Solving Real Business Problems, Not Just Hypothetical Ones

Effective governance, risk management, and compliance (GRC) delivers the ability to meet requirements, achieve human and financial efficiency, and meet the demands of a dynamic business environment that requires agility. It eliminates silos of risk and compliance that emerge from parts of the organization that have historically worked independently of each other.

The goal is to provide a process, technology, and information architecture that can be used for a range of GRC purposes throughout the organization. To make the solution effective, however, different business roles must share information and work in harmony. Harmony is a vital GRC concept: Harmony means various risk and compliance roles cooperate, collaborate, and share, to create a big picture of GRC and make sure the organization is properly governed.

When it comes down to it, the “GRC” acronym is not important. There are many GRC initiatives that do not use the term. The goal is the same — to drive efficiency, effectiveness and agility across risk and compliance processes to support a dynamic and extended business environment. GRC is about process improvement, technology automation, collaboration, and sharing of information.

Software vendors often confuse organizations about what GRC is, and in an effort to land a bigger deal, ignore the real needs of the business. GRC is about solving real, existing business problems while enabling a collaborative approach to address areas of future interest. GRC initiatives are often impaired by the legion of vendors marketing their solutions and labeling them GRC. Many vendor searches struggle with:

- **Ignorance:** Vendors betray their ignorance by talking about GRC as a technology. GRC is broader than technology — it starts with strategy.
moves into process, and technology becomes the enabler. Without GRC strategy and processes, the technology will not be effective.

- **Generic messages**: Vendors use a generic message, and come into buyer situations telling them they have the best and most adaptable solution available — it slices, it dices, it does your laundry. They miss the point — GRC is about solving problems, and generic answers do not cut it.

- **Fixing huge organizational problems to get the big deal**: A serious issue is the fact that the many GRC vendors are focused on large enterprises, and are pressured to close the big deal. Vendors come into a situation trying to fix organizational political issues and silos the organization is not ready to address. Many GRC strategies are trashed or postponed because vendors insist on making the deal bigger than what the organization is ready for today.

**GRC starts focused on specific issues and then tackles others**

With new risk and compliance issues constantly coming to bear, organizations need to tackle the problem at its roots with a GRC strategy that can focus on specific issues, and then moves on to others. The goal is to define a common GRC strategy — a methodology, framework, process, technology, and information architecture to address today's critical risk and compliance issues — that is also flexible enough to address other issues later on. You cannot boil the ocean — taking on too much will only lead to frustration and disaster.

The old paradigm of reactive and fragmented risk-management is a recipe for disaster. A reactive approach leads to siloed initiatives that never consider the big picture. The result is complexity, redundancy, and failure. These outdated processes don't look at how GRC processes can be architected to meet a range of needs over the long term, while solving today's critical problems. An ad hoc approach to GRC results in poor visibility across the organization and its control environment, as there is no framework or architecture for managing risk and compliance in a cohesive context.

What may seem like an insignificant risk in one part of the organization may very well appear more serious when other relationships are factored in. Organizations that lack structures for GRC face inefficiency, out-of-sync controls, and inadequate corporate policies. Organizations fail and are encumbered by unnecessary complexity because they manage GRC as point-in-time projects, and not as an ongoing process. Executives are becoming aware that these redundant projects waste time and resources with manual and laborious assessments that fail to provide accountability at all levels of the organization.

The cost to the business of inadequate GRC processes is significant. Areas where organizations report significant issues and cost include:

- **Excessive paper and spreadsheets**: Organizations rely on manual paper trails, email, and spreadsheets to deliver surveys and assessments with little or no accountability or follow-through. This approach lacks a clearly defined audit trail, and does not allow for non-repudiation. It's not possible to verify that someone who answered a question did not change their response later to cover a trail or paint a rosier picture. Multiply this by the thousands of documents and emails that manage risk and compliance and it grows quickly out of control.

- **Limited and fragmented reporting**: Trying to make sense of data collected in both manual processes and electronic documents is a nightmare. How do you aggregate and provide meaningful reports from hundreds or thousands of disparate sources of information? The answer: A lot of labor and time.

- **Files and documents out of sync**: Adding to this behemoth of labor is the effort to track and control versions of all of these documents, which quickly become out of sync, effecting their accuracy and relevance.

- **Significant spend on auditors and consultants**: Legions of out-of-date documents mean more work for auditors and consultants who come in to validate and attest to risk and compliance practices. The more incomplete, inaccurate, and complex sources of data they have, the more these resources cost.
In today’s environment, ignoring GRC means that processes, partners, employees, and systems will behave like leaves blowing in the wind. Risk and compliance issues and corresponding processes are constantly coming to bear on the business. GRC solutions that operate autonomously introduce further risk in today’s complex, dynamic, and distributed business environment.

**GRC Delivers Value to the Business**

Organizations need to focus on addressing the burning issues in front of them, but make sure there is enough flexibility to address tomorrow’s problems. An effective GRC strategy enables organizations to proactively protect the organization by aggregating and reconciling information, assessments, policies, controls, risk, and the processes that ultimately monitor and control them.

This requires a GRC technology and information architecture that allows risk and compliance processes to deliver on business agility, efficiency in human and financial resources, and effectiveness in meeting requirements.

A GRC application focused on solving real business problems achieves:

- **Agility**: Organizations need a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that have become onerous. Further, organizations need to sustain risk and compliance management practices on a continuous basis, as business continues to change rapidly. The dynamic nature of business demands that an organization address GRC collaboratively and continuously.

- **Consistency**: Organizations require multiple roles to work together in an integrated framework and technology architecture. Consistency must be part of the technology environment where risks, requirements, and controls are defined and directly integrated into business processes.

- **Efficiency**: The line-of-business is pushing back on redundant assessments, policies, controls, and audit processes. Redundant calls for similar information for different purposes gets in the way of getting business done. Effective GRC eases the burden on business by leveraging common processes, assessments, and information through technology integration and enablement.

- **Transparency**: Business demands transparency across performance and risk to monitor the organization’s health, take advantage of opportunity, and avert or mitigate disaster. Managing GRC in the context of business is essential.

- **Accountability**: Organizations are in the hot seat — multiple risks, mandates, and requirements are attacking from every angle. This requires a system of accountability where executives can see the status of GRC issues, events, incidents, and unresolved findings, and hold individuals accountable for their resolution. When issues arise, a lack of accountability and ownership of specific issues is a warning sign for regulators or investigators to dig deeper.

**Easy2Comply Delivers GRC that Makes Business Sense**

As they approach GRC, business must focus on fixing specific problems that effect the organization today, with plans to expand and take on others over time. Organizations want to leverage processes and technologies for other areas — but first, they need to solve the problem before them. This requires vendors to select a software vendor to support their GRC strategy as it grows. Vendors that want an enterprise deal up front are doomed to be unsuccessful as they take on too much too soon.

Easy2comply is a technology solution from Dynasec in the GRC space that Corporate Integrity has researched and evaluated. With customers across the U.S., Europe and Middle East, they have over 50,000 users on easy2comply to solve mission critical business GRC issues. Easy2comply delivers capabilities that address the specific need for organizations to:
Gain control of current business problems: Easy2comply streamlines the management of risk and compliance across existing and emerging issues. Easy2comply implementations reduce GRC overhead by an average of 50% annually by decreasing the time required to manage GRC processes while empowering management with improved reporting and information flow.

Build with the future in mind: Easy2comply enables companies to effectively manage pressing issues today and expand to multiple GRC processes on a single platform in the future. Implementations can span the management of a single regulation or multiple GRC processes such as internal control, Sarbanes-Oxley (SOX), operational risk, Basel II, Solvency II, ITIL, ISO27001, internal audit, business continuity management (BCM), reputational risk, and FSA.

Address current risk and compliance realities: The Easy2comply platform is comprehensive and supports existing and emerging regulations with built-in best practices, full functionality, and adaptable workflow. Rapid implementation in an incremental approach enables organizations to minimize time, cost, and impact on normal daily operations. Easy2comply is flexible and customizes to the way the company operates, instead of requiring the company to adjust to the application.

Provide business value: Easy2comply minimizes risk of regulatory non-compliance with enhanced risk management capabilities. It provides centralized control of GRC processes on a single platform and information architecture, allowing for independent, yet integrated modules that reduce the time, cost and effort required to manage GRC functions.

The right delivery model: Easy2comply offers the organization a flexible choice in implementation that scales to the needs of the business problems before them. An organization can choose a Software-as-a-Service model — cost effectively minimizing the support required from IT operations and infrastructure — or a traditional on-premise software implementation.

Easy2comply by Dynasec is a GRC vendor that delivers on GRC process automation and reporting. The end result is that customers have confidence in the accuracy and integrity of GRC processes. This confidence around proper oversight enables better interaction and allows business teams to properly manage risk and compliance issues pressing on the organization today. For executives, this closes the loop between top-level corporate strategies and risk management, and the risk and compliance processes the business uses to deliver real-world results.

About this Paper . . .

This white paper is brought to you by Dynasec, a provider of Governance, Risk Management and Compliance solutions offering the easy2comply family of practical and reliable GRC applications. These solutions can be deployed either on-demand (SaaS) or on-site to suit each customer’s preferred configuration. easy2comply adapts to any business environment by offering a flexible, cost-effective alternative than standard GRC solutions.

The easy2comply platform provides tools and functionality that enable building a powerful, long term GRC architecture in which each compliance application can be managed autonomously, while sharing relevant information with the other GRC projects running in parallel.

Whether you manage a single regulation or multiple GRC processes such as: Internal Control, Sarbanes-Oxley (SOX), Operational Risk, Basel II, Solvency II, ITIL, ISO27001, Internal Audit, Business Continuity Management (BCM), Reputational Risk, FSA, general compliance, internal policies and procedures, special projects, local laws and more, easy2comply helps organizations worldwide achieve on-time, cost-effective and manageable GRC.
About Corporate Integrity . . .

Corporate Integrity, LLC is a GRC strategy advisory firm providing leadership in education, research, analysis, and advisory services by monitoring the challenges and trends of the business roles accountable for corporate governance, enterprise risk management, and compliance (GRC).

Through ongoing research, interactions, and analytics Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” - where integrity is central to governance, risk, and compliance (GRC) practices. Corporate Integrity educates organizations - and GRC professionals within those organizations - on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices so they maintain a position of integrity aligned with corporate values and business performance.

About Michael Rasmussen . . .

J.D., CCEP, OCEG Fellow: Risk & Compliance Lecturer, Writer, & Advisor

Michael Rasmussen is an authority in understanding Governance, Risk, and Compliance (GRC) processes. He is a sought-after keynote speaker, author, and advisor on risk and compliance issues around the world and is noted for being one of the earliest advocates for GRC.

With more than 15 years of experience, Michael’s objective is to assist organizations in defining GRC processes that are efficient, agile, effective, accountable, and transparent.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in “Governance and Compliance: Saving the Planet and the Corporation.” Most recently, in October 2008, he was recognized as a “Rising Star in Rocky Times: Corporate America’s Outstanding Executives Under the Age of 40.”

During his career, Michael has worked in market research, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and ‘top analyst’ at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael’s educational experience consists of a Juris Doctorate and a Bachelor of Science in Business. Michael is currently in the Master of Divinity program at Trinity Evangelical Divinity School.