

The collapse of Enron, WorldCom and other corporate accounting scandals of 2002 not only almost brought Wall Street to its knees; it also signaled the beginning of a new age of compliance. Companies have been forced to adopt better governance and risk management approaches, and in large part they have responded well.

However, compliance is much more than a one-off challenge to be addressed with a point solution; it's an ongoing concern that requires continuous monitoring and that impacts the business as a whole. And with a dazzling array of technologies and tools currently hitting the market in response to the overwhelming need for greater governance and control, companies are now presented with myriad options for tackling their compliance requirements. So how do they ensure they're making the right decisions? *Business Management* caught up with a panel of top compliance solutions vendors to find out.

Regulatory pressures and greater scrutiny are putting more pressure on companies across a range of industries than ever before. What challenges does this present to senior management?

PB. New regulatory pressures from legislation such as Sarbanes-Oxley have increased scrutiny by regulators and auditors and created new risks for senior managers. Managers are now accountable for ensuring that their organizations are in compliance. The net result has been more time and money spent on internally oriented compliance initiatives.

But while senior managers are ultimately accountable for their company's compliance efforts they must rely on people from all parts of their organization to design and implement compliance programs. In addition, since many of these new regulations are relatively new there are also challenges in understanding how auditors and regulators will interpret and enforce them. Sometimes it can seem like you are aiming at a shifting target. As auditors and regulators gain more experience and use more sophisticated tools, they are starting to raise the bar and expand the scope of what 'compliance' means.

GOOD GOVERNANCE IS GOOD BUSINESS

JG. Senior management is faced with a significant lack of visibility in regard to regulatory compliance. Today, many companies used a 'silo' approach to compliance, creating an extremely complex and disjointed structure. The fact is, most companies today cannot respond quickly and effectively to management questions about compliance – their information systems were simply not designed for it.

HW. With legislation such as the Sarbanes-Oxley Act, there are two major challenges currently facing corporate executives, creating pressures above and beyond those that companies faced before.

First, internal audit cannot continue to be tasked with primary responsibility for conducting the ongoing testing and monitoring of internal controls effectiveness. As the de facto internal controls experts in most organizations, internal audit's insight and understanding of the COSO framework was deemed critical to tackling compliance with this new legislation. But this situation has consumed internal audit re-

sources, compromised their independence and limited their ability to complete the necessary financial and operational audits that underpin sound business performance. Companies are going to have to automate the ongoing testing of controls – with responsibility for this task sitting with the financial and business unit managers. This, in turn, will free audit to return to their role of independent assessment and review of broad organizational risk – that encompasses, but is not limited to, compliance concerns. Auditors can and should still be involved in the cross-disciplinary compliance team, but they can't remain in the roles many found themselves thrust into when this all started.

Second, is the need to shift the view that monitoring IT access and authorization controls is sufficient for compliance. The intent of SOX 404 is to provide stakeholders with assurance over the accuracy and integrity of a company's overall financial health and performance. Testing for segregation of duties conflicts or user access privileges alone won't give you the complete picture, or even necessarily the most im-





PRASHANTH 'PV' BOCCASAM is Chairman and CEO at Approva Corporation. He is a recognized expert on compliance and application controls and brings more than 15 years of experience in enterprise software and security management to the job. Before founding Approva, PV was co-founder and President of Entevo, Corp., which was sold to BindView (now Symantec) in January 2000. PV's pioneering work in developing a cross-control and cross-application controls management solution based on an open architecture is enabling companies to take a unified approach to addressing controls across their enterprise.



JASVIR GILL is Founder and CEO of Virsa Systems, Inc. and also serves as the Chief Technology Officer. He is an acclaimed thought leader in the compliance industry for his visionary work in shifting the compliance model from after-the-fact detection to a real-time preventative approach. Gill founded Virsa Systems in 1996 and is principal designer of Virsa's Continuous Compliance Suite software solution. Long before the Sarbanes-Oxley Act was passed, Gill was a pioneer in developing solutions for enterprise risk management and reducing the cost of compliance and audits for leading global enterprises such as Kodak and Kimberly-Clark.



As President and CEO of ACL Services Ltd, **HARALD WILL** is responsible for the foundational requirements necessary to create and successfully execute on ACL's vision. Will's focus is on guiding the company's product line extension and market expansion, leveraging ACL's core competencies to support growth and revenue targets. His entrepreneurial spirit has fueled ACL to become the leading global supplier of software solutions for the internal, external and public sector audit markets. He was recently named one of Treasury and Risk Management magazine's '100 Most Influential People in Finance' for 2005.



Co-Founder and CEO of LogicalApps **CHRIS CAPDEVILA** has more than 15 years of experience in the enterprise software space. Prior to founding LogicalApps, he was a senior consultant at Price Waterhouse LLC, and was instrumental in delivering critical process improvements during the implementation of enterprise applications at Western Digital, Disney, General Electric, Eaton Corporation and Iomega. He has been a visionary and key contributor in the business process management community and actively promotes industry best practices in business process automation and enterprise application governance.

portant part of the picture. The key business controls governing financial transactions must be tested and monitored on a continuous basis to assure the integrity of a company's financial reporting.

CC. Unfortunately, all of the media hype and scrutiny resulting from regulations such as Sarbanes-Oxley are causing senior managers to focus on compliance as the end-game, rather than as a means to a much more powerful goal. To date, most companies have focused on meeting the 'letter of the law' instead of focusing on the root causes of their control and financial integrity problems. In 2005, companies spent approximately two percent of gross revenue (or

"No matter which path you choose, the important thing is that you take a systematic, long-term approach to compliance"
 – Prashanth Boccasam

more for smaller companies) on meeting compliance requirements, yet most saw no return on that investment. Even worse, the tremendous manual effort directed towards SOX compliance resulted in a huge opportunity cost of diverting people away from growing the business. The challenge faced by senior management is how to use compliance efforts as a catalyst for running a better business. Ultimately, when you focus on compliance for compliance's sake, you're going to spend a lot of money, but you're not going to get any business value out of it.

What can companies do to ensure better management of their compliance needs? What do they need to do better?

JG. It is absolutely critical that management avoids the temptation to approach compliance from a project or 'bolt-on' perspective. This approach seems appealing because it tends to look less expensive and time-consuming. More often than not, it creates a reactive organization with little or no ability to detect or prevent control problems and actually increases costs.

Management should seek to integrate compliance tasks into daily business processes and eliminate compliance silos. By using compliance and risk management that is tightly integrated

with their ERP and legacy transaction systems, management can implement preventive, real-time controls, automate control testing and monitoring, and detect and correct violations early. The best compliance and risk management solutions can centrally manage end-to-end compliance activities and work in tandem with existing enterprise systems.

CC. Companies need to change their approach to compliance from one that is project-based to one that is process-based, essentially embedding governance controls directly into the core business systems that provide the foundation for managing their organization's performance.

To see the difference, let's compare the financial reporting process (which is the target of Sarbanes-Oxley) to a mature process like manufacturing. In manufacturing, you take high-quality raw materials and a trained labor force, put them through a comprehensive quality control process and the result is a reliable product that everyone trusts. Surprisingly, financial reporting has historically been treated more like a sausage factory – few controls over what's going into business applications and no clear idea of how the financial results were generated. At the end of each reporting period, out comes a 'sausage', with who-knows-what inside the wrapper, being passed off to shareholders as a filet mignon. Without quality controls embedded into the 'factory' that produces financial reports, how can you ensure the integrity of the output?

HW. Compliance can't be treated like a one-time project that can be done off the side of someone's desk. It's a process that must be embedded in the organization, with cross-disciplinary involvement from finance, IT and audit. And it requires that organizations leverage technology to minimize reliance on manual testing processes and people-based controls. By automating controls monitoring at the financial transaction level, companies gain greater visibility into the effectiveness of their internal controls and more reliable financial information – both essential for sustainable and cost-effective compliance.

PB. Many companies treat compliance as a project. They want to know what they need to do to earn a passing grade; cross-functional teams are established and consultants are often hired to make sure that the deadline is met. But this approach is costly and can be disruptive to the or-

ganization as employees are taken away from their day-to-day responsibilities to solve the immediate compliance need. Companies need to look at ways to make their compliance initiatives sustainable over the long term. Many of our most forward-looking customers have approached compliance as its own business process. Some have even gone so far as to create C-level positions that own compliance across the company.

No matter which path you choose, the important thing is that you take a systematic, long-term approach to compliance. Controls need to be clearly documented and there must be a single owner for each control. That individual needs to be responsible for testing and measur-

ing that control. In addition, the best-in-class companies we've seen have automated as much of the compliance process as they can so that they can focus on the exceptions and not consume unnecessary time gathering, documenting and analyzing data. Not surprisingly, these companies have all been able to implement a sustainable compliance initiative without adding additional costs and resources. In fact, companies can frequently reduce resources as they improve their business processes and automate certain compliance-related activities.

How important is 'the tone at the top'? Does compliance need to be integrated into company culture? What are the benefits?

CC. The only way governance policies and controls will be embedded into daily operations is if top management sets the tone at the top. The reality is that executives are just one group of stakeholders affected by compliance, with completely different needs than the other stakeholders (who include internal and external auditors, controllers, line-of-business managers and the IT department). When it comes to compliance, these stakeholders are naturally misaligned with each other, creating an environment that is disruptive, expensive and ineffective.

For example, the internal audit group is charged with making sure controls are in place, and ensuring the integrity of the processes and controls, but they are dependant on the very

people they are auditing to get their information. The line-of-business folks, who are being asked for audit information, see those controls as a burden that makes it harder for them to do their job. What used to be a three-step process now takes eight steps to accommodate the manual controls. What's the incentive for line-of-business to support auditors' compliance needs? There isn't one. But, if governance is embedded into the core business systems used by the employees, they don't have to think about compliance – they just focus on their job.

PB. Senior executives are ultimately accountable for their company's compliance initiatives and so the tone at the top is critical. Unless executives

"The fact is, most companies today cannot respond quickly and effectively to management questions about compliance – their information systems were simply not designed for it" – Jasvir Gill

set a high standard and hold their managers accountable, compliance will always be a second priority. Without exception, companies that have been recognized as best-in-class by their auditors all have a senior business executive who has taken ownership of their compliance program and made it a priority. If rank and file employees see executive management taking compliance seriously and measuring and monitoring their success against key metrics, they will quickly embrace these efforts and make it part of the company's culture.

JG. A positive tone at the top and a regard for addressing compliance in the company culture is extremely important because it paves the way for a better-run business and provides significant business benefits. By improving the way the business is run, managers can boost revenues and cut costs, thereby increasing competitiveness, market valuation and customer retention.

HW. It's critical that it be fully integrated. We've seen what happens when there is unethical behavior in the highest levels of management – just recall the WorldCom and Enron accounting scandals. But let's be very clear: compliance technology alone could not have prevented fraud on that scale. When you have corporate executives intent on defrauding a company and lying to their own audit committees, no technology solution can stop them. But

what an integrated compliance technology solution can do is provide all organizational stakeholders, including external audit and regulators, with greater insight into control breaches and gaps. When business unit owners and financial managers have daily updates on how the internal controls over financial transactions are working, organizations are in a better position to stop fraud – even massive fraud – before it escalates and results in material deficiencies.

How can greater use of IT help support and drive compliance requirements?

HW. It goes back to my earlier point about the importance of taking your compliance activities from a project to a process. Invest in technology that allows you to automate internal controls testing. And don't limit it to a review of static SOD controls, which is frequently the approach taken by IT to respond to this compliance challenge. Make sure your technology solutions can independently monitor financial transactions to identify controls-related issues that cross traditional system silos. Such technology solutions can give management visibility into controls effectiveness across the enterprise, in all core business processes.

PB. IT can help support sustainable compliance initiatives by automating the documentation, testing and monitoring of key business controls. For example, solutions such as Approva's BizRights Platform and Enterprise Controls Suite can enable business, finance, IT and audit professionals to automate the on-de-



CC. The first step many companies took to satisfy compliance requirements was to document their risks and controls. Although there is some value in having a single system of record, if those controls aren't integrated into the enforcement of the policies you still have no assurance your business is running the way it should. The idea of embedded governance is to marry control documentation with control enforcement so you have visibility into your compliance status any time. For example, auditors

JG. Ideally, the CIO and CFO work together very closely to find ways to automate compliance, integrate compliance across the enterprise and implement real-time controls. Companies can achieve this by deploying a compliance and risk management solution to automate testing, monitor controls in real time and deploy preventive controls within their ERP systems and reporting applications. Automation, real-time monitoring and preventive controls eliminate manual sampling and testing costs and break down silos among various compliance requirements.

“We’ve seen what happens when there is unethical behavior in the highest levels of management – just recall the WorldCom and Enron accounting scandals. But let’s be very clear: compliance technology alone could not have prevented fraud on that scale” – Harald Will

mand testing, remediation and continuous monitoring of all of their application controls. And automated solutions can also serve as mitigating controls. For example, they can be used to monitor sensitive transactions such as manual entries to the general ledger. This can help companies significantly increase visibility into their controls, streamline their audit process, lower costs and reduce their exposure to mistakes, fraud and inefficiencies.

need the evidence to measure the effectiveness of controls and assess risk, end-users need built-in workflows to handle exceptions with appropriate approvals and CFOs need early warning to potential problems before they have to be reported. Embedded governance technology in ACTIVE Governance from LogicalApps is unique in that it provides the visibility and assurance that compliance requirements are being enforced in real-time.

Most commentators agree that a ‘tick the boxes’ approach to compliance is not enough. Why is it important that companies make regulatory compliance part of their business culture? What business advantages can they gain from such an approach?

HW. You're right. Good controls that support good governance are simply good business. If your automated controls testing can quickly identify business problems such as duplicate or overpayments, missed discounts or purchases that exceed credit limits, these aren't just compliance concerns – they affect companies' bottom-line performance. At ACL, we have nearly 20 years' experience providing technology to the audit and controls professions, and have seen again and again the importance of embedding 'audit best practices' within organi-

zations' business culture and business processes. It creates a twofold benefit – companies can assure stakeholder confidence and gain a competitive advantage.

CC. By incorporating governance best-practices directly into business processes, managers gain better control over their processes, employees have reduced opportunity for errors or fraud and executives have increased visibility to the overall risk profile of the company. Currently, employees and management think of compliance as an incremental activity – basically, a new tax on the business. If governance is embedded into your business systems, it is integrated into the business culture and, more importantly, it is a non-invasive value-add that is transparent to employees.

JG. An integrated approach to compliance can actually boost revenues and cut expenses. Integrating compliance reduces revenue leakage, prevents errors such as duplicate invoice payments, granting unearned discounts or not taking discounts owed to the company. Integrated compliance also prevents misusing or circumventing controls such as splitting purchase orders to avoid executive level oversight. Integrated compliance also helps to prevent fraudulent activities such as ghost employees or billing schemes.

PB. As regulatory compliance and legislation like Sarbanes-Oxley becomes a fact of life, I think we will start to see a lot more companies take a similar approach to compliance as they did to their ERP implementations in the 1990s. In the run-up to January 2000, everyone rushed to get a new ERP system in place to reduce the risk of Y2K problems. While the business justification was Y2K, these projects forced companies to look at their enterprise-wide business processes, and in the process they made significant improvements. With compliance we've got a similar situation. Almost 10 years have passed since those Y2K initiatives were first initiated and now compliance is forcing companies to take a second look at their business processes as they document and test enterprise-wide business controls. In addition to reducing risk and strengthening their overall controls environment, these compliance initiatives are creating improved insight into their business processes.

Let me give you an example of how some of our customers have strengthened their busi-

ness processes by building compliance into their work processes. In the past when companies added a new user to their ERP system, they had to manually assess the compliance impact. They pored through reports, worked from memory and used rules of thumb to figure out if they were granting people the right level of access in their financial systems. Managers often just didn't have the time to do detailed analysis and so new violations were created every day. Now, with the help of new automated controls monitoring solutions, companies are implementing compliant provisioning systems that analyze the compliance impact of new user requests in real time and make it almost impossible to get a new violation into the company.

What will be the overarching trends in compliance management over the next 18 months? And what will be the key developments?

PB. I think we're going to see companies move from treating compliance as a project to treating it as a business process. Along the way,

we're also going to see material weaknesses and restatements become a lot more common as auditors utilize new tools to look more closely and broadly at their clients' business controls. Companies are also going to adopt these tools as well and try and reduce their audit and compliance costs by automating the testing and monitoring of their business controls. I think we're also going to see large companies start to realize tangible business value from SOX as they treat compliance as a 'business initiative' and gain insights about how to improve their end-to-end business processes. By taking a holistic view of strengthening internal controls companies are going to see a rapid return on investment for their compliance investments.

JG. We expect an increased focus on integrating real-time compliance into business processes across multiple enterprise systems. Ultimately, these trends will lead senior managers to implement leading compliance and risk management solutions like the Virsa ComplianceOne suite, which monitor compli-

ance and mitigate risks in real-time across multiple enterprise applications. Such solutions also break down silos of compliance by addressing multiple compliance regulations in a single, integrated platform.

HW. In the next 18 months, I think we're going to see greater clarity from the PCAOB, the SEC, Big 4 and others on what constitutes effective and sufficient compliance management. For the last three years, companies have struggled to adhere to legislation that made the punitive aspects of non-compliance very clear, but did not offer organizations much direction on how to successfully meet their regulatory obligations.

As a result of this improved guidance, I think we can expect to see greater integration between best-of-breed technology solutions that combine compliance, governance and risk management with financial transactional monitoring, independent of the underlying business applications. We'll also see a growing demand from companies that their compliance activities demonstrate real business value. And final-

"At the end of each reporting period, out comes a 'sausage', with who-knows-what inside the wrapper, being passed off to shareholders as a filet mignon" – Chris Capdevila

ly, we'll see an increased investment in technology that can continuously monitor financial transactions – spurred by the need for both faster payback and increased assurance in the integrity of financial reporting.

CC. This new regulatory climate isn't a temporary condition – it's a permanent change in how business is conducted and how performance is measured. As a result, one of the fundamental developments we're beginning to see is that the traditional approach of auditing based on a point-in-time snapshot, or sampling of the data to ensure its accuracy, is no longer acceptable. The evolving requirement is towards continuous auditing of transactions such that controls can be verified at any point in time. If this can be done cost-effectively, it would dramatically decrease audit costs while providing greater assurance to the integrity of financial information. Forward thinking companies are already laying the groundwork for continuous auditing through embedded governance. ■