

Draft
January 18, 2006

Navigating the Compliance and Governance Swamp: A Survival Guide for Executives



Paisley Color Commentary



PAISLEY CONSULTING

Business accountability solutions.

Navigating the Compliance and Governance Swamp: A Survival Guide for Executives

by Tim J. Leech

THERE HAS TO BE A SIMPLER SOLUTION

We recently paid to have the basement finished in a new home we purchased last year. Part of the project included buying and installing our first-ever high definition widescreen television. After reviewing the confusing proliferation of technology options, brands, and features available, we finally settled on one. I came home from work one day and received a “lesson” on how to use the new system from my technology-wise and more patient wife Elaine. There were three separate controllers – one for the set-top box to convert cable signal to digital format, one for the VCR/DVD player, and one for the TV. All three had similar, but different, button configurations and similar, but different, navigation protocols. All three had buttons far too small for my 50 plus year old eyes to see without reading glasses, especially in dim light. As the lesson progressed I became increasingly frustrated and finally said to my wife “All I want to do is watch TV, isn’t there some easier way?”

As a result of a recommendation from our savvy renovators (who also need reading glasses) and an outlay of 400 Canadian bucks we finally found someone that eliminated the need for all three



“specialist” controls and provided us with a single, large button “HARMONY” controller that lights up in the dark. You click what you want to do (i.e. Watch TV, Watch Movie, Play Music, or Play Games) and the frustration and setbacks are history. We now have one simple device

that even I can use effortlessly to watch events of global importance such as the Super Bowl, Stanley Cup or golf in beautiful, high definition, widescreen views. A tool that actually explains what you are doing wrong if you make a misstep. Problem solved.

Tens of thousands of senior level executives and stressed boards of directors around the world are now wishing for a similar, easy to use, reasonably priced, simple solution to help them successfully navigate the increasingly complex, forbidding and dangerous regulatory compliance and governance swamp.

THE SWAMP IS GETTING A LOT MORE DANGEROUS

Each week new stories emerge of executives being charged, put on trial or going to jail, executives negotiating plea bargains to testify against fellow executives, executives being pilloried in

the press for being paid too much/ disclosing too little, executives being sued for negligence and inability to foresee the future, executives being fired to pacify regulators and demonstrate appropriate "tone at the top", corporate fines and settlements that sometimes exceed annual earnings, executives being sanctioned and forced to sign consent decrees to stay in business, executives being forced to disgorge "ill-gotten gains", directors having to personally reimburse plaintiffs and more. Just as the process to watch an everyday TV program has evolved over the past 20 years to an experience fraught with problems, so has the task of keeping even the best run, most ethical companies out of trouble. Executives want to avoid jail time and fines, keep their companies out of the "bad press" limelight, keep their directors' personal assets and reputations intact and, if possible, actually turn a profit and increase stock price.

INCIDENCE OF DEADLY DISEASES AND DANGEROUS PREDATORS IS GROWING

Each year has brought new more complex and onerous laws and regulations that must be managed and complied with. The Sarbanes-Oxley Act of 2002 ("SOX") enacted in the U.S. to address concerns about widespread corporate malfeasance is a classic example. The SEC originally estimated SOX would cost the average company less than \$100,000 to comply. The actual bill is coming in well over \$4 million per company with some larger companies having to spend in excess of \$50 million in round one to comply. Repeated and increasingly vocal complaints to the SEC have, at least so far, met with little more than lip service, delayed implementation dates, and band-aid fixes. The SOX regulatory debacle comes on top of a growing mountain of securities laws and corporate governance legislation like the Health Insurance Portability and Accountability Act

("HIPAA"), the Occupational Safety and Health Act, the Gramm-Leach-Bliley Act, Basel II in the banking sector, and many, many more. Just knowing what laws and regulations a company needs to comply with is a major challenge, let alone understanding them and actually complying to the satisfaction of often inexperienced and work stressed regulatory staff. Senior level executives and boards of directors desperately want a simple and easy to use solution to address the increasingly onerous and confusing compliance and governance burden.

WHAT ARE THE BIG DANGERS IN THIS SWAMP?

1. **The laws and regulations are sometimes complex, confusing and impractical.** Again, the SOX regulations provide a case in fact. SOX regulations have forced CEOs and CFOs of all public companies registered in the U.S. to assert they have effective accounting control systems in accordance with a suitable recognized framework, a framework capable of producing repeatable quantitative and qualitative conclusions. Unfortunately, it would appear that the SEC was unaware that no such generally accepted framework currently exists anywhere in the world. Thousands of CEOs and CFOs are now asserting that their companies have effective control frameworks "in accordance with COSO". Many don't realize that COSO is a committee, not an assessment framework. More than a few CEOs and CFOs couldn't name the categories in the old 1992 or new COSO ERM control frameworks, even on penalty of death, let alone explain the technical support for their COSO effectiveness claims. Their external auditors are OK with certifying these claims since nothing better is available. In "off-the-record" discussions and a new research study

being conducted by the Institute of Management Accountants (IMA), a shocking percentage of companies are admitting that they actually did their SOX control assessments in accordance with Auditing Standard No. 2, the new rule enacted by the young and inexperienced Public Company Accountability Oversight Board set up to police external auditors, not in any substantial way with the old COSO 1992 or new COSO ERM control frameworks.

2. **Companies created new “compliance silos” as new regulatory regimes and dangers emerged.** Just as the task of watching TV and movies has become increasingly complex, so has understanding the output from the growing number of internal compliance and assurance silos and outside consultants devoted to, or at least profiting from, helping companies navigate the swamp. Each year the number of lawyers necessary to try and identify and interpret the steadily escalating blizzard of laws and regulations increases. Thousands of companies have been told that they should hire internal auditors to check and report on the state of danger in the swamp. Some companies, because of the size, complexity and the vigilance of the wardens in their particular swamp (i.e. pharmaceuticals, insurance, banking, nuclear energy, and others), created and staff large “COMPLIANCE DEPARTMENTS” to increase their chances of survival in the swamp. Health and safety departments have emerged in a wide range of industry sectors. Risk and insurance specialists continue to grow to help decide on what to insure, what companies to insure and/or reinsure with, process claims, litigate claims, and other related tasks. Each of these new silos created their own unique language to assess and report on different dangers present in the swamp. Diligent senior

executives and boards needed more and more data from each silo to understand what was really going on.

3. **Business units are being overwhelmed with the demands of the proliferating compliance silos.** As the laws and regulations and the number of specialists to deal with each of the different compliance regimes have increased, so have the demands on the work units that must do the bulk of the work to actually comply with rules. As the compliance burden has increased, the imperatives to generate more revenue and increase stock price have not abated. The work must still get done. Customers must still be serviced. Products and services must still be delivered. Profits must still be generated. Costs must be controlled and reduced whenever possible. The ever present conflict between complying with the steadily worsening blizzard of laws and regulation and growing shareholder value makes navigating the swamp especially dangerous.

TACTICS TO NAVIGATE THE SWAMP

Just as I have found a solution to simplify my life and watch TV without the pain and frustration, new solutions are emerging to help senior executives and boards successfully navigate the compliance and governance swamp.



1. **A common language to communicate is evolving – the universal language of risk management.** The world is increasingly recognizing that the language of risk management is capable of dealing with securities laws,

health and safety, product quality, customer service, environment, fraud prevention, and virtually any area of activity that a public or private sector organization engages in. There is even a global risk management vocabulary, Guide 73, published by ISO, the International Organization for Standardization, to foster a common language. Instead of attempting to understand the different arcane dialects of the external auditor, internal auditor, compliance specialist, lawyers, insurance specialist, safety specialist, quality specialist, HR specialist and others, all can be asked to report to senior executives and boards on the subject of "residual risk status", something that all diligent execs and boards should care about. Residual risks, very simply, are risks that remain after considering "risk treatments" or the controls and/or risk sharing mechanisms in place.

2. **New technology and hardware is emerging to provide a single, easy to understand view of residual risk status.** Just as \$400 bought me a new controller to simplify my TV experience, new integrated risk and assurance management software systems and decision support portals are emerging capable of providing senior executives and boards with a single, real-time view of the most significant residual risk situations, whether they relate to legal compliance, contract compliance, accounting disclosures, cost control, health and safety, fraud, product quality, customer service, environment, sexual harassment or any other area. Companies make money by strategically managing risks. The better risk is managed, the higher the chance of sustained long term financial success and the lower the chance of shipwrecks that have been the fate of Enron, Andersen, WorldCom, HealthSouth, Parmalat Hollinger and many others.

3. **The "SANE GOVERNANCE" lobby movement is growing.** Organizations like the U.S. Chamber of Commerce, AEA (American Electronics Association), the IMA, and others are increasingly taking steps to aggressively lobby regulators for more cost effective and practical laws and rules - laws and rules that achieve what society needs for orderly and responsible conduct of commerce at a lower overall cost and with less frustration, confusion and missteps.
4. **New sources of "swamp survival" guidance and training are emerging.** The arcane and conflicting approaches now used by the many different specialist silos will give way to a common approach all organizations, both public and private sector, can use to assess, manage and report on the true residual risk status in their organizations. The IMA announced in December 2005 bold new steps to launch a more management centric, simpler, easier to understand and apply risk and control assessment and reporting framework. The IMA has called on other associations around the world to join with them to create and maintain a simpler, more cost effective assessment and reporting framework.

SAFELY NAVIGATING THE SWAMP IS POSSIBLE

Just as naturalists regularly and vigorously assert that swamps, rather



than being forbidding and dangerous places, are, in fact, beautiful and an important part of our environmental eco structure, there are signs that navigating the compliance and governance swamp is not only possible, but can be hugely rewarding over the longer term. Organizations, executives and boards

willing to support and implement the new swamp survival tactics and tools will be able to successfully navigate around the dangers and pitfalls, realize the full benefits available and, most importantly, get on with the business of doing business.

ABOUT THE AUTHOR

TIM J. LEECH, FCA·CIA, CCSA, CFE, MBA

Tim J. Leech is Principal Consultant & Chief Methodology Officer with Paisley Consulting, the world's leading provider of integrated business accountability software and training solutions. From 1991 to 2004 Tim was CEO and founder of *CARD[®] decisions*, a global pioneer in the ERM and CRSA areas. Paisley acquired *CARD[®] decisions* in June of 2004. Other positions he has had include Managing Director of a subsidiary of the Hambros Bank, Director Control & Risk Management Services with Coopers & Lybrand Consulting, and a range of comptrollership and internal audit roles with Gulf Canada. Tim was elected Fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession.

Leech's responsibilities include providing design advice on all Paisley software products; consulting and training services related to Sarbanes-Oxley, Basel operational risk management, enterprise-wide risk and assurance management; Collaborative Assurance & Risk Design™ ("*CARD[®]*") training and software development; control and risk self-assessment ("*CRSA*") training and implementation services; specialized litigation support services; business ethics advisory services; internal audit training and consulting; and control/risk governance consulting services. He has provided training for public and private sector staff located in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. Leech has received worldwide recognition as a pioneer and thought leader in the fields of enterprise risk and assurance management and control and risk self-assessment.

ABOUT PAISLEY CONSULTING

Founded in 1995, Paisley Consulting is the recognized leader in providing more than 1,200 organizations—including 35 percent of the Fortune 100—with comprehensive and tightly integrated solutions to better identify and reconcile the risks impacting organizations, thereby ensuring that evaluations of operational risk are completed quickly, consistently and accurately.

Leveraging industry best practices, a common technology platform and a unified database to facilitate standardized, automated and collaborative processes across the enterprise, Paisley Consulting customers are empowered to improve the accuracy, consistency and efficiency associated with Sarbanes-Oxley compliance, internal audit, general compliance and operational risk management initiatives. Developed for companies of every size and across multiple industries, Paisley Consulting's solutions can be implemented as an integrated whole for maximum value or may be deployed as individual point solutions. Either way, our best-of-value solutions can help you reduce costs and target opportunities for continuous improvement.