BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

The Commoditization of Sarbanes-Oxley Compliance

Lessons learned from ten years of Sarbanes-Oxley to apply to Enterprise GRC management

There are some anniversaries that business may not want to remember, for example December 2, 2011 or July 19, 2012. Those dates signify the ten-year anniversaries of the fall of Enron and WorldCom respectively. For the modern businessperson the question, "Where were you when Enron fell?" is as memorable as, "Where were you when the housing market collapsed?" or "Where were you when gasoline hit $5.00 a gallon?" is not unusual. The enduring legacy of the fall of Enron and WorldCom is not the revealing, rumor filled documentaries and books that followed, but a more far-reaching, and self-sustaining regulation, the Sarbanes-Oxley Act, better known as SOX, passed into law in 2002. Ultimately, during the anniversary it is opportune and prudent to ask, "What has happened to the management of financial controls during the last ten years and what lessons can we learn from it?"

Note

I remember very well where I was when Enron and WorldCom collapsed. I was working for a large Midwestern company with two major business lines, Energy and Telecommunications. This particular company's stock plunged from a previous high of approximately $50.00 a share to $0.75 a share. While the enterprise survived, none of the personnel who were present during this tumultuous period is planning any big anniversary celebrations for the collapse of these two giant American companies.

2002- 2005 Throwing money at the problem

The passage of SOX in 2002 sent publically held companies into a furious race to comply with the regulation. It was a disturbing time for executives and Boards of Directors especially CFOs and CEOs. CEOs and CFOs were not only concerned about the new regulation, but also the possibility of penalties and jail time.

Many companies' risk and control departments quickly mobilized. Departments hastily worked to create a process to identify, test and certify financial controls. The thought at the time by many was that executives may not want to suffer the consequences of non-compliance, but employees did not welcome the thought of losing their job and joining the unemployment line due to another failed enterprise. In fact, at the time, most companies thought this was a short-term requirement that would not last long. Some companies even went so far as to out-source the problem or turn to particular experts within the enterprise. Specialists such as external auditors and internal spreadsheet gurus were used. In many cases, the spreadsheet experts' overlooked talents were now used to formulate complex workflows and spreadsheets. In addition, the external auditors were more than glad to have the billable hours.

Note

The author remembers CFOs proclaiming, "Take care of this new regulation. I don't think I'll look good in prison stripes."

What came out of this process for most companies was a giant, confusing, overreaching and overlapping list of financial risks, controls and convoluted processes to test and certify. Looking back at the time now, many practitioners would think the gurus and auditors, internal and external, were being paid for the volume of risks and controls they produced. The more controls, the better, seemed to be the mantra of the day. One must remember though, that at the time, there were no true guidelines or best practices for this new initiative. There only was the SOX Act and a real desire to not be the next Enron or WorldCom.

Unfortunately, for many enterprises, throwing money at the problem was the solution. In 2005, a study by the Financial Executives Institute (FEI) reported that companies expected

to spend an average of $3 million to comply with Section 404 of SOX. Companies with revenues in excess of $5 billion expected to spend an average of $8 Million.[1] Richard J. Wayman, CFA writing for researchstock.com on March 11, 2005 commented that, "Direct costs consist of the reduction in earnings, earnings growth, and dividends that result from the high cost of complying with SOX. The increased accounting and auditing fees that are required in order to comply with SOX are new and sizeable expenses that increase with the size of the company." [2]

Then, a short three years later, we find that the selfsame executives who were once concerned about non-compliance and troubled with the idea of incarceration for misreporting financials, were now fearful that the escalating costs of SOX would mean there would be no financials to report. As a result, enterprises found that something had to change, but that change was slow in coming.

2006 - 2007
SOX becomes entrenched

On April 30, 2007, the Financial Executives International's website headline read, "FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million -More Companies See Benefit, Note Positive Changes to Audit."
The findings in the article went on to report that, "In the fourth year of Section 404 compliance, accelerated filers managed to reduce costs within direct control of their companies, reporting drops in both internal and external people hours, as well as auditor attestation fees." The FEI provided the following examples of savings.

- Companies reported requiring an average of 11,100 people hours internally to comply with Section 404 in 2007, representing a decrease of 8.6% from the previous year.
- Companies reported requiring an average of 1,244 external people hours to comply with Section 404 in 2007, representing a decrease of 13.7% from the prior year of compliance.
- Auditor attestation fees paid by accelerated filers in 2007 constituted 23.7% of the accelerated filer's total annual audit fees and averaged $846,000, representing a 5.4% decrease from 2006.

FEI President and CEO, Michael P. Cangemi summarized the findings in this way, "As companies continue to find efficiencies in complying with Section 404 and make compliance part of a routine practice, we have seen a continued decline in costs."

What was happening to decrease these once astronomical enterprise costs? Here are some conclusions that the Author has found:

1. Companies came to the realization that SOX was not going away and began to embed and institutionalize the process.
2. Company operations were taking proprietorship of their Financial Risks and Controls. What was once seen as an Auditor's job was now becoming a part of how the enterprise does business.
3. The massive original design work to create process maps, identify risks and controls, build test plans for design and effectiveness, and creating certification roll up processes was beginning to stabilize and steady.
4. The Business was beginning to understand and see the value of their SOX process, past the standard compliance with the Act. The identification of Risks and Controls was creating opportunities for real savings in the enterprise financial process.

5. Control identification and testing halted its attempts to manage everything. Controls began to be segmented into Key and Non-key designations. Key controls became a significantly smaller subset, which reduced testing, and certification time, and resources.
6. 404 requirements were eased somewhat by the government, although their own publications showed it had a negligible impact on overall costs.

2008 - 2012
SOX Compliance Improves

Now, as one looks in the more recent past, just 2011, we find SOX costs have continued to decline. In 2011, Protiviti produced its 2011 Sarbanes-Oxley Compliance Survey. The survey showed that for companies participating in the survey:

1. The cost of SOX compliance was down by 50 percent compared to Year One Costs for companies in fourth year compliance and beyond.
2. Most respondents indicated that the benefits now exceed the cost. Whereas this finding was reversed in year one.

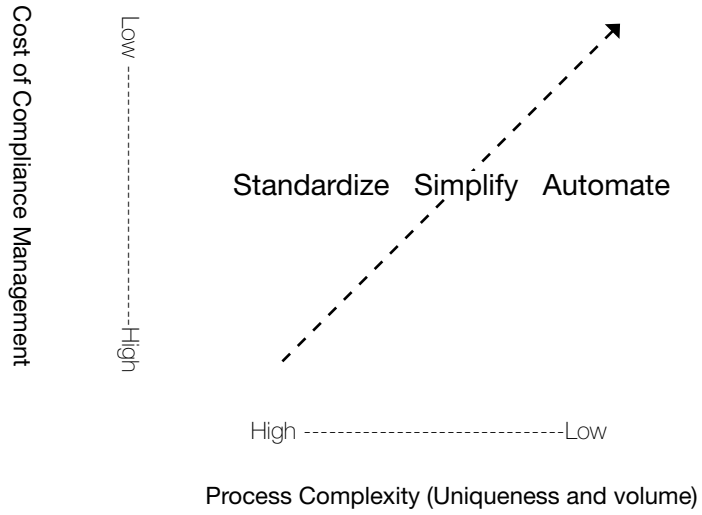

Figure 1. Cost to Complexity

Note

While Figure 1 may seem obvious to the point of being irrelevant, obtaining these results has been a long and costly journey for most companies. At the beginning of SOX, this new opportunity to create and maintain financial control was very profitable for the external auditing firms and extremely expensive for the enterprise.

So what drove this continued decrease in costs and increase in benefit over ten years of compliance and will most probably continue to drive this positive trend? What can other GRC teams learn from this? Commoditization. When a product or service has become indistinguishable from others like it and consumers purchase it simply based on price alone, it becomes a commodity. This commoditization can be applied to GRC initiatives.

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

2012 and Beyond
How the lessons of the past can be used for SOX and GRC in the future

SOX compliance, which started as a bespoke, custom built and tailored effort, unique from company to company, and even more costly for enterprises, unique from business unit to business unit within the same company, is now a commodity process. At any modern enterprise managing SOX compliance, you will find that the SOX process is usually immediately recognizable and understood. Financial departments and their support departments have overcome the myth of uniqueness and distinctiveness. Unfortunately, the same can rarely be said for operational risk management, regulatory and internal compliance, IT governance and the other forms of GRC maintenance at the enterprise. The dreaded "We are special" mindset that drove SOX costs to exorbitant levels ten years ago now infects the other risk and compliance areas.

The lessons that SOX compliance taught us over this recent period are relevant for other risk and compliance projects as enterprises seek to reduce complexity and the costs of GRC initiatives. Here is a set of best practices learned from SOX, which may be used as future guidance.

1. Standardize

a. Stop using GRC silos for compliance, IT governance, risk and SOX. A siloed approach creates insurmountable barriers to effectiveness and efficiency. See your processes as commodities not as unique activities.
b. From the enterprise's organizational structure to processes to risks and controls, create commonality across the GRC groups. The enterprise must ask, are different groups assessing and/or testing the same risks and controls?
c. Reduce the number of risks in the enterprise risk library. A critical review will often reveal a significant number of duplications and redundancies.
d. Reduced risks should bring reduced controls.
e. Find the appropriate risk and control framework and use it as the starting point, but also only use it as a guide. Too often, risk groups try to make their risks and controls fit the framework, rather than modifying the framework to meet the company's needs.

2. Simplify your processes

Risk assessments and control testing are areas of the business where companies may have too much complexity with too little return. These humble questions should be asked:

a. Can the enterprise justify the cost benefit of multiple rating scales and heat maps?
b. Does assessing residual risk still add value? Why is assessing inherent risk not enough?
c. Is there value in complex weighting formulas that have to constantly be explained?
d. Are risk assessments creating clear actionable activities and improvements?
e. Do we have multiple and overlapping testing?

3. Automation of GRC processes

As comfortable as using spreadsheets for risk and compliance may seem to be, they are ineffective, error prone and limit the ability to gain efficiencies.

GRC software systems can dramatically simplify processes through automated workflows, real time data management, continuous controls monitoring and robust reporting.

4. Remember to exercise dogged, persistent and resolute determination to find measurable benefits from compliance activities. Compliance activities such as Sarbanes-Oxley are a proven means to gain efficiency and bring about improvements in the modern enterprise.

What has SOX taught us?

BWise firmly believes in, as do most expert analysts and consultants that a move towards a concerted, integrated approach to Governance, Risk Management and Compliance can significantly assist and improve the modern enterprise, just as SOX processes have helped to improve the financial controls process. The enterprise must begin moving away from silos and individual small projects from department to department. Sarbanes-Oxley compliance has set down and proves to be an ideal manner in which to introduce an integrated approach at the enterprise.

SOX initiatives in real world practice

BWise customers such as an international pharmaceutical leader and a global oil and gas company have seen and experienced profound results as they have integrated their SOX and other corporate initiatives. At the global pharmaceutical enterprise its senior management concluded that it must more effectively manage its internal controls and corporate governance. Using BWise software, the enterprise was assisted to effectively report on its Internal Controls for Financial Reporting (ICFR) and report on the effectiveness of local compliance with regulations such as Sarbanes-Oxley, Japanese SOX and similar regulations throughout South East Asia and South America, without duplication of efforts across the many compliance initiatives. The global oil and gas company was assisted by the BWise eGRC solution to more effectively report on its compliance initiatives. The enterprise must report on a multitude of organizational and financial controls for local, provincial and federal regulators. The enterprise sought to find ways to standardize and reduce the costs of its collection and reporting of these controls. With BWise, the enterprise was enabled to better manage its risks and controls associated with its compliance, while also reducing duplication of efforts. As a result of the program, the enterprise has gone on to add more initiatives to its program such as Payment Card Industry (PCI) compliance.

By using an Enterprise GRC solution, such as BWise, large complex enterprises can more effectively track, measure and manage their organizational risks in one single integrated solution. Such a solution should reduce efforts and increase effectiveness through the gradual reduction in the duplication of controls, commoditization of efforts and decrease in labor and the costs associated with GRC and ERM programs. Please contact BWise for additional information.

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

About BWise

BWise, a NASDAQ OMX company, is the global leader in Enterprise Governance, Risk Management and Compliance (GRC) software. Based on a strong heritage in business process management, BWise delivers a truly integrated and proven GRC platform.

With this platform, BWise supports an organization's ability to track, measure, and manage key organizational risks in one integrated system. By doing so, BWise helps customers to truly be in control by sustainably balancing their performance and financial and reputational risks. BWise enables customers to increase corporate accountability; strengthen financial, strategic and operational efficiencies, maximize performance, and better understand risks. Using BWise, organizations are able to comply with regulations such as Sarbanes-Oxley, ISAE3402/SAS-70, PCI, Solvency II, Basel II and III, Dodd-Frank, ISO-standards, European Corporate Governance Codes and many more.

BWise provides for the GRC needs of hundreds of customers worldwide, across all industries. Customers include adidas, AEGON, Ahold, AngloGold Ashanti, Connexxion, Health Alliance Plan (HAP) of Michigan, LeapFrog, Liebherr, Marathon Oil, Southern Company, Swiss Life, and Transcontinental. BWise has offices in the Netherlands, United States, Germany, France and the United Kingdom. For more information, visit www.bwise.com.

BWise® GRC Platform

BWise offers multiple role-based software solutions for Risk Management, Internal Control, Internal Audit, Compliance & Policy Management, IT GRC and Sustainability Performance Management. Each solution derived from the BWise integrated Governance, Risk management, and Compliance Platform supports the end-to-end process of a given role.

[1] Kristen Crofoot, (April 6, 2006), FEI Survey: Sarbanes-Oxley Compliance Costs are Dropping; Average Compliance Costs are $3.8 Million, Down 16% from Prior Year; Reductions About Half of What Were Anticipated, Financial Executives International, from http://www.financialexecutives.org/KenticoCMS/News---Publications/Press-Room/2006-press-releases/FEI-Survey--Sarbanes-Oxley-Compliance-Costs-are-Dr.aspx

[2] Richard J. Wayman, CFA, (March 11, 2005), The Trickle Down of SOX, ResearchStock.com, from http://www.researchstock.com/cgi-bin/rview.cgi?c=bulls&rsrc=RC-20050311-F

BWise
BUSINESS IN CONTROL
A NASDAQ OMX COMPANY

Contact Information

BWise Headquarters
Rietbeemdenborch 14-18
5241 LG Rosmalen
P.O. Box 321
5201 AH Den Bosch
The Netherlands
Tel: +31 (0)73 - 6464911
Fax: +31 (0)73 - 6464910

BWise, Inc.
1450 Broadway, 38th Floor
New York, NY 10018
USA
Tel: +1 212-584-2260
Fax: +1 212-730-6918

BWise Germany GmbH
Kaiserswerther Strasse 115
40880 Ratingen
Germany
Tel: +49 (0)2102 420 663
Fax: +49 (0)2102 420 62

BWise
19, boulevard Malesherbes
75008 Paris
France
Tel: +33 (0) 1 55 27 37 28
Fax: +33 (0) 1 55 27 37 00

BWise
1 Bell Street
Maidenhead
Berkshire, SL6 1BU
United Kingdom
Tel: +44 (0)1628 421750
Fax: +44 (0)1628 421501

Disclaimer