Enterprise Risk Management vs Governance-Risk-Compliance: An Introduction

Enterprise risk management (ERM) and governance-risk-compliance (GRC) are fledgling industry categories, having only been recognized for approximately ten years. As such, there are many conflicting views even within industry circles on the scope of ERM v GRC practices. Further, ERM and GRC processes and software may be incorporated as methodologies or modules into related domains such as business intelligence (BI) and enterprise resource planning (ERP). Make Sence Florida, Inc. recognizes a clear distinction between ERM and GRC.

ERM vs GRC

In the current understanding of governance, risk and compliance (GRC) within an enterprise, GRC is a holistic methodology enabling a top-down approach to enterprise governance, risk and compliance. The ideal implementation of GRC is believed to result in a trickle-down indoctrination of corporate risk attitudes from the executive level to the enterprise front lines.

The current reinforcing understanding of enterprise risk management (ERM) within an enterprise is that ERM is a useful rib in the protective umbrella that is GRC. ERM is viewed as a risk-centric methodology that utilizes source data collected into risk databases to provide risk reporting to enterprise divisions. The ideal implementation of ERM is believed to ensure an effective enterprise response that acts to mitigate or eliminate risks to enterprise assets and objectives as prioritized within the GRC-endorsed model.

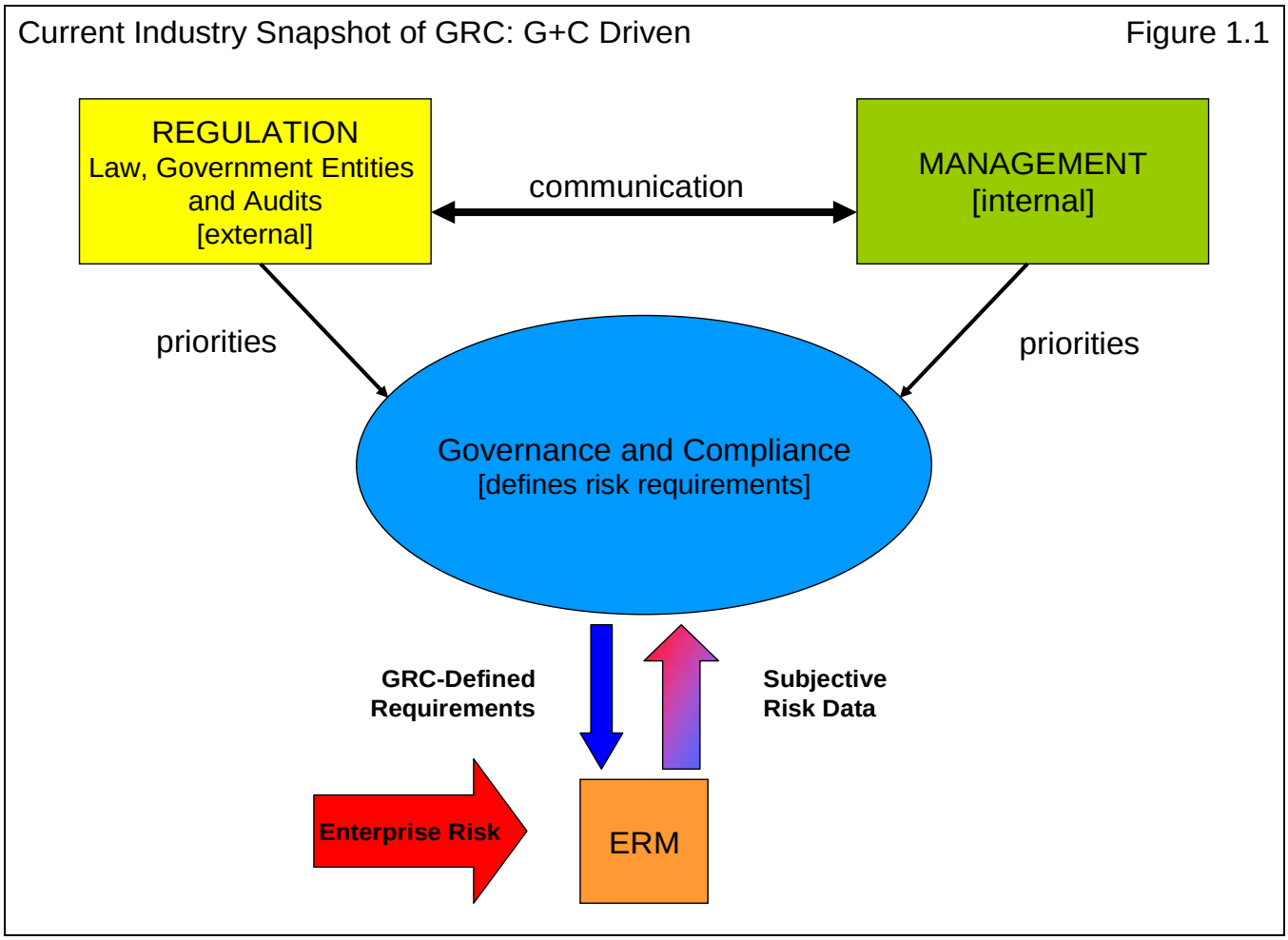
These views of GRC and ERM are fantasies.

In fact, genuine ERM is a disciplined, scientifically approached risk-driven methodology that utilizes enterprise risk data to inform governance and compliance policy. When implemented properly, ERM will effectively minimize risks to enterprise assets and objectives.

In contrast, GRC is a fiat-driven regulation and compliance-facing, management and governance pseudoscience designed by and for largely bureaucratic objectives. GRC may poorly align with facts and realities of a particular enterprise's actual risk environment. GRC currently pulls from ERM resources to validate GRC-endorsed business processes and functions. The power that GRC is currently accorded over ERM ignores a vital truth:

Risk management is the most important discipline that must be mastered by an enterprise.

Current Industry Snapshot of GRC: G+C Driven Figure 1.1



As seen in Figure 1.1, management and regulatory bodies act on governance and compliance divisions, which then set and prioritize risk issues to be addressed by ERM divisions. ERM divisions evaluate any identified risks and then inform governance and compliance divisions as to the range of risks and mitigating procedures for those risks. This information is then passed along by GRC back to management and regulators. Management is then expected to formulate strategies and make decisions based upon this information.

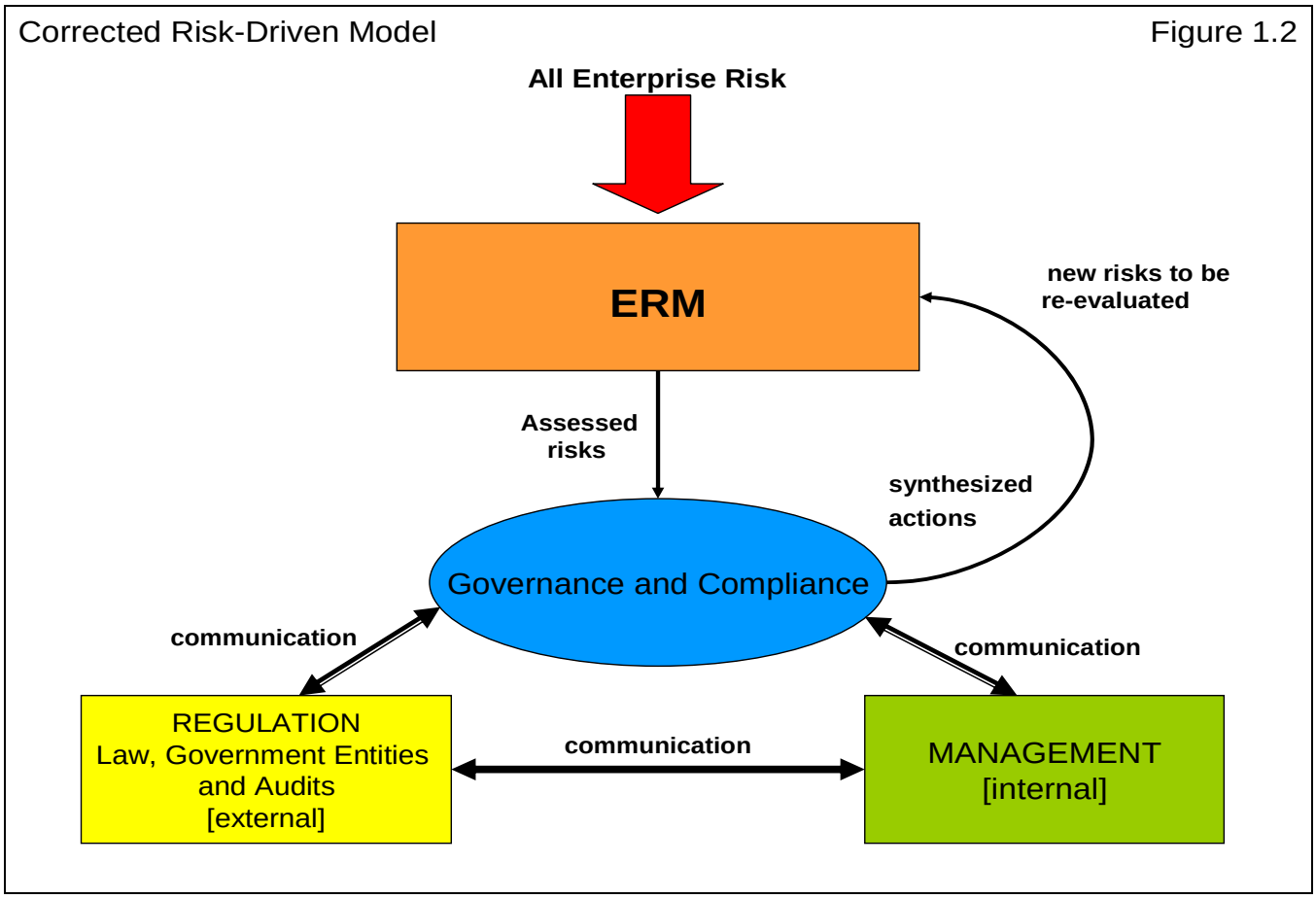
Despite popular belief in the risk-centric nature of GRC, GRC's actual interests in real business environments are vastly different. Governance and compliance functions are aimed at satisfying federal and state regulators as well as external auditors. This GRC focus is primarily driven by executive aversion to the penalties and consequences imposed by regulators and boards of directors if regulations and policies are breached. The scope and volume of risk reports generated by GRC are intended to insulate executive and line management from the consequences of adverse events, regardless of actual culpability. When external entities and governance, compliance and management entities make inquiries, the reports are produced to prove that the laws and regulations were followed to the letter.

Under a dominant GRC regime, risk profiles and mitigation procedures may not cover the actual risk landscape in which the enterprise operates. Governance and compliance divisions may not understand that entire risk landscape, but still seize responsibility for formulating the scope of risk requirements.

Risk management divisions receive poorly defined requirements and duly deliver muddled data sets. Subsequent evaluations derived from risk reports may underrate critical risk issues that threaten actual corporate interests, and overrate risks that appear to have greater impact on favored corporate policies. The policies based upon evaluations are biased or distorted in favor of bureaucratic concerns. These distorted policies are then propagated throughout an entire organization.

When adverse risk events occur, mitigation procedures are found to be ineffective and result in high impact consequences. Ensuing internal investigations are hampered by the inability to properly identify risk owners. In an organizational failure, no single division is found to hold ownership of either process or risk. The limited latitude allowed to ERM divisions to objectively assess the domain of risk creates gaps in enterprise risk intelligence. These deficits can result in poor decision-making, adverse risk events and potential loss of enterprise reputation, revenue and market share.

Corrected Risk-Driven Model Figure 1.2



ERM is commonly viewed as a part of GRC. It should not. Risk acts as a force on all enterprise inputs, outputs, processes and assets, and is therefore pervasive throughout an enterprise. When ERM best practices are in place, they require that governance, compliance, management and regulatory concerns do not define enterprise risk aptitude but instead adapt risk aptitude to align with real world threats. Risks, whether external or internal, can act on any breach point of an enterprise. Wherever the primary breach point may be, it is the role of embedded risk teams that specialize in risk disciplines to assess and report risks to a centralized ERM. As seen in Figure 1.2, ERM then formulates a risk mitigation strategy

based on facts. Timely comprehensive reports are communicated to operational entities, and senior management tiers, and regulators. Using these reports, management synthesizes strategies in consultation with ERM, governance and compliance process owners. The well-constructed policies that result from such composite-build strategies are then implemented throughout the organization. Ownership of risk is clear: risk discovery, identification, assessment, reporting and response are the responsibility of a centralized ERM and its embedded specialists.

In real business environments, truly holistic risk-centric enterprises require all divisions - not just governance and compliance - to adapt operations to mitigate all external and internal risks to enterprise assets and objectives, using ERM-validated assessments and responses. Shifting risk responsibility entirely to ERM ownership reduces inter-divisional workloads drastically, allowing each division to properly focus on its primary discipline. Effective communication between embedded risk specialists and centralized ERM creates clarity and increases the impact and value of enterprise risk intelligence. Further, as a historical database is built, risk intelligence is integrated into a holistic, data-driven and flexible enterprise risk framework. Such a framework supports a more comprehensive and complete knowledge of the risk landscape.

With empowered ERM divisions, executive benchmarks are informed and set by the facts of enterprise risk, not pervasive misconceptions. In turn, governance and compliance divisions are able to focus solely on risk-driven policy management, regulatory compliance and audit compliance. This reinforces the conclusion that governance and compliance success flows directly from competent ERM implementation.

Business and risk communities worldwide are well aware of the issues Make Sence, Inc. has identified in current GRC/ERM roles and implementations. A substantial corpus of material has been published supporting these conclusions on the misalignment of GRC and ERM in enterprise environments. Our analysis of that material is validated by recent well-documented and highly public failures of current risk practices by high profile players in critical industries. In subsequent sections of this dossier, critical issues identified in the preceding paragraphs will be examined in-depth:

- How conflicts between executive, governance, risk management and compliance tiers and the subsequent consequences of those conflicts affect enterprise functions, assets and objectives.
- Why successful governance and compliance flows directly from competent ERM implementation. What undesirable outcomes can occur when governance and compliance are given dominance over ERM.
- What impact massive data and inadequate data have on effective data gathering, and data dissemination, collection, analysis and reporting. The specific industry problems directly related to incorrect use of quantitative and qualitative methodologies will be examined.
- Why existing software product implementation have similar weaknesses and consequences of those weaknesses to enterprises.
- What is the current structure of the risk management industry, and how it contributes to the risk management issues of GRC and ERM. How the industry would be transformed by enterprise realignment to a comprehensive ERM implementation.
- Who are the current industry players and companies of interest. A comprehensive SWOT analysis will be used in a side-by-side assessment.

- Why a new ontology of risk is needed. A new risk ontology rationalizing the discussion of risk by academics, risk experts and industry professionals will be presented.
- How Correlation Technology will radically change the approach and practice to enterprise risk theory, methodology and implementation. Innovations powered by Correlation Technology will provide never-before-seen solutions to challenges presented by current GRC and ERM implementations, the limitations of existing software, and the pervasive misconception of the true nature of risk.