

## **“A Practical Approach to ‘GRC’: Risk-Advisory and IT Collaboration”**

By Alex Joseph, SAP Process Manager, Logistics & GRC, itelligence; Alec Arons, Partner, Tatum; and Nicole Crawford, Partner, Tatum

- Chapter II: The Project Steering Committee: Breaking Down Silos from the Start
- Chapter III: Third-Party Advisors and Outsourcing
- Chapter IV: Assessing Risk
- Chapter V: Beyond the Board Room: Promoting Enterprise-Wide Collaboration
- Chapter VI: Maintaining Collaboration
- Chapter VII: Change Management
- Chapter VIII: Finding the Right Risk-Advisory/IT Service Providers
- Chapter IX: The Organization Afterwards

The term “GRC” has been applied to such a wide array of governance, risk and compliance issues that the term carries no commonly accepted definition around the world. Widespread usage of the acronym has increased confusion, so that organizations often encounter a great deal of frustration when attempting to identify and then mitigate risk via processes, procedures and policies. Despite this lack of clarity, concerns relating to GRC remain top-of-mind with key decision makers, and for good reason.

For example, according to Accenture’s 2009 Global Risk Management Study of more than 250 of the world’s largest enterprises (represented by chief financial officers, chief risk officers and other risk executives), risk management capabilities are not currently sufficient to meet today’s challenges. The global financial downturn is widely acknowledged for highlighting this discrepancy and the potentially far-reaching vulnerabilities.

Simultaneously, the Accenture study found that increased regulation is expected in the coming years, thus creating the need for most organizations to ramp up efforts at a time when resources generally are at historic “lean” levels. An expanding list of regional compliance mandates and ongoing complexities includes Sarbanes-Oxley (SOX) and new SEC rules in the U.S., the Turnbull Report in the UK and Japan’s JSOX regulations, among others.

C-level executives, and increasingly corporate board members, continue to face a myriad of pain points related to heightened shareholder expectations and the potential negative consequences of noncompliance, including the loss of customers, diminished brand equity, financial penalties, and reputational risk for the organization and its officers and directors. These corporate navigators wrestle daily with how to comply with financial and industry regulations and lender covenants, how to ensure processes and systems support the planning, measurement and reporting of operational and execution decision-making needs, and how to effectively measure corporate performance against industry best practices.

## **Changing Landscape**

At the country level, there is ongoing legislative and regulatory activity in the U.S. regarding measures that would either exempt or require small public companies, described as having a market capitalization of less than \$75 million, from SOX compliance requirements. While the SEC announced in October 2009 that these companies will be required to submit to reviews of internal financial controls, beginning with fiscal years ending on or after June 15, 2010, the U.S. House Financial Services Committee passed legislation in December 2009 with a provision that would either exempt or provide yet another delay for smaller public companies to comply with SOX requirements.

Part of the Wall Street Reform and Consumer Protection Act of 2009, the law, if enacted, will allow a 12-month compliance delay, an exemption for the smallest companies, and a study of the costs and benefits of extended SOX compliance. The U.S. Senate will now review the bill at some time during the 2010 session and could either strip the bill of these provisions or make considerable modifications.

Additionally, at the time of this writing, the U.S. Supreme Court is weighing arguments that call into question the validity of the Public Company Accounting Oversight Board—and thus SOX, the repeal of which would send reverberations throughout all markets. Another current Supreme Court case highlights the impact of worker privacy rights on data networks, which places effective deployment of enterprise-wide policy at the forefront of discussion.

The SEC in December 2009 issued new proxy reporting requirements in advance of the upcoming annual reporting season. The new requirements are designed to improve corporate transparency regarding risk, compensation and corporate governance matters. Specifically, the new rules require a public company to disclose in proxy and information statements the extent of its board's role in the risk oversight of the company and the relationship of a company's compensation policies and practices to risk management.

Escalating global trade continuously involves more supply chain partners, resulting in increased documentation and ever-changing regulations—all of which heightens the necessity to assess and improve core processes.

In 2010, European Union countries are complying with changes to the Value Added Tax (VAT) system, which has been in use for more than 40 years and applies to most sales tax and purchase transactions in the EU. The European Commission enacted the new rules to reduce fraud and give suppliers equal treatment regardless of their country since every individual country currently has its own rules, legislation and rates.

Even companies with no apparent critical risks have begun to look to GRC, in order to capitalize on global markets. When going through SOX compliance

activities, these companies realized that although their operations ran on a single IT platform, processes and controls lacked consistency on a global scale, representing an under-leveraging of investment in enterprise resource planning (ERP) software.

Recognizing an opportunity to drive more systems, these companies now seek to tighten business rules and enhance consistency across business processes. Other currently healthy public companies—who have yet to encounter critical pain points relating to compliance problems, earnings surprises or material SOX weaknesses—now consider GRC as a potential response to the SEC, which in overall risk management remains U.S. companies' top GRC motivation, based on a November 2009 AMR Research survey of 151 companies representing all sizes and industries. These same companies plan to spend \$29.8 billion on GRC activities in 2010, up 3.9 percent, according to AMR Research. From a broader global perspective, leading analyst firm Gartner predicts worldwide corporate GRC spending to top a robust \$1.3 billion by 2011.

### **Eyes Wide Open**

While these instances serve as the primary talking points around GRC, prescient executives have begun to consider a subtler factor: the potential ramifications of an economic upturn. Significant cost and workforce reductions have become widespread in the last few years, as companies scaled back operations to levels proportionate to business activity. Now decision makers must ask themselves if they are prepared for growth from a control perspective, or whether their cost-avoidance initiatives created more risk by eliminating the resources necessary to accommodate increased commerce. Senior management must assess their current processes and decide whether increasing workforce or better leveraging technology represents the best way to prepare for growth.

Regardless of the outcomes of stand-alone legislative and economic events, ongoing business realities will continue to challenge companies to examine their governance, risk and compliance processes. Enterprises must define business goals and identify the opportunities to achieve those goals—all while satisfying external laws and mitigating risk via internal standards. With those objectives in mind, companies can begin to grasp the broad principles that anchor a practical approach to GRC.

For example, far too many organizations incorrectly believe effective risk management can be managed via spreadsheets or that today's robust Enterprise Resource Planning (ERP) systems that deliver integrated, robust GRC functionality are only accessible to the largest of companies. The reality is that fully integrated ERP systems, incorporating GRC functionality, are now readily available and are designed to address the unique needs of small-to-medium size businesses. Enacting a forward-looking approach to holistic risk management policies, procedures, controls, and enabling technology early in the company

growth life cycle will allow these companies to realize how much more effective their programs will be and benefit from early recognition of market opportunities.

For the purposes of this discussion, we will define GRC more specifically, as an integrated framework of board and management activities that examines the organization in terms of overall governance model and structure. This includes identifying and managing the risks deemed critical to business success; achieving compliance with applicable laws; and creating an effective control environment. Each element of this overarching framework can be satisfied with straightforward, practical activities. These activities often are supported by external risk advisors and information technology (IT) professionals.

Enlisting an integrated team of risk-advisory and IT subject matter resources helps an organization successfully deploy an enterprise-wide GRC program in several ways. Risk advisors with senior-management experience provide the objectivity and oversight demanded by each stage of implementing the new governance structure. By assisting processes and addressing critical issues during the lifecycle of the project, these advisors also allow the internal decision makers to continue functioning in their day-to-day roles.

Meanwhile, the advisors work closely with the IT service provider to ensure that the developing business vision is reflected in the technological solution that will ultimately be deployed to support and sustain governance measures. With these resources in place, the organization can embark on the first step towards successful GRC implementation.

## **Chapter II: The Project Steering Committee: Breaking Down Silos from the Start**

Organizations often find themselves tempted to regard technology as a “magic bullet” for governance, risk and compliance needs. The IT professionals who collaborate with risk advisors do indeed offer software products that can drive and sustain dramatic change. However, if the organization has not thoroughly prepared itself to manage and maximize this potential change, the software alone will not prove beneficial.

For instance, if a company exports to 150 countries, it needs to ensure compliance with 150 different sets of specific regulations, while also cross-referencing its partner roster with domestic embargo and “denied parties” lists. While a GRC-optimized ERP solution can automate the compliance reports required for these activities, the accuracy of those reports ultimately depends on a workforce that understands how to properly enter and source information. Policies, procedures and training thus become necessary in order to fully capitalize on the IT solution.

As this example illustrates, the challenge involved with achieving true GRC is cultural, not technological. The organization must adopt the capacities and

capabilities that come with enhanced technologies. This adoption relies on first understanding what direction the organization wants to pursue. Organizations cannot gain this knowledge while working in silos.

One of the end results of successful GRC implementation is shop-floor workers fully understanding how their combined actions affect the direction of the organization. Before this is possible, that direction must first be clearly communicated through policy, which begins with senior management working closely together to create a unified vision for the enterprise.

Many GRC implementations are hampered by insufficient communication between the offices of the CIO and CFO. Clearly defining the roles that these officers will fulfill before, during and after implementation is critically important. The CFO has the opportunity to help the board understand the risks facing the enterprise and then link this perspective to risk-mitigation strategies. It is equally important for the CFO and CIO to collaborate from an IT standpoint to map what route to take and how to address risks. Both parties must remain aware of the ultimate outcome of implementing GRC: the ability to confidently go before the board with good information, without having to invest in tools beyond a base reporting system.

The formation of a project-steering committee creates broad representation of key stakeholders, including board members. Having the right people together in the same room from the start not only facilitates the creation of a unified vision, but also ensures that when departmental differences arise regarding how the project should proceed, the right decision is made for the business as a whole. Risk advisors can assist with forming the committee as well as assisting each of its functions, beginning with risk assessment.

### **Chapter III: Third-Party Advisors and Outsourcing**

Many corporations increasingly believe in leveraging the capabilities of specialized consultants to help management achieve their organizational risk management objectives. Working as advisors to, and liaisons for, senior management and IT teams, third-party risk advisors can help establish common goals and work toward their achievement.

Dean Marino, director of IT for Cobra Electronics Corporation (NASDAQ:COBR), a leading global designer and marketer of communication and navigation products, is a firm believer in the value of outsourced consultants. "Our decision to outsource SAP hosting was primarily based on a need for a flexible, cost-effective solution which could be implemented quickly, eliminating the complexities surrounding in-house expertise and infrastructure investments," said Marino.

Marino believes similar advantages could be realized in risk management. He added, "The outsourcing decision has allowed our internal IT staff the ability to

focus on value-add core business issues. Any midmarket company using this same approach toward GRC should benefit from the same versatility and knowledge, outsourced consultants offer in making strategic recommendations, providing hands on support or a combination of both."

According to the 2009 Accenture survey, 63 percent of global executives believe one or more aspects of risk management can be outsourced to improve efficiencies. Specific examples of activities or processes executives believe can be enhanced include model validation and back testing processes, application development of expert tools and report production for standardized risk reports and disclosure.

Sixty-eight percent of respondents cited "cost considerations" as the top reason for outsourcing, according to Accenture's research. Other important reasons included "advantage of unified risk procedures across units of the same company (55 percent), "process improvements and better turnaround time of risk responses" (50 percent), "improved ability to deal with regulatory requirements" (46 percent) and "enhanced scalability" (45 percent).

At the process level, consultants often provide a cost-effective alternative to additional full-time staff by processing overwhelming data integration challenges and conquering burdensome time-resource requirements of IT application management. Corporations that leverage outsourcing options to handle these responsibilities can, in turn, use internal risk professionals to provide more strategic value through individual business unit or system-wide management.

Additionally, industry references such as the nonprofit Open Compliance Ethics Group (OCEG), which includes charter member SAP, can provide comprehensive guidance, standards, benchmarks and tools for integrating governance, risk and compliance (GRC) processes. The OCEG's robust framework and toolset offer benchmarks and methodology from thousands of subject matter resources and companies of all sizes to help develop a GRC program. Fundamentally, there is no way to have any confidence that a company is in full compliance with all regulatory and industry requirements, much less in a cost-effective way, without leveraging GRC technology functionality to assimilate the sum of the parts. Executives can then have a predictive and detective view of their governance, risk, and compliance universe with significantly enhanced chances of detecting "black swan" early warning signs.

#### **Chapter IV: Assessing Risk**

With the steering committee in place, the project can begin in earnest. Working with the senior management team and board sponsors, the advisory/IT team helps determine organizational risk. If the company already has a risk-assessment program in place, the advisor helps evaluate that program. If no program is in place, the advisor helps build a new risk framework. In either case,

all involved parties have the opportunity to define what they perceive as the most critical issues facing the company.

Companies with existing assessment programs might have already identified and mapped hundreds of risks, while organizations new to the process may not have identified a single factor. Regardless, organizations always benefit from honing in on the Top 10 risks and designating which persons within the organization are responsible for those areas of concern. The lists compiled by committee members usually contain similar risks, but the way in which each person ranks these risks frequently varies and can usher in substantial insight.

For instance, CFOs often focus on the accuracy of financial data produced by the company's existing ERP system. If the CFO cannot vouch for the integrity of financial reporting, this creates major hazards in terms of compliance with imposed auditing standards. The CIO might be primarily concerned with maintaining user access within the enterprise's information architecture, especially if no controls are in place to automate access for third parties. Adhering to shipping and environmental regulations frequently preoccupies the COO, and so on, with unique risks affecting different departments to varying degrees.

Executives quickly see that their contrasting priorities indicate varying levels of risk tolerance, meaning that some members of senior management are currently accepting risk beyond their tolerance levels. This often leads to a robust discussion about what risk means to the company, and what policies, procedures and processes can help ensure that assumed risks remain proportionate to the company's capabilities. Thus begins the collaborative vision of the company's future.

The risk advisors, in conjunction with their IT counterparts, clearly explain the tools available for management to address each area of concern. Senior management comes away from this stage with an awareness of the organization's biggest risks and how to identify all activities that contribute to each pain point, from both an IT and management control perspective.

Even at this preliminary stage, the advisory relationships begin to pay dividends. Having discussed and reached a consensus on the top risks facing the company, management and the team can begin developing a remediation strategy. This strategy will establish a timeline in which the risks deemed most critical are mitigated by leveraging improved controls and methodology. Equipped with this blueprint, the IT team begins optimizing the software solution based on the company's needs. A good software solution will come with out-of-the-box modules that address hundreds of specific risks. With the remediation strategy as a guide, the IT professionals tailor a solution for the enterprise.

On the other hand, companies that enlist software providers without seeking the counsel of risk advisors may find themselves with a product that creates a high volume of data that cannot be used due to a lack of a clear understanding of risks and overriding framework to mitigate and manage them. Only by structuring implementation so to manage risk over time can an organization gradually implement governance initiatives in a manner that coincides with the development of the software solution. This is another example of why IT-only solutions do not suffice, while IT/risk advisory collaborations often flourish.

## **Chapter V: Beyond the Board Room: Promoting Enterprise-Wide Collaboration**

In addition to formulating a remediation strategy to deal with risks, the risk advisor also turns the committee's attention to what the company does well. Executives often overlook the successful elements of the enterprise, assuming that satisfactory productivity presupposes efficient processes. It is possible, however, to do things effectively but not efficiently. Risk advisors help committee members see where the company excels and how the processes surrounding those successful components can be further enhanced. Capitalizing on these areas often involves automating processes via the IT solution so to increase efficiency and thus reduce operational costs.

At this point, managers temporarily break away from the steering committee and, with the assistance of risk advisors, set up a series of meetings with personnel in their respective departments. Explaining the results of steering-committee activities, senior management clearly sets forth organizational goals.

By pinpointing which processes to monitor in order to mitigate risks and capitalize on opportunities, management begins to establish accountability, which will prove essential to sustaining the implemented GRC program.

These secondary meetings generate a tremendous amount of dialogue and discussion. Top-level objectives filter down the chain of personnel, who freely offer feedback and voice concerns. Supervisors can thus register the perspective of the end-users, who will have their day-to-day tasks altered by the enterprise software.

Worker response then flows back up to the steering committee, which can weigh the merits of reported concerns and fine-tune the remediation strategy where necessary. Here we see how a practical teaming approach to GRC breaks down silos and engenders collaboration. Many companies have reaped such benefits from this methodology that they incorporate risk assessment into their annual strategic planning exercises.

By this point, the IT specialists have set up the software solution and fully examined the client's informational landscape. Working off the remediation strategy, the IT team has tested the effectiveness of existing controls in relation to perceived risks. Additionally, the technology partners have gone beyond the remediation strategy and examined the existing system from a best-practices approach. With particular attention paid to security, the IT team has gauged the organization's ability to perform a number of critical processes.

Back in the steering committee, the IT specialists reveal the organization's current ability to establish audit trails, manage third-party access and perform other essential tasks, giving senior management a precise understanding of how current capabilities compare to industry best practices.

The ultimate goal of the software team in this instance is to make all risks transparent. The initial risk assessment established which areas needed to be addressed with improved policies and practices. Now the IT specialists show the steering committee what risks look like from a granular level inside the system. Risks can never be completely eradicated, but they can be identified, mitigated and subjected to strict controls, but only after being made transparent. By examining whether the existing client software can support optimized GRC modules, and by uncovering additional pain points, the IT team helps the steering committee round out its planning for implementation and further develop policies as additional needs become apparent.

## **Chapter VI: Maintaining Collaboration**

Allied resources will continue to ensure success at every stage of the GRC implementation, particularly when the risk-advisory/IT collaboration and the steering committee encounter resistance. Even though department heads have articulated enterprise vision all the way to the shop floor, every implementation will face some degree of challenge, however small.

The IT team might discover that controls suggested by the remediation strategy create segregation-of-duties conflicts by granting multiple workers access to a specific performance activity. If the IT team cannot find an alternative solution, the underlying business process might need to change to avoid the conflict. Particularly when dealing with product-and-loss functions, workers rarely welcome news of changing integral process from a systems or control perspective. In these situations, executive sponsorship proves invaluable: senior management must share the same overriding perspective in order to mandate new procedures.

Smaller businesses typically employ fewer workers, increasing the likelihood of certain conflicts. Whenever personnel perform multiple tasks, it heightens risk. In this case, management likely understands the risks inherent in assigning multiple duties, but considers the situation unavoidable due to scarcity of resources. Seasoned IT professionals with deep industry-specific knowledge

and a proven record for assisting mid-sized enterprises will most likely have either helped resolve a similar issue or possess sufficient knowledge to negotiate the risk within the IT landscape.

Consistent interaction amid senior management ensures that all challenges can be effectively resolved. With the steering committee in place and communication flowing up and down the organizational structure, the enterprise has created an equal and comprehensive partnership that incorporates senior management, the internal IT organization, end-users and the risk-advisory/IT team.

In this way, true GRC incorporates all operational components of the business to focus on enabling a framework of policy, procedure and processes that will be supported by software functionality. Rather than a mere concept, collaboration becomes the vital engine behind a series of straightforward activities devoted to implementing a system that will result in tangible organizational benefits designed to improve the overall measurement and execution of governance activities, risk management and automation of compliance functions.

## **Chapter VII: Change Management**

At its most basic, a practical approach to GRC involves three steps: (1) understanding what changes need to occur and why; (2) recognizing the impact of these changes on the organization in terms of sheer effort required to innovate processes; and (3) making sure that a change management program is in place to sustain change.

Knowing what needs to change enables an organization to develop better policies, procedures and processes. A comprehensive GRC software package establishes the potential to sustain these governance measures. However, if the enterprise has not readied all of its members to competently utilize the software, a gap will remain between envisioned and realized success.

Risk advisors can assist with extensive training sessions presided over by the IT team, but true change comes from senior management driving accountability across the enterprise. The specific sequence and duration of formal change-management exercises that an organization undergoes will vary case by case, based on each enterprise's needs and capabilities. Risk advisors will help determine the best route to take, and also stress the need for sustained change management.

Following the completion of training and preparatory exercises, change management needs to become ingrained in daily interactions within the organization. Let's take for example a vice president who achieves fluency with the new software system. The VP can request a manager to provide information contained in automated reports that are readily available. If the manager cannot obtain the information, the VP can demonstrate how to access the information

and clearly express the expectation that in the future the information will be sourced independently.

This rudimentary example shows how accountability drives change management. Personnel adopt new ways of performing tasks due to executive mandates and are given all the necessary tools to suffice requirements. Importantly, this accountability goes all the way up to senior management reporting to the board. In order to sustain change by effectively mitigating risks and capitalizing on available opportunities, all personnel must understand their changing roles and functions.

### **Chapter VIII: Finding the Right Risk-Advisory/IT Service Providers**

Although the service providers help engender collaboration across the enterprise, some cooperation needs to be in place even before deciding on which team to engage. The CFO and CIO should work together to thoroughly research their options and select a team that can fully service both the financial and IT sides of a solid GRC program. Queries regarding what exact methodology the risk advisors and IT specialists employ will help ensure that the selected service providers work from a clearly defined set of GRC activities.

The field experience of candidates is also essential. Once the implementation begins, risk advisors will focus on a variety of financial issues including accounting and control; operational assessments; and business processes, while simultaneously looking at governance structure; processes for risk management; and the adequacy and effectiveness of policies. Qualified advisors will have a wealth of relevant senior-management experience. Additionally, the right IT team will have industry experience specific to the organization, and possess the expertise to apply best practices within a sophisticated software environment.

When assessing potential IT partners, management should also closely examine the viability of offered software products, which will become an integral part of the enterprise's underlying structure. Software with "out-of-the-box" functionality offers the enterprise a pre-designed template based on industry-specific best practices. After the risk assessment, the IT team begins optimizing a software template, rather than building the system from scratch, which accelerates implementation time and immediately addresses the organization's most critical risks.

The template design also allows the IT team to make the GRC software directly mirror ongoing governance activity. Effective GRC software addresses tasks, not roles. Instead of being geared toward a shipping clerk, for example, the software would concentrate on the exact functions that companies need in order to ship effectively. As senior management redefine processes, procedures and policies, the way that shipping clerks do their jobs might change, but the core tasks involved with effective shipping remain the same. It is therefore important that

the team offers software designed to accommodate the fluidity of ongoing governance.

A good software solution will place two new modules on top of the existing ERP system. One of these modules will monitor security by maintaining audit trails, which not only track users' activities inside environments but also run simulations of that activity prior to granting access, in order to maintain segregation-of-duties integrity. The other module will service the company's global tracking and shipping needs. Not only will this second solution contrast required documentation for multiple countries against actual available data, but it will also cross-reference all trade partners with lists of countries designated as "no trade" risks.

With these capabilities in place, the organization will meet reporting requirements for finance and operations, in addition to validating the integrity of informational infrastructure. More importantly, these automated assets allow decision makers to identify and capitalize on future opportunities.

### **Chapter IX: The Organization Afterwards**

We previously considered how different officers might respond during the preliminary risk assessment. In our example, the CFO identified financial reporting as the chief concern. The CIO focused on maintaining integrity within core system processes, while the COO gave highest attention to managing shipping reports. Having gone through an exhaustive GRC implementation, these parties find themselves able to negotiate their priorities in an integrated, automated environment.

The CFO now has a dashboard where current risks can be assessed against the adequacy of environmental and critical controls. Financial information constantly fluctuates, which traditionally means that decision-making processes involve sifting through massive amounts of outdated data. The GRC dashboard continuously updates information and provides transparency as to who enters what information and in what manner. Thus the CFO can constantly monitor the integrity of information and reports provided to the board and outside agencies.

From a CIO perspective, the GRC dashboard allows total transparency in terms of system access. Access-management software tools document all activity for a given user throughout that individual's tenure with the organization. When a new user enters the system, the software runs a simulation to test potential impact on segregation-of-duties policies enacted through governance. These capabilities act as a catalyst for risk prevention by resolving basic oversights, while also eliminating more nuanced phenomenon such as "user creep," in which organizations grant credentials that exceed the scope of prescribed activity. The ability to generate audit trails also advances personal accountability, bolstering governance.

In terms of shipping risks, the operational dashboard not only provides visibility throughout the supply chain, but also prioritizes preparedness activities. If new legislation requires that customs authorities in certain countries receive advance notification of a given material traveling in certain quantities, the dashboard alerts management as to what activities need to transpire, in what order, and when. Additionally, the operational components within the system automate all importing and exporting documentation, correlating massive amounts of information concerning each supply-chain partner.

With this level of transparency and availability of information, collaboration becomes seamless. The monitored actions of all personnel directly factor into how the enterprise functions. Software capabilities sustain governance measures, as IT functionality corresponds with enhanced enterprise vision. Yet this highly sophisticated environment became obtainable only after implementing a practical and measured approach to governance, risk and compliance.

### **Success in Any Language**

While creating a uniform definition of GRC will likely continue to be a challenge for years to come, organizations can meet their most ambitious objectives in 2010 and beyond by following proven best practices to proactively implement a consistent, enterprise-wide program. No matter their size or industry, businesses that take a holistic approach to identifying stakeholders, mapping effective strategies, realistically assessing and managing resource options and tools, and committing to change will be positioned for long-term risk management success. By doing so, these organizations can reap the rewards and more easily achieve a wide range of strategic objectives, from improved cost and resource efficiencies to business diversification to global expansion.

### **Industry Links**

SAP BUSINESSOBJECTS GRC SOLUTIONS (CUSTOMER REFERENCES)

<http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/customers/index.epx>

OPEN COMPLIANCE & ETHICS GROUP

<http://www.csrwire.com/members/profile/10096-OCEG-Open-Compliance-Ethics-Group>

<http://www.tatumllc.com/>