STRATEGY PERSPECTIVE

Governance, Risk Management & Compliance Insight

The Rise of GRC Architecture in GRC 3.0

Moving Beyond the GRC Platform to GRC Architecture

Executive Summary

The modern organization is encumbered by change. The onslaught of changing business, risk, and regulatory environments while keeping change in sync is a significant challenge for executives and governance, risk management, and compliance professionals (GRC). GRC fails when it is addressed as a system of parts that do not integrate and work as a collective whole. GRC 3.0 shifts the focus from a GRC platform to a GRC architecture that connects the fabric of GRC across the organization with its disparate systems, processes, and data. This allows integration of distributed risk information and best of breed GRC solutions where they make sense while allowing for a central hub of GRC. The concept of a GRC platform does not disappear but moves from a single centralized technology solution to be a hub of integration and oversight. This requires a federated capability to integrate and manage GRC information, reporting, and analytics. Distributed business systems are integrated to analyze, measure and deliver relevant GRC data and metrics. Business agility and value go beyond functional checkboxes to deliver a harmonious relationship of GRC information that supports the business through dynamic interactions of GRC integration, information, analytics, reporting, and monitoring.

September 2013

Michael Rasmussen, Chief GRC Pundit

Table of Contents

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

Organizations Encumbered by Complexity

Business is complex. Gone are the years of simplicity in business operations. Exponential growth and change in regulations, globalization, distributed operations, changing processes, competitive velocity, business relationships, disruptive technology, legacy technology, and business data encumbers organizations of all sizes. Keeping this complexity and change in sync is a significant challenge for boards, executives, as well as governance, risk management, and compliance professionals (GRC) throughout the business.

The modern organization is:

- **Distributed.** The smallest of organizations can have distributed operations complicated by a web of global supplier, agent, business partner, and client relationships. Traditional brick and mortar business is a thing of the past: physical buildings and conventional employees no longer define organizations. An interconnected mesh of relationships and interactions that span traditional business boundaries now defines the organization. Complexity grows as these interconnected relationships, processes, and systems nest themselves in intricacy, such as deep supply chains.

- **Dynamic.** Organizations are in a constant state of flux. Distributed business operations and relationships are growing and changing at the same time the organization attempts to remain competitive with shifting business strategy, technology, and processes while keeping current with changes to risk and regulatory environments around the world. Multiplicity of risk environments that organizations have to monitor span regulatory, geo-political, market, credit, and operational risks across the globe. Regulatory change has more than doubled in some industries in the past five years and has grown for all industries. Managing risk, regulatory, and business change on numerous fronts has buried many organizations.

- **Disrupted.** The explosion of data in organizations has brought on the era of "Big Data" and with that we now have "Big GRC Data." Organizations are attempting to manage high volumes of structured and unstructured data across

> *"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."*
>
> Fritjof Capra

multiple systems, processes, and relationships to see the big picture of performance, risk, and compliance. The velocity, variety, and volume of data is overwhelming – disrupting the organization and slowing it down at a time when it needs to be agile and fast.

GRC cannot be managed in isolation. That is what fails. The decentralized and disconnected distributed systems of the past catch the organization off guard to risk and expose the organization. Complexity of business and intricacy and interconnectedness of GRC data requires that we have an integrated approach to business systems, data, and GRC.

> *"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."*
>
> Fritjof Capra

In 1996, Fritjof Capra made an insightful observation on living organisms and ecosystems that rings true when applied to GRC and broader business today: "The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."[1]

Capra's point is that biological ecosystems are complex and interconnected and require a holistic understanding of the intricacy in interrelationship as an integrated whole rather than a dissociated collection of parts. Change in one segment of the ecosystem has cascading effects and impacts to the entire ecosystem. This is true in business. Dissociated data, systems, and processes leaves the organization with fragments of truth that fail to see the big picture of performance, risk, and compliance across the enterprise.

What further complicates this is the exponential effect of risk on the business. Business operates in a world of chaos. Applying chaos theory to business is like the 'butterfly effect' in which a small event actually results, develops and influences what ends up being a significant event. The concept uses the analogy that the simple flutters of a butterfly's wings create tiny changes in atmosphere that ultimately impacts the development and path of a hurricane.

The Bottom Line: The organization requires complete situational and holistic awareness of GRC across operations, processes, relationships, systems, and data to see the big picture or risk and its impact on organization performance and strategy. Distributed, dynamic, and disrupted business

[1] Fritjof Capra, The Web of Life: A New Scientific Understanding of Living Systems (New York: Anchor Books, 1996), 3.

Case in Point . . .

Understanding exposure to risk is not a trivial or linear process. To truly comprehend risk requires the gathering and analysis of many data points across multiple systems. Unfortunately, many do not see the truth of the interrelationship of risk while it remains a risk (probability) as it has materialized into a major loss event.

Consider the 2012 loss in derivative trading by the "London Whale" trader Bruno Iksil. His series of credit default swaps led to a multi-billion dollar loss for JP Morgan Chase (JPMC). JPMC originally estimated that the trading loss was $1.8 billion but later had to correct itself as it discovered that the actual loss was over $6 billion, leading to an extensive investigation of the firm's risk management systems and controls. It took JPMC five weeks to come to an understanding that the loss and impact on the business was much greater than the original estimate as they pieced together data from multiple disparate systems and traced the cascading, interrelated, and compounding effects of risk materialization.

requires the organization to take a strategic approach to GRC architecture. GRC fails when risk issues are addressed as a system of parts that do not integrate and work as a collective whole. GRC also fails when it is thought of as a single platform to manage workflow and tasks. GRC is about the interactions and relationships of cause and effect across strategy, process, transactions, information, and technology supporting the business and requires a GRC architecture approach.

Why not see BOTH the forest and the trees?

The individual components of GRC -- governance, risk management, and compliance -- are a necessary and intricate challenge to business. GRC is not optional: every organization has some approach to GRC from the ad hoc to the agile. The primary directive of a mature GRC program is to deliver effectiveness, efficiency, and agility to the business in managing the interrelationship of performance, risk, and compliance. This requires a strategic approach that connects the enterprise, business units, processes, transactions, and information to enable transparency, discipline, and control of the ecosystem of business and operational activities. Doing this is not easy as all of these elements are in a constant state of change.

GRC maturity increases as the ability to connect, understand, analyze, and monitor interrelationships and underlying patterns of performance, risk, compliance across the business grows. Various systems and processes interrelate in apparent and not so apparent interactions that can surprise the organization and catch it off guard. When risk is understood and compartmented in silos the organization fails to see the web of risk interconnectedness and its impact on performance and strategy leading to greater exposure than any individual silo understood.

To maintain integrity, and execute on strategy, the organization has to be able to see the individual area of risk (the tree) as well as the interconnectedness of risks (the forest).

GRC relationships are non-linear. They are not a simple equation of 1 + 1 = 2. They are a mesh of exponential relationship and impact in which 1 + 1 = 3 or 30 or 300. What seems like a small disruption or risk exposure may have a massive effect or no effect at all. In a linear system effect is proportional with cause, in the non-linear world of business and GRC it is exponential. Business is chaos theory realized. The small flutter of risk can bring down the organization. If we fail to see the interconnections of risk on the non-linear world of business the result is often exponential to unpredictable.

Chronology of GRC from Business Antiquity to Today

GRC is an integration governance, risk management, and compliance in the context of business performance, strategy, and objectives. The official definition of GRC is:

> *A capability to reliably achieve objectives [governance] while addressing uncertainty [risk management] and acting with integrity [compliance].*[2]

GRC relationships are non-linear. They are not a simple equation of 1 + 1 = 2. They are a mesh of exponential relationship and impact in which 1 + 1 = 3 or 30 or 300. What seems like a small disruption or risk exposure may have a massive effect or no effect at all.

The reliable achievement of objectives is governance, understanding and addressing uncertainty is risk management, and acting with integrity is compliance. All three of these provide a natural flow. Governance provides strategy and objectives that deliver the context for risk management. Risk management, in turn, aims to comprehend and predict uncertainty and set boundaries and expectations so the organization can reliably achieve those objectives. Compliance then ensures that the organization stays within the boundaries set by risk management as it aims to reliably achieve objectives.

Organizations have done GRC since the dawn of business. Business did not need a three-letter acronym to all of a sudden do GRC. Every

[2] This is the only definition for GRC found in a publicly vetted and available standard, the OCEG GRC Capability Model.

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

organization has one or more approaches to governance, risk management, and compliance: from the ad hoc and disorganized to the mature and agile. GRC is part of every business whether it is called GRC, something else like ERM, or has no name at all.

The question to consider: how mature is the organization's approach and architecture for GRC?

While GRC has pre-existed the acronym GRC, there have been phases of how organizations have approached GRC as an integrated strategy since the acronym was first used in 2002.[3] These are:

- **GRC 1.0 (2002 through 2007).** Birth of GRC Platforms. In this phase organizations focused on documenting internal control to address regulatory and reporting requirements established by the Sarbanes Oxley Act (SOX) in the wake of major financial and accounting scandals. GRC 1.0 was focused on addressing the challenge of internal controls over financial reporting, SOX compliance, as well as related IT controls. GRC platforms came into existence to help bring a cohesive view to this scope.

- **GRC 2.0 (2008 through 2012).** Expansion of GRC Platforms. In this period, GRC took an expanded view to encompass audit, risk management, corporate compliance, and IT security. GRC was focused on a broader cross-department integration back-office GRC functions. Most GRC strategies and activities were department focused with some top-down enterprise GRC strategies being done in organizations. GRC solution providers claimed to have it all and were the single answer to all the organizations GRC challenges. The truth was discovered was that the GRC platform is not a 'silver bullet.' The GRC platform, as represented in major analyst reports, was focused on workflow, task management, surveys, content management, with some dashboarding and reporting across areas of risk, policy, compliance, incident, and audit management.

- **GRC 3.0 (2013 and beyond).** Organizations are discovering that GRC platforms are not enough. Yes, managing surveys/assessments, workflow, tasks, and content is needed. There is still a need to orchestrate GRC activities. However, the growing awareness of the distributed nature of GRC and business data, process, and systems combined with risk and regulatory requirements have created a fundamental shift in GRC approach. GRC is NOT what a single solution provider offers in a GRC platform; instead, GRC is an architecture that brings together strategy, process, information and technology across a range of business systems, activities, and data. The organization strives for the integration and engagement of GRC throughout the enterprise to provide complete situational awareness to how risk is pervasive and interconnected to business strategy and operations.

[3] The author of this report, Michael Rasmussen, was first noted to define and model an integrated approach to GRC using technology, process, and information and use the acronym in February 2002.

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

Evolution of GRC Technology . . .

Before GRC 1.0, GRC was scattered and reactive. With GRC 1.0 there was a focus on a few risk areas involving selective silos and transactions, particularly for internal control over financial reporting (e.g., SOX). GRC 2.0 took a broader view bringing more functions into perspective while focusing on an integrated perspective of risk and compliance. GRC 3.0 is about aligning strategy, process, information, and technology into a GRC architecture to deliver a holistic understanding of risk in the context of strategy and objectives amidst organizational velocity and change.

GRC 3.0, Moving Beyond the GRC Platform to GRC Architecture

The core of GRC 3.0 is operationalizing GRC across the fabric of business strategy and operations – seamlessly, agilely and non-invasively. This involves bringing GRC to the 'coal-face'[4] of the organization through employee engagement in GRC with systems that are simple, mobile, and easy to use at the frontline of the business. It is about leveraging and harmonizing existing data and systems that deliver results in focused areas but now need to feed into the bigger picture of enterprise transparency in the context of distributed and dynamic business.

The challenge is how to reconcile business agility with GRC strategy and architecture? Most GRC decisions were considered as a base reaction to the newest regulatory demand. This resulted in billions of dollars spent in GRC with a limited understanding alignment to the business. GRC was approached tactically and not strategically. Organizations have ended up with topography of GRC projects individually focused on risk at department or regulatory/risk issues that have often failed to deliver cross-enterprise insight needed. To use an analogy from anatomy, the enterprise GRC body has functioning heart, kidney's, limbs, lungs, and other organs that operate as separate entities and not as part of a unified body. What is often missing is a level of integration that provides a central nervous system that connects everything and makes it operate as a body. This is more than a GRC platform as it has been understood for the past decade.

GRC Platforms: Problem or Cure?

In GRC 2.0 organizations approached GRC as a platform to document and manage content related to risks, policies, and controls, enhanced with workflow to manage assessments, issues, and reporting. There was limited integration and correlation of GRC information and analytics and reporting was

[4] The 'Coal-Face' is a term originated in the United Kingdom referring to the miners deep in the shafts extracting coal for the business. Every organization has a 'coal-face.' These are the front-line employees that make decisions every day impacting GRC and business performance.

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

on fairly static information collected over time. Organizations suffered when GRC did not connect all the dots and provide context to business analytics, performance, objectives and strategy in the real-time business operates in. GRC delivers limited value to the organization when it simplifies risk management to being just surveys and forms that lead to subjective analysis. GRC has been tactical and focused on putting out fires, particularly compliance fires.   GRC platforms have been primarily workflow, task management, and content systems to document controls and compliance and provide some subjective reporting on risk. GRC in 1.0 and 2.0 has not delivered on a true integrated understanding of risk and performance. Organizations often have a diverse set of independent and disconnected systems to address a range of credit, market, interest, operational, strategic, reputation, capital, and regulatory risks with no integrated view across these systems. It is not uncommon for an organization to have six different GRC platforms from different solution providers and a dozen or more other risk and compliance solutions scattered across the organization.

Organizations need to move beyond the concept of a GRC platform as it only addresses part of the challenge and focus on an integrated view of GRC data and systems through a GRC architecture that is a cohesive part of the broader business fabric of the organization. GRC technology is not about a single GRC platform that promises to be all things and fails to deliver them.

The goal of GRC 3.0 is to enable a GRC architecture that effectively reconciles organization strategy, process, information, and technology into a federated architecture model. There still can be a central core system for GRC, but GRC is not defined as this one central system (or platform) but the integrated whole.

GRC 3.0 is: an architecture that is enterprise wide; delivers consistent and uniform value from the boardroom to the 'coal-face' of the front office; focused at value protection and creation; and is proactive in measurement, management and interdiction. GRC 3.0 provides an integrated GRC architecture that connects the fabric of the business together across the organization and its disparate systems, processes, and information.

GRC 3.0 is . . .

An architecture that is enterprise wide; delivers consistent and uniform value from the boardroom to the 'coal-face' of the front office; focused at value protection and creation; and is proactive in measurement, management and interdiction. GRC 3.0 provides an integrated GRC architecture that connects the fabric of the business together across the organization and its disparate systems, processes, and information.

Characteristics of GRC 3.0

GRC 3.0 is about delivering value, integration, and alignment of strategy, process, information and technology throughout the organization in the context of governance, risk management, and compliance. It is an integration of GRC information, processes, and systems to deliver value to the business. Characteristics of GRC 3.0 include:

- **GRC Architecture.** The core of GRC 3.0 is to understand and approach GRC as an architecture involving strategy, process, information, and technology working together across the business and its operations. GRC architecture operates in the context of enterprise/business architecture and requires the integration of applications and data to achieve efficiency, effectiveness, and agility in a dynamic and distributed business environment. This necessitates that organizations understand the business and how it operates. GRC 3.0 is about integration of systems and data.

- **Operationalizing GRC.** Achieving a mature GRC architecture involves operationalizing GRC by integrating business applications, processes, and data. It is about enabling GRC within business systems such as business intelligence, performance, and ERP environment. This provides real-time insight into business decisions, operational intelligence, and monitoring in the context of risk and compliance. This is best done as non-invasively as possible. GRC needs to integrate with a range of applications and interface and share data between them to provide holistic awareness of risk in the context of business. GRC 3.0 is a way to connect and leverage existing investments.

- **Dynamic integration of actionable content.** The integration of content and technology is core to GRC 3.0. This involves the delivery of content from knowledge/content providers through GRC technology solutions to rapidly assess changing regulations, risks, industry and geopolitical events. Content is tagged so it can be properly routed to the right subject matter expert to establish workflow and tasks for review and analysis. Standardized formats for measuring business impact and review of existing processes, policies, and controls can take place. This integration of actionable content with GRC technology delivers on GRC maturity in 3.0 through achievement of risk and regulatory intelligence.

- **360° GRC contextual awareness.** GRC 3.0 brings GRC architecture, operationalization, and integrated content to the points where the organization gains a complete view of what is happening: this is what GRC 20/20 refers to as 360° GRC contextual awareness. Where risk and compliance is monitored and understood in the course of business operations, changing risks and regulations, and interactions. Delivery of GRC contextual awareness requires that GRC be a central nervous system to capture signals found in processes, data, and transactions as well as changing risks and regulations for interpretation, analysis, and holistic awareness of risk in the context of business.

- **Bringing GRC to the 'coal-face'.** Organizations are recognizing that effective GRC includes those on the front lines of the business – the 'coal-face' of the organization. GRC 3.0 is about delivering an exceptional end-user experience: getting employees involved by providing

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

elegant interfaces into GRC that are interactive, intuitive, and social. GRC solutions need to instruct, inform, and be easy to use in the context of business as risk may materialize at those front-lines of operations. GRC done right allows employees to participate in GRC without feeling overwhelmed and confused. This includes employee engagement through GRC gamification, getting employees involved through social networking, games, and interactive content to drive the culture of GRC into decision-making. GRC gamification is used to conduct risk workshops, understand compliance in the context of business, and getting individuals involved in GRC at all levels of the organization. Organization may implement training and awareness programs that enable employees to earn points or badges for completion. It can involve recognizing individuals when they make good risk decisions or alert the organization to an issue.

- **Mobility.** There's an app for GRC! GRC is embracing mobile technology on tablets and other devices. Issue reporting is readily done through mobile devices. Tablets can deliver policies, training, and other interactive content to employees, particularly those without desktop workstation access; or they can be used as a mobile policy and training kiosk for a group of employees. Mobile devices are to be used in conducting investigations, audits and risk/compliance assessments to provide increased agility and responsiveness. The ability to record pictures and video right into mobile GRC applications will make these processes more efficient and effective.

A Tale of Two GRC Architecture Strategies

The problem with GRC in many organizations is that it has not been designed properly, particularly when it has been designed to solve a small subset of problems. The result opaques risk management and fails to see the web of risks across the organization that impact strategy and performance. Organizations have significant risk gaps within their operating models despite significant investment in excellent individual GRC solutions that are scattered and disconnected across the business. This has resulted in a poor return on investment of repetitive GRC projects that fail to drive value or opportunity that enterprise GRC transparency and velocity should create.

In GRC 3.0, a GRC architecture approach allows best of breed solutions to exist where they make sense but has a federated capability to integrate and manage GRC information, reporting, and analytics. The truth is: organizations often have multiple GRC solutions in house and they often are not looking to replace all of them. Different departments have invested in best of breed solutions that make sense where they are and provide functionality specific to their needs. Gutting and replacing solutions means the department loses functionality and even forces the entire organization to manage GRC to the lowest common denominator as it does not address the unique requirements of certain business areas. No GRC platform does everything related to governance, risk management, and compliance. GRC involves a range of different roles, processes, technologies, and content. One platform simply

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

does not do it all – or at least it cannot do it all very well.

GRC architecture allows for consolidation where it makes sense while simultaneously allowing for best of breed where it is needed. GRC 3.0 is about building a GRC architecture that enables oversight, reporting, accountability, and analytics through integration with other technologies, data repositories, and enterprise systems. The objective is to let GRC work with and throughout the business and not force parts of the business into a mold that does not fit. It allows for diversity while still providing integration, discipline, and consistency. The organization needs a GRC ecosystem of process, technology, and information that integrates to provide optimal alignment and value to the business. Note the word "centralization" is being avoided. To "centralize" – the traditional model of GRC 1.0 and 2.0 – immediately imposes alien constructs that undermine agility. Instead "Orchestration" of the diverse elements of GRC through an integrated approach to both enterprise and GRC architecture enables agility, stimulates operational dynamics, and, most importantly, effectively leverages rather than vainly tries to control the distributed nature of the modern enterprise. Orchestration also allows for discord or tension where and when necessary. Different areas of GRC require checks and balances. This is why audit should not be involved in managing aspects of GRC and the business. This is why compliance often does not report into legal.

GRC architecture delivers the ability to effectively mitigate risk, address requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment that requires agility. GRC, when designed properly, should achieve better-performing processes that use integrated and reliable information. This enables a better-performing, less costly, more flexible business environment.

GRC 20/20 measures GRC architecture value around the elements of efficiency, effectiveness and agility. The value goals of GRC architecture is enable the organization to be:

- **Effective.** GRC architecture achieves effectiveness in risk, control, compliance, audit, and business process. This is delivered through greater assurance in the design and operational effectiveness of controls to mitigate risk, achieve performance, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the controls and policies set by the organization and provide greater reliability of information to auditors and regulators. Effectiveness of the GRC architecture is measured around both the design and the operation of the GRC architecture as it integrates and supports the broader business.

- **Efficient.** GRC architecture provides efficiency and savings in both human and financial capital resources. GRC processes, and GRC technology solutions, should reduce operational costs by automating processes, particularly those that take significant time consolidating and reconciling information to manage, analyze, report, and mitigate risk and meet compliance

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

requirements. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **Agile.** GRC architecture delivers business agility when organizations are able to respond rapidly to changes in the internal business environment (e.g., employees, business relationships, operational risks, mergers and acquisitions) as well as the external environment (e.g., economic risk, new laws and regulations). GRC agility is also measured in responsiveness to events and issues so that the organizations can identify and react quickly to control failures/weaknesses, non-compliance, and adverse events in a timely manner so that action can be taken and damage/loss is contained.

To deliver on the vision of GRC 3.0 and an enterprise GRC architecture requires an integrated view of GRC information and metrics across departments and systems. The challenge is, how does the organization:

- **Find the right source of data.** GRC information is buried across multiple departments, processes, and systems. Regulatory reporting and situational awareness require that the organization have visibility into risk data and metrics, and their interrelationships, which is scattered across the business.

- **Transform business data into GRC intelligence.** Each silo of data brings a piece of the picture or a partial version on the truth. These are elements, but they do not tell the full story. In fact, relying on only a partial view of data may be misleading. Bringing data together requires that the organization have consistent and quality data to work with and analyze. With reliable data the organization can turn data into information that drives GRC intelligence.

- **Understand real-time GRC situational awareness.** To deliver a holistic view of GRC information and 360° GRC contextual awareness of risk impacting strategy and operations requires that the organization get to the source of the information rapidly. GRC has to be able to present accurate information to the right people at the right time. To do this data needs to be accessible as well as accurate.

Designing an approach to GRC architecture requires that the organization address the critical question:

How does the organization aggregate, analyze, and report on distributed risk data?

There are fundamentally two very different approaches to GRC architecture to consider:

1 - GRC "Big Data" Warehouse

This is the "Big Data" approach in which the organization creates another mammoth data warehouse, in this case for GRC information adding another "Big Data" pandemic of complexity, integration, and cost to the organization.

The challenge is that GRC information draws from so many disparate and distributed systems that the organization ends up with multiple GRC "Big Data" warehouses to address the variety of individual risk and regulatory needs. This ends with more mammoth databases, and is particularly true in highly regulated industries like financial services.

The GRC Big Data Warehouse is achieved through replicating systems that store GRC data to a central repository, and often multiple repositories as they are replicated and deployed to address more risk and regulatory challenges. As risk information is scattered the issues of data integrity and quality arise because different sources may be inaccurate and data can be corrupted in replication and distribution. This approach is expensive, slow, inflexible, and leads to inefficiency and gaps in risk information. It costs resources and quality to identify data, normalize, move, optimize, and acquire GRC information and the solutions to support, analyze, optimize, and report. As it scales it becomes a nightmare. GRC becomes a central monolithic and bloated application that takes a lot of resources to maintain and the business is frustrated with data quality and integrity issues in GRC analytics and information.

2 - Integrated GRC Information Architecture

Another approach, and one where new directions in technology innovation are leading GRC, is a non-invasive approach that enables access to risk data and functionality across broad and diverse systems and orchestrates integration of both new and existing GRC systems and analytics.

This is achieved through establishing a uniform GRC integration architecture that supports the diverse heterogeneous network of enterprise as well as GRC solutions without a focus on more data warehouses and the cost to support and maintain them. This involves a paradigm shift in which existing systems and applications are leveraged to analyze, measure and create risk intelligence and forward the relevant information without the need to move and store massive amounts of information into a centralized GRC system for analysis. Analysis is distributed and only the necessary information is forwarded.

The benefits are the establishment of holistic, non-invasive GRC transparency and awareness across the enterprise. Think of it: leave data where it is - send only what is needed. This delivers enterprise GRC agility in a highly adaptable environment that is less expensive to maintain while avoiding GRC data redundancy and quality issues. Instead of solving a problem by point solutions, the organization can invest in an infrastructure that is flexible and adaptable to harness the needed information,

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

analyze it, and report on it. This approach can span regulatory and risk areas instead of building multiple redundant data warehouses for GRC for each challenge that creates more headaches. Each system/process manages the data that drives its area and reports to a central repository. Endpoints are not slaves, but active participants. The GRC architecture is to be a conductor that orchestrates data, analysis, and applications across the enterprise to achieve one goal – effective, efficient, and agile GRC in the context of business strategy, performance and objectives.

The GRC architecture is to be a conductor that orchestrates data, analysis, and applications across the enterprise to achieve one goal – effective, efficient, and agile GRC in the context of business strategy, performance and objectives.

Simplicity: GRC taking a queue from Apple

It has been stated that:

> *Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius – and a lot of courage to move in the opposite direction.*[5]

A primary directive of GRC 3.0 is to provide GRC architecture that is operationally integrated while being non-invasive. Organizations need a GRC approach that is simpler and more useful. Like Apple, in its innovative technologies, organizations need to approach GRC architecture in a way that re-architects the way it works as well as the way it interacts. A mature GRC architecture design is one that serves the business and provides the right information. GRC done right minimizes its impact on the business while still maintaining insight and control of risk across the business.

The goal is simple; it is itself "Simplicity." Simplicity is often equated with minimalism. Yet true simplicity is so much more than just the absence of clutter or the removal of embellishment. It's about offering up the right GRC information, in the right place, right when the organization needs it. It's about bringing orchestration and order to the complexity of distributed GRC process and data. GRC should be intuitive to the business and GRC architecture should provide the right information in a way that works for the business. By taking away costly GRC data replication and warehouse elements that don't add value, there is a greater focus on what matters most: understanding risk in the context of business.

GRC architecture, and particularly technology, should never get in the way of business. Why do

[5] This quote has been attributed both to Einstein and E.F. Schumacher.

enterprise GRC projects take two years to roll out at times? The primary issue is overhead in extensive services and technology implementation to integrate and develop massive GRC implementations that end up slowing the business down and delaying value (if value is ever achieved). The problem is that by what organizations call integration they really mean consolidation, replication, and redundancy. There is a huge gap between being functional and agile.   GRC architecture is to be beyond functional to be agile and valuable to the business. GRC architecture is to deliver harmonious relationship or GRC information that supports the business. GRC is to enable enterprise agility by creating dynamic interactions of GRC information, analytics, reporting, and monitoring in the context of business.

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

SOLUTION SPOTLIGHT: Pneuron

Bringing GRC Agility to the Enterprise

Pneuron, with its Business Oriented Architecture (BOA), is a vendor in the GRC architecture and integration market that GRC 20/20 has researched. Pneuron delivers a GRC information, analysis, and data integration architecture that is cohesive while being non-invasive to business systems and applications. Pneuron integrates distributed components of risk – analysis, data, processes, systems – into a uniform architecture, event when the components are diverse in technology, location, or source.

Organizations implement Pneuron's agents across a range of data sources, analytical models, and applications. Pneuron in this way aligns relevant but diverse and distributed GRC data and analysis as an orchestrated architecture that bypasses the need for traditional data integration, software procurement and database pre-requisites. Pneuron's BOA technology provides the integration core needed to be a central nervous system to manage the range of GRC data harvesting, integration, and analytics in highly regulated organizations. Existing GRC components are not changed by Pneuron. Organizations continue to leverage existing GRC investments. Pneuron enables clients to leverage the GRC investments that traditionally have required large data remediation or data centralization projects to integrate and allow the organization to add new functions, processes or practices in a single interoperable architecture.

Specific capabilities within the Pneuron BOA that GRC 20/20 has identified as valuable to organizations requiring a strategic approach to an integrated GRC architecture are:

- **Efficiency.** Pneuron's BOA approach allows for increased human and financial capital efficiency through integrating business applications and data throughout the enterprise. This enables the business to have the right risk information for the right context without the cost of overwhelming GRC data replication and consolidation. Pneuron delivers utility: it is not about gathering all the data it can because it can, it is about gathering the right data to get the job done.
- **Effectiveness.** Pneuron's BOA allows the organization to be more effective at GRC by allowing best of breed solutions and existing systems to continue to operate where they have been successful and integrate the necessary data to deliver an overall contextual awareness of risk. This brings to GRC the ability to configure and deploy in real time GRC functions, components, products, rules, models, or analytics from distributed sources (third party, proprietary or developed) to any system or set of systems without the need for an intermediary database or data warehouse.
- **Non-invasive.** The Pneuron zero-infrastructure approach is a minimalist approach. Simply deploy Pneurons (these are mini-interoperable applications) on systems where critical GRC data rests and allow the Pneurons to harvest, analyze, and forward relevant intelligence to other systems needed for more comprehensive analytics and reporting. This offers up the right data, in the right place, right when it is needed. Pneuron brings order and simplicity to complexity without imposing monolithic solutions.
- **Enterprise GRC agility.** By integrating existing systems and data the organization operates with agility allowing for dynamic and real-time situational awareness of risk. The GRC data that takes weeks to

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

consolidate and analyze is not needed as the organization has an architecture to integrate and manage the right information when and where it is needed. By removing the requirement for intermediary technologies – ETL, MDM, and databases – Pneuron provides real time risk analytics directly from distributed components on business systems.

- **Simplicity.** Pneuron provides a fresh and new perspective on integrated GRC architecture that approaches things correctly, but also simply. This enables the organization to create a GRC and performance management experience that is simpler, more useful, and more engaging to the business. Pneuron takes away bloated data stores that do not add value - the outcome is a greater focus on what matters - the GRC information in the context of business – but does not replace existing systems and value already invested.

- **Integration.** Pneuron BOA is about creating connections so that things can work in harmony - orchestrating the different elements of data to make the organization effective, efficient and agile at GRC in the context of business. Pneuron enables these connections to be integrated and combined, creating any number of new GRC capabilities and analytics without forcing change or integration between those components. Pneuron's design of uniform interoperability across all elements of the GRC process enables transparency and interdiction quickly and simply, without forcing change or replacement of existing systems.

- **Performance.** Volume and analytical scale is achieved through dynamic distribution of load and processing using redundant existing capacity across the client's network. This zero infrastructure design has provided large volume processing ability without the need for centralization or large hardware procurement and database optimization projects.

- **Leveragability.** Pneuron enables clients to leverage distributed data sources and functionality that is traditionally isolated or poorly leveraged across the enterprise. Organizations can fill gaps between different components by adding new components (or Pneurons) from a single screen. These components include Analytics, Predictive Models, Matching, NLP, any existing applications and multiple other functions that the client configures and deploys as a single uniform architecture that integrates and networks GRC components that resides across the organization's operations.

- **Cost and Time to Value.** GRC 20/20 finds that Pneuron's deployments are efficient and have returned vale to the organizations using the solution. This includes complex risk and compliance analytics such as: AML; regulatory reporting (e.g, Dodd Frank); FormPF; FATCA; CCGR and Insolvency; real-time global risk reporting; global derivatives management and optimization in Financial Services; and claims risk and optimization for Insurance.

©2013 GRC 20/20, LLC; Licensed to Pneuron for Redistribution

About . . .

GRC 20/20, LLC

GRC 20/20 provides independent and objective research and analysis on the topics related to governance, risk management and compliance (GRC). Our analysts bring real-world expertise, independence, creativity and objectivity to help organizations understand and apply strategies and technology to meet their GRC challenges. Whether it is focused on a specific issue or an enterprise-wide GRC strategy, clients seek GRC 20/20 analyst advice in achieving sustainable and pragmatic innovation. GRC 20/20 advises the entire ecosystem of GRC solution buyers, solution providers and vendor clients. We serve the needs of organizations that seek insight, guidance and advice in dealing with a dizzying array of disruptive business models and technologies.

Michael Rasmussen, Chief GRC Pundit

Michael Rasmussen is an internationally recognized pundit on governance, risk management and compliance (GRC) — with specific expertise on the topics of corporate compliance, business ethics, policy management and corporate culture. With 18+ years of experience, Michael helps organizations improve GRC processes and choose technologies that are effective, efficient and agile. He is a sought-after keynote speaker, author and advisor and is noted as the "Father of GRC" — being the first to define and model the GRC market in 2002.

© 2013 GRC 20/20 Research, LLC and/or its affiliates. All rights reserved. This publication may not be reproduced or distributed in any form without GRC 20/20's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. GRC 20/20 disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of GRC 20/20's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although GRC 20/20 research may include a discussion of related legal issues, GRC 20/20 does not provide legal advice or services and its research should not be construed or used as such.

4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@grc2020.com
www.grc2020.com