White Paper
IT GRC: A Unified Approach

WP0201 | August 2015

Michael Lane

Mike is a respected technology professional with nearly 20 years experience, having held senior manager positions in Information Technology, Communications and Consulting.

Over his career he has managed a vast number of Telecoms, IT, Business and Consulting projects and programmes, and the associated global cross functional teams, with a strong track record of results. Mike is a specialist in many aspects of information technology, including infrastructure, architecture, systems development, business processes, service management, policies and standards, leadership, governance and management.

Summary

There may be no such thing as the 'Perfect Storm', but when looking back over the last decade or so one can argue that the severity and number of adverse Enterprise events and factors which unfolded on a global basis more than warrant consideration for being branded with such a title. Call it what you will, but from the start of the new millennium when Enron collapsed and crashed, the world entered a period of unprecedented corporate and later governmental crises that not only left indelible memories, but embedded wounds that are still healing today and changed the game forever.

From the United States of America's Levin-Coburn, to South Africa's King III to the United Kingdom's Cadburys, a range of reports surfaced detailing root causes, and offering counter-measures and solutions to avoid and prevent a repeat of what had happened previously. The analyses were intense and unforgiving, the identified failures deep and wide, and the prognosis was to adopt transformational change or ascend into perennial chaos, recession and depression. Indeed, the outlook alone was incentivization enough to catalyze sweeping reforms focused not only on regression but assuring progression to a brighter future than ever before.

Out of the fire new micro, macro and market environment demands emerged, fueled by the shortcomings of the recent past, and necessitating organizations to operate on a new playing field. Enterprises were not just to be challenged to transform practices and cultures, but were to be mandated to do the right things, to make the right decisions,

and to follow a path of sustainable value creation. What better place to start than with the status quo.

It didn't take long for enterprises to diagnose these new bound necessities as more than things they simply had to satisfy and tick-off, but rather as openings to differentiate and build competitive advantage. And so they began to seek solutions for the fresh regime they faced, and to help them meet their contemporary obligations and needs as efficiently and effectively as possible. Organizations quickly began to realize that not only was it essential for the left hand to know what the right hand was doing and vice versa, but that actually holding hands armed them with even greater business strength, agility and opportunity.

With that in mind, it was no surprise at all when a new concept surfaced that looked to cohere the missing links, to unify and empower the business in these new environs, and use IT to do it… Enter the glue that is IT Governance, Risk and Compliance or as it's more universally known – IT GRC – and the business world will never be the same again.

Unifying Governance, Risk and Compliance: IT GRC

Traditionally, many organizations didn't have Governance or Compliance functions within their enterprise architectures and when they did, they were likely to have been informal, rather than adequately resourced and well-practiced and Risk management was typically contained within the finance department or domain of the enterprise rather than organization wide. As management theory evolved and the concept of Governance began to emerge and establish itself as an independent and essential function in its own right, organizations slowly began to qualify and quantify their need for good Governance in the business. In parallel, driven by a variety of internal and external factors, so too did the world of Compliance start to rise to a level of some prominence within the organization. In the eighties and nineties a stereotypical blueprint of the enterprise began to take shape, where isolated and incongruent disciplines of Compliance, Governance and Risk Management were a common, albeit disparate, trio (feature).

It was therefore the norm when enterprises entered the twenty-first Century to be managing these functions or disciplines in silos. What is concerning though, is that many organizations, to their detriment, still find themselves in that very same boat, 15 years down the line. Especially, considering what has happened all around us in between. But it didn't come as a surprise when Enron collapsed, or when Lehman Brothers went down… as the saying goes "If in silos we stand, in silos we'll fall". What does surprise me nowadays is any contemporary organization that still chooses to manage their Governance, Risk and Compliance in silos. Give me a reason why, and I'll give you a hundred why you shouldn't…

The operating environment of any business in the 21st century is characterized by a complex web of regulatory and compliance prescriptions, ever changing and potentially devastating enterprise risk, and an exponentially increasing level of global competitiveness and accountability. For many businesses, simply staying alive is burden enough, never mind trying to irk out an advantage over the company next door. The clear and ever present threat of failure and liability looms large in a landscape where every big decision feels of strategic consequence, and the pressure to make the right one, and fast, never seems to subside. Comply or fail, risk or return, the right things or the wrong ones… businesses today are faced with tough challenges every single day, and they want it all - complete compliance, rationalized risk and good governance. But how on earth can you get it all, is there a solution? The answer is yes.

Governance, Risk and Compliance never have and never will exist in vacuums. They go together as much as bread and butter. By their very definition alone, they are intrinsically intertwined. IT Governance, Risk and Compliance, or IT GRC, is the solution that unifies these once silo'd disciplines into a whole that is far greater than the sum of its parts. By integrating these interdependent functions through a unified IT GRC approach, organizations are able to empower themselves to make better, smarter and faster strategic decisions than ever before. In doing so, enterprises that choose IT GRC position themselves to create competitive advantage and sustainable value in the long term, more efficiently and effectively than those with unaligned governance, risk and compliance efforts in their organizations.

Boards of Directors across the globe are tasked with ensuring and assuring enterprise performance and conformance, and satisfying the primary governance objective of sustainable value creation for today, tomorrow and the future. Stakeholder demands and requirements mandate that organizations are continuously doing the right thing and when they stray off the righteous path, it is necessary that prompt and effective active direction is provided and corrective action is applied to get their business back on track. Internal organizational policies and strategic direction, set by the executive levels with the enterprise, serve as the guidance, framework and parameters within which an organization operates and delivers its products and services to meet its strategic goals. Put another way the Board of Directors, or in SME's a managing team or individual, are there to steer the organization to create value, whilst optimizing the deployment of the enterprises resources and minimizing the risk exposure to the business. It's a common misconception that governance, and strategy for that matter, are one-offs or done once a year only. In reality governance, like strategic management, is implemented on an ongoing and continuous basis and relies extensively on timeous, accurate and relevant information being made available for active review and decision making. So when it comes to executing governance in the enterprise of the new millennium, information technology plays a vital role in its success or failure.

But governance alone, or in isolation, is not enough. Organizations today exist in an environment of unrelenting risk and uncompromising compliance. Fail to effectively manage risk and meet compliance prescripts, and you will have failed to govern the organization. Fail to govern the organization and the very life of your entity will be at risk. New business risks can spring up at anytime from anywhere, just as new compliance requirements can come into play from a growing number of sources. Continuous scanning of internal and external environments for new or changed risks and requirements is a critical component of governance for the modern enterprise, as organizations strive to stay one step ahead and avoid being hit by the proverbial train. Forward thinking organizations have come to realize that IT GRC acts as a central integrator, driving communication and collaboration between an enterprises processes, information flows and initiatives constituting the organizational wide Governance, Risk and Compliance undertakings. Whether it's internal controls for Sarbanes Oxley, an ISO standard or internal policies which need to be complied with, a new competitor on the block which requires a risk mitigation strategy or evaluating the performance of the organization, IT GRC is able to create a unified information architecture to meet even the most complex of enterprise needs.

Today, we don't need to wait for static reports from various functions to be presented and then spend hours or days trying to reconcile them. We can have real-time information that tells us where we went wrong, what could hit us, or that we need to meet a new regulatory requirement. We can become more efficient in implementing Governance, Risk Management and Compliance in the organization, by automating processes, reducing manual and often duplicate human effort, and making smart information available to all stakeholders for more effective business decision making, all through the adoption of a unifying IT GRC approach.

Conclusions

Information technology has pervaded nearly every aspect of our organizational and social existence, and is key for almost every enterprise's operation and survival. We used to say that IT needed to be aligned to the business strategy and objectives, but today it's far more than that. IT is no longer just a support function, or a contributor, it's a true enabler within the organization. IT enables organizations to do things and go to markets they perhaps never thought possible, to create new strengths and opportunities, reduce threats and weaknesses, and to bring people, processes and products together. What we have learned since the dawn of the new millennium, is that organizations without good governance can and do implode, with dire consequences.

Organizations of every size and description, in any industry, in any part of the world, are trying to come to terms with the overhead and seemingly onerous demand for sound governance, effective risk management and comprehensive compliance. With disparate pockets of people, processes and technology all attempting in their own way and using their own systems to provide these critical business functions, it should be expected that the results will be less than optimal and in most cases simply not good enough.

Governance is tasked with overarching oversight spanning the length and breadth of the organization, every function and department, every action and inaction, and to assure the business is performing and conforming as required. Risk Management is tasked with keeping risk levels in the business in line with its risk profile and appetite, and maintaining mitigation strategies for dealing with risk of all types be they corporate, operational, financial, technological or reputational. Compliance is there to ensure that the enterprise is satisfying every organizational and regulatory requirement and continually preventing a state of non-compliance. And IT GRC is the glue that bonds it all together.

IT GRC purports and delivers a unifying platform for the delivery of the enterprise's full portfolio of governance, risk and compliance processes and projects. By providing a consolidated, single-view across the organization, IT GRC has been able to fill the gaps left by entrenched silo based efforts of enterprises to realize their GRC goals. A new breed of enterprise has emerged, not only looking to placate stakeholders, shareholders and regulators alike, but for a solution it can use as leverage to empower them to make more informed strategic business decisions, better, cheaper and faster than ever before, for the benefit of the business. By unifying Governance, Risk and Compliance activities of the contemporary organization into a single solution, IT GRC is able to provide exactly that and perhaps give your organization just the competitive edge it needs on the never-ending quest for sustainable value creation. After all, wasn't it Aristotle who said "The whole is (always) greater than the sum of its parts" – IT GRC, why wouldn't you want to unify?

Additional Reading:

http://www.orbussoftware.com/governance-risk-and-compliance/

References

ISACA and Deloitte Governance, Risk and Compliance [PDF] Available from: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20132305%20Governance,%20Risk%20and%20Compliance.pdf [Accessed June 2015]

http://www.metricstream.com/solution_briefs/Unified_Governance_Risk.htm

http://grc2020.com/2014/11/04/unified-compliance-framework/

http://commissum.com/services/managed-security/unified-governance/

http://robertkugel.ventanaresearch.com/2012/07/12/companies-need-unified-approach-to-grc-for-it/

Orbus Software UK
London

Orbus Software US
New York

Orbus Software AUS
Sydney

Orbus Software RSA
Johannesburg

enquiries@orbussoftware.com | **www.orbussoftware.com**
Seattle Software Ltd. Victoria House, 50-58 Victoria Road, Farnborough, Hampshire, GU14 7PG. T/A Orbus Software. Registered in England and Wales 5196435