Addressing the data aspects of compliance with industry models

M. Delbaere
R. Ferreira

A fundamental aspect of compliance involves the capability to produce business reports which constitute adequate audit and control records. This presents two significant challenges. Very often, international and government regulators do not coordinate their policies, creating a great deal of overhead for the implementing organizations, particularly those represented in multiple geographical areas. In addition, the information required to produce these reports may be in inconsistent formats throughout the enterprise or unavailable at the right level of detail. To overcome these challenges, organizations need to develop an enterprise-wide data architecture that enables the consolidation of regulatory reporting requirements and the integration of data from different business areas. The definition of data standards and the use of common data-modeling techniques throughout the enterprise can assist in this effort. IBM has developed a series of industry models that address these challenges based on the principles of data warehousing and business intelligence. This paper describes in detail the technical and business challenges of information management in the context of compliance and presents a few practical examples of how customers in the financial services industry have addressed compliance requirements such as Basel II and Solvency II by using enterprise-wide information management approaches based on industry models and related technology.

INTRODUCTION

This paper focuses on one specific aspect of compliance: that is, the ability to support regulatory reporting requirements. We begin by discussing the different compliance drivers—in particular in the context of the financial services industry—and their consequences on IT (information technology) requirements. Some aspects are applicable to other industries as well; for example, the Sarbanes-Oxley Act applies to public companies in general.

We then focus on two specific issues: the inconsistency between different regulatory requirements and the integrity of data within the enterprise. We

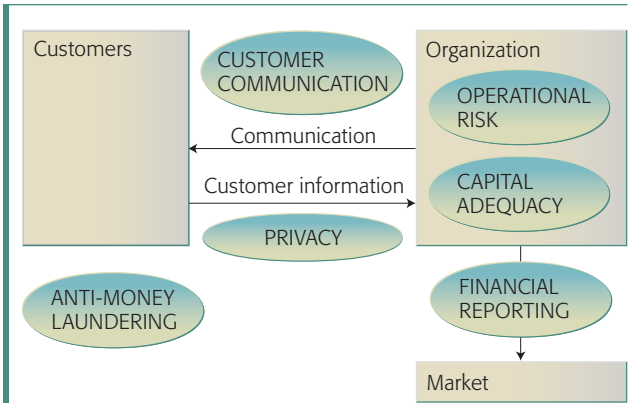


Figure 1
Types of compliance issues in the financial services industry

propose an approach to addressing these issues which involves adopting an enterprise-wide data architecture, including corporate data standards based on industry models. We also examine some of the organizational aspects of governing such a program, such as strategic positioning, appropriate funding, decision processes, and technology.

Business context: types of compliance issues

In the financial services industry, current regulations and industry standards can be categorized by the types of compliance issues they address.[1] As shown in *Figure 1*, these six types are related to privacy, financial reporting, operational risk, capital adequacy, customer communication, and anti-money laundering.

From a customer perspective, privacy refers to the appropriate protection of customer data, in particular, limiting access to the data to authorized personnel and nondivulgence of customer data to unauthorized third parties. Anti-money laundering[2] (AML) is concerned with the monitoring of suspicious customer activity, which may be linked to crime, terrorism, and other illegal activity. Customer communication controls ensure that information provided to customers (in particular on the products and services of the company) contains no misleading information.

Compliance in financial reporting ensures that companies publish financial data which is comparable in quality to that of their competitors. Compliance in operational risk relates mostly to the control of internal processes, people, and systems[3] and to the disclosure of new and different aspects of a business. Finally, capital adequacy compliance ensures that financial services institutions have enough capital to support their overall risk exposure.

Table 1 describes how the most important regulations relate to these six types of compliance issues.[1] The motivation for these compliance regulations is to improve the level of customer protection (privacy, customer communication, and capital adequacy), to fight against crime (AML) and to enhance transparency, to allow better peer comparisons, to promote efficient cross-border investment and access to capital, and to facilitate merger and acquisition transactions (financial reporting and operational risk).

Impact of compliance requirements on IT

The impact of compliance requirements on IT is similar for all regulations of a specific type. There are individual differences, but these are not very significant from a technological point of view. The impact on IT can be categorized in four main areas[4]: (1) data and network security, (2) data and information integrity, (3) policies, procedures, and processes, and (4) record retention and accessibility. The correspondence between the types of compliance issues and these four IT areas is described in *Table 2*.

Data and network security

This involves verifying that there is no internal or external tampering with corporate data sources or applications.[5] The goal from a compliance point of view is to ensure that financial and risk information is accurate and that there is no fraud.

Data and information integrity

Data integrity involves maintaining the quality of information throughout the enterprise so that regulatory reporting is accurate and reliable. *Information integrity* is defined by how effectively data supports the transactions and decisions needed to meet an organization's strategic objectives, as embodied in its ability to manage its assets and conduct its core operations. Information integrity can be measured across multiple dimensions, each of which is used to gauge how well a data element meets a company's information integrity goals, and ultimately, its information needs.

Table 1 Correspondence of type of regulation with major compliance regulations

Compliance Issue Types	Examples of Corresponding Regulations
Privacy	• Gramm-Leach-Bliley Act (United States) • Insurance Conduct of Business Rules (Europe) • Anti Money Laundering Directive (United States) • Proceeds of Crime Act (United Kingdom)
AML	• Patriot Act (United States) • Anti Money Laundering Directive (United States) • Proceeds of Crime Act (United Kingdom)
Customer communication	• Insurance Mediation Directive (Europe) • Gramm-Leach-Biley Act (United States)
Financial reporting	• Sarbanes-Oxley Act (United States) • International Financial Reporting Standards incorporating the International Accounting Standards (IFRS/IAS) • Financial Services Authority Prudential Source Book (United Kingdom)
Capital adequacy	• Basel II (International) • IFRS/IAS • Solvency II (European Union)
Operational risk	• Basel II • IFRS/IAS • Solvency II

Policies, procedures, and processes

This area incorporates compliance into IT tasks and deals with the documentation of processes, authorizations, and controls as they change. The compliance goal is to ensure that the appropriate procedures are effectively followed within the organization.

Record retention and accessibility

This involves keeping evidence sufficiently long to enable record cross-checking in case of conflicts and also ensuring that only authorized personnel have access to confidential information (in particular customer information in the context of privacy). Evolving regulations require compliance with a staggering variety of retention periods, storage methods, and other specifics corresponding to the many types of company records generated in the course of doing business.[6,7] This paper focuses on the aspect of compliance related to data integrity.

Inconsistency in regulatory requirements

With the proliferation of regulatory, legislative, and corporate requirements established each year (as shown in *Table 3*), the task of managing compliance throughout an organization has become a consid-

Table 2 Impact of compliance on IT

	Data and Network Security	Data and Information Integrity	Policies, Procedures, and Processes	Record Retention and Accessibility
Privacy	X	X		X
AML		X		X
Customer communication		X	X	X
Financial reporting	X	X	X	X
Capital adequacy	X	X	X	
Operational risk	X		X	X

Table 3 Examples of compliance with industry mandates and government legislation

Regulation	Country	Publication Date
IFRS/IAS	International (United States not covered)	1973–2006
Federal Deposit Insurance Corporation Improvement Act (FDICIA)	United States	1991
Health Insurance Portability and Accountability Act (HIPAA)	United States	1996
Financial Services Action Plan (FSAP)	European Union	1999
Gramm-Leach-Bliley Act (GLBA)	United States	1999
Sarbanes-Oxley Act (SOX)	United States	2002
Basel II	International	2004
ISO 17799	International	2005
Markets in Financial Instruments Directive (MiFID)	European Union	2006
Solvency II	European Union	2007

erable challenge. Multinational organizations have to support a large number of compliance requirements from different countries or international bodies. These requirements may overlap and even conflict with each other.

Various working groups are doing significant work to reconcile regulatory overlap and to improve compliance efficiency by minimizing redundancy.[8] For example, as a result of regulatory overlap between the existing requirements of the regulations of FDICIA (Federal Deposit Insurance Corporation Improvement Act), GLBA (Gramm-Leach-Bliley Act), Sarbanes-Oxley Act, and the proposed Basel II—Advanced Measurements Approach (AMA) for operational risk, large United States banking organizations must establish overlapping internal-control reporting and compliance structures and specific operational-risk data collection, validation processes, and IT systems requirements.

Another challenge involves the increasing convergence between International Financial Reporting Standards (IFRS) for risk and capital-management disclosures and those that will be required by Pillar 3 of Basel II and Solvency II.[9] This convergence is likely to open financial services organizations to greater market scrutiny. Consistency between the different disclosures is therefore imperative. Risk management, regulatory and financial reporting, and investor relations teams need to work together to optimize the synergies between IFRS and Basel II and Solvency II.

As far as reporting is concerned, inconsistencies can arise because the regulators defining the various compliance requirements can standardize on different vocabularies and request information at different levels of granularity. Moreover, each of these individual regulations can evolve, sometimes going through vastly different versions. The authors estimate that there is roughly a 10 percent difference between the IFRS published version of January 2005 and that of May 2005, for example. There is no synchronization between the release schedules of different publishing regulatory organizations. Furthermore, some regulations are imprecise, requiring a great deal of interpretation. Recent research studies on the implementation of IFRS has revealed that extensive judgment had to be exercised in the selection and application of IFRS accounting treatments. This reduces the consistency and comparability of these implementations, and organizations do not seem confident that IFRS financial information is sufficient, or in some cases entirely appropriate, for the purpose of communicating their performance to the markets (see Reference 10, for example.)

Finally, there is a fine line between self-motivated best practices (also known as nonregulatory re-

quirements) and externally imposed regulatory constraint. With nonregulatory requirements, the organization can decide unilaterally to change its own reporting requirements as long as they still perform the same informational function. In other words, there can be a trade-off between the business value of the information and the difficulty to obtain it. In the case of regulatory reporting, this trade-off does not exist—the information must be reported regardless of the difficulty in obtaining it.

STRATEGIC APPROACH TO COMPLIANCE

According to a research study on optimized Enterprise Risk Management[11] (ERM), the response of businesses to risk evolves along a "risk and compliance maturity continuum." They start with a strategy of penalty avoidance, mostly effected through manual auditing and control procedures on top of existing processes. This is known as the "comply" stage. Due to a number of factors, including urgency of compliance deadlines and lack of systems capabilities, this stage typically contributes to additional overhead costs, is time consuming, and is not integrated into the overall daily operations of the business.

In most organizations, compliance projects are very fragmented, with activities embedded in individual business units. Funding is approved on a case-by-case basis, with little cost/benefit analysis and no strategic oversight of the total compliance process. Because projects are not coordinated, governance is diluted, and there is considerable potential for overlap and duplication of effort. The lack of a strategic focus means that few organizations have adopted suitable IT systems to readily measure, monitor, and report on compliance on an enterprise-wide basis. At best, the "comply" stage can help businesses react and accurately report on financial performance and risks after the fact.

Due to the increased emphasis by regulators on the implementation of ERM frameworks (e.g., COSO [Committee of Sponsoring Organizations of the Treadway Commission], Basel II, and Solvency II), where compliance is seen as part of risk management, organizations must evolve along the risk and compliance maturity continuum, from the "comply" stage though the "improve" stage to the "transform" stage. In this context, compliance cannot be seen as an end in itself, distinct from business strategy. When planning their approach to compliance, organizations should take advantage of compliance projects to support their strategic direction and improve business efficiency. Compliance projects are no different from any other major capital expenditure project, requiring an initial effort to conduct scoping studies, impact analysis, and cost/benefit analysis.

Leading financial services organizations have implemented an enterprise-wide risk management framework that gives them a holistic view of risk and compliance and enables them to more readily assess how a particular regulation affects their company. For example, by refining their understanding of operational risk, they can better assess and measure the risks of activities throughout their organization. The resulting improvement in the transparency of risk and compliance means that these organizations are able to make decisions about allocating capital that are more closely linked to the level of risk, which can, in turn, lead to a lower cost of capital.

For leading organizations, compliance can constitute an opportunity for business and IT transformation rather than a nuisance. In order to realize the benefits offered by this opportunity, compliance needs to be addressed strategically in a well-designed way. The next section aims at applying these principles to regulatory reporting.

Strategically addressing regulatory reporting requirements

In the preceding discussion, we outlined two types of data consistency problems: the inconsistency between different regulation reporting needs (inconsistency in regulatory requirements) and the inconsistency between source systems (data and information integrity). These are represented conceptually in *Figure 2*.

Adapting to inconsistency in regulatory requirements

The combination of variability, lack of coordination, and the moving boundaries of different regulations forces organizations to build regulatory compliance implementations in a particularly extensible way. This is similar to the situation that pertains in most modern application software development, but it is even more of a necessity in the compliance arena.

Although there are many inconsistencies between the different regulations and management reporting

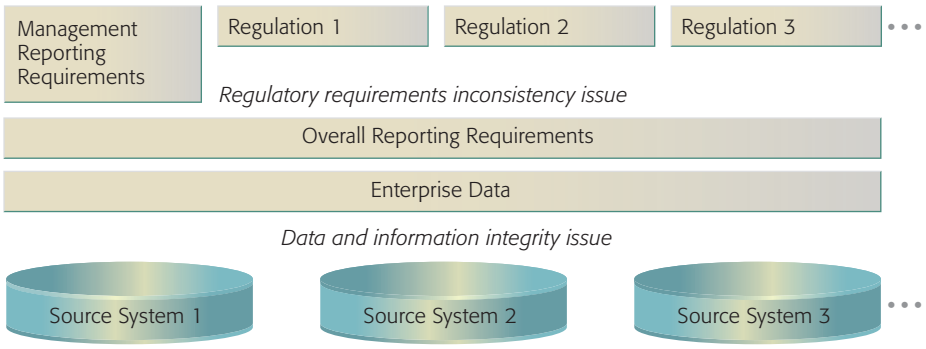


Figure 2
Addressing reporting requirements strategically (conceptual view)

needs, there are also many commonalities in terms of business definitions and specific measures. Any requirement that is identified as common only needs to be supported once, which means less effort is involved in data extraction and transformation from source systems. This leads to the first imperative in dealing strategically with regulatory reporting: defining a consistent overall set of reporting requirements. In order to accomplish this task, one has to define a taxonomy that covers the entirety of the reporting requirements. It consists of defining all measures (i.e., lines in the reports) as well as their decomposition into submeasures, all the way down to the definition of atomic data and the dimensions (i.e., the categories of information) for data aggregation.

Ensuring data integrity

In order to accomplish all the activities required for successful compliance, organizations need data that is accurate and aggregated enterprise-wide. In practice, however, data is maintained in different source systems, which may have slightly (or even radically) different data formats. In order to reconcile this data with a minimum of errors, data management systems must be integrated and must facilitate automated collection and consolidation of data.

The tactical approach to address this problem is to implement a series of mini-warehouses or datamarts, each specialized in the data required for a single business reporting function. Although this can be a successful approach, it increases the number of interfaces and, most important, introduces the need to reconcile data with different granularity across datamarts. Sophisticated business intelligence tools can help to synchronize data and prevent erroneous information from entering the database, but the delivery of consistent, reliable, and timely financial and risk reports is still a very complex process.

A more strategic approach consists in defining standard data models and building an enterprise-wide consistent view of enterprise data. Implementing enterprise-wide data standards is not simple though, as organizational challenges add to the already complex technical issues. The organizational impacts of enterprise-wide data strategies are examined in the section "Organizational aspects."

Table 4 summarizes the common issues faced by organizations in the area of data quality and data aggregation and shows what leading organizations are doing to successfully implement enterprise-wide compliance and risk management solutions.[12]

The importance of dealing with data strategically by defining enterprise data models is well recognized in the IT and business worlds. In the financial services industry, a research study[13] has indicated that 90 percent of the participants believe that enterprise models are a strategic asset for the organization and 55 percent have already implemented or are implementing enterprise models. Businesses that are structured around an enterprise model of their business are better positioned for change and innovation. They can treat data as a strategic enterprise asset on its own,[14] design business

Table 4 Maturity levels of enterprise data management

	Base Level	Median	Best Practice
Data Quality	Low and incomplete, no standards	Medium, questionable consistency and reliability	Enterprise-wide data
Aggregation	Manual extraction, manual entry, no protection of data sources	Some integration and some data warehouses	Comprehensive data warehouse
Timelines of Information	Daily (batch processes)	Ad hoc basis, availability in 2 hours for emergencies	Near real time

processes aligned to business objectives, and more easily analyze the impact of change.

Once the importance of enterprise data models is established, the challenge is to assess what enterprise data models need to be built and for which purpose. Data models can be built at different semantic levels with proper separation of concerns. A distinction can be made between analysis models and logical and physical design models. *Analysis models* are typically used as mechanisms for communication about the domain, whereas *design models* describe the logical and physical structure of the actual databases. These different semantic levels can be linked to each other through traceability links. Model transformations between different semantic levels can typically be realized by a combination of manual transformations and the application of model transformation patterns.

At all levels, enterprise models must be generic and flexible. Generic models allow the identification of recurring patterns that help in understanding and designing more effective and resilient systems. Flexible models are needed to handle the many different business scenarios that can occur in an organization or industry.

Analysis data models are typically easier to manage by a wide variety of entities, including business and IT resources. Although some organizations consider them as overhead, others see them as the cornerstone of their enterprise data architecture and use them extensively to communicate the business view of enterprise data.

Whichever decision is made for the selection of models to deploy enterprise-wide, the creation of these models from scratch can be very difficult, as their creation requires a great deal of consensus. One way of addressing this particular issue is to start from existing industry models and frameworks and to customize them for the specific needs of the enterprise. The next section describes existing industry models from IBM.

IBM's industry models

While industry models take many forms, this section focuses mainly on the industry models defined by IBM in partnership with insurance companies and banks over the last 15 years[15–17]: the Insurance Application Architecture (IAA) and the Information Framework (IFW) respectively. This family of models has been extended more recently to other industries, such as telecommunications and retail; further development is under way for the financial-services and health-care industries.

These models provide structured business content, addressing both the business-architecture and the application-architecture levels. They consist of a set of models linked together through traceability and addressing data from the conceptual level to physical levels, functions, processes, services, components, and multidimensional informational analysis.

Data warehouse models, such as the Insurance Information Warehouse (IIW) or the Banking Data Warehouse (BDW) are relevant subsets of these models. They focus on business content and how that content can effectively be stored in an efficiently designed data warehouse. As such, they are mostly technology-agnostic and do not address concerns such as Extract-Transform-Load (ETL) methodology. The components of the warehouse models are discussed in the following subsections.

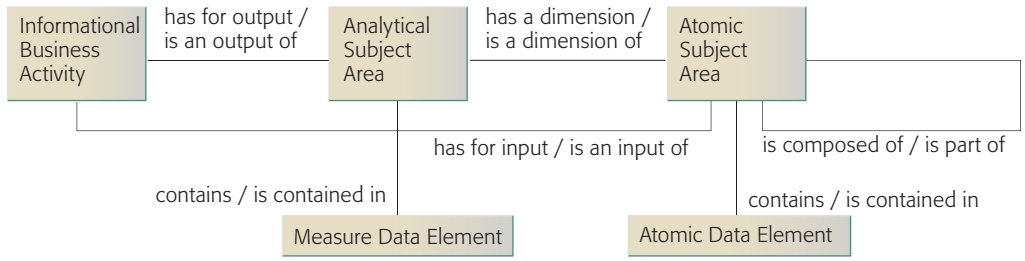


Figure 3
BST metamodel

Business solution templates

Business solution templates (BSTs) are sets of analytical requirements of a specified scope. It is in this format that the different regulatory reporting requirements are expressed. Their structure is shown in the metamodel of ***Figure 3***. The metamodel consists of several metaconstructs: an *informational business activity* realizes an informational business objective, such as responding to the analytical queries of business users or delivering information to decision makers; an *analytical subject area* is a high-level grouping of business information needed and used by the enterprise to express business measures along multiple axes of analysis; a *measure data element* is a formula that derives required business information. It is used by information analysts in their queries to measure the performance or behavior of the business; an *atomic subject area* is a grouping of business information needed and used by the enterprise to qualify business measures; and an *atomic data element* is an elementary piece of business information known by the business. It is used by information analysts to interpret the business measures they work with.

Business model

The business model provides an implementation-independent view of the business. Its main purpose is to serve as a communication mechanism between business professionals and IT professionals and to provide a formalized view of the business to be used as a reference at any time in the life cycle of a development project.

Such models can optionally be represented in ER (Entity-Relationship) notation. IBM's industry models provide two representations of the business model: one in ER notation and a semantically equivalent model in UML**.[18]

Data warehouse model

The data warehouse model is an enterprise-wide ER model designed for data warehousing. Its objective is to provide an enterprise-wide, generic, and flexible data structure whose content serves as an overall design reference point for developing the informational environment of the enterprise (e.g., data warehouses and datamarts). It represents the information of the data warehouse in its two distinct aspects: core atomic data with full history and multidimensional data structures with facts and dimensions. It transforms the business information modeled within the business model into a logical data model that can be physically implemented and takes into account physical-access and performance constraints. It also transforms the analytical requirements expressed within the BSTs into appropriate data structures, such as multi-dimensional models, profile entities, and helper entities. It is meant to serve as the unique, most granular point of consistency and consolidation between all the informational data stores, such as datamarts or flat files for data mining.

Industry models, standards, and regulatory reporting

The industry models are not meant to be used as they are but rather to be customized to reflect the precise needs of each company that uses them. This means that each company will have its own customized version of the industry models. The models' architecture and structure are specially geared towards this usage and allow the users to easily extend the model, enabling them to represent areas of their business that are unique to them and thus derive competitive advantages. In addition, industry extensions, jurisdiction-specific extensions, and company-specific extensions can be easily

incorporated into the models, as the base structures are already in place.

Although industry models could become de facto standards in many markets, their purpose is not to standardize at the level of an entire industry but to provide the basis for defining corporate standards. From a regulatory-reporting point of view, one has to adhere entirely to the definitions described in the legislation, but the internal representation of data and data aggregation is open, resulting in individual corporate standards.

As stated previously, there is little coordination between the different regulatory bodies, and each set of reporting requirements tends to be disconnected from other sets. Each set of requirements essentially forms its own standard and can be documented using a format such as XBRL (eXtensible Business Reporting Language), an emerging XML-based data interchange standard, aiming at improving the quality and value of reported information.[19,20]

From the perspective of industry models, the different regulatory requirements are expressed formally as BSTs and are integrated in the overall information architecture based on a customization of the other models.

PRACTICAL EXAMPLES

This section gives some examples of how the issues of inconsistency in regulatory requirements and data integrity can be concretely addressed.

Example 1: Addressing regulatory inconsistency

We start by illustrating the representation of a requirement in the form of a BST, as described previously. In this example, we use a BST related to compliance with the Sarbanes-Oxley Act. *Table 5* shows the structure of a BST.

One of the measures included in this BST is that of deposits, depicted in detail in *Figure 4*. This measure is decomposed into three other measures represented by A (customer deposits), B (official checks issued), and C (Vostro accounts, i.e., accounts held by a bank as a correspondent on behalf of an overseas bank). Total deposits are the sum of these three measures.

Figure 4 shows that the measure deposits, in addition to three different Sarbanes-Oxley related analyses, are also reused for reporting purposes in the context of compliance with International Accounting Standards (IAS).

Table 5 Structure of a BST

Business Identifier: ASB0174
Name: Balance Sheet Classified Approach Analysis
Definition: Analyzes a financial institution balance sheet that reports the financial institution's assets, liabilities, and net worth at a specific time. The classified approach is used for the associated measures and dimensions.
Example: Reference to Association of Chartered Certified Accountants (ACCA)
Dimensions: • Financial institution group reporting structure • Line of business • Measurement currency • Reporting currency • Organization unit • Scenario • Time
Measures: (incomplete selective list of measures) • Assets classified • Current assets • Accounts receivable • Common stock repurchased • Funds sold • Investment securities • Current liabilities • Deferred income • Deposits • . . .

This example demonstrates the importance of consistently handling measures across different compliance issues (Sarbanes-Oxley and IFRS/IAS). It also demonstrates the importance of properly handling the decomposition of measures, so that a company can report independently on each of the submeasures (A, B, and C), and easily reuse these submeasures in different reporting contexts.

Example 2: Addressing data integrity

In this example, business users from different departments in an organization have defined the following reporting requirements: claims ratio per product and total losses on policies underwritten (underwriting department), yearly claims per product (claims management department), and claims paid in reference period (compliance department, as required for reporting on solvency margins).

At first glance, these could be seen as different measures. However, they can all be represented by

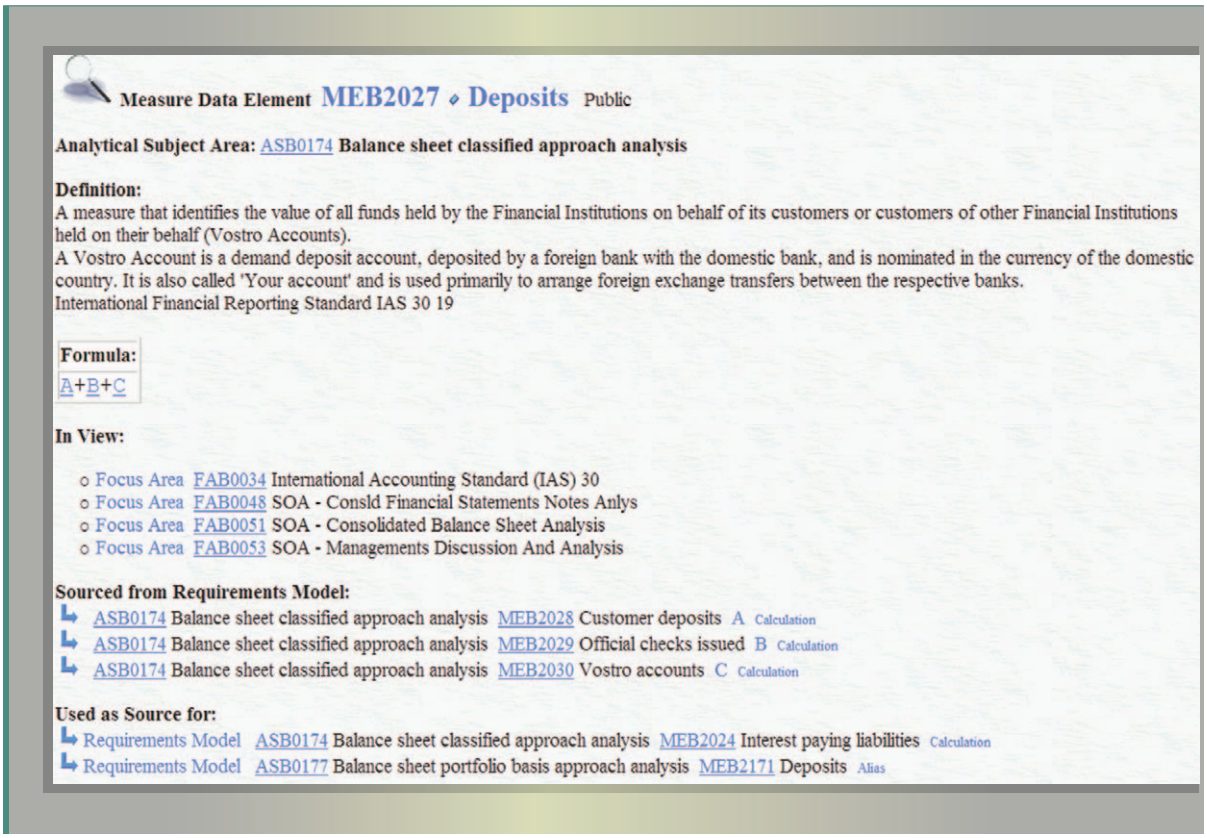


Figure 4
Representation of a measure with a BST

(and mapped to) the same enterprise-wide measure, namely "claimed amount," as shown in ***Figure 5***. In the non-life-insurance (i.e., property and casualty insurance) context, claimed amount represents the amount of money paid for claims incurred in a given time period.

Claimed amount is used in a consistent manner across the enterprise to report on total losses on policies underwritten, but can also be reused to report on the claims ratio per product, yearly claims per product, and claims paid in reference period (for reporting on solvency margin). This provides the right metadata foundation to address data integrity.

In a data-warehousing environment, measures are called facts. Facts are analytical measures that are typically numeric. They are the result of calculations performed on a database and are the focus of analysis. Facts are semantically dynamic; the values they return depend on the dimensions with which they are used. Facts are generally grouped in fact tables that share common dimensions of analysis. Facts that are defined and used consistently across functional areas of the organization, such as claimed amount, are called *conformed facts*.[21]

In the enterprise data model, claimed amount is derived from the amount attribute in the claim offer entity for claims with the status of "requested." This derivation is done in a unique way and does not need to be redone. In practice, this implies that the process used to calculate the claimed amount by extracting the data from the source systems and transforming and loading it into the data warehouse ensures consistency of data throughout the organization.

To ensure consistent business reporting across functional areas of the organization, it is also critical to identify and consistently define the axes of analysis or dimensions to which each department in the organization conforms, also known as the *conformed dimensions*.[21] Dimensions are used to

Figure 5
Representation of claimed amount measure as a fact in the Loss Event Fact Table

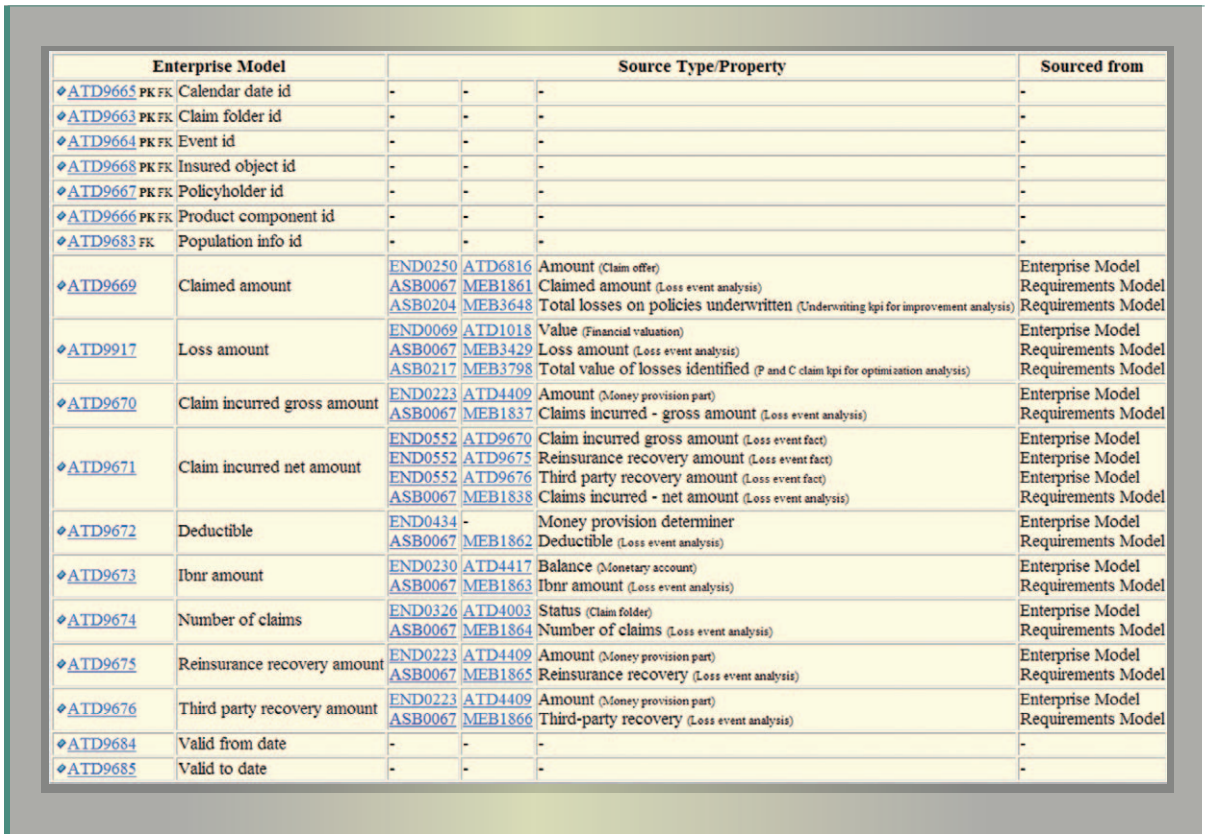
specify the perspectives and level of detail for analysis of facts. They can also be used to restrict the scope of analysis. Dimensions are often organized into aggregation hierarchies to facilitate analysis at different levels of detail. Typical examples of conformed dimensions include time, customer, product, and location. In *Figure 6*, the Loss Event Fact Table records measures that are fully identified by a set of dimensions—time, product, claim, event, and so on. These measures are defined at the lowest level of granularity (e.g., the product dimension at the insurance product component level).

Conformed dimensions are standardized designs that are reused for all relevant analyses in an organization and are represented by fact tables. They are fundamental to the functioning of a data warehouse as an integrated whole. Their use has many advantages. A single dimension table can be used with multiple fact tables in the same database space; this reduces data volumes and database administration. ETL routines can be reused in cases where multiple copies of a conformed dimension are maintained in a distributed architecture. "Drilling" across fact tables (i.e., data analysis across dimensions) is facilitated. User interfaces and data content are consistent whenever the dimension is used; this simplifies development and accelerates the learning cycle for end users. Conformed dimensions support incremental development of the enterprise-wide data warehouse.

In our example, we are interested in reporting on the claim ratio per product from an underwriting perspective and on the claims paid in a reference period from a solvency compliance perspective. To obtain consistent results, these measures conform to the same product dimension and time dimension, so that the time period used in the calculation of the claim ratio per product is the same as the one used in the calculation of the claims paid in the reference period.

ORGANIZATIONAL ASPECTS

The approach recommended in this paper relies heavily on an enterprise-wide approach to data and as such requires crossing organizational boundaries. This means that organizational aspects need to be



Enterprise Model		Source Type/Property			Sourced from
ATD9665 PK FK	Calendar date id	-	-	-	-
ATD9663 PK FK	Claim folder id	-	-	-	-
ATD9664 PK FK	Event id	-	-	-	-
ATD9668 PK FK	Insured object id	-	-	-	-
ATD9667 PK FK	Policyholder id	-	-	-	-
ATD9666 PK FK	Product component id	-	-	-	-
ATD9683 FK	Population info id	-	-	-	-
ATD9669	Claimed amount	END0250 ASB0067 ASB0204	ATD6816 MEB1861 MEB3648	Amount (Claim offer) Claimed amount (Loss event analysis) Total losses on policies underwritten (Underwriting kpi for improvement analysis)	Enterprise Model Requirements Model Requirements Model
ATD9917	Loss amount	END0069 ASB0067 ASB0217	ATD1018 MEB3429 MEB3798	Value (Financial valuation) Loss amount (Loss event analysis) Total value of losses identified (P and C claim kpi for optimization analysis)	Enterprise Model Requirements Model Requirements Model
ATD9670	Claim incurred gross amount	END0223 ASB0067	ATD4409 MEB1837	Amount (Money provision part) Claims incurred - gross amount (Loss event analysis)	Enterprise Model Requirements Model
ATD9671	Claim incurred net amount	END0552 END0552 END0552 ASB0067	ATD9670 ATD9675 ATD9676 MEB1838	Claim incurred gross amount (Loss event fact) Reinsurance recovery amount (Loss event fact) Third party recovery amount (Loss event fact) Claims incurred - net amount (Loss event analysis)	Enterprise Model Enterprise Model Enterprise Model Requirements Model
ATD9672	Deductible	END0434 ASB0067	- MEB1862	Money provision determiner Deductible (Loss event analysis)	Enterprise Model Requirements Model
ATD9673	Ibnr amount	END0230 ASB0067	ATD4417 MEB1863	Balance (Monetary account) Ibnr amount (Loss event analysis)	Enterprise Model Requirements Model
ATD9674	Number of claims	END0326 ASB0067	ATD4003 MEB1864	Status (Claim folder) Number of claims (Loss event analysis)	Enterprise Model Requirements Model
ATD9675	Reinsurance recovery amount	END0223 ASB0067	ATD4409 MEB1865	Amount (Money provision part) Reinsurance recovery (Loss event analysis)	Enterprise Model Requirements Model
ATD9676	Third party recovery amount	END0223 ASB0067	ATD4409 MEB1866	Amount (Money provision part) Third-party recovery (Loss event analysis)	Enterprise Model Requirements Model
ATD9684	Valid from date	-	-	-	-
ATD9685	Valid to date	-	-	-	-

Figure 6
Detailed dimensional model representation of Loss Event Fact Table in the enterprise data model

carefully examined, as they will have a decisive impact on the success or failure of projects implemented with this approach. This can be put in perspective with other initiatives embracing an enterprise-wide approach, such as the deployment of common enterprise processes or of service-oriented architectures.[22] For the purposes of this paper, the organizational aspects are usually considered together as part of data governance initiatives.

The authors have been personally involved in many corporate programs with different levels of success. They agree with the high-level framework outlined by Griffin[23] that describes four critical success factors: the recognition of data governance as a strategic responsibility at the corporate level, appropriate and ongoing funding, a transparent decision process, and efficient technology. The following subsections elaborate on these four dimensions by presenting some of the literature and the authors' experience in the matter.

Data governance as a strategic corporate function

Managing data governance starts with the assignment of a dedicated team. The organizational positioning of this team varies from company to company, but in most cases it is an architectural responsbility within the IT organization. Functionally, the responsibilities of this group span the business and IT organizations, and some companies even establish this scope as part of their organizational structure.

Some authors[24] have gone so far as to promote all of enterprise architecture (and not just data governance) as a strategic department under the direct responsibility of the CFO or CIO, as exemplified in Reference 24: "Forward-looking companies are coming to realize that enterprise architecture is a strategically important capability that requires its own funding, line of control, and business metrics—in other words, enterprise architecture can be a separate line of business in its own right. As such, it

makes no sense to separate this capability without giving the architecture group its own budget."

The majority of the team should consist of data modelers or data stewards, but a large part of the responsibilities of the team also involves driving the deployment of the standards and making sure that they are properly understood and used within the corporation. The team can only be strategically successful with the appropriate level of sponsorship within the organization. The sponsorship can come from either the business or the IT side of the organization; in the most successful programs, it comes from a combination of the two.

Funding aspects

Higgins[25] makes the point that compliance can be self-funded through the derived benefits in software quality and control. However, the benefits that he highlights are typically hard to quantify for a business case and as such will not be taken into consideration in any funding mechanism.

In essence, by proposing to deploy an enterprise data architecture to support informational regulatory requirements, one finds oneself in the classical position of having to justify enterprise architecture efforts. The individual projects cannot justify the cost associated with the architectural and infrastructural elements. For business executives, it is not always obvious that their business can benefit from adopting an architectural approach as "architecture efforts ... typically don't have any features."[24] If the company recognizes the importance of compliance as a corporate program, there should be associated funding that can support the initial costs of the projects. For the most successful companies, this is managed as a business capability and not just as an IT issue. The funding issues are not limited to the initial investment but need to extend to maintenance of the shared elements as well.

When enterprise initiatives can be connected directly to business objectives, in particular to measurable business objectives, it becomes much easier to create business cases. We are starting to get ROI (return on investment) feedback from companies having used a strategic approach to regulatory compliance, and their results are quite impressive, with figures of over 100 percent being quoted.[26]

In the case of compliance, it is undeniable that the capability has to be implemented, as this is a legal requirement. The way in which this capability is actually implemented and its impact on cost (both initially and on an ongoing basis) are left open for the organization to decide. It is important to realize that regulatory compliance constitutes an opportunity to fund strategic architecture and to move from the "comply" state to the "transform" state of maturity.

In Reference 27, Weill and Ross describe a system of "dividends" to fund the initial investment. This is a combination of two mechanisms: a corporate investment fund for projects assessed by the CEO to have significant enterprise reuse potential and an investment recovery mechanism when the infrastructure is reused by other projects.

The authors recognize this as a growing field of experimentation that goes well beyond the scope of this paper. More and more complex funding structures will emerge as enterprise initiatives continue to grow in importance. An untested idea, for example, would be a system of fines. In order to take into consideration future maintenance costs while maintaining some level of autonomy in the individual projects, an initiative that would favor reinvention instead of reuse would have to bear the extra funding cost of a fine. This would leave open more possibilities for innovative development while recognizing the cost for the corporation of nonstandard elements. Of course, balancing the objectives of standardization and innovation will continue to provide challenges.

Many organizations are not entirely clear that reuse is actually the combination of two different elements: the creation of reusable assets and the actual usage of those assets beyond the scope of the original project. Efficient funding mechanisms that encourage enterprise development need to relate to both of these elements.

In international groups, the issue of funding is even more complex, as every country's development group may be waiting for the others to bear the initial investment cost. The ideal way to resolve such stalemates is to allocate funding above the individual project level, in this case through international architecture initiatives.

In summary, one can argue that regulatory compliance is similar in nature to Customer Relationship

Management (CRM) and Enterprise Resource Planning (ERP) investments in that it requires an enterprise approach to funding and as such could justify central allocation of enterprise investment of a similar magnitude. Although it is always possible to implement informational regulatory requirements through tactical means, they represent a significant opportunity to pursue the architectural agenda.

Transparent decision processes and accountability

Once the organization is properly set up and the funding is secured, it is necessary to put a clear governance process into place. Conformity to data standards needs to be properly enforced, and the group in charge of data standards should have the authority to decide on the introduction of new data elements.

An example of a successful deployment of data standards in a financial services organization with which the authors have been heavily involved was based on the principles described in the following.

The data standards organization had the final word on the introduction of any data or metadata element within the enterprise. This data standards organization was led by a high-level executive (chief knowledge officer) and included representatives of both the IT and the business organizations.

A business data model was used as the basis for documenting data standards. Of course, the organization was also managing data standards at the design level, but the business model was the actual base checkpoint. Any new data element had to be formally justified and approved. The organization was geared to provide quick response time (no more than a few days). As soon as new data elements were approved, they were published as part of the enterprise conceptual model. New allowed values for enumerated types also had to be formally justified, through a simpler process.

Such a process is still relatively rare today, and the most general case is still one involving a posteriori reconciliation. In that case, every group defines its own set of informational requirements and the required extensions to the base model, and this is reconciled afterwards though mapping to the common representation of data.

The process that is put in place needs to clearly identify the dependencies among the different groups. Service Level Agreements need to be very effectively documented so that development plans can be properly put into place. If at any time the common pieces appear to be causing unacceptable delays or lack of reliability, the entire program will be put in question very quickly, which can undermine years of efforts of promoting the right enterprise architecture approach.

Effective technology

The final component of an efficient data governance program is the usage of effective technology. The goal of this section is not to provide an exhaustive description of available technology but to describe the major requirements without entering into specific product considerations. These requirements have been captured through industry model user groups and advisory sessions, such as the IAA Steering Committee.[28]

First, the enterprise data models have to be maintained and published. They are developed in an ER modeling tool and are typically published within the enterprise through HTML pages published on the company intranet. HTML pages provide a lightweight publication mechanism and a good way of publishing traceability between different semantic models. The published information includes (for the most advanced companies) the ownership of the definitions and their mapping to the analytical requirements.

The models need to be properly versioned, and this can be performed using any version control tool. They need to be kept in alignment across semantic levels, and this is done through traceability and model transformation technology. The reconciliation of project-level with enterprise-level models is also an important consideration.

The mapping to core systems can be done in metadata repositories, but these tend to focus only on deployed databases and do not normally include reconciliation to the level of requirements, although some level of alignment between the modeling domain and the runtime metadata domain is starting to happen.

Data-quality and data-stewardship tools ensure that data which comes into the system is complete, standard, and consistent and support performance

indicators that measure data quality, both at a given instant and over time. Part of data stewardship is also classification; that is, specifying which data is important from a compliance perspective. This classification indicates what other sorts of control need to be applied. Additionally, tooling should include tools that examine the data for anomalies (and report on them), tools that secure the data from being accessed improperly, and tools for auditing and reporting. Finally, the implementation of the decision process, including, for example, the workflow for authorizations, is typically developed as a custom application or is based on the overall change management framework.

CONCLUSION

This paper has focused on one specific aspect of compliance, the ability to support specific reporting requirements through an integrated information architecture. We have examined two key issues—inconsistency in regulatory requirements and data integrity—and have recognized the need for building an enterprise information architecture to support those dynamic requirements.

The approach presented here can provide a way to consolidate regulatory reporting requirements, which by defining common measures decreases the overall quantity of data manipulation required. It can also define a convergence format for the integration of data from different disconnected source systems. Unfortunately, defining appropriate enterprise data standards, although an absolute necessity, can also be a daunting task. Reducing the complexity and risk of this task can be achieved by starting from industry-level frameworks such as IBM's industry models.

Finally, we have defined the need to treat compliance as a strategic corporate function and to properly incorporate it into the organizational structure through the definition of clear mandates, budgets, and accountability. Regulatory reporting needs to be seen as a key opportunity to invest in the development of enterprise information architecture, not only to assist in integrating future compliance requirements more easily, but also to improve overall business and IT agility.

ACKNOWLEDGMENTS

The IBM industry models represent a vast collective effort, and this paper would not have been possible without the hard work of the development team. Special thanks to Christian Palmaerts, Susan Cotter, Neil Ryan, and Pat O' Sullivan for their significant contribution to the support of regulatory compliance in the industry models and to Dan Wolfson and Ivan Milman for their invaluable technical expertise.

CITED REFERENCES

1. C. Chapman, M. Josefowicz, and E. C. Walsh, *Panel Discussion: The Compliance Conundrum*, Insurance Standards Leadership Forum (2004), http://i.cmpnet.com/financetech/download/104-1532004ISLF_Matt_Josefowicz.pdf.
2. *Guidance on a Risk Based Approach for Managing Money Laundering Risks*, The Wolfsberg Group (2006), http://www.wolfsberg-principles.com/risk-based-approach.html.
3. *Internal Ratings-Based Systems for Corporate Credit and Operational Risk Advanced Measurement Approaches for Regulatory Capital*, Federal Register **68**, No. 149, 45949–45988 (August 2003), http://www.fdic.gov/news/news/financial/2003/fil0362b.pdf.
4. M. Josefowicz, *The Virtuous Cycle of Compliance and IT?* Celent Communications Report (2004), http://www.celent.com/PressReleases/20041104/ComplianceIT.htm.
5. R. Graves, "Business Intelligence Tools: The Smart Way to Achieve Compliance," *DM Review Magazine* (December 2005).
6. J. Montaña, J. E. Dietel, and C. Martins, *Sarbanes-Oxley Act: Implications for Records Management*, ARMA International (2003).
7. *IT Control Objectives for Sarbanes Oxley Act—The Role of IT in the Design and Implementation of Internal Control over Financial Reporting, 2nd Edition*, IT Governance Institute (September 2006), http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=12383.
8. *Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in U.S. Financial Institutions*, BITS Operational Risk Management Working Group (2005), http://www.bitsinfo.org/downloads/Publications%20Page/regrecoct05.pdf.
9. *IFRS: A Step Towards Basel II and Solvency II Implementation*, PriceWaterhouseCoopers Report (November 2005).
10. *Observations on the Implementation of IFRS*, Ernst and Young Report (September 2006).
11. C. Abrams, J. von Känel, S. Müller, B. Pfitzmann, and S. Ruschka-Taylor, "Optimized Enterprise Risk Management," *IBM Systems Journal* **46**, No. 2, 219–234 (2007, this issue).
12. C. Petit, *The Clairvoyant CRO: Risk Management That is Insightful, Illuminating and Ingrained Enterprise-Wide*, IBM Corporation (2005), http://www-935.ibm.com/services/us/index.wss/consultantpov/imc/a1013073?cntxt=a1000058.

13. M. Josefowicz, "The CIO Agenda 2006: Laying Foundations for Competitive Advantage," Insurance and Technology Executive Summit (2006); register for paper at http://www.insurancetech.com/events/summit2006/.
14. R. Losey, "Enterprise Data Architecture: Who Needs It?" *DM Review Magazine* (January 2004), http://www.dmreview.com.
15. IBM Insurance Application Architecture, http://www.ibm.com/industries/financialservices/doc/content/solution/278918103.html.
16. M. Delbaere, *IAA White Paper, Insurance Application Architecture (IAA)*, IBM Financial Services Solutions Centre, http://www.baoxian119.com/xiazai/updownload/iaa2002whitepaper.pdf.
17. J. Huschens and M. Rumpold-Preining, "IBM Insurance Application Architecture (IAA)," in *Handbook on Architectures of Information Systems*, 2nd edition, P. Bernus, K. Mertins, and G. Schmidt, Editors, Springer Verlag, Berlin (2006), pp. 669–692.
18. H. Erikson and M. Penker, *Business Modeling with UML: Business Patterns at Work*, John Wiley and Sons, Hoboken, NJ (2001).
19. XBRL International, http://www.xbrl.org.
20. *Improve Regulatory Reporting: Realizing the Benefits of XBRL*, KPMG International Report, Audit and Risk Advisory Services (2004).
21. R. Kimball, *The Data Warehouse Toolkit: The Complete Guide to Dimensional Modelling*, John Wiley and Sons, Hoboken, NJ (1996).
22. N. Bieberstein, S. Bose, L. Walker, and A. Lynch, "Impact of Service-Oriented Architecture on Enterprise Systems, Organizational Structures, and Individuals," *IBM Systems Journal* **44**, No. 4, pp. 691–708 (2005).
23. J. Griffin, "Data Governance, A Strategy for Success," *DM Review Magazine* (June 2005), http://www.dmreview.com.
24. R. Schmelzer, "Funding SOA," *ZapThink* (April 2005), http://www.zapthink.com/report.html?id=ZAPFLASH-200547.
25. J. Higgins, "How To: Self-Funding IT Governance," *Information Week* (April 7, 2005), http://www.informationweek.com/management/compliance/160502237.
26. "World Class Solution Award Winners: ING Americas with Informatica," *DM Review Magazine* (2005), http://www.dmreview.com/awards/wcs/2005/ing.cfm.
27. P. Weill and J. W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press Cambridge, MA (May 2004).
28. IAA User Group of North America Steering Committee, http://tinyurl.com/y52p25.

Accepted for publication November 23, 2006.
Published online March 21, 2007.

Marc Delbaere
IBM Software Group, Industry Solutions, Avenue Du Bourget 42, Brussels, Belgium 1130 (delbaere@be.ibm.com). Mr. Delbaere is the product manager for IBM's industry models. He has worked for 10 years on enterprise-wide model-driven development for the financial services industry. In particular, he engineered the IAA (Insurance Application Architecture) Specification Framework, a generic product and agreement design, the IAA Business Object Model, and the IAA-XML approach to enterprise-wide integration. He has also worked with many insurance companies to help them deploy model-driven solutions in their enterprises. Before joining IBM, Mr. Delbaere worked as a bond trader and as a consultant in actuarial science. He has an engineering degree in business administration and a Masters degree in actuarial science from the Université Libre de Bruxelles.

Rui Ferreira
IBM Software Group, Industry Solutions, Avenue Du Bourget 42, Brussels, Belgium 1130 (rui_ferreira@be.ibm.com). As an insurance-industry solution specialist, Dr. Ferreira has worked on Enterprise Risk Management and compliance solutions for the insurance industry. He has worked on IBM's Insurance Application Architecture and Insurance Information Warehouse models for the last seven years. Before joining IBM, Dr. Ferreira worked in asset management for Generale Bank in Brussels (currently known as Fortis Bank), as a developer of risk management analytical tools in support of the Research and Strategy group. He has also done research in physics at CERN—the European Laboratory for Particle Physics in Geneva. Dr. Ferreira has a Ph.D. degree in physics from the Technical University of Lisbon and an Executive M.B.A. degree from the European University in Geneva. ■