Optimized enterprise risk management

C. Abrams
J. von Känel
S. Müller
B. Pfitzmann
S. Ruschka-Taylor

As the result of the increasing costs of risk and compliance activities, enterprises are beginning to integrate compliance and risk management into a comprehensive enterprise risk management function and thus proactively address all sorts of risk, including operational risk and the risk of noncompliance. We present the IBM Research enterprise risk management framework, designed to address risk and compliance management in a strategic, integrated, and comprehensive manner. We demonstrate how enterprises evolve along an enterprise-risk-management maturity continuum from a state of mere penalty avoidance through a state of improvement until they finally reach a state of continuous, risk-based transformation. We then explain our high-level model of the enterprise and its environment and describe the central issues, systems, models, and technologies involved. We conclude by presenting the tactical steps necessary to successfully launch enterprise risk management in accordance with our framework.

INTRODUCTION

In the last few years, many organizations have been challenged by a surge of new cross-industry and industry-specific regulations. Examples are the ubiquitous Sarbanes-Oxley Act (SOX),[1] the USA Patriot Act,[2] and, in the financial industry, the Basel II Accord.[3] In many enterprises, regulations such as these have resulted in a multitude of individual compliance projects that consume a large share of available resources, thereby leading to significant costs. To attain and demonstrate compliance, enterprises have been gathering large amounts of historic financial and business data.

Similar to financial statement reporting and performance management, however, initial compliance management initiatives have been conducted with a rather backward-looking perspective with penalty avoidance as the main goal. With their strong focus on periodic audits, expensive point projects geared to individual regulations have often failed to deliver additional value to the company. In fact, those companies that have delegated regulatory compliance to the various lines of business often find they have incurred costly duplication of effort. TowerGroup estimated that up to 30 percent of information technology (IT) compliance-associated spending in the financial services industry consisted

of wasteful duplication.[4] According to Jorge Lopez, managing vice president, Gartner Research, costs for compliance are currently growing at twice the rate of IT costs.[5] A year ago, AMR Research expected that the United States economy was looking at an $80 billion total cost for compliance over the coming five years.[6] The most recent estimates for total compliance spending, including $27.3 billion for 2006 and another $27.9 billion for 2007,[7] suggest that these costs are continuing to grow.

With the mounting expense and inefficiencies of compliance projects, businesses have started to embrace a new approach by treating noncompliance as a risk, and thus embedding compliance management as part of a larger enterprise-wide risk management approach geared to bringing greater transparency and value to the business. This resulted from the realization of the great potential that lies in the large amount of gathered compliance data. But simply gathering data does not automatically provide business insights. Enterprise-wide information needs to be integrated by focusing on data standardization and harmonization and through enterprise-wide data governance. This integration of reporting disciplines and overall risk management principles at the corporate level helps the business change from simple compliance to increased business efficiency. Value for the company is created through the generation of information aimed at delivering insight into performance, growth, and risk.[8] This is paralleled by the mitigation of structural complexity through process and policy simplification, standardization, and optimization.

Compliance itself then becomes a benefit of this approach, rather than just a costly proposition. As a result, effective organizations monitor business-relevant events, assess them as either threats or opportunities, and take the necessary actions to address them. In other words, the use of enterprise data reaches far beyond compliance and focuses on enhancing risk insight and delivering business value.

To make enterprise risk management (ERM) viable and consistent, businesses must first optimize their operations and eliminate duplicate business functions. For example, in many banks, account opening is often duplicated multiple times for each financial product and can easily account for 20 percent of the operations cost. Further complexity is added to the account-opening process by the USA Patriot Act Section 326 requiring a "Know Your Customer" investigation,[2] which Federal Regulation 31 CFR 103.121 further regulates to be done ". . . within a reasonable time after the account has been opened."[9] Rather than implementing this separately across the duplicate account-opening processes, many banks started to optimize their business into business components. Optimizing the business is a crucial part of gaining the most from an enterprise-wide risk-management approach and, as a side effect, costs can often be saved when duplication is eliminated.

Hence, effective organizations leverage their compliance efforts, gain predictive information and business insights from collected data, and establish an enterprise-wide optimized ERM function. ERM takes advantage of classical risk-management disciplines, such as the management of credit and market risk, and integrates them with the management of new risk types, such as operational risk,[10,11] technology risk,[12] and compliance risk.[13] Holistic ERM starts with a focus on events that could potentially happen and their classification into opportunities and risks. Keeping track of these events requires good data and data governance managed at the enterprise level. It also requires a taxonomy or classification scheme of the most important risks to the entity and a common language for understanding those risks. Improved management of data allows the enterprise to take advantage of modern analytical methods to determine the quantitative impact of risk. Data analysis enables the enterprise to gain an overall view of the current risk as well as trends and possible future risks.

In addition to other causes, regulations can also motivate the adoption of ERM practices, which focus the business on operating the "right way" as a normal business practice. Compliance thus becomes a side benefit of good business conduct. For instance, Basel II explicitly prescribes that operational risk must be adequately managed. In addition, regulations such as SOX require the adoption of a control framework, such as the control framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO),[14] which has become a de facto standard for accounting. The COSO framework itself has been revised to incorporate a

strong risk-management focus. Accordingly, the emergence of ERM as a new business function delivers proactive and predictive business insight and identifies growth opportunities by extending beyond compliance to enhance risk insight.

Integration of various risk-management functions across individual business units of the same organization yields a number of advantages: There are large potential synergies in terms of both risk identification and assessment and with respect to adopting appropriate responses to specific risks. Furthermore, information collection and risk identification is conducted on a higher enterprise level, leading to risk responses that are better aligned with the business strategy.

To gain greater insight into risk, regulators are also pushing enterprises to adopt a more quantitative approach to risk management. Basel II is a very good example: Organizations can achieve financial benefits through reductions in capital allocations when risks are estimated by using techniques such as those in quantitative modeling.[3] However, although there is a drive to use more quantitative models, qualitative risk management methods need to flank the quantitative methods, as most people do not think of risk in terms of probabilistic models and because populating quantitative models with meaningful input data may be impossible.

Although adopting an enterprise-wide, holistic risk-management approach can help gain business insight, there are additional complications for large global businesses or businesses embedded in a global supply-chain ecosystem. These complications range from abiding by differing and often contradictory laws and regulations in different geographical areas to achieving a much better understanding of the ecosystem. (For an example of contradictions, see Reference 15, which discusses how regulators are addressing issues where SOX is in conflict with European regulations.) In a global supply chain, the assumption of mitigating concentration risk by choosing two suppliers (to reduce the risk of reliance on a single source) may be faulty if these two suppliers themselves share a common supplier. To get a better understanding of how risks are managed among businesses within an ecosystem, standards are necessary to describe and track risk across these ecosystem boundaries and interfaces. It is important to trace business processes and the risks associated with these processes as they cross company boundaries. Also it is important for global organizations to think about country-specific treatment of risks, an example being the treatment of information protection (privacy) and how the regulations differ by country.

ENTERPRISE RISK MANAGEMENT

Motivated by the need to gain better insight into their business processes and more transparency throughout the enterprise to understand and control risks and align them with their business strategy, organizations must develop an overall approach to how they define, establish oversight for, manage, and monitor events within their corporate boundaries and with respect to external events. Events need to be assessed in terms of the opportunities they present and the risk thresholds they carry.

■ It is important for global organizations to think about country-specific treatment of risks ■

Before we present our ERM framework, we provide a coarse definition of what ERM is commonly understood to encompass.

Defining ERM

There are many definitions of ERM. A representative example is the following from the COSO framework: "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[14]

A study of the various ERM definitions reveals that all share three critical characteristics:[15]

1. *Integrated*—ERM must span all lines of business.
2. *Comprehensive*—ERM must include all types of risks.
3. *Strategic*—ERM must be aligned with overall business strategy.

As companies begin to manage risk, they typically come to the conclusion that they cannot manage risk in an ad hoc manner by vertical business unit, by specific regulation, or by domain; it becomes apparent that risk management must be conducted in a structured way and *integrated* throughout the whole enterprise. This entails a number of elements, such as the definition of risk, the formation of a risk oversight role, defined tolerances, policies and procedures for dealing with risk, the inclusion of risk as a factor in business decision making, and the reporting of risk in a consistent manner.

Furthermore, risk management must be *comprehensive* and span all risks to understand and manage the interplay among various types of risks and the fact that certain events carry with them more than one type of risk. For example, having a transactional processing system malfunction not only carries financial risk, but also reputational risk, as happened to Amazon.com in 2005 when its Web site went down for a few hours in the pre-Christmas season, which was widely reported in the news (e.g., see Reference 16).

Futhermore, risk must be managed from a business *strategy* point of view. Not all risk is bad, and the business strategy must set a risk appetite policy to govern the ERM approach. For example, the insurance industry lives from assuming risk and managing it.

ERM maturity continuum

Businesses evolve their response to risk and compliance along an ERM maturity continuum. They begin by complying in order to avoid penalties, progress through improving to optimize and sustain, and finally achieve a state of continuous risk-based transformation where they can make use of compliance for competitive advantage.

In the *comply* stage, a company starts with a strategy of penalty avoidance, often implemented through manual auditing and control procedures on top of existing processes. Frequently, laws also require changes to business processes, which are done manually and in an uncoordinated manner in this stage. Adding specific customer verification activities in account-opening processes to comply with the "Know Your Customer" mandate from the Patriot Act is an instance of this. Such activities are often done multiple times as many businesses have duplicate account-opening processes for different products and lines of business. This stage typically adds additional overhead cost, is time consuming, and is not integrated into the overall day-to-day operations of the business. At best it can help the business react and accurately report on risk events after the fact. Although this may satisfy the letter of the law—for example, in SOX by accurately disclosing business results—stakeholders may not be happy with the results. In the long run, having predictive capabilities to sense increased risk and the potential of impending problems would help a business much more.

As businesses realize that compliance is not limited to a one-year project but is rather an approach that must be sustained and adapted to meet changing regulations year after year, they enter the *improve* stage. Most companies in the improve stage initially focus on improving the efficiency of their compliance and control procedures to minimize cost by standardizing procedures throughout the enterprise and adding automated status monitoring. The processes in turn are instrumented with the necessary control points, metrics, and measurements needed to enable automated monitoring. In the long term, this reduces the current redundant control procedures and replaces them with lighter-weight random audit checks and control procedures to ensure the separation of duty and increase overall accountability.

Due to the costs of compliance (e.g., for SOX 404), many organizations seek to improve operational efficiency, for instance, through the reduction of overlapping or ineffective controls and the use of automated controls. Many will start to realize that there is another option: integrating risk and compliance management as part of the overall business strategy and execution, where doing the "right" thing begins to be the most efficient for the business. By eliminating duplicate business activities (e.g., duplicated account-opening procedures) and improving the remaining processes (e.g., including greater automation and controls), costs are reduced and actions are taken as soon as potential risk events are detected. In addition, as enterprises further integrate their risk management, the organization becomes more transparent and preemptive in its detection and handling of risks. This reduces remediation costs, limits waste, and improves visibility into the operations of the business.

The benefits of the improve stage start to show as enterprises migrate their initial compliance investments to become compliant to a steady-state model that makes use of technology to improve cost efficiency and begins to provide value (beyond compliance) to the organization. At this stage, enterprises also start to think more from an enterprise-wide risk-management paradigm and begin having risk analysts assess the impact of external events and suggest appropriate actions to the chief risk officer (CRO).

As enterprises enter the *transform* stage, they embrace a holistic, optimized risk management approach by looking at events and classifying them into risks and opportunities based on well-defined policies that take risk and regulations into account. In this stage, the enterprise is focused on achieving internal improvements by streamlining and rationalizing processes at an enterprise level and by adding automated control points directly into the business procedures to replace error-prone manual controls. It is during the process of assessing and reducing risk that organizations often uncover inefficiencies in their processes and unnecessary costs. As a result, general risk analysis and optimization of business components are often done as a precursor to establishing an ERM approach.

In the transform stage, events are standardized throughout the enterprise and flow over a common event infrastructure, which collects all events from internal systems and sensors as well as from external sources. These events are correlated and related back to business processes and regulations, allowing them to be visualized not in the context of a singular event but in the context of the process and regulation these events impact. To enable trend detection and prediction, current events are analyzed in conjunction with historic event data in analytics engines, and then, the analysis is used to visualize the risks. This allows business leaders to gain insight into current operations and the associated risks.

This integrated view of risk allows enterprises to optimize activities around events and to assess the risks and opportunities associated with them. The processes and policies are automated and deployed to the systems with general monitoring and holistic, sometimes automated, response and mitigation strategies. An example might be the automatic interpretation of security intrusions in the enterprise, signaled by security events, and then linked or correlated to a common component or cause. Policies can be automatically applied upon the detection of such events. The policies and processes have been built to take into account all constraints from regulations and standards that the senior leadership decided to follow, as well as the risk models relating to the business processes and infrastructure.

■ To make ERM viable and consistent, businesses must first optimize their operations and eliminate duplicate business functions ■

The key is to change the approach from simply automating processes to optimizing them. This means taking an enterprise-wide point of view and including risk factors. By doing so, it is possible to avoid ending up with faster but suboptimal or outright risky processes. Instead, optimized processes allow a transformation beyond cost savings by offering competitive advantages and differentiation to the business. Advanced operational risk modeling can be used to identify risk in the processes and to guide their optimization.

There are probably no businesses today that are fully optimized and performing at this transform stage. However, there are a number of businesses that have started the journey. According to Mark Beasly's 2005 ERM Status Report,[17] about half of the companies surveyed had either no ERM plans, had not yet decided, or were thinking about it for the future. About 37 percent claimed to have partial ERM plans implemented, and 11 percent claimed to have a full ERM system in place. Most companies today are still in the comply stage and working their way toward the improve stage. For example, only 12 percent of companies have a high level of automatically generated reports.[18]

A year after the 2005 report, the situation seems to have shifted. According to the latest chief financial officer (CFO) study of the IBM Institute of Business Value,[19] more than 75 percent of the studied finance

departments "frequently or sometimes" support their company in designing an ERM framework and in developing a corresponding culture. Furthermore, more than 90 percent of the involved finance organizations already "fully or partially manage compliance risk," while less than 70 percent manage event risk.[18]

Once a company starts to holistically integrate risk management into its overall enterprise business management strategy, it embarks on the journey toward the transform stage of the continuum. At this stage the value generated by the integrated risk and compliance approach (as part of the overall business strategy) outweighs the costs of compliance. This is achieved by making use of gathered compliance data for business analysis, optimization, and business insight. Key advantages of this approach are enhanced decision making, increased transparency and speed, process robustness, risk mitigation, streamlined reporting, and increased accountability, which in turn increases investor confidence.

ERM becomes increasingly important in a global environment as complexities increase for large businesses with multiple lines of business and for businesses in larger ecosystems with interorganizational integration, such as supply chains. The various organizations in such a network all display different levels of maturity within the ERM continuum. Rogue organizations may impact a business, even if the business is not directly connected to the rogue organization. Cases like Enron, Worldcom, and Parmalat have illustrated what could happen to ecosystems when one company collapses. But not only rogue organizations are at risk; a large ecosystem may also contain unexpected single points of failure, such as alternative suppliers relying on raw materials from a single source. If the source of raw materials fails to deliver, both suppliers will be unable to deliver. Knowing the relationships of the whole ecosystem becomes more important to determine the exposure to risks from other companies. (An example is the 2002 water shortage at Taiwan's Hsinchu Science Park.[20]) On the other hand, reasons of business confidentiality and privacy may make full-information solutions, which may at least sometimes work in one large enterprise, not applicable for an entire ecosystem; hence, a well-balanced global approach to sharing just the right information is necessary.

To help enterprises better understand where they are and how they can move toward an improved maturity state, we have developed a high-level ERM framework. This framework and its merits are described in the next section, followed by a description of the tactical steps needed to launch the enterprise toward ERM.

OPTIMIZED ERM FRAMEWORK

To build an enterprise-wide risk-management system, an overall "big picture of the world" is needed to frame an organized way of thinking about business risks. The context is that an organization needs to think about external risks and externally imposed rules and regulations which, in turn, require an internal- and an external-facing risk perspective. The next sections outline this big picture and describe its layers in detail with respect to the transform stage.

Overview

Figure 1A depicts a model of how people, processes, and technology interact in an enterprise. It shows a very mature stage of the enterprise, one that IBM calls *On Demand*, which, according to Samuel J. Palmisano, Chairman, President, and CEO of IBM, is ". . . an enterprise whose business processes—integrated end-to-end across the company and with key partners, suppliers and customers—can respond with speed to any customer demand, market opportunity, or external threat." In this context, we call it the *transform stage*. In the figure, the orange arrows and the blue technology elements occur only in this transform stage. In our framework, we model an enterprise and its environment in five layers. The enterprise is embedded in the external world, which is represented through the jurisdictional layer and partly by the events layer. The enterprise itself spans the three middle layers and reaches partly into the events layer. We first describe the layers briefly, and then look at them one by one.

On top, the *jurisdiction* layer includes the external influences on the enterprise, such as the regulatory environment and the social and competitive landscape. It shows from whence come the regulations with which an enterprise may have to comply and what influence enterprises may have to ease their compliance tasks (e.g., through industry organizations that publish best practices). Represented are all the external issues senior business leadership

must take into account when developing the company's overall business goals and strategy.

The *strategy* layer encompasses the enterprise business strategy. This is where senior leadership defines business goals, policies, strategies, procedures, processes, controls, and organizational structure to achieve their objectives. They define the roles and responsibilities needed to execute the procedures and processes, and they define the overall risk appetite and risk model under which the enterprise operates. We look specifically at how regulations should be treated here and how risk comes in.

The *deployment* layer is where high-level strategy procedures, processes, and policies are implemented either as manual or automated processes, and where systems and applications are designed and developed. Thus, it specifies how the business strategy is transformed into something that can be acted upon. From the IT perspective, one would call it the modeling, development, and deployment layer, but it also contains non-IT deployments.

The *operation* layer contains the day-to-day operations of the enterprise. In IT terms, it contains the runtime systems, but it also contains the employees and methods used to aid them in keeping the enterprise in compliance with the relevant regulations.

The *events* layer contains real-time and historic event collections (detection, aggregation, and logging) and the correlations and statistical analysis of these events to allow the operation layer to act on them. These events can come in many forms, ranging from the expected flood of transactional events as part of the overall execution of the business to the external events impacting the business. A large majority of these events are expected, and the overall business processes and policies are designed to handle these events as either risks or opportunities. Expected events also contain such possibilities as disasters, security incidents, and fraudulent transactions. However, there are gray areas around what exactly constitutes a risk or opportunity. For example, insurance firms manage their business according to stochastic models of the probabilities of disastrous events and their expected damage, adjusting their premiums accordingly (in fact their business is to manage and mitigate this risk). Other events may not be expected, and the business will have to deal with them as they come up (and in the future they may add those events to the universe of expected events and put procedures in place to address them). The events layer could logically be considered part of the operation layer, as it is what the operation layer deals with, but it contains so many new aspects for an enterprise, as well as events external to the business, that we treat it as a separate layer.

■ Not all risk is bad, and the business strategy must set a risk appetite policy to govern the ERM approach ■

Overall flow

While the detailed interactions among the layers are quite complex, there is an overall flow pattern between the five layers (***Figure 1B***). In essence, jurisdiction provides guidance, which is interpreted by the business and operated upon. However, external (unexpected) events impact the business and are then brought to the attention of regulators for review, further guidance, and rule making. Starting from the jurisdiction layer, laws and regulations, industry best practices, and stakeholder input all impact the strategy layer. These are interpreted and turned into policies and procedures by the senior business leadership. These procedures then flow to the deployment layer for subsequent implementation. Policy implementations are deployed, and the processes are then provisioned to the operation layer. Events occurring at the event layer are identified, analyzed, and assessed before actions are taken to deal with those events. In much the same way, risk data is extracted and aggregated from events on the event layer. This data is then processed, categorized, and quantified on the operation and the deployment layers. These layers also manage controls or mitigation, their effectiveness, and remediations based on the generated information. Obtained risk information is further propagaged to the strategy layer, where it is visualized based on severity, impact, and corrective measures. Possible mitigations are planned and aligned with the business strategy before they are delegated to the deployment and operation layers for execution. Reports are generated from the process-

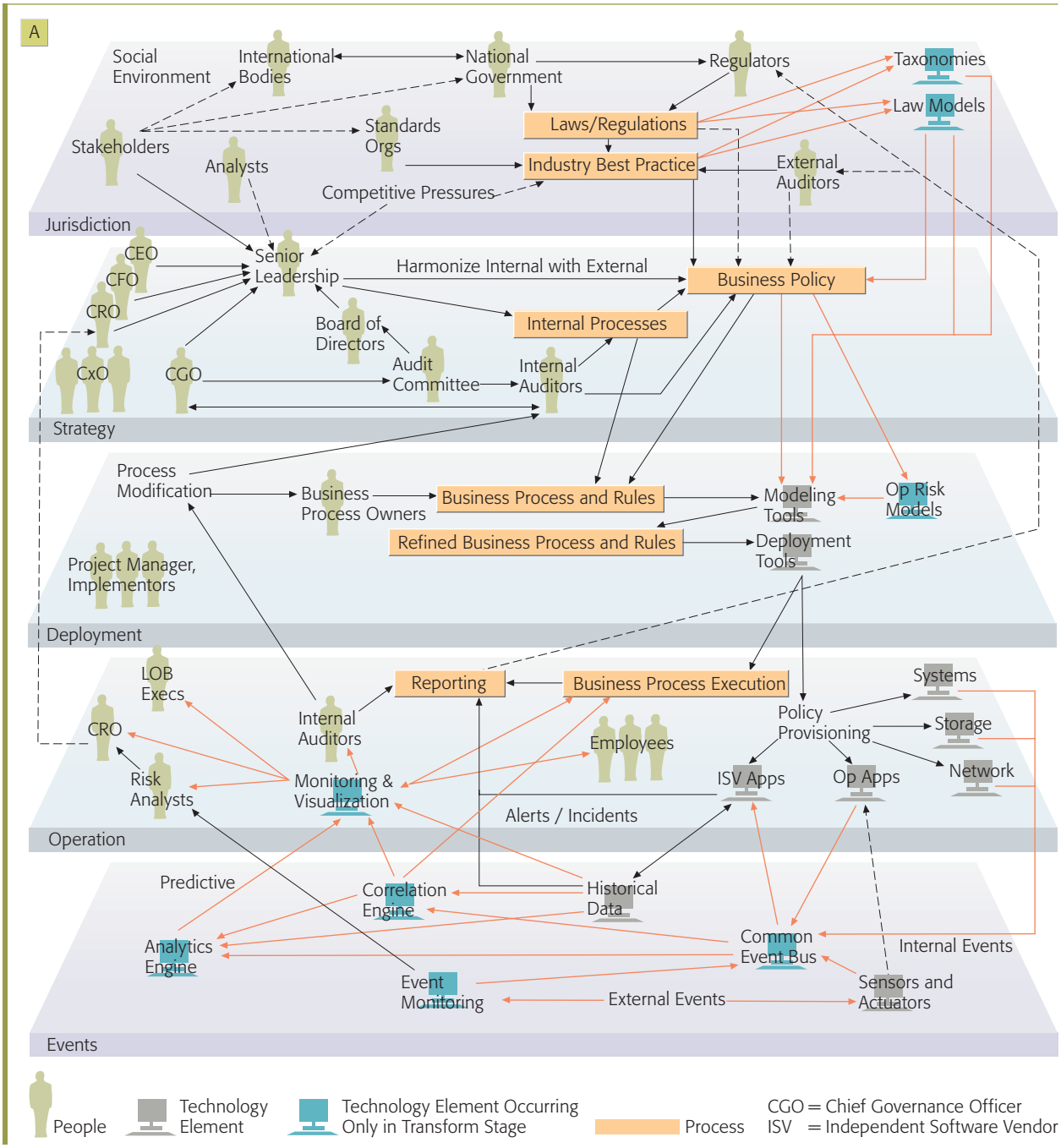

Figure 1A
ERM framework: Overview

ing layer and flow from internal managers and auditors back out to the external auditors in the jurisdiction layer. Furthermore, there is an interaction of lobbying and negotiation between the strategy and the jurisdiction layer. Hence, there is a general feedback loop mechanism in place.

While we have now described the information flow between the different layers from an overall perspective, there is also a general communication pattern between superimposed layers, that is, small feedback loops (not depicted in Figure 1B). The upper layers provide the goals to be achieved and

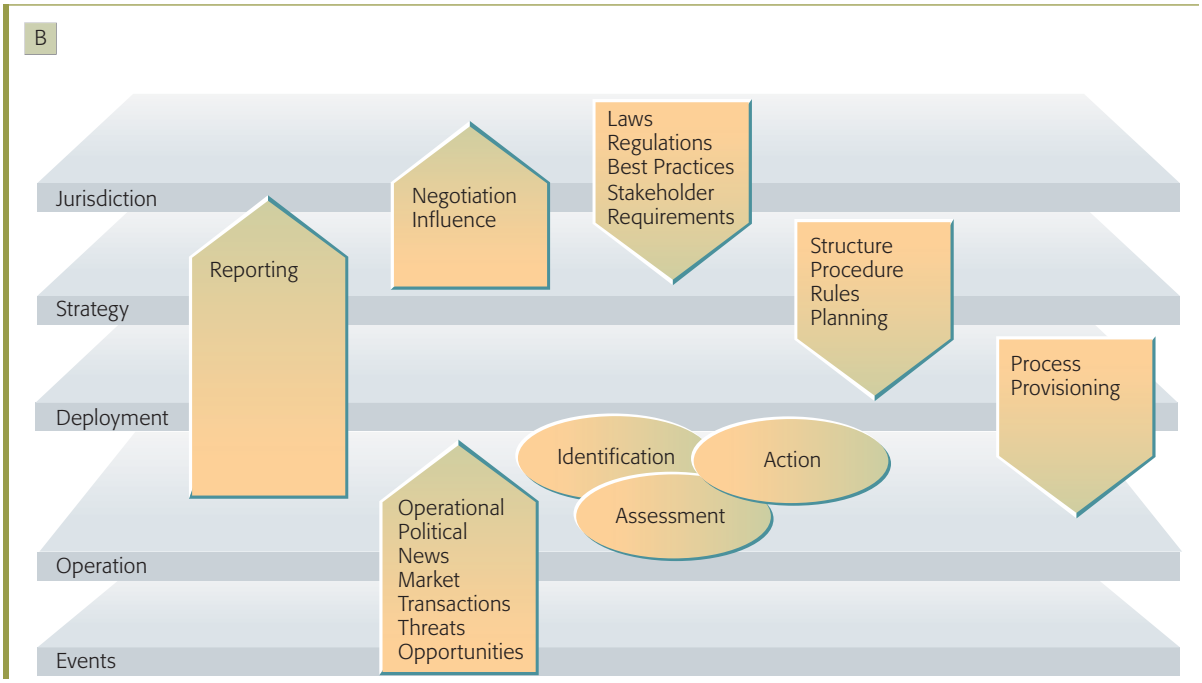

Figure 1B
ERM framework: Basic flows

suggest the mechanisms and resources to achieve them. The lower layers, in contrast, report on the current goal achievements, suggest improvements with respect to the mechanisms used, and provide estimates of resources required to implement these improvements.

Jurisdiction layer

The most important parts of the jurisdiction layer are the two tan process boxes. The upper box contains laws and regulations, that is, actual legal documents put into force by legislative bodies. The lower box (Industry Best Practices) contains refinements of laws and regulations that may not be binding but that sometimes play a larger role for enterprise deployment than the laws and regulations themselves, because those are not concrete enough for deployment. Such refinements are typically made either for many enterprises together by standards organizations or by the enterprise's external auditors or a legal council for a specific enterprise.

The concept of laws as opposed to regulations, where governments make laws and regulators make regulations, is of no large importance for us. Laws are typically quite generic, and then lower-level bodies (e.g., in the United States, the Federal Trade Commission [FTC] and the Securities and Exchange Commission [SEC]) work out more detailed requirements. In particular where IT is concerned, one tries to be technology-neutral in laws. Regulations start to address technology, but details may still be hidden in terms like "appropriate," "reasonable," and "state-of-the-art." Such terms are then refined further by industry best practices.

Currently there is almost no technology on the jurisdiction layer. However, in the long run (i.e., in our transform stage), it will be beneficial to start the formalization of policies right on this layer in order to have the smallest possible semantic gap. In particular, instead of individual enterprises trying to derive actionable policies from regulations or best practices one by one, standards organizations can aid by producing such policies for the industry as a whole to the benefit of all. The results of such formalizations are taxonomies and regulation models over those taxonomies, that is, actual rules of what should or should not be done in the given terms. The REALM (Regulations Expressed As Logical Models) approach to the formalization of regulations and their transformation into executable artifacts, such as correlation rules or retention policies, represents a first step in this direction.[21,22]

If the taxonomies of different regulations and standards can be unified to at least some extent, then regulation models can be combined. For instance, one could then join the privacy laws or the retention requirements of several countries into one model for a multinational enterprise.

It may sound futuristic that regulators themselves would produce formalized taxonomies or even regulation models, but it may not be so far off. For example, consider the advent of the Extensible Business Reporting Language (XBRL) as a reporting language with a unified taxonomy and its recognition by the SEC.[23–25]

Strategy layer

The strategy layer is where the corporate leaders set the direction for the enterprise abbreviated as a business policy and define internal processes and controls for bringing their strategies into real life. As we concentrate on risk and compliance, we mention in particular a possible CRO and a chief compliance officer (CCO). At least for SOX, the CEO and the CFO are personally responsible, and in general, a risk and compliance strategy should have support from these roles in order to be successful. Internal auditors also play a large role.

For the lack of space for more arrows in the five-layer version, Figure 1A does not show that there will be specific risk and compliance parts in the business policies and in specific internal processes that ensure risk and compliance. Compliance policies at this level may just be the identification of the regulations that apply to the given enterprise or to specific lines of business or geographical areas within it, or they may be the choice of a standardized best practice to follow. Where there is no such best practice, the enterprise itself must make similar refinements of a regulation by defining its own practice. This policy may also go somewhat further than a best practice, taking some of the specific processes and roles of the enterprise, as far as they are known on the strategy layer, into account. For instance, within a given enterprise it is easier to state what "need to know" means than in general.

Risk policies may be general thoughts about the risk appetite of the company. They may concern issues where the financial value cannot be derived easily from data at the present, for example, the loss of brand value in the case of noncompliance with certain laws or publicized security incidents.

Risk and compliance processes are initially about how the enterprise sets about implementing better practices, that is, typically a project-style process such as "the SOX project." There are some standards in this space, such as the COSO control framework[14] and the COSO ERM framework,[26] or, when starting to consider IT, the COBIT (Control Objectives for Information and Related Technologies) control framework[27] or the ITIL** (IT Infrastructure Library) governance processes.[28] There are also other, more industry-specific control frameworks. In the transform stage as we propose it, parts of such frameworks will already be coded on the lower layers and have become a policy-driven, natural part of the business.

Deployment layer

On the deployment layer, strategies are put into practice; that is, it is about transitions and change and documentation of what is being done. For IT (or technology in general), this layer covers enterprise modeling, application and infrastructure development, and application and infrastructure deployment.

The major issue is to model business processes and rules. The tan boxes in the deployment layer in Figure 1A show that the processes may exist even without formal models, but in the transform stage we assume that models already exist and that modeling tools are used to represent them. Such a tool may be the IBM WebSphere* Business Modeler. While most enterprises did not have business process models until recently, SOX forced them to at least model their financial processes (although a simple graphic documenting the process is a sufficient model), and we believe that many other laws that aim at accountability for actions and their consequences will carry modeling beyond financial processes.

We stress that rules or policies derived from regulations or from strategic business policies (as the incoming orange arrows show) should remain separate entities in the models, even where business processes are changed to accommodate them. This is important because the business processes may be changed again for many other reasons, and each new version has to be checked for policy compli-

ance. Hence, the policies should be expressed in the modeling tools, but as separate constraints. This separation is also crucial to track changes in laws and regulations over time. A long-term goal in this context is automatic compliance checking, as proposed by Liu et al.[29]

For regulations, the best case is if they were already modeled on the jurisdiction layer; otherwise, the formalization has to take place on the deployment layer. If there are business process models in the enterprise that predate the current compliance issues, a terminology mapping will usually be necessary between the existing business-process vocabulary of the enterprise and the vocabulary of the regulations or standards. The deployment layer is also the first layer where one can make risk models, in particular, for operational risk. This means to associate potential adverse events with elements of the business process. It is then possible to assign probability distributions to them and to compute their effect over the business-process model. The business processes may then be optimized for risk as one of several optimization criteria and weighted according to the risk strategy.[10,11,30]

The first abstract business-process models are typically refined into more practical, deployable models. This may include programming those parts of the processes that are done automatically, designing user interfaces for the borders between automatic parts and human parts, and providing guidance for the humans who execute the human parts. In automatic parts, the risk and compliance policies should, as far as possible, be automatically followed but remain policy-based as far as possible for later changes. For the human parts, one should try to integrate risk and compliance policies directly with the task explanations. There may also be specific learning material that humans in certain roles need to go through as separate processes.

Operation layer

The operation layer is about the actual execution of the business processes. Given the business-process models and rules from the deployment layer, one wants to ensure that the actual execution follows the processes and adheres to the rules. Referring to Figure 1A, this is shown by the two incoming black arrows from the deployment tool on the deployment layer to business process execution and to policy provisioning on the operation layer. In reality, however, for a long time the arrow to business process execution will still be the other way around; that is, the enterprise has existing processes, and the model is derived from them, typically informally.

Furthermore, humans currently play a large role in many business processes, and some of them necessarily have considerable freedom in their business decisions. One can neither assume that the risk and compliance guidance for people is perfect nor that they all honestly and carefully adhere to the guidance.

■ The key is to change the approach from simply automating processes to optimizing them ■

This already motivates why there are monitoring and reporting components on this layer and special roles, such as internal auditors and risk analysts. This is true not only for the deployment layer. More uses for these components will become clear with the events layer.

For technical implementations, the policy provisioning part is of particular importance. This is where risk and compliance play a specific role in deployment. For instance, rules about who is authorized to do what may be translated into access control policies. Likewise, privacy rules may be translated into access control policies, but also into encryption rules or data-labeling rules. Retention rules for business data may be translated into storage settings. Accountability rules may be translated into logging, but also into digital-signature rules. Human knowledge will initially be needed, and later, at the least, detailed IT models and trust models will be needed on the deployment layer. Special hardware support may also be needed on the operation layer, for example, write-only storage may be needed to ensure that log records can be written, but not deleted or revised.

Events layer

The events layer contains components for dealing with internal and external events. One type of event, the so-called internal event, originates in the

operation layer of the enterprise, as the downward arrows on the right show. The assumption is that all applications and middleware are equipped with event emitters for a common event bus because the rules that work on events may be so global that one cannot provision them all to the individual components.

The second type of event is external. While some of these events may come in the same nicely structured way as internal events (only from other enterprises);

■ Risk policies may be general thoughts about the risk appetite of the company ■

some may be much more vaguely defined and need specific, sometimes human, monitoring; for example, political developments or certain market shifts.

Sensors are specific components whose primary goal is to notice events. In particular, there are sensors that detect problems with such physical variables as temperature, humidity, fire, and power; but there are also sensors to detect digital network problems and human burglars.

Correlation engines and analytics engines are the components that evaluate events. By evaluation, we mean determining correlation in real-time analysis. These operations on an event stream are typically relatively simple and fast. Analytics denotes more complex operations that are normally conducted offline. Both may use historical data; in fact, analytics almost always does. Furthermore, not shown in Figure 1A, at the least, analytics often uses the models from the deployment layer to give more semantics to the raw events. Also, at the least, correlation usually needs rules, also derived from the deployment layer, to know what to look for—typically deviations from policies that could not be perfectly enforced.[22]

The results of all these components, at least those results that indicate that something is not as it should be, are fed back into the operation layer. At the beginning, the results of the event processing are fed primarily into a visualization tool so that humans can react to them. Later, or where well-known expected events are considered part of this layer and not of the business processes, the events may be fed back directly into a business or IT process.

Most of our description thus far has focused on the transform stage layers. As enterprises evolve through the various stages, they generally move from a delegation of compliance to the business units and manual implementations at the comply stage to enterprise-wide governance and automated controls at the transform stage. In the comply stage, the strategy layer contains little more than the policy to comply with and the delegation to lower levels to implement compliance procedures and reporting standards, which are executed at the lower levels in a mostly manual fashion. When an enterprise moves into the improve stage, policies become established at an enterprise level, and the focus is on sustainable processes, often with significant increases in staff to execute those processes and generate the needed reports. Detailed documentation of the processes and reporting needs are formulated at the deployment layer and executed at the operation layer. As an enterprise moves on to the transform stage, policies are managed from an enterprise governance stance, and the senior leadership has defined the risk appetite for the enterprise. Process and documentation standards are formally modeled at the deployment layer, and controls are installed into applications and the infrastructure to automate the event processing and report generation at the operation layer. The event layer carries events on an enterprise-wide bus, and analytical tools are employed to correlate events or combinations of events back to the enterprise policies.

EMBARKING ON THE ERM JOURNEY

This section describes at a high level the necessary tactical steps for enterprises to implement an ERM strategy and the necessary governance. In brief, executive sponsorship at the senior management level of the company is critical to achieving a holistic, enterprise-wide ERM approach. The senior management team needs to commit to ERM as part of their vision for their company's future, and the current state of the firm's ERM readiness must be assessed before any formulation of further steps toward ERM can be undertaken. The following are the tactical steps that comprise this journey:

1. *Gaining executive sponsorship*—Executive leadership articulates the benefits of ERM and develops an overall business case to justify the investment

in it. Management is typically motivated by a recent risk event, mandatory regulation, or audit finding or a realization that the current approach to risk or compliance is costly and inefficient. For example, account opening is often implemented on a product-by-product basis in financial services firms. With the advent of the Patriot Act, the firm is required to implement the "Know Your Customer" function across these many duplicate processes. This often leads to an approach that optimizes business components by gathering all of the duplicated account-opening processes into a single business component. Management can then establish a core team and communicate the high-level business case for the related investment of resources. The core team will consist of representatives of the organization who are responsible for the ongoing management of risk, representatives of the company's core risk and legal teams, and any consulting team engaged on this project. The team will become familiar with the ERM framework and its components, concepts, and principles. This familiarity will provide a common understanding and language, and the foundation required to design and implement ERM in a manner that will effectively meet the needs of both the corporation and the division.

2. *Assessing the current state*—The assessment of the current state identifies where the organization is on the maturity continuum and identifies gaps. Different units within an enterprise may be at different stages simultaneously, depending on the risk area being evaluated. This includes an assessment of how ERM components, concepts, and principles are currently being applied within the business. The core team also identifies formal and informal policies, processes, practices, and techniques currently in place, and existing capabilities in the company for applying the framework principles and concepts. Industry-specific assessments of ERM readiness may already exist and are a good starting point. For example, the IBM Institute for Business Value has used such an assessment in a CRO survey.[18]

3. *Developing an ERM vision*—The core team will develop a vision that sets out how ERM will be used and how it will be integrated within the organization to achieve its objectives, including how the corporation focuses its risk management efforts on aligning risk appetite and strategy, enhancing risk-response decisions, identifying and managing enterprise risks, seizing opportunities, and improving the deployment of capital. Depending on the actual law or risk considered, this will include the use of business-line-specific frameworks, such as COSO for accounting and COBIT for IT.

4. *Developing capabilities*—Given the current state (assessed in step 2) and the ERM vision (defined in step 3), the capabilities needed to reach the vision must be defined and developed. This includes the definition of roles and responsibilities for risk management, and the policies, processes, methodologies, tools, techniques, information flows, and technologies to manage risk. It also requires the development of an appropriate risk culture, which may be the most difficult part.[18] This is typically the job of the CRO and the core team, who define a plan of execution and associated milestones to achieve a maturity level for all layer components.

5. *Planning implementation*—The initial plan sets out key project phases, including defined work streams, milestones, resources, and timing. The plan is continuously updated and enhanced, adding detail discovered during previous steps. Additional responsibilities are defined, and the project management system and project plan are refined as required. Actions are developed as required to implement and sustain the ERM vision and desired capabilities, including deployment plans, training sessions, reward reinforcement mechanisms, and monitoring the remainder of the implementation process.

6. *Monitoring and governance*—Management continually reviews and strengthens risk management capabilities as part of its ongoing management process. This includes continual reviews on the effectiveness of the implemented capabilities, the implementation progress with respect to the defined execution plan and milestones, and the verification of strategy alignment.

CONCLUSION

In this paper, we stressed the need for ERM. In particular, we presented the IBM Research ERM framework, which addresses risk and compliance management in a strategic, integrated, and comprehensive manner. In accordance herewith, we have

described how enterprises evolve along an ERM maturity continuum, starting from a state of mere penalty avoidance through a state of improvement until finally reaching a state of continuous, risk-based transformation.

In our five-layered model, the enterprise is embedded in the external world, represented through the jurisdictional layer and partly the events layer. The enterprise itself consists of a strategy layer, a deployment layer, and an operation layer. The jurisdiction layer includes the external influences on the enterprise, such as the regulatory environment and the social and competitive landscape. It shows where regulations affecting an enterprise come from and what influence enterprises may have to ease their tasks complying with them. The strategy layer encompasses the business strategy of the enterprise. On this layer, the senior leadership defines business goals, policies, strategies, processes, controls, and organizational structure to achieve their objectives. They also define roles and responsibilities and the overall risk appetite and risk model under which the enterprise should operate. The deployment layer is where high-level strategy procedures, processes, and policies are implemented, either as manual or automated processes, and where systems and applications are designed and developed. The operation layer contains the day-to-day operations of the enterprise, including the runtime systems and the employees, and how they can be aided in keeping the enterprise in compliance with the relevant regulations. Finally, the events layer contains real-time and historic event collections (detection, aggregation, and logging) and the correlations and statistical analysis of these (expected and unexpected) events to allow the operation layer to react to them.

In our model, enterprises proactively address all sorts of risk, including operational risk and the risk of noncompliance, and bring them all into a cohesive framework to govern risk at the enterprise level. We have used this five-layered framework ourselves to guide our own research and to manage strategic risk and compliance projects. This ranges from the abstract vision of formally modeling laws and regulations to the concrete, quantitative modeling of operational risk and effects of mitigating factors at the business-process level. It also includes enterprise-wide visualizations of risk, making risk accessible at a glance.

CITED REFERENCES

1. *Sarbanes-Oxley Act of 2002*, Public Law 107-204 (116 Statute 745), United States Senate and House of Representatives in Congress (2002).
2. *USA Patriot Act of 2001*, Public Law 107-56, HR 3162 RDS, United States Senate and House of Representatives in Congress (2001).
3. *International Convergence of Capital Measurement and Capital Standards* (Basel II), Basel Committee on Banking Supervision (2004), Bank for International Settlements, http://www.bis.org/publ/bcbs107a.pdf.
4. V. Garcia, *The Avant-Garde of Enterprise Risk Management in Financial Services: From Vision to Value,* Research Report, TowerGroup, Rockville, MD 20852 (2004).
5. J. Lopez, *Gartner Predicts: The Cost of Compliance,* Gartner Research, Stamford, CT 06902 (2005), podcast available at: http://www.gartner.com/it/products/podcasting/asset_140998_2575.jsp.
6. J. Hagerty and F. Sirkisoon, *Spending in an Age of Compliance, 2005*, Research Report, AMR Research, Boston, MA 02110 (2005).
7. J. Hagerty and F. Sirkisoon, *Spending in an Age of Compliance, 2006,* Research Report, AMR Research, Boston, MA 02110 (2006).
8. *The Agile CFO–Acting on Business Insight*, IBM Institute for Business Value, (2005), http://www-935.ibm.com/services/us/bcs/html/2005_cfo_survey_gen.html.
9. *Money and Finance: Treasury*, U.S. Department of the Treasury, Code of Federal Regulations, Title 1, Volume 1, 31 CFR 103.121 (2005).
10. C. Supatgiat, C. Kenyon, and L. Heusler, "Cause-to-Effect Operational-Risk Quantification and Management," *Risk Management* **8**, No. 1, 16–42 (2006).
11. M. Leippold and P. Vanini, "The Quantification of Operational Risk," *Journal of Risk* **8**, No. 1, 59–85 (2005).
12. L.-F. Kwok and D. Longley, "Security Modelling for Risk Analysis," *Proceedings of the 19th IFIP International Information Security Conference (SEC2004)*, Toulouse, France (2004), pp. 29–46.
13. S. Müller and C. Supatgiat, "A quantitative optimization model for dynamic and risk-based compliance management," *IBM Journal of Research and Development* **51**, No. 3/4, forthcoming.
14. *Internal Control—Integrated Framework*, Research Report, Committee of Sponsoring Organizations of the Treadway Commission (COSO), AICPA/COSO, Jersey City, NJ 07311 (1992).
15. *EU-U.S. Dialogue on Financial Market Regulation—A U.S. Perspective,* Remarks of Cynthia A. Glassman before the Annual Washington Conference of the Institute of International Bankers, Washington, D.C., March 14, 2005.
16. T. Kontzer, "Under Pressure: Technological Glitches at Experienced e-Commerce Companies Serve as a Warning

to Others Not to Take a Scalable IT Infrastructure for Granted," *InformationWeek* (January 10, 2005), http://www.informationweek.com/showArticle.jhtml?articleID=57300668.

17. M. S. Beasley, R. Clune, and D. R. Hermanson, "ERM: A Status Report," *Internal Auditor* **62**, No. 1, 67–72 (2005).
18. C. Petit, D. W. Latimore, and P. Pourquery, *Risk, Regulation and Return: Delivering Value Through Enterprise Risk Management*, IBM Institute for Business Value (2005), http://www-03.ibm.com/industries/financialservices/doc/content/resource/thought/1595397103.html.
19. IBM Institute for Business Value, http://www-935.ibm.com/services/us/bcs/html/bcs_whatwethink.html.
20. A. Hesseldahl, "Taiwan's Dry Chips," Forbes.com (May 13, 2002), http://www.forbes.com/2002/05/13/0513drought.html.
21. C. Giblin, A. Y. Liu, S. Müller, B. Pfitzmann, and X. Zhou, "Regulations Expressed as Logical Models (REALM)," *Proceedings of the 18th Annual Conference on Legal Knowledge and Information Systems*, Brussels, Belgium (2005), pp. 37–48.
22. C. Giblin, S. Müller, and B. Pfitzmann, *From Regulatory Policies to Event Monitoring Rules: Towards Model-Driven Compliance Automation*, Research Report RZ-3662, IBM Research GmbH, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland (2006), http://domino.research.ibm.com/library/cyberdig.nsf/le4115aea78b6e7c85256b360066f0d4/8568614878e51e9b85257205003600d7?OpenDocument.
23. Spotlight On: Interactive Data and XBRL Initiatives, U.S. Securities and Exchange Commission, http://www.sec.gov/spotlight/xbrl.htm.
24. Welcome to XBRL International, http://www.xbrl.org/Home/.
25. *The Promise of Interactive Data*, Remarks of Christopher Cox before the 14th International XBRL Conference, Philadelphia, PA, December 5, 2006, http://www.sec.gov/news/speech/2006/spch120506cc.htm.
26. Enterprise Risk Management—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), AICPA/COSO, Jersey City, NJ (2004).
27. Control Objectives for Information and Related Technology (COBIT), Version 4.0, IT Governance Institute and the Information Systems Audit and Control Association (2005).
28. IT Infrastructure Library (ITIL), Office of Government Commerce (2006), http://www.itil.co.uk/.
29. Y. Liu, S. Müller, and K. Xu, "Static Compliance-Checking Framework for Business Process Models," *IBM Systems Journal* **46**, No. 2, 335–361 (2007, this issue).
30. F. Cheng, D. Gamarnik, N. Jengte, W. Min, and B. Ramachandran, *Modeling Operational Risks in Business Processes*, Research Report RC-23672, IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598 (2005).

Accepted for publication October 16, 2006.
Published online March 21, 2007.

Carl E. Abrams
IBM Research Division, Thomas J. Watson Research Center, 19 Skyline Drive, Hawthorne, New York 10532 (carl.abrams@us.ibm.com). Dr. Abrams is the Financial Services Sector Business Executive for the IBM Research Division. He received a B.S. degree in chemistry from the University of Connecticut, an M.S. degree in computer science from the Stevens Institute of Technology, and a Ph.D. degree in computing from Pace University. Dr. Abrams began his career as a chemist for Lederle Laboratories. Between 1977 and 1992, he worked for Chase Manhattan Bank, where he held the positions of Division Executive for the Trading and Treasury department and the International Individual Bank. He was the Director of Applications Development for Swiss Bank (New York) from 1992 to 1997. In 1997, he joined PricewaterhouseCoopers Consulting where he specialized in program management. Dr. Abrams assumed his current position at IBM Research in January 2003.

Juerg von Känel
IBM Research Division, Thomas J. Watson Research Center, 19 Skyline Drive, Hawthorne, New York 10532 (jvk@us.ibm.com). Dr. von Känel is a senior research staff manager in the Computer Science department. He received an M.S. degree in mathematics and a Ph.D. degree in computer science, both from the Swiss Federal Institute of Technology (ETH), Zurich. He joined IBM Switzerland in 1984 and IBM Research in Zurich in 1986. He moved to the Thomas J. Watson Research Center in 1991. Dr. von Känel was named by *Risk and Treasury Magazine* as one of the 100 most influential people in finance for leading the risk and compliance work at IBM Research.

Samuel Müller
IBM Research Division, IBM Zurich Research Laboratory, Säumerstrasse 4, 8803 Rüschlikon, Switzerland (sml@zurich.ibm.com). Mr. Müller obtained an M.S. degree in computer science and an M.A. degree in economics, both from the University of Zurich. He joined IBM Research in Zurich in 2004, where he is currently doing research in the area of risk and compliance. In parallel, he is working toward his doctorate degree as an external Ph.D. student at the Swiss Federal Institute of Technology (ETH), Zurich, where he is a member of the Information Security group. Mr. Müller's research interests include modal logics, formal methods and modeling, risk and compliance management, game theory, and economics.

Birgit Pfitzmann
IBM Research Division, IBM Zurich Research Laboratory, Säumerstrasse 4, 8803 Rüschlikon, Switzerland (bpf@zurich.ibm.com). Dr. Pfitzmann is a senior research staff member. She received a diploma in computer science from the University of Karlsruhe and a Ph.D. degree from the University of Hildesheim. Since joining IBM she has been responsible for research in risk and compliance, identity management, Web services security, cryptographic key management, and formal verification of cryptographic protocols. She has served on various task forces defining IBM technology and strategy in security and privacy. She is the author of more than 100 research papers in security, privacy, and cryptography. Dr. Pfitzmann is a member of the Association for Computing Machinery (ACM), the German Society of Computer Science, the International Association for Cryptologic Research, where she served on the Board of Directors, and a senior member of the IEEE.

Susanne Ruschka-Taylor
IBM Global Business Services, 120 Bloor Street East, Suite 104, Toronto ON M4W 1B7, Canada (sruschka@us.ibm.com). Ms. Ruschka-Taylor holds an internal executive role as partner-Americas internal controls, IBM Business Consulting Services,

where she has operational responsibility for all financial, operational, and compliance internal controls for IBM Global Business Services operations in the United States, Canada, and Latin America. She was recently global leader for business risk management in IBM Global Business Services, responsible for strategy and execution. Before joining IBM as part of the PricewaterhouseCoopers Consulting acquisition, she was a partner in the consulting group of PricewaterhouseCoopers. Ms. Ruschka-Taylor is a chartered accountant and has a B.S. degree with high distinction from the University of Toronto. ■