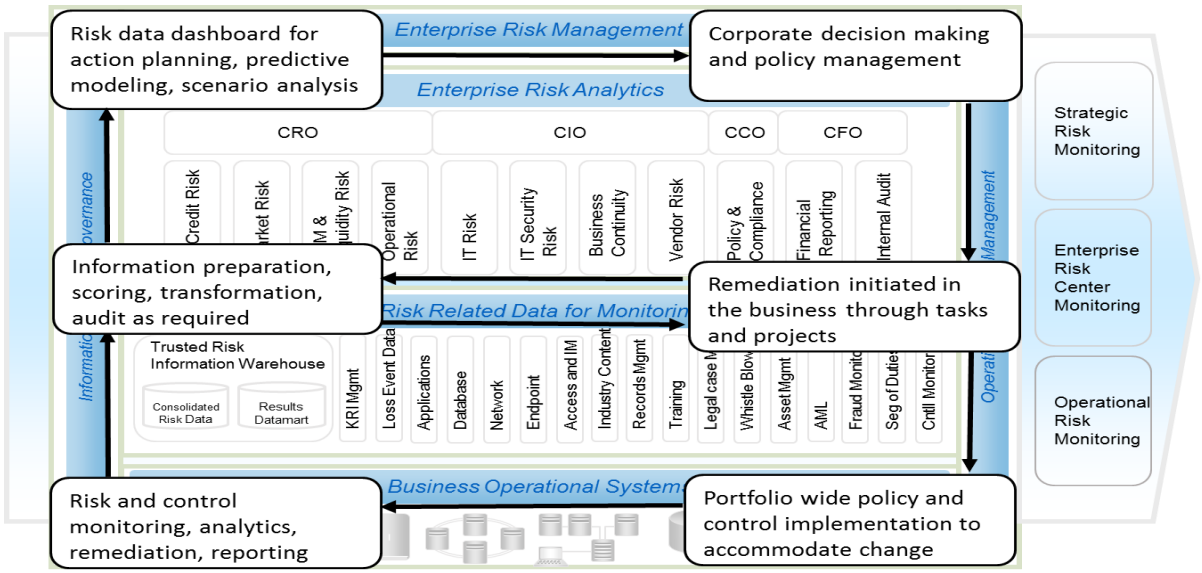
Many of today's GRC applications can also be enhanced by integrating them with both data-feeding and data-receiving systems. For example, some GRC systems can be integrated with operational monitoring or alerting systems and can feed emerging risk data points to business managers via mobile applications. Future evolutions of GRC technologies will also provide the basis for an even more integrated ERM capability. They will provide this integration functionality via application programming interfaces and more powerful system development and integration tools.

Moreover, the evolution of cloud-based IT environments is also something one might want or need to understand and consider when evaluating GRC applications. Cloud-based IT environments that provide "on-demand" GRC software as a service (SaaS) exploit inherent virtualization capabilities of platform-based operating systems and related infrastructures and middleware software and provide "tenant" users with even more efficient and cost-effective alternatives to buying a GRC application and running it in house. Cloud-based applications, or "tenants," and the organizations that use them provide and charge for just the processing

power that users of such applications need. Demand-based usage and charging schemes give users more flexibility by requiring them to spend only on the applications they need to run the business. Cloud-based applications take advantage of economies of scale, and SaaS allows a cloud-hosted application to be made available to multiple tenant user organizations while supporting a wide mix of IT use cases. As mentioned previously, virtualization allows cloud providers to divide processing across multiple IT platform environments, so each cloud tenant only consumes the processing resources needed. Technically speaking, virtualization optimizes system resources and tenant usage demands that require either more or less system resources over time.

In the future, many large globally-integrated enterprises may also benefit from implementing a centrally or optimally managed enterprise risk center (ERC). An ERC combines all of an organization's relevant risk and control operational functions into a single operation center that can also provide even more risk visibility across the enterprise. Using segregation of duties and organizational reporting lines to avoid potential independence issues, the idea is to place an organization's legacy operational risk functions, such as the ERM function, the network operations center, security operations center, the physical security monitoring, financial operations, and customer service or call center functions into one business unit and enable these with technology. An ERC also provides risk information to key stakeholders and provides some contextual analysis to drive risk response and risk event or incident response capabilities. However, establishing an ERC may require some adjustment of the role of IT within an organization because to operate effectively, the ERC will need to change its direction to focus IT on also supporting the business from a risk and sustainability perspective rather than a traditional focus of monitoring and managing IT platforms and data. The ERC should operate using the organization's own data warehouse because these become inputs to the "central nerve center" that manages the broad inventory of risks each organization faces. The ERC works to enhance legacy data management capabilities with real-time monitoring using dashboarding tools and physical and environmental data inputs (weather, security, operational control, asset and inventory movement data points, and so on). The ability of the ERC to establish and monitor operational controls to keep the organization better aligned from a risk management perspective will be key to the future deployment of ERCs in globally-integrated enterprises. Therefore, having seasoned IT data management, risk, operations, and data analytics and tools integration experts supporting the ERM program's risk technology goals will be key to the setup, operation, and management of an ERC-driven program.


Enterprise Risk Management
Enterprise Risk Analytics
CRO
CIO
CCO
CFO
Credit Risk
Market Risk
ALM & Liquidity Risk
Operational Risk
IT Risk
IT Security Risk
Business Continuity
Vendor Risk
Policy & Compliance
Financial Reporting
Internal Audit
Risk Related Data for Monitoring
Trusted Risk Information Warehouse
Consolidated Risk Data
Results Datamart
KRI Mgmt
Loss Event Data
Applications
Database
Network
Endpoint
Access and IM
Industry Content
Records Mgmt
Training
Legal case Mgmt
Whistle Blower
Asset Mgmt
AML
Fraud Monitoring
Seg of Duties
Cntll Monitoring
Business Operational Systems
Information Life Cycle Governance
Operations Lifecycle Management
Strategic Risk Monitoring
Enterprise Risk Center Monitoring
Operational Risk Monitoring


Risk data dashboard for action planning, predictive modeling, scenario analysis
Enterprise Risk Management
Corporate decision making and policy management
Enterprise Risk Analytics
Information preparation, scoring, transformation, audit as required
Remediation initiated in the business through tasks and projects
Risk Related Data for Monitoring
Risk and control monitoring, analytics, remediation, reporting
Business Operational Systems
Portfolio wide policy and control implementation to accommodate change
Strategic Risk Monitoring
Enterprise Risk Center Monitoring
Operational Risk Monitoring

Another important characteristic of an effective ERM program is the program's ability to integrate the organization's people in a more operationally aligned manner by formally establishing and explicitly defining risk-taking authorities, risk tolerances (that is, across key, organizationally important functions and processes) and setting risk tolerance "levels" within the context of an organization's strategic, operational, and financial objectives. Although many ERM programs are still evolving and may not yet be mature enough to tackle the challenges that come with formally setting risk appetites, risk-taking authorities, accountabilities, and risk tolerance thresholds, these activities should drive the evolution of maturing an existing ERM program, that is, one that currently does not have these processes formally defined.

Another software tool many organizations already use is statistical analysis software. This software is very useful for modeling and evaluating the probability and impact of risk events or scenarios, especially those affecting financial assets and investments. Because market-wide, geographical, or economic changes may not be immediately anticipated or felt until reported by management, some organizations are using statistical modeling tools for supporting an ongoing ERM program's risk analysis. Risk managers may already monitor ongoing changes in geopolitical conditions, severe weather, market movements, or other events that might cause disruptions to normal "business as usual" operations; but, statistical tools allow even more diverse risk scenarios to be evaluated so better decisions can be made.

> According to an Ernst & Young study, "financial performance is highly correlated with the level of integration and coordination across risk, control and compliance functions." Clearly, the inability to effectively coordinate risk management activities in an integrated way across an organization limits effective ERM implementations.

In addition to the data points listed previously, more sophisticated risk systems might provide users with information about the following:

- Risks within an organization, its departments, operations, functions, assets and asset classes, and risks to capital, processes, and the established accountability of those responsible for managing risk
- Potential risks in geographies and industries where the organization operates and the duration of such risks, their magnitude, and time horizons
- The ability of the organization to continue to meet regulatory and compliance requirements and contractual obligations and commitments

For a source of reference material related to risk technology, readers are encouraged to browse the Risk and Insurance Management Society (RIMS) webpage at www.rims.org and a white paper RIMS published in 2009 on Enterprise Risk Management Technology Solutions.[1]

Many risk functions already find it very useful to leverage enterprise financial data used in routine accounting, reporting, and business operations. Such data helps risk managers identify, escalate, and address evolving enterprise risks. This same enterprise data currently used to monitor and calculate pension liabilities, track and account for changes in the fair value of assets and liabilities, and support compliance, financial, and operational processes can also be captured, analyzed, and summarized for decision makers or to support ERM or ERC processes.

ERP systems used by many organizations can also be primary enterprise risk data sources. Complex statistical and analytic software tools can be integrated with ERP systems and used to extract and model potential risk events or exposures and perform predictive scenario analysis or evaluate changing risk factors that might affect

[1] Michael Thoits, "Enterprise Risk Management Technology Solutions," Risk and Insurance Management Society, Inc., www.rims.org/resources/ERM/Documents/ERM%20Technology%20Solutions.pdf.

the current or fair carrying value of assets and liabilities. Such tools already help many financial firms to make more informed decisions on allocating equity capital and for keeping cash deposits in reserve for expected (non-outlier) and unexpected economic losses and provide capital resilience and "stress test" details. International banking regulations, including UK Financial Services Authority (FSA) Living Will guidelines and Bank of International Settlement rules such as Basle II & III, also require organizations to effectively model and keep track of their regulatory capital. Although complex financial services companies build their business by managing valuation, liquidity, and counter-party risks to assets they manage, smaller organizations with concerns about asset valuation and liquidity risks can also benefit from a mix of less costly and less sophisticated technology tools and risk treatment tactics.

Accounting rules already require many organizations to monitor and track the fair value of assets and identify patterns that might signify a financial loss event for recording and disclosure purposes. However, applying an enterprise view of risk will most likely expand this concept of focusing on enterprise value through the continual collection of data on the organization's breadth of operations, operating environments, people, and capital, plus data on internal and external factors that introduce risks to the enterprise as a whole. As ERM capabilities within an organization naturally mature over time and become even more effective in protecting enterprise value, the deployment of more sophisticated IT-enabled ERM operating capabilities for gathering, collecting, and analyzing more risk data points will also push IT departments to become more important to the enterprise's future value.

Related Risk Tools and Technologies

Most organizations already use technology to help management visually depict, size, assess, and address risk concerns. Some of these tools include the following:

Information "dashboards." These tools organize and visually showcase data and information from various sources by employing sophisticated graphics to organize and highlight pertinent data or distinguish relationships in the data that may be meaningful for management. A dashboard might feature color coding for various levels of risks or "heat maps" that categorize risks based on their probability of occurrence or their financial impact as depicted on an X-Y axis or allow users to perform "what if" scenario analysis to measure the impact on an asset's value when certain causal factors are present or changing. To be truly valuable, the dashboard tool focused on enterprise risks should be able to provide a broad range of risk data points from inside and outside the organization and have risk-alerting capabilities (for example, to highlight underlying real-time market changes that affect the current or future value of assets) that prompt a financial manager to make a "buy or sell" decision sooner than originally anticipated due to a change in the underlying value.

Dashboards are useful for aggregating information about organizational risks and communicating this as aggregated risk data. According to a McKinsey & Company report,[2] one industrial company developed a risk dashboard that presented an overlay of updated cash flow projections, pointing out risks associated with particular changes in value using color coding that illustrated likelihood, potential impact, and level of preparedness. Another company chose a more narrative dashboard format that focused on past performance, ambitious current projects, and what they might mean going forward given certain assumptions. Each approach responded to management's unique needs. In a landmark 2005 *Harvard Business Review* article,[3] Robert Merton from Harvard Business School described a risk balance sheet approach to managing a business enterprise's capital, and these concepts are now being applied in financial risk analytical systems that also model financial risks.

ERM software. As discussed previously, ERM software can help organizations identify, measure, and analyze risks, monitor changing risk factors, track loss events, and mitigate potential risk loss exposures. Specialized ERM software for particular industries is also available. (Again, readers are encouraged to search for GRC and ERM software using Internet search engines or subscribe to fee-based research publications to find information on most of the leading tools). Most software vendors provide demonstrations of their tools and can be engaged to assist potential customers in fully understanding the costs, challenges, strengths, weaknesses, and value in an ERM system. However, as discussed throughout this paper, when using such software, organizations may face challenges integrating such ERM tools with existing in-house financial and operational systems in addition to finding and locating reliable risk data. Many organizations will also face difficulties identifying

[2] Andre Brodeur and Martin Pergler, "Top down ERM: A Pragmatic Approach to Managing Risk from the C-Suite," McKinsey Working Papers on Risk, Number 22, August 2010.
[3] Robert C. Merton, "You Have More Capital Than You Think," *Harvard Business Review*, November, 2005, www.people.hbs.edu/rmerton/More%20Capital%20than%20you%20think.pdf.

and capturing external risk data from trading partners, counterparties, and information news services that provide data on changing market dynamics, prices, and global risk events. Much of the available internally-sourced data are in structured formats (data in tables or represented in extensible formats like eXtensible Business Reporting Language or XBRL), whereas externally-sourced data can be in unstructured formats, such as text, PDF, or other formats, which require some effort at extraction, transformation, and loading into existing internal databases. Therefore, it is important to recognize that a robust ERM system will not depend on one system but on the effective integration of reliable data sources from both inside and outside the organization.

Data storage and software used in managing data. As introduced earlier, Big Data is regularly discussed in information management circles as the vast array of information—from a tweet to a cell phone GPS signal—that can be gathered on a regular basis but is generally too unwieldy as a whole to be analyzed and put to use by most databases. According to IBM, Big Data represents up to 2.5 quintillion bytes every day.[4] A McKinsey & Company report says that "data can create significant value for the world economy," [5] and it can certainly contribute to ERM efforts. Storage and management of this data can pose significant hurdles. [6]

Many approaches are being used to make it easier to use Big Data. For example, *mash-ups* are tools or websites that pull together information from various sources to create a new service or overview that can be used to address business scenarios and patterns.[7] *Web-crawling tools* provide users with search portals that gather information on a topic from a wide variety of sources. [8] *Data fusion* combines multiple types of data from a variety of sources into a single representation.

ERM data and linkage with overall information management strategy. As organizations evaluate their current risk information and data needs, executives involved with ERM will find it valuable to work with their CIO and IT functions and consider the organization's information management strategy and capabilities as they make decisions to purchase, enhance, or build ERM support systems. As a best practice, organizations should consider including IT executives on their ERM steering committees. These organizations might also find it beneficial for the ERM program to actively participate in the overall IT governance process so their needs for risk information can be incorporated into the organization's information management strategy. More mature ERM programs will find it beneficial to align their activities with their organization's strategic planning and goal-setting processes. Therefore, ERM executives will benefit from collaborating with their organization's strategic planning and budgeting functions and working with the IT function to better manage the performance information available to the ERM program. The goal in collaborating is to help ensure that the IT function is fully supporting the organization's evolving ERM data needs, especially as they become more in demand as the ERM program matures through experience. As risk technology and data supports ERM program functions and operational risk monitoring processes, the need to continually update, refine, and improve an entity's risk inventory and tracking processes will also grow to the point where some organizations will perform this updating on a continuous rather than periodic basis.

Information aggregation providers and subscriber-based financial and market data sources can also be useful in identifying and sourcing risk data in support of mature ERM processes.

An example of how these tools are being used was discussed in an article that appeared for a limited time in a now out-of-print issue of *Hedge Funds Review* that details how risk aggregation provides users in that industry a higher quality of information for investors. According to the article at the time it was published, "By employing a risk aggregation strategy, [institutional investors] are directly measuring how the different parts of the portfolio contribute to returns and to risk." The challenge in having a comprehensive enterprise-wide risk management program is identifying and collecting risk-related data and information to support and sustain the program. Being able to identify and aggregate or correlate risks and potential or actual risk loss events can be a challenge when a risk management function lacks the necessary IT tools to do so. Managing the downside aspects of risk can lead to upside opportunity, but many organizations struggle with understanding changing market dynamics and looking for and finding opportunities as they manage their risks. Gathering and

[4] IBM, May, 2011, www-01.ibm.com/software/data/bigdata/.
[5] McKinsey & Company, *Big Data: The next frontier for innovation, competition, and productivity,* June 2011.
[6] Arik Hesseldahl, "Meet Compuverde, Sweden's Answer to Big-Data Storage Problems," *Wall Street Journal,* August 20, 2012, http://allthingsd.com/20120820/meet-compuverde-swedens-answer-to-big-data-storage-problems/.
[7] IBM developerWorks, www.ibm.com/developerworks/lotus/products/mashups/.
[8] *PC,* Encyclopedia, www.pcmag.com/encyclopedia_term/0,1237,t=WebCrawler&i=54372,00.asp.

collecting external data and information from internal operational and financial systems is becoming much more important as ERM functions improve their capabilities and maturity and contribute to goals focused on value creation over some time intervals. Risk aggregation, therefore, requires well-defined and well-architected data and information management capabilities because without a clear sense of how an organization's environment is changing, it is difficult for the organization to achieve its objectives while managing the risks that threaten its achievement.

ERM-Specific Information System Technologies

ERM-specific technology applications are valuable for supporting the operation of a robust, effective ERM program. These systems provide functionalities that can help management do the following:

- Identify, define, and establish formal risk appetite and tolerance objectives and measurements
- Define risk criteria, such as causal risk factors and levels
- Define risk measurement standards
- Effectively apply technology to enforce or re-enforce workflows that also support accountability and results-oriented organizational governance structures, processes, functions, and roles

Putting into practice the specific administrative activities required of a mature ERM program, however, is also possible, for example, with some of the currently available GRC modules that now accompany ERP systems. ERP systems such as SAP and Oracle also provide (for a fee) GRC support modules that can enhance and integrate with stand-alone GRC tools. These ERP-based GRC tools can be used to set and define an application's user access security parameters and enhance transaction-monitoring control capabilities by tracking and providing "auditable" application controls over a time period. With a GRC-enhanced ERP system, internal control requirements and criteria can be configured using pre-defined application-specific control parameters, and these can be applied to a particular user or group of users. Group-access privileges and user classes can be pre-established to enforce appropriate segregations of duties (for example, allowing a user to post, execute, or record transactions and also adjust the chart of accounts) or be applied to specific transaction types to formally define transaction approval limits. Such capabilities help management establish effective controls within an ERP system and prevent certain users from performing incompatible system activities. These also can escalate and provide alerts when certain transaction value thresholds are exceeded or met. In other cases, parameterization can be used to formally define transaction execution thresholds that enforce corporate risk limits, confirm and validate risk appetite thresholds, or help ensure transactions above a certain value threshold. For example, such systems might be configured to require two electronic signature authorizations or approvals when transactions exceed a certain amount.

GRC systems might be one part of the evolution of an organization's ERM "journey to maturity" because these tools provide organizations with entity-wide views of risks and controls plus functionality to support the build-out of a more effective integrated risk management program. However, such capabilities are not easy to implement with current spreadsheet and document-sharing systems.

When considering the inherent capabilities of risk management systems found in many organizations these days, it's important to also realize that the next generation of truly integrated risk management systems can help management oversee and monitor the organization's diverse business activities and provide more visually appealing real-time risk alerts. Fairly sophisticated workflow technologies within these systems provide functionalities now used to execute the sale or trade of assets, such as commodities, equity, or debt instruments in investment, hedge fund, or broker-dealer businesses. These programmed workflow capabilities are useful to support risk mitigation and prevention controls because automated mechanisms promote and discourage certain risk-taking activities, such as selling assets for less than fair value or binding the organization to a future event that is beyond a seller's or buyer's explicit risk-taking authority.

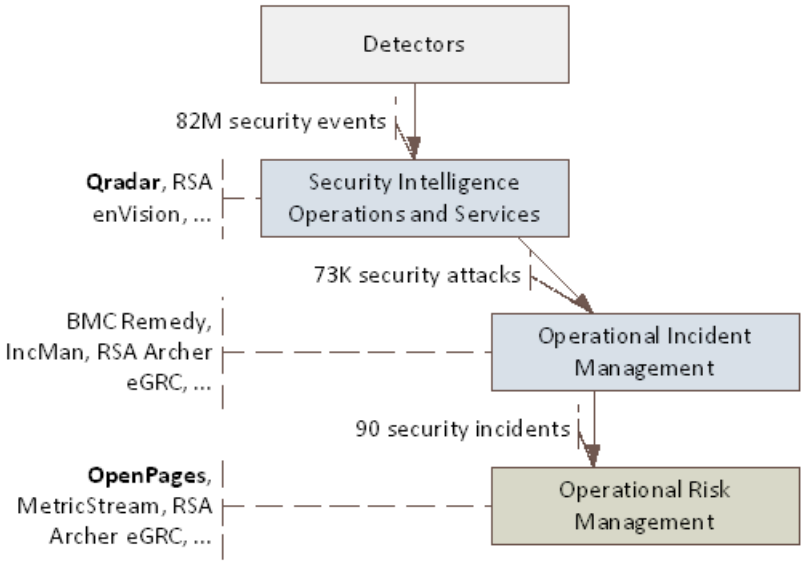
ERM functionalities found in many information systems are also now being used in some industries to define criteria and baseline limits on explicit risk-taking activities and support risk-related decisions. Many banks, financial services companies, and regulators are using sophisticated statistical modeling software to evaluate real-time impacts of risk exposures on the value of intangible assets they own or have an interest in protecting as fiduciaries. Such technologies are already being used in real-time equity trading, for example, in electronic (technology-dependent) stock exchanges and stock-trading firms that "flash trade" on behalf of customers or their own corporate balance sheets. In some of these situations, risk appetites and tolerances are first set at the corporate internal environment level through existing governance mechanisms, then programmed into systems as execution and risk-taking controls within asset trading systems as "limit" controls to prevent traders from

exceeding established limits. Front, middle, and back-office trade clearance and settlement systems also use limit controls to enforce the evaluation of potential trades and changes in the aggregate values of current trading positions that can affect the equity capital of a business. In such complex technology-dependent environments, these internal systems might be connected with external market exchanges, banks and asset custodians, and trade settlement organizations in a real-time ecosystem where counterparty risks also need to be managed. Controls within IT platforms and end-user-based systems reduce risks from data breaches or unauthorized access to an organization's data.

One relevant example is when organizations have deployed "endpoint security" software on host systems (that is, mobile, personal computer, or network devices) to monitor device and data security using a system's configuration settings. Agent software captures, filters, and applies logic or rules to monitor data transiting across or through the host or remote system to look for specific risk event indicators (that is, malicious code, data theft, and so on). Software on the user's desktop, mobile phone, tablet, or laptop captures operational risk events as log entries, and these devices might be inappropriately altered as data are transited within a system or network or might cause a security configuration control to be modified or disabled. Endpoint security tools integrated with Security Incident and Event Management (SIEM) tools can be configured to filter thousands of application or platform system logs to seek out and report suspicious or problematic network events reflected in such logs. SIEM tools perform tasks, such as file and attachment inspection (as these are sent or received) and can protect an organization against the risks from attempts to introduce malicious software or viruses via a host. SIEM tools also automate the collection of system logs from within an organization, from laptop and desktop computers to mid-range servers, mainframes, and distributed network devices. SIEM dashboards alert management when suspicious activity is detected. Because system logs contain lots of historical data points representing many different types of system or user events (or incidents), they can be powerful tools for identifying and taking immediate action on such things as computer viruses, malware, data being taken or sent outside the organization, or users who have escalated or promoted their own access to a system beyond their current need for that access. These tools also alert IT management when employees or insiders transfer sensitive or legally protected data outside the organization's boundaries (these are known as *data loss prevention systems*).

Configurable controls are generally embedded in IT devices, such as routers, firewalls, or hosts, when they are installed and put into operation. These devices can be continually monitored using *agents* or *detectors* (that is, programs designed for a very specific data-gathering or analytic purpose). For example, agent software is used to identify, capture, and accumulate data from other feeding systems. Software agents and detectors extract data from remote networks or internal IT devices and apply pre-defined rules to aggregate and make such data available for alerting and reporting system risk events from external and internal sources.

A key requirement when implementing such operational (risk management) monitoring tools is to identify and determine what log data is available and needed because many target systems have extensive logging capabilities, but only certain log entries are of interest. An example of a SIEM or operational monitoring system feeding a GRC tool is depicted in the figure that follows. The SIEM needs to distinguish and process large numbers of potentially meaningful events or incidents out of millions of log records (that is, transforming 82 million log files into 90 security incidents) and report these to the GRC system.



The evolution of IT will increase the use of real-time "continuous monitoring" for IT-specific, financial, or operational risks. Such monitoring will be possible across each user's connected device, so that all IT devices that link a user to another user or third party can also be monitored. This logic can be applied when monitoring financial events that are captured in systems linking trading partners.

As discussed earlier, technology can also be used to formally define organizational roles and responsibilities and establish specific risk accountability via existing human resources (HR) and corporate governance processes. Corporate governance and HR functions will be better served as they incorporate and use risk technologies to support ongoing interaction and the monitoring of individuals, teams, departments, and organizational performance against established objectives and goals. HR functions routinely engage in managing individual performance, defining organizational processes, and delivering human capital management tools used to define and formalize individual job duties and responsibilities. From a risk perspective, the human capital management dimension includes the following:

- Establishing formal authorizations and allowing officers or employees to legally bind an enterprise and execute transactions on its behalf
- Tracking knowledge and staff training so staff become more effective and risk aware in their job performance and directing employees to follow established ethical standards
- Defining formal boundaries regarding what constitutes acceptable risk-taking behavior
- Reporting key human capital risk performance indicators and other important business measures as part of management's ongoing monitoring of executive and employee effectiveness

Human capital technologies can be useful for uncovering or preventing a variety of internal and external risks, including the following:

- Providing anonymous disclosure avenues for whistleblowers and capturing anonymous employee or trading partner tips, complaints, and other instances of suspected illegal or damaging behavior of employees, officers, or directors
- Supporting board and executives in managing reputation risks posed by insiders, vendors, customers, or trading partners
- Capturing and monitoring potential organization, director, executive, or employee conflicts of interests
- Tracking ethical matters relevant to the enterprise's overall risk and compliance programs

Some of these HR systems require officers, directors, and employees to directly record and report their financial holdings and disclose personal, legal, or financial relationships with an organization's customers, suppliers, or related parties. As an organization takes on new relationships with suppliers or when customers enter into legal or financial arrangements with outside entities, these systems can also be used to identify and

alert compliance staff to potential conflicts of interest and allow them to take action to avoid reputation risks or increased regulatory scrutiny.

Risk Taxonomies

Another important discussion topic to the evolution of risk technology involves the classification and use of data. This also applies to managing risk data. But, from a technical perspective, a risk data taxonomy can help risk managers evaluate their risk information needs. A risk taxonomy can be thought of as a type of data dictionary that provides a technically useful way of defining risk data and meta-data elements within a risk-focused information system. Think of a risk taxonomy as a formalized way of defining and representing risk data from a technical perspective. Whether a risk taxonomy exists should be an important factor for risk managers interested in maturing an existing ERM program's risk information needs. "Be it a taxonomy designed for storage and management or one that supports better search, without them, all types of management systems are near useless, regardless of the platform," according to a ComputerWeekly.com article, [9] which defines a *taxonomy* in this context as "a set of chosen terms to retrieve online content." So, a risk taxonomy should be an essential tool that helps risk and IT executives define their risk information needs across an organization. As noted by the Treasury Board of Canada Secretariat, a risk taxonomy provides a comprehensive, common, and stable set of risk categories. With such a taxonomy, the organization will be better able to identify risk data in a more consistent manner, aggregate that data for analysis, and perform that analysis to report risk issues in a more transparent manner. Information on taxonomy-based risk identification from the Software Engineering Institute at Carnegie Mellon University offers more details.

> Taken from database and master data management concepts, comprehensive risk taxonomies can help an organization focus on its risk data and information needs as it works to integrate its existing systems and ultimately embed a "common risk language" in risk systems and related ERM processes.

Among other things, risk data taxonomies can

- serve as an inclusive guide for targeting and understanding risks in pursuing different business goals;
- be used in identifying risk patterns and creating common approaches to them;
- enable the organization to aggregate risk assessments across the business;
- make it easier to communicate about and consider risks; and,
- make global optimal management of risks possible.

Questions organizations might ask themselves related to risk taxonomies include the following:

- What data elements are needed in the risk management system?
- Where should we get the data, how reliable must it be, and do we need to cleanse the data before we use it?
- What set of inputs, processes, and outputs does management use to provide oversight of an activity?
- What part does technology play in gathering, analyzing, and monitoring them?

Finally, the Open Compliance and Ethics Group, or OCEG, is a non-profit organization that provides "open standards" for GRC-related technologies, including guidance on using XML (that is, eXtensible Markup Language) tools and applying them in GRC applications. These GRC XML standards are also related to XBRL (eXtensible Business Reporting Language), which are technology standards for defining business-reporting data elements used, for example, in financial reporting applications. These XML-based GRC standards and taxonomies can be found at www.oceg.org/resources/grc-xml/.

[9] Michael Pincher, "A guide to developing taxonomies for effective data management," *ComputerWeekly.com*, www.computerweekly.com/feature/A-guide-to-developing-taxonomies-for-effective-data-management.

Challenges in Implementing Risk Technologies

Using technology to help manage broader areas of enterprise risk outside of particular point-specific financial risk situations is not a new concept. However, given the current state of risk technology tools, it's unlikely that any one specific tool will address all of an organization's current or future ERM information needs. Such needs might include the need to manage and report on an entire "portfolio of risks" for which an organization is exposed, including risk categories such as strategic, business, financial, operating, legal, supply-chain, regulatory, and reputation risk exposures.

However, the task of connecting all these diverse data points can be challenging if not fully built with a clear, concise project plan, one that captures all the requirements in terms of technologies, resources, architectures, data flows, and data management.

Global organizations operating across legal boundaries already know how difficult it is to identify and keep track of their local, regional, and national legal obligations and the regulations they must adhere to because there are no systems available in the market that help them track these legal obligations. As a result, many organizations find themselves bringing together a variety of difficult-to-integrate, point-specific system applications to address their overall legal, regulatory, and ERM-related compliance needs.

Risk information and risk management systems also play a critical role in helping boards and executives charged with governing organizations to identify, measure, and work through continuous control monitoring, the independent verification of control performance over time. Such systems can help management when they need to lead and facilitate effective crisis management and damage control, especially when unexpected loss events occur that are not within management's appetite for risk and cause brand, reputation, or more financial losses than the organization is able to bear. Because of this imperfect ability to easily integrate the currently available set of enterprise systems and technology tools and for these to also effectively support an integrated ERM process, there will continue to be challenges in managing and mitigating enterprise risks. The current market portfolio of ERM and GRC technologies is inadequate in helping to define an organization's risk appetites and tolerances. This is further exacerbated when one considers the implications and impact of an organization's natural misperceptions about the significance and variability of particular risks within their business operations. This is why organizations struggle trying to identify, define, understand, and formally establish individual accountabilities for setting and monitoring risk appetites and tolerances. In a business context, *risk appetite* includes a stakeholder's "results-oriented" expectation that an organization's value must be increased and optimized rather than simply being pursued. To reduce some of the risks and challenges when implementing ERM or GRC technologies, it is also important to leverage strong project management and system development life cycle methodologies that enforce strong organizational and system change controls, so that the resulting tools meet and exceed the risk management needs of the organization.

> According to the Institute of Risk Management, "Risk Appetite, correctly defined, approached and implemented could be a fundamental business concept that will make a substantial difference to how businesses and organisations are run."

Choosing the Right Risk Tools and Technologies

Selecting and deploying risk technologies should be a key activity for an effective ERM function. The choice of a risk technology should also depend on the organization's overall maturity in risk management and the ability of a risk function to capture, analyze, and address risk data points. Therefore, when selecting a risk technology, return on investment (ROI) analysis can be useful for calculating the expected value from the system's inherent functionalities and capabilities and any potential long-term benefits. Risk-oriented systems will require some investment in upfront configuration prior to implementation, and afterwards, ongoing tuning and data loading. Therefore, the cost of external and internal assistance in implementing will also be a factor in the total cost of ownership and ROI analysis, as will initial and ongoing software licensing and maintenance costs.

Determining anticipated future returns and benefits can be a challenge because it is not easy to accurately justify the value of an investment in risk management. However, it is important that the risk management executive partners work with finance and IT to help ensure that sufficiently reliable and timely risk

information is available to feed and sustain the risk system that is chosen. However, the integrity of the data used in the risk management system, and the reports the system produces, can increase the importance and value of a risk management function over time and given experience. As risk treatment decisions are made, the risk management system's reports should become more valuable to the business. Although risk management systems will generally be used to support internally focused use cases and internal decision-making processes, the trend over time will be that these systems will become more "mainstream" as financial risk thermostats and barometers of the enterprise's risk appetite, risk tolerance, and risk mitigation effectiveness.

The Future of Risk Technology

The evolution of technologies used in information and business analytics and their impact and use in modern risk management applications and enterprise IT continues to interest financial engineers and those involved in statistics and the application of quantitative analysis to financial valuation and measurement. The use of analytics in this area is not new, but it has evolved rapidly in recent years. IT has become more useful in providing leading indicators or predictors of potential future technologies for risk management.

> "Historically, analytics has been synonymous with business intelligence – knowing the facts and reporting past and current performance," according to a Deloitte publication. "But today risk analytics is more focused on data exploration, segmentation, statistical clustering, predictive modeling, and event simulation and scenario analysis."

Readers should refer to evaluations by technology industry analyst firms, such as IDC, Gartner, and Forrester, for the names of specific ERM and GRC tools; but, keep in mind that internal audit support functions can use GRC tools, for example, to support a public company's requirement to self-evaluate internal controls over financial reporting via control testing and other aspects of compliance programs associated with Section 404 of the Sarbanes-Oxley Act.

Future risk management systems will have functional tools, like agent software, that will "crawl" across the Internet, social media sites, or an organization's internal Big Data warehouses and collect emerging risk event data for analysis. The next generation of cognitive computing and natural language programming applications, as mentioned earlier, will fundamentally transform the ability of users to correlate and connect data in ways never before dreamed. Future risk technologies will use this evolution in computing to enhance the automation of traditionally manual control activities, and this will form the basis for effective information and communication, monitoring, and related processes critical to a future organization's enterprise risk framework.

Conclusion

Information technologies will continue to evolve and provide organizations with more and better capabilities in identifying, collecting, organizing, analyzing, and managing data. The same applies to risk data. With time and investment, the evolution of risk technology will continue to help drive further investment and the integration of core risk and control processes across organizations to allow decision makers to exploit risk analytic functionalities, as well. ERM program executives should, therefore, continue to collaborate with key stakeholders and other key functional areas to seek continuing investments, support, and resources to drive risk technology adoption across an enterprise. But a fundamental goal of adopting new technology should be improvements in efficiency and risk awareness across an enterprise; the application of a widely accepted "risk language" within governance, operations, and financial process areas; and the alignment of objective setting, risk management, and organizational control capabilities. This fundamental goal should, therefore, drive the development of each organization's ongoing ERM capabilities.

Glossary of Acronyms

BI – Business Intelligence, a class of software that allows greater ease in using structured data for analysis and reporting purposes.

CIO – Chief Information Officer, the senior C-suite executive responsible for the selection, application, and operation of IT and information management within an organization.

COSO –The Committee of Sponsoring Organizations of the Treadway Commission, a joint initiative of five professional organizations (including the AICPA) dedicated to providing thought leadership through the development of globally accepted frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

EDW – Electronic data warehouse, a data storage and management system specifically designed to handle large and dissimilar databases and data types and integrate these data sources with external business applications.

EDM – Enterprise data management addresses the need to govern, manage, and provide data for use within a larger enterprise and includes technology, such as EDW, and foundational data management concepts, such as Master Data Management, Data and Information Governance, and Electronic Content Management.

ERC – Enterprise risk center, a concept in which the organization places all risk management and compliance-related business activities and functions in one business unit to collectively draw benefits from various operational and performance management activities so that enterprise risks can be better managed over time.

ERP – Enterprise resource planning, a business application system that facilitates enterprise resource planning and management by integrating corporate business processes across an enterprise with traditional sub-ledger and general ledger accounting systems. ERP applications provide functionality for executing, recording, processing, and reporting financial transactions within one integrated system, rather than within separate and dissimilar business applications.

ERM - Enterprise risk management, the ability to view the risks an organization faces from an enterprise-wide perspective and to do so in a way that recognizes the inter-connectedness of each risk to each part of the organization.

ETL – Extract, transform, and load, a set of information management tools that allow different types and formats of data to be extracted or collected, evaluated, and transformed into more usable formats and loaded into existing enterprise applications for processing and analysis.

GIE – Globally integrated enterprises, organizations that operate across global country and geographic boundaries and, when regulation and custom allow, use integrated business processes to execute business activities, capture business results, and manage global, regional, and local resources.

GRC – Governance, risk, and compliance, a term used to describe the alignment of an organization's governance structure and processes with its risk management and compliance-related activities.

OCEG – Open Compliance and Ethics Group, a non-profit organization that provides "open standards" for GRC-related technologies, including guidance on using XML tools and risk taxonomies and applying them in GRC applications.

RIMS – The Risk and Insurance Management Society, Inc., a global risk management advocacy and education organization that serves the needs of risk management professionals and their organizations.

SaaS – Software as a service, a term used to describe business software that can be rented or leased, generally on a month-to-month subscription basis. Such software can be provided to paying users via secure and encrypted network connections that are established between service organizations and user organizations. Some SaaS is offered by cloud-based service organizations that provide financial and operational benefits to users because they only pay for the business software and processing they actually consume.

SIEM – Security Incident and Event Management, tools designed to automate the collection of various types of system logs throughout an organization, from laptop and desktop computers, to mid-range servers, mainframes, and distributed network devices and to alert management of suspicious activity.

XBRL – eXtensible Business Reporting Language, a freely available and global standard for exchanging business information.

XML – eXtensible Markup Language, a programming and technical language for use in Internet-based business application systems. Originally developed as a standard way of enabling communications between applications connected via the Internet, the language has evolved to cover specific business needs, such as for financial reporting. XBRL is commonly used by public companies around the world to capture and deliver data on financial activities to regulators and financial information users.