Compliance Intelligence: Measuring and Monitoring Risks and Responsibilities

www.ITCinstitute.com

Sponsored by:

Business Objects™

www.ITCinstitute.com
Compliance Intelligence: Measuring and Monitoring Risks and Responsibilities

Instead of regarding compliance as an unwelcome and expensive intrusion, agile companies are striking a balance between compliance goals and performance goals. By melding compliance with business intelligence, they’re creating a competitive advantage.

About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today’s regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi’s primary goal is to be a useful and trusted resource for IT professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.ITCinstitute.com

Table of Contents

2 The Convergence of Performance and Compliance

2 Building the Case for Compliance Intelligence

5 Aligning Compliance and BI on Common Corporate Goals

5 Methods and Metrics for Measuring Compliance

6 Using Dashboards to Drive Compliance Intelligence

7 Architectural Considerations for Compliance Intelligence

8 Data Considerations for Compliance Intelligence

8 Six Steps to Intelligent Compliance

10 Footnotes

11 Solution Sponsor

12 Appendix A: Additional Resources

13 Appendix B: The Truth Will Keep You Free: Analytics, BI, and Compliance

15 Appendix C: Looking Agents: The Rise of Compliance Dashboards

17 Appendix D: Metrics with Meaning: Setting Measurement Priorities
The Convergence of Performance and Compliance

Few companies are taking advantage of the huge areas of overlap between business performance management (BPM) and compliance management.

Most enterprises unfortunately see compliance as a regulatory nightmare in which unpredictable rules dictated by external forces siphon spending away from business-defined projects. But some smart companies are embracing compliance management for what it really is—an opportunity to achieve competitive advantage. By realizing how compliance management converges with BPM and business intelligence (BI), companies can reduce the cost of compliance and hone the competitive edge that BI provides.

That overlap between compliance and business intelligence (in part because so few companies recognize it) presents a huge opportunity to develop a distinctive competency around compliance intelligence. This represents the application of business intelligence principles to achieve the strict analysis and reporting that compliance demands. Compliance intelligence ultimately has the goal of improving performance and risk management, which facilitate compliance—and the cycle continues.

When chosen carefully and used correctly, tools such as enterprise compliance management solutions and performance dashboards, good architectural standards, and solid methods and metrics for compliance measurement can lead companies to a better understanding of business activities and risks, and thus better financial accountability and transparency.

The work that companies have done around Sarbanes-Oxley in the last several years has focused on collecting data, and lots of it, argues Lee Dittmar, a principal with Deloitte Consulting. The challenge for companies now is to move to the next step: turning those reams of data into usable, actionable information. Since that in a nutshell defines business intelligence, by turning data into information, companies can also fulfill compliance obligations.

“The challenge of making compliance more efficient, more effective, and less risky,” Dittmar says, “is just the other side of the coin of improving internal capabilities and turning data into information, then getting that information to the right place at the right time.” That, again, points back to business intelligence.

Dittmar, who counsels clients and speaks often on the topic of compliance and business intelligence, says that, while significant barriers to turning data into information exist, they are hardly insurmountable. Companies need to resolve complexities in data structures and close gaps in the information layer of the information architecture—to instigate good BI tools and processes, in other words. “There’s not been a lot of focus on that,” he says. “There’s been more focus on tracking transactions, and enabling e-commerce, than there has been on getting information.”

Building the Case for Compliance Intelligence

No one would argue that compliance is an inappreciable effort. Companies will spend close to $15.5 billion on compliance programs in 2005, according to AMR Research, with Sarbanes-Oxley accounting for 40 percent of those costs, or $6.2 billion. Other analysts’ spending estimates are comparable. But these tremendous sums, in addition to proving just how onerous the compliance burden is, actually suggest another approach.

Companies using legacy financial reporting systems, basic budgeting and planning tools, or Excel spreadsheets (which are still the de facto standard for finance reporting, despite compliance-driven revamping), need to start looking for better ways of tracking diverse, distributed controls. The problem with most limited reporting tools is that they are hard to replicate on an ongoing basis; they lack security and versioning or change tracking; they have limited scalability; and their reports draw on multiple, possibly inconsistent, versions of data from across the enterprise.
Vendors certainly see the link between compliance and business intelligence. In response to the Sarbanes-Oxley Act of 2002, several companies with strong BI products have repackaged or retooled their offerings as fairly mature compliance solutions. These are often developed in partnership with big consulting firms. Many analysts suggest that large vendors that have teamed with consulting firms to offer enterprise-wide compliance products that draw deeply on BI, performance management, and risk management represent a solid long-term solution to compliance.

Meanwhile, a silver lining to the compliance cloud is that it encourages executives to open the corporate purse strings for BI and risk management solutions—investments that often are hard-sold into conventional corporate environments. Spending on risk management itself is simply too arcane for most companies, says Ted Frank, president of a consortium of companies called the Open Compliance and Ethics Group (OCEG). “You don’t see companies investing material dollars in technology, because they want to better manage their market risk. [Instead,] they want to address burning issues” like compliance. Frank suggests using compliance drivers as a catalyst for spending on risk management and enterprise BI tools.

Few companies ask questions about business intelligence when purchasing software for compliance, Frank says. This surprises him, given the link between the two. “In the RFP process, very few companies ask BI questions like, ‘How do you feed data into our corporate data warehouse so we can drive business performance?’ Those questions don’t yet exist…. But a good CIO should be demanding that those questions get asked.”

---

**Business intelligence and compliance share many processes and goals.**

<table>
<thead>
<tr>
<th>Leadership</th>
<th>Decision making</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and oversight</td>
<td>Business modeling</td>
</tr>
<tr>
<td>Risk management</td>
<td>Risk management</td>
</tr>
<tr>
<td>Reporting</td>
<td>Scorecarding</td>
</tr>
<tr>
<td>Analysis</td>
<td>Operational monitoring</td>
</tr>
<tr>
<td>Data management</td>
<td>Records management and storage</td>
</tr>
<tr>
<td>Consolidation or integration layer</td>
<td></td>
</tr>
<tr>
<td>Enterprise data sources</td>
<td></td>
</tr>
</tbody>
</table>
Still, top executives and boards of directors are clearly willing to break out the corporate checkbook when it comes to compliance tools and consulting. Given the amount of compliance spending and the number of vendors devoting products and consulting services to helping firms meet their compliance goals, perhaps a wiser approach to compliance is to look at ways to invest in solutions that identify risky business and operational weaknesses—tools that promise long-term fixes and benefits beyond the regulatory scope. That means melding the reactive task of compliance management with the more progressive one of business intelligence to create corporate compliance intelligence.

As astute companies realize the overlap between risk management, performance management, and compliance, they are realigning their organizational structures to reflect this new reality. That, in turn, is spawning new responsibilities under titles like Chief Risk Officer and Chief Compliance Officer.

According to Geoffrey Fallon, managing director of Marsh, a global insurance broker, compliance and risk management used to be separate entities; but that’s now changing. “Traditionally,” Fallon says, “compliance reported to general counsel, and risk management to finance or the treasury department. SOX puts executives and the board in the hot seat, driving risk management and compliance up the organizational chart to chief risk officer and chief compliance officer, respectively.” That sort of corporate understanding of the link between risk management and compliance management, with key personnel in place, can help companies with early warning of emerging risks and possible failures. That’s compliance intelligence.

<table>
<thead>
<tr>
<th>KEY PERFORMANCE INDICATOR</th>
<th>RELATIVE RISK</th>
<th>KEY RISK INDICATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in customer logins, month to month</td>
<td>Increase in malicious traffic</td>
<td>Increase in unsuccessful logins, month to month</td>
</tr>
<tr>
<td>Percentage of successfully resolved help desk tickets</td>
<td>Increase in number of customer complaints (decrease in satisfaction)</td>
<td>Change in help desk call volume, month to month</td>
</tr>
<tr>
<td>Account balances for a given customer segment</td>
<td>Atypical balance changes signal potential fraud</td>
<td>Account balances for a given customer segment fluctuate by more than a defined percentage per week</td>
</tr>
<tr>
<td>System down time</td>
<td>Revenue lost due to business discontinuity</td>
<td>Number of system failures resulting in revenue losses that exceed defined budget thresholds</td>
</tr>
</tbody>
</table>

As these examples show, the line between key performance indicators (often used in business intelligence) and key risk indicators (more often used in compliance monitoring) is not sharply defined. Risk sensitivity can define corporate tolerances for key performance variables. Applying business intelligence principles to compliance monitoring can serve as an early warning system for compliance breakdowns.
In the end, of course, these moves towards more analytical compliance strengthen and support upper management attestations. Using enterprise BI tools, you can pass customized, drill-down reports to the board of directors, CEO, and CFO, confident that the information you’re gathering on compliance is as strong as the information you’re gathering on the business itself.

Aligning Compliance and BI on Common Corporate Goals

When BI is a critical strategic component of compliance, it tends to align on and support common business goals. Although they use different measurement criteria (compliance tends to focus on risk, BI on performance), those measurements overlap.

Unfortunately, compliance is often constrained, in a sense, from full contribution to the business simply because it isn’t driven by excellence. Rather, its ambition is limited to meeting baseline auditor and regulator expectations. This limitation—which so often fosters one-off, incompatible, and redundant development—often proves more resource expensive than more inclusive integrated systems.

Because compliance requirements are externally defined and enforced, businesses often see them as outside the company’s best practices—its drive for excellence, or its pursuit of usable information. To the contrary: companies that integrate compliance data management and reporting practices into the company’s principles and daily practices have added a powerful competitive ally. If knowledge is power, it stands to reason that business insight strengthens competitive standing.

Another challenge to compliance sustainability is the dynamic regulatory landscape. New regulations appear, sometimes vague and unfocused, and clarifications of existing regulations can shift the compliance focus almost overnight. For example, in March of 2005, dozens of corporate representatives testified to the SEC that their first-year SOX audit had been a “check-box” exercise with little accommodation for the actual business characteristics. Compliance efforts had to be comprehensive, panelists said, because auditors were indiscriminate. In May, the SEC handed down additional guidance directing auditors and compliance managers to prioritize compliance efforts according to their material relevance. Over the course of a couple of months, compliance strategy went from “do everything” to “do only what matters.”

To some degree, the redirection provided relief, since it limited the scope of expected compliance efforts. However, to rise to the new requirements, businesses large and small suddenly had to know, demonstrate, and in some cases defend their risk prioritization. For many, that meant adopting a whole new intensity of data analysis, risk assessment, and risk capitalization.

Regulatory changes can present a real problem for static, manual compliance practices—but some of this stress can be alleviated if compliance is essentially a reporting layer that sits on top of a consolidated data foundation. In such an environment, the query and reporting structures can be adapted to new regulatory requirements without the scrap and rework of entire reporting systems.

When compliance follows such BI principles, it helps companies adapt to rapid change. BI provides the data and analytics that executives need to recognize change when it happens and to measure the company’s adaptive performance. In fact, that’s partly what BI is about: turning reams of business and customer data into usable knowledge and doing it as quickly as is needed.

Methods and Metrics for Measuring Compliance

Executives are persuaded to invest in compliance because they want to ensure that data, procedures, and policies meet compliance guidelines. That means that the key performance indicators (KPIs) defined as performance metrics must be reliable, consistent, and credible.

BI and compliance both pose a challenge when it comes to metric definition and measurement. The
trick to deriving more valuable compliance intelligence is to identify metrics that meet both compliance and competitive goals. In this sense, the KPIs used in business performance management and the key risk indicators (KRIs) used for Basel II, SOX, and other compliance efforts aren’t that different. All are metrics—the challenge is identifying which you want to track, and for what purpose.

Some indicators can span both BI and compliance; inventory latency, for example, could be a key performance indicator (reflecting sales against projection) or a key risk indicator (representing costly overhead). Other indicators can have both risk and performance aspects represented by complementary, targeted metrics. For example, increased server traffic might be a good KPI for an online retailer; under that metric, the ratio of malicious to legitimate traffic would be a complementary key risk indicator (KRI). In some cases, however, there’s no overlap at all.

How do you decide what information you want to monitor and what metrics will be useful? Deloitte’s Dittmar suggests beginning by sequentially answering these questions:

- What are the risks?
- What information do I need in order to know whether a risk is occurring?
- What alerts do I want to put in place?
- What query capabilities do I need?
- What monitoring do I want on an ongoing basis so I can feed that to the decision-makers and the people who govern the organization?

In terms of monitoring risk, Dittmar suggests first breaking down specifically just what kinds of risks the company needs to monitor. Credit risk? Competitor risk? Employee turnover risk? Using this exercise, you may well find that the information you want to monitor taps into transaction engines all over the infrastructure.

It all boils down to integrated performance management, Dittmar says. Identifying what is really important and what you need to monitor is key. He draws an analogy to the sorts of “markers” used in biology—critical measures that are predictive of things like future behavior. “The art of the business deal,” explains Dittmar, “is to figure out the most critical markers and make sure that’s where your emphasis is.”

Using Dashboards to Drive Compliance Intelligence

Compliance intelligence is a refinement on massive amounts of raw data generated by your company. It is information—meaningful distillations of the volumes of data that your software products siphon off the enterprise daily. And when it is understood by business managers it becomes knowledge. Recently the conversion of information to knowledge has seen an exciting development: compliance dashboards that customize, summarize, and present relevant information effectively and efficiently—and not just for CEOs and the board. Line-of-business managers of all stripes need their own take on the data, from various depths, areas, and perspectives within the organization.

According to Wayne Eckerson of The Data Warehousing Institute (TDWI), analytical dashboards are an excellent tool for helping organizations focus on the information they really need to achieve their goals. A good performance dashboard, Eckerson explains, consists of a multilayered application built on a business intelligence and data integration infrastructure. A well-designed dashboard based on a solid BI infrastructure lets a wide variety of users drill down into the performance metrics they need to effectively monitor, analyze, and manage their part of the business.

By helping business leaders to monitor, analyze, and manage performance, different types of dashboards provide information to various kinds of users. Eckerson divides performance dashboards into three types, based on the kinds of information they deliver and to whom. Operational dashboards provide front-line workers and supervisors with a way to monitor the day-to-day processes that drive the business. Tactical dashboards pull in large volumes of information from across the enterprise to allow managers and business analysts to investigate
historical trends and issues. Finally, **strategic** dashboards highlight strategic objectives, helping users see the tasks needed in the interim to accomplish those objectives.

In short, as Eckerson notes, “performance dashboards put business performance in context.” Their visual interface and analytic and management tools can be invaluable in furthering the art of business performance management—and thus compliance intelligence.

It might seem that your challenge is to integrate compliance intelligence into performance dashboards. However, if your dashboards are drawing on a solidly constructed business intelligence infrastructure, integration is already happening.

Set up and used correctly, performance dashboards can alert users to exactly the sorts of out-of-bounds conditions that need to be flagged for compliance. But users should consider, in light of compliance, issues such as what information is delivered to whom, what layers of data the dashboard displays, and who has access to the data.

But a central consideration for many companies—what information to base compliance reporting on—is already solved. By using a solid business intelligence infrastructure, good dashboards augment compliance intelligence.

Again, it comes down to making sure your business intelligence is in place. According to Dittmar, the market is full of portals and dashboards. All too often, he says, “they’re not really tied to the transaction engines. They don’t really give you a direct line of sight to what’s happening in the business.”

Dittmar cites spreadsheets as public enemy number one when it comes to getting a consistent view of the truth. Spreadsheets are everywhere, and are, of course, seldom tied into transaction engines. In his book, Eckerson discusses this phenomenon as well, describing corporations rife with “spreadmarts”—spreadsheets or databases that function like individual data marts, with unique sets of data, metrics, and rules that don’t align with other analytical systems in the organization. Thus, there’s no consistent view of the business and no single version of the truth.

Key to making a dashboard effective, then, is making sure that it’s working with that centralized, single version of the truth. “Without centrally defined metrics and a single version of corporate information, organizations cannot compete effectively,” Eckerson writes.

While not all organizations are ready to implement performance dashboards—it requires strong leadership, a receptive culture, and a robust technical environment—they can be an effective tool in reaching and maintaining compliance intelligence.

### Architectural Considerations for Compliance Intelligence

Today, chaos is still the name of the compliance game, as companies struggle to get a grip on their diverse and complex compliance universe. Many companies lack standards-based development and an architectural framework that supports it. They don’t reuse processes that have already proven compliant, nor do they design processes for reuse. Mergers, acquisitions, legacy systems, and constant new development all contribute to silos of data locked in a variety of databases and software. Programming between them is difficult and expensive, when it’s possible at all.

Most IT organizations strive for some degree of architectural standardization, but to better move toward compliance intelligence, companies need to start enforcing the use of new, agile architectures that center on widely adopted standards such as XML, XBRL, and MDDL (a version of XML for market data). A service-oriented architecture can also encourage standardization, insofar as it promotes open standards development and leverages platform-neutral technologies such as Java application interfaces and SOAP messaging.

Enforcing architectural and development standards also supports enterprise agility in the face of fluctuating market and regulatory variables. Companies are more able to pull off quick projects driven by business objectives at the department level when all systems are built using the same types of blocks.
Interoperability is also enhanced when modular design standards are enforced, in which simple, replicable processes can be called, combined, and repeated as needed. This sort of design also gives control at the interface level, so that core systems remain untouched.

Such architectural design drives toward compliance intelligence because standardized APIs protect systems from unauthorized change. That’s a dramatic compliance benefit, realized through development standards that benefit the enterprise as a whole.

Data Considerations for Compliance Intelligence

In order to be able to rely on BI and business performance management data, of course, you need to be sure that your BPM system is delivering the solid information you need for compliance goals. To do that, take a hard look at the data variables that determine how well your BI system can help you address compliance issues. For example, what does your BI system do with unstructured data?

SOX, 17 CFR 21, and other rules mandate record storage and retrieval policies. SOX in particular indicates the need for controls on unstructured data, such as word processing documents, images, and voice recordings—at least to the extent that the data is materially relevant to the company or part of the financial reporting chain.

And if you’ve been using a batch reporting or batch consolidation system, you also may not be meeting the requirements of SOX Section 409, which requires that information be disclosed on a “rapid and current basis” to the public. Since few if any systems on the market today address this need for rapid consolidation of data, moving toward good compliance intelligence may mean an evaluation of your BPM system is in order.

Six Steps to Intelligent Compliance

Armed with the facts about how building true compliance intelligence can give you greater control of your information, your ability to achieve company goals, and your immediate and long-term returns, what’s the next move? Here are six steps along the road to an intelligence-based compliance program.

1. Let Business Steer
According to Michael Rasmussen of Forrester, “risk and compliance management needs to be driven by the business, not IT.” Since business managers and other information owners are ultimately responsible for risk acceptance and integration of controls, it makes sense that they should be involved in the process from the beginning.

2. Simply First
Complexities in data structure and architecture, along with a lack of standardization, hurt your BI and compliance efforts. Instead of focusing on data, think about information. Who needs to know what? When do they need to know it? How often does that information change? What sorts of metrics do you need to capture that? Look for gaps in your information architecture, and start the discussion there.

3. Select and Use the Right Tools
Good compliance intelligence uses enterprise information based on that elusive single version of the truth. That’s where the right tools come into play, such as enterprise compliance products and performance dashboards. Enterprise performance management runs deeper than high-level metrics, KPIs, and dashboards, of course, but set up properly, they give you a visibility into the enterprise that you can’t get otherwise.

4. Start Slowly Out of the Gate
The most important thing is to get started. Tempting as it may be on some levels, the best approach isn’t a five-year, all-encompassing rearchitecture of the entire enterprise.
Don’t imagine that you can fix everything at once. Choose one or two hot compliance issues where you know adequate information isn’t being made available, and start with those.

Try picking some smaller project that will create early wins, suggests Deloitte’s Dittmar. That can help foster buy-in all the way to the top as you gradually demonstrate the concepts of compliance intelligence. To determine where to begin, Dittmar suggests stepping back from the day-to-day business and setting some information quality objectives. “Do an information diagnostic,” Dittmar says, to assess both the benefits and barriers to making significant changes to how data and information is thought of and treated. If you’re facing five accounts payable processes spread over five platforms, for example, that’s a problem you can tackle now by starting to standardize gradually.

5. Secure Management Support

According to BI experts Rajeev Rawat and Claudia Imhoff, securing the support of the enterprise’s senior managers and top executives is the most important step for IT managers and CIOs seeking resources to retool the enterprise for compliance and competitive advantage. IT must demonstrate, they say, that it has evolved from its technology-centric past to serving as a directed weapon for competitive advantage in the enterprise arsenal.

How is that support garnered? Among other things, Rawat and Imhoff advise selecting a critical success factor for the enterprise, then dazzling the business side with the power of a new tool to both meet compliance and revitalize the enterprise. Examples include BI undertakings like dashboards, improvements in the speed of data access, or analytic tools—all things that not only help data collecting and documentation for compliance reporting, but also provide good compliance intelligence by adding competitive advantage. Compliance intelligence means emphasizing the earnings opportunity that such tools present, as well as the compliance aspect.

6. Create an Overall Plan

Most companies don’t have a business plan that addresses how to integrate risk management, and thus compliance, into the company’s overall efforts, says OCEG’s Ted Frank. Whether you’re dealing with risk or compliance, Frank points out, the processes you put in place are really the same. Compliance simply looks at whether those processes are being followed. “But if the vocabulary doesn’t exist, you can bet that companies don’t have a good strategy around compliance.”

He counsels companies to think about the big picture first, then drill down. His advice, which he says resonates well with clients, encourages companies to start by considering what information they want to provide to the board of directors and others with respect to risk management. “Start there, and you’ll understand what you need to do to produce the [right] data for a world view.”

Once you have that data model, work backward to determine the tools you need to drive business intelligence, and thus compliance intelligence. Frank suggests an overarching product for tying together disparate parts of the business under one umbrella. Then use that product to build a data warehouse that really produces the kind of information you need to build the business. In that way, you can turn compliance requirements into compliance intelligence and a true business advantage, not just boxes checked off on a never-ending list.
Footnotes

1 Ted Frank is also CEO of Axentis, a vendor that offers governance, risk management, and compliance products and services.


5 Reid Karabush, *Business Performance Management: Sarbanes-Oxley Considerations*, Business Intelligence Network.


Business Objects is the world’s leading business intelligence (BI) software company. With more than 30,000 customers worldwide, including over 80 percent of the Fortune 500, Business Objects helps organizations gain better insight into their business, improve decision making, and optimize enterprise performance. The company’s business intelligence platform, BusinessObjects™ XI, offers the BI industry’s most advanced and complete platform for performance management, planning, reporting, query and analysis, and data integration. BusinessObjects XI includes Crystal Reports®, the industry standard for enterprise reporting. Business Objects has built the industry’s strongest and most diverse partner community, and also offers consulting and education services to help customers effectively deploy their business intelligence projects.

More information about Business Objects can be found at www.businessobjects.com
Appendix A: Additional Resources

The following resources can provide additional information on the intersections of business intelligence, performance management, risk management, and compliance.

ITCi Unified Compliance Project
This research and development effort by the IT Compliance Institute assists companies in working through differing regulatory compliance requirements. By helping them deconstruct the overlapping requirements among various regulations, the UCP enables firms to adopt a strategic approach to compliance that can cut costs and maximize efforts and spending. More information is at www.ITCinstitute.com.

COSO standard
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary, private-sector organization of accounting experts that offers guidance on financial reporting, business ethics, internal controls, and corporate guidance. The committee issued recommendations in 1992 that later formed the basis for much of SOX. Because COSO offers a framework for establishing management ownership of a company’s risks and controls and a methodology for institutionalizing controls, it can be extremely helpful to companies looking for a structure for SOX compliance. More information is at www.coso.org. Specifically, a copy of the committee’s “Enterprise Risk Management—Integrated Framework” can be found at http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

ISACA COBIT standard
The Information Systems Audit and Control Association (ISACA) created the Control Objectives for Information and related Technology (COBIT) framework specifically to offer guidance on IT risk management. COBIT is useful because it provides generally accepted IT control objectives, not just for auditors, but also for managers and users. SOX has given COBIT new visibility and importance in U.S. corporations in particular, since it can help IT management assess the level of security and control necessary for SOX compliance. More information is at www.isaca.org.

Performance Dashboards
Performance dashboards are a critical component for viewing and analyzing business performance information. They offer staff at all levels a tool to view and drill down on key business performance metrics. Wayne W. Eckerson’s book, *Performance Dashboards: Measuring, Monitoring, and Managing Your Business* (2006, John Wiley & Sons) outlines what performance dashboards are (and aren’t), and helps readers understand how to create and use effective dashboards to drive organizational change.

White Papers from Business Objects
Business Objects, a leading provider worldwide of enterprise business intelligence solutions, offers a range of white papers that provide insight on business intelligence, compliance, and risk management, among other topics. All are available with registration at http://www.businessobjects.com.

Evaluating a Business Intelligence Standard:
There are three key areas to consider when evaluating business intelligence solutions: functional capabilities, infrastructure requirements, and vendor criteria. Based on that, this paper explains how to evaluate a BI standard.

Implementing Business Intelligence Standards:
This extensive field guide to implementing business intelligence explains how to determine the BI maturity of your organization, build a long-term BI strategy, and understand the critical project success factors for BI standardization.

The Benefits of Business Intelligence Standardization:
Why standardize your business intelligence tools? By doing so, even gradually, you can save money, take better control of how information is used, and lessen risk. This paper explains the benefits and how to begin standardizing.
Appendix B: The Truth Will Keep You Free: Analytics, BI, and Compliance

Compliance is a risky business, even if your business isn’t risky. From scoping to control remediation, risk defines compliance. So, why are companies with robust business intelligence systems still slogging through financial spreadsheets for compliance?

By Cass Brewer

Risk valuation is required by financial accountability regulations, such as Sarbanes-Oxley (SOX) and Basel II. To comply, companies must document operational risks. To scope compliance efforts, they must determine a corporate risk threshold. And finally, there’s the risk of jail time if you fudge your calculations. Compliance is a risky business, even if your business isn’t risky.

Of course, risk is nothing new to corporate executives. It’s the static electricity on the doorknob of opportunity: drag your feet, and it will zap you. Thus, with or without the impetus of legislation, most companies perform some degree of business analytics, and larger enterprises employ increasingly sophisticated business intelligence (BI) systems to identify and avoid costly contingencies. In fact, in the US alone, companies spent more than $5.5 billion on BI in 2004, a figure expected to increase to $7.3 billion by 2008, according to “Business Intelligence Driven by Compliance, Standardization, and Performance Initiatives,” a Forrester Research report published last April.

Compliance and business intelligence are overlapping efforts on a continuum of enterprise risk management (ERM). Budgeting, ERP, CRM, supply chain management, and other business processes are integral to compliance, because they impact the financial systems to which regulations apply. They are also subject to the technical and process controls that compliance requires. It, therefore, stands to reason that risk management—whether it’s expressed in terms of compliance or any other business process—should draw on the same data sets and share common analytical elements.

If you sense there’s opportunity in the alignment of BI and ERM, you’re right. Consider these potential benefits:

1. ERM reporting becomes more reliable if it’s based on a single version of business “truth” that also supports BI
2. Use of existing reporting software reduces dependency on expensive manual analysis and problematic financial spreadsheets
3. Access to drill-down reporting gives auditing committees and accountable executives greater confidence in results
4. BI systems adhere to technical and process controls over the management of financial data
5. Companies realize business value from ERM and compliance investments
6. Businesses are better able to meet SOX section 409 “real-time” reporting requirements
7. Analytical software provides early warnings of trends that might impact SEC filings

The flip side of the opportunity coin is the high cost of non-alignment. In 2005, public companies reported that the IT costs of compliance run from 30 to 50 percent of the total compliance bill. Often, these costs are inflated by redundant development and manual processing. Even where sophisticated BI reporting systems are implemented, companies still slog through spreadsheets for financial analysis—particularly for ad hoc analyses, but often as the main reporting tool. Spreadsheets rarely leave an audit trail, are difficult to secure, and are prone to error from manual manipulation. Such a practice engenders a greater likelihood of noncompliance, and probably higher audit fees.

But “year-one” costs are only part of the story. Manual compliance analytics will always be expensive and error-prone. Even companies that do automate compliance reporting in a vacuum, however, will also face scrap-and-rework costs for reconciling complex, incompatible reporting systems down the road.

Breaking the Compliance Quarantine

Clearly, technology is not the most significant barrier to integrated reporting. From the top down, companies must re-conceive the role of compliance in the
enterprise and evaluate the processes, stakeholders, and development resources required to integrate compliance reporting into BI systems. Moreover, because BPM and compliance look differently on risk analysis, companies should also understand how reporting requirements differ.

For many, the initial hurdle is conceptual: overcoming the urge to quarantine compliance. At high levels, it’s worth remembering that most regulations are good faith (if arguably misguided) efforts to standardize and mandate best practices. And, in fact, few companies deny the benefit of SOX, even if they deride compliance costs. At the end of the day, compliance is a business goal. In the same way that BI is evolving from data-focused analytics to process-driven reporting, compliance must morph from a box-checking exercise into an integrated framework for better business processes.

Companies should also strive to remove process prejudices. By nature, new legislation is disruptive: an alien imposition on the existing business mechanism. Accordingly, there’s a tendency to treat each incoming regulation as a discrete project in order to minimize the impact on production systems and allow project teams to focus on meeting regulatory deadlines. The downside to this approach, however, is redundant development and ill-placed investment in incompatible solutions, the increased likelihood of error, and integration headaches down the line.

A more efficient approach views compliance holistically to standardize, simplify, and unify compliance efforts and ease the integration of compliance requirements with existing systems.

In terms of IT, most corporate legislation has recurring themes: for example, technical security, risk management, records management, operations management, measurement and reporting, among others. Each theme encompasses a number of controls which can be internally defined or follow an external standard, such as HIPAA, COSO, or CobiT. Any given control might apply to multiple regulations or already exist on enterprise systems. (Several resources, including ITCi’s Unified Compliance Project, WEDI’s crosswalks, and ISACA’s Information Security Harmonization elucidate control-level alignment.)

Deconstructing existing IT processes and incoming regulations into standardized control definitions allows companies to identify control gaps and overlap processes, where possible. The alignment of compliance and BI reporting is just one example of where this sort of alignment might produce concrete benefits.

A final conceptual hurdle is the use of a single system to meet disparate types of goals. Executives want to see BI beyond the scope of compliance, and they’re required to sign off on financial information that BI doesn’t directly factor. Reporting requirements are different. Additionally, BI strives for improvement; whereas compliance settles for fulfillment. But none of these disparities make BI systems unsuitable for compliance—or even ineligible for dashboarding, as vendors such as Hyperion and DecisionPoint demonstrate.

They say the truth will set you free. BI analytics put power in the pedal, helping companies recognize and avert business risk. In the bigger corporate picture, however, the stakes are even higher. A single version of the truth based on integrated risk analyses can help keep you free when regulatory enforcers come knocking at your door.

This article was written by Cass Brewer, editorial and research director for the IT Compliance Institute, http://www.itcinstitute.com.
Compliance dashboards promise instant access to performance indicators and rapid detection of potential problems. But while vendors have been quick to offer dashboard solutions, comparing the diverse forms can be a challenge in a young and fractured market.

By Susan Jendrey
Einstein penned $e=mc^2$ equation a hundred years ago. Yet, organizations are just now discovering its compliance equivalent: enterprise dashboarding equals measurable, computerized compliance. With compliance here to stay, automating processes makes sense and saves cents. A compliance dashboard—essentially tools that display summaries of relevant performance indicators—allows organizations to integrate and automate continuous compliance measurement and gain communication efficiencies.

The concept of dashboards is not new—but applying a dashboard approach to compliance metrics is a fairly recent innovation. According to Michael Rasmussen, vice president of enterprise risk and compliance management at Forrester Research, “the dashboard provides a portal view into the state of compliance. Ultimately, the purpose of the compliance dashboard is to gather metrics and show measurement of compliance. It is a detection and reporting tool for things that can or have gone wrong.”

Multiple Vendors, Varying Approaches
Like parents and children, vendors and businesses alike have a keen interest in seeing compliance dashboards mature. In Jacqueline Coolidge’s AMR Research report, “A Run on Dashboards and Scorecards: Viable Alternatives Beg Integration Question,” she writes, “Many users are clamoring for dashboards and scorecards as a way to filter and elevate key metrics in operational, market, and financial performance. And the market is responding in kind from more than one direction.”

For example, Mike Malwitz, senior product marketing manager of consolidation, reporting and compliance products at Hyperion, customers are asking for a one-stop shop—a single dashboard with all of the compliance information that they need to know to get their daily jobs done. They want continuous and real-time data with risk assessments linked to traffic light indicators. They also want role-based access and real-time reporting with the ability to drill down into the source data.

“Regulations are pushing our customers toward risk assessment and materiality. Our customers want an easy-to-use framework that contains a risk assessed financial statement package. Tracking and trending are also important to our customers,” adds Malwitz. They not only want to know where they are today, but how they got there, and where they are going. But Hyperion’s view is not universal in the young and fragmented compliance dashboard market. The scope of available compliance dashboards runs from holistic enterprise risk and compliance dashboards to dashboards specific to IT risk and compliance dashboards specific to one regulation, such as Sarbanes-Oxley (SOX).

“If you ask any IT vendor if they have a compliance dashboard, the vast majority of them will step up and state that they do,” muses Rasmussen. Early corporate adopters must be savvy in selecting a viable solution, since there is no single standard for information display, data integration support, and system architecture standards.

“For example, CXO Systems’ dashboard focuses on key IT risk indicators, which include compliance. There are a number of vendors building specific IT risk and compliance management dashboards, such as Archer Technologies, BindView, Hewlett-Packard, ITM Software, and Brabeion. There are specific SOX solution dashboards from vendors such as Certus and HandySoft. Then there are vendors such as Axentis, Paisley, Qumas, Open Pages, and IBM that provide broader enterprise risk and compliance dashboards,” Rasmussen explains.

In writing about the broader dashboard market, Coolidge adds, “neither Business Intelligence (BI) nor Enterprise Performance Management (EPM) vendors have the
sometimes Web-based, sometimes client-server-based, sometimes using standard office productivity tools.

“A well-defined dashboard allows the organization to [determine] the metrics that are important, and manage and report on adherence to them,” Rasmussen states. “It alerts the decision-makers who can take action so that compliance can be managed to business expectations. A dashboard also allows the organization to intelligently learn and track deviations to the defined compliance policies and regulations and allows management processes to be tuned effectively.”

This article was written by Susan Jendrey, contributing editor for the IT Compliance Institute, http://www.itcinstitute.com.

Specific to compliance dashboards, companies including Virsa Systems, Approva, SecureInfo and Applimation specialize in providing users with secure, auditable access to enterprise systems.

Key Indicators
Dashboard indicators are built around an organization’s control statements. To start, “organizations can break out compliance requirements into policy, procedural and technical controls that are cross-referenced to the regulations, legislation and standards that they support. Some organizations have as few as 100 controls for IT [Sarbanes-Oxley] compliance. In other companies, such as one commercial mortgage company, there are a thousand controls in the IT environment for multiple compliance initiatives,” explains Rasmussen.

With controls defined, companies can set metrics and user roles and responsibilities. Rasmussen explains that enterprise risk and compliance dashboards might include metrics on internal controls; credit, market, and operational risks; privacy; workforce; public safety; environmental, ethics or vertical market regulations.

Vendors integrate the metrics from what are often complex and disparate data sources throughout the organization. Then, using rules engines, vendors analyze the metrics and present the results into dashboards—
Appendix D: Metrics with Meaning: Setting Measurement Priorities

The tendency among organizations to continually add new performance metrics without retiring old ones is ultimately self-defeating. How many metrics should you have, how often should the data be refreshed, and how can you avoid conflicting metrics?

Prioritizing Metrics

Less Is More

One thing many people ask about KPIs [Key Performance Indicators] is: “How many should we have?” The short answer is: “As few as reasonably possible.” There is a natural tendency among organizations to keep adding metrics and never delete any. As a result, they lose their power to grab the attention of employees and focus their behavior on key value-added activities. “There is always a temptation to add more metrics as time goes on,” says [Ripley] Maddock [director of customer management at Direct Energy Essential Home Services]. “When people have too many metrics to track, the message gets blurred.”

Guidelines for Metrics per User

Some experts say that organizations should limit the number of KPIs to between three and seven metrics per user, because most people have difficulty concentrating on more than seven things at a time. However, the optimal number of metrics depends more on a person’s role and level in the company than on an arbitrary number.

As a rule of thumb, workers managing operational processes should track fewer metrics, probably less than a handful, because they have less time to respond to issues, whereas executives responsible for setting strategic direction should view many more metrics, perhaps a dozen or more. To reduce the visual confusion of displaying a lot of metrics on the screen at once, designers should group metrics in folders or tabs or nest related metrics under a lead metric.

Guidelines for Metrics per Dashboard

From an organizational perspective, a performance dashboard may have dozens of metrics or more. The total number of metrics depends on the size of the organization, the scope of the project, and the complexity of the organization’s business model. Large organizations with complex processes may require hundreds of metrics to measure performance accurately.

Hewlett Packard TSG’s [Martin] Summerhayes, [program manager] for example, says that it often takes multiple metrics to measure key processes from end to end. For example, a repair call resolution metric might require five sub-metrics to capture performance accurately at each stage in the repair process, from taking an order and scheduling the repair to validating the repair and receiving customer payment. One metric may not shed enough insight to help managers know what part of an end-to-end process is experiencing problems.

If in doubt about how many KPIs to create, err on the high side. What does not get measured, does not get done, and what does not get done can hurt the organization. The key to selecting metrics judiciously is to validate that they are aligned with strategic objectives and distribute them to performance dashboards at the appropriate level in the organization. Not all metrics need to appear on the top-level scorecard; most, in fact, should be delegated to lower-level ones.

According to research from TDWI, most organizations adhere to the “less is more” rule regarding KPIs. Organizations deploy a median of 20 KPIs in the entire Performance Dashboard and a median of seven KPIs per user...

Another common question that people ask is how often they should refresh metrics with new data. The primary factor is the role of the user of the metric and the frequency with which they need to make decisions. If the person is an executive with primarily strategic decision-making responsibilities, then monthly or quarterly updates are probably fine. Of course, if the executive wants to monitor critical operational processes, as many do, then the updates should happen in real time.

Balancing Metrics

The most important characteristic of a KPI is that it leads to positive outcomes. This is easier said than done. A KPI...
alone will not change behavior or improve performance. It is merely a tool to communicate what workers need to do to help the company achieve its strategic objectives and, in the process, improve their position in the company.

“Measures without meetings are useless,” says Maddock. “Unless managers hold regular sit-down meetings with their staff to review performance, nothing will change. Managers need to ask, ‘What are you doing about this number? How will we avoid this happening next time?’”

Organizations as a whole appear to be struggling to find KPIs that impact employee performance, according to research from TDWI. Only 13 percent said their KPIs are “very effective” at changing employee performance; 34 percent said they were “fairly effective.” Meanwhile, 23 percent said their KPIs were only “somewhat effective,” and 19 percent were not sure....

Finding Loopholes
One problem is that users often try to circumvent established KPIs out of laziness or personal gain. “Users always look for loopholes in your metrics,” says Direct Energy’s Maddock. At Hewlett Packard’s TSG, to prevent users from “fudging” customer satisfaction numbers, the company hires a market research firm to audit customer surveys.

Sub-Optimization
In other cases, KPIs may unintentionally undermine each other. For instance, logistics groups that are trying to streamline inventory costs may decide to reduce inventory, which makes it difficult for a retail store to prevent stock-outs of fast-moving items—a key performance measure for them. “We’ve seen our staff take unexpected action to boost a metric that turned out to undermine other measures,” Maddock says.

Strategy Maps
One way to avoid having metrics undermine each other and sub-optimize processes is to create strategy maps that show cause-and-effect linkages among objectives and the metrics that represent them. Strategy maps can help executives clarify their assumptions about what drives the business and debug the objectives and metrics that comprise the strategy. If a positive improvement in one metric doesn’t lead to an expected bump in a related one, then this is a sign that executives need to examine their assumptions behind the linkages. It may cause the team to revise the metrics or create a new one that sits between the previous two and links to both.

This article has been excerpted from chapter 11, “How to Create Effective Metrics,” of Performance Dashboards: Measuring, Monitoring, and Managing Your Business (0-471-72417-3, October 2005) with permission from the publisher John Wiley & Sons. You may not make any other use, or authorize others to make any other use, of this excerpt, in any print or non-print format, including electronic or multimedia.