



INCREASING BUSINESS AGILITY

AN INTEGRATED APPROACH TO GOVERNANCE,
RISK, AND COMPLIANCE MANAGEMENT



Today's business climate is complex and increasingly difficult to predict. Stakes are rising in a global market in which competition is fierce and brand loyalty is fickle. Across all industries, companies are grappling with high expectations and margin pressures. And at the same time, businesses face unprecedented numbers of legal, regulatory, and business partner mandates, as well as value chain requirements that affect nearly every aspect of their operations.

According to a September 2006 benchmarking survey conducted by the Americas' SAP Users' Group (ASUG) and SAP on governance, risk, and compliance (GRC), most organizations today have a reactive approach to GRC management – a fire-drill method of channeling precious resources and management attention to address specific regulatory mandates independently in isolation from each other. The end result is a series of fragmented GRC activities and data sources that increase costs, limit visibility into business risks – and ultimately hinder business agility.

To help companies become less reactive – and increase their organizational agility – executives need a clear path to GRC maturity. This *SAP Executive Insight* focuses on helping executives determine:

- What are the consequences of today's typical GRC approaches?
- Where do their organizations stand from a GRC maturity perspective?
- How can they lay the foundation for an effective GRC strategy?

EXECUTIVE AGENDA

AT A GLANCE

Overcoming Barriers to Business Agility

In today's business environment, the most successful organizations are often the most agile. It's this agility that allows organizations to sense and respond to opportunities with ease and stay competitive in the midst of turbulent and fast-changing business conditions. But for most, this doesn't come easily. According to a recent SAP survey conducted with The Economist Intelligence Unit of more than 4,000 corporate executives, more than 33% ranked "ability to change" as their top challenge, ahead of "speed of innovation" or even "maintaining customer loyalty."

Major trends of the last five years – such as globalization and radical shifts in business models – have escalated the need for business agility while simultaneously throwing up roadblocks. The impacts of these trends have triggered ripple effects from a governance, risk, and compliance (GRC) perspective. The problem is that most businesses today are taking far too narrow an approach to managing GRC, leaving them slow to respond, driving up costs, and leaving them open to unexpected and potentially harmful business risk.

Enabling Integrated GRC

To address these requirements, forward-thinking organizations are taking a broader, more integrated approach to managing interrelated strategic planning activities and business risks. The path to reaching GRC maturity typically leads through four phases:

- Blissful unawareness
- Reactive, fragmented implementation
- Consolidation
- Operational excellence

Essentially, this approach is an evolution toward an integrated program of GRC management and away from the current fire-drill method of channeling precious resources and management attention to address specific regulatory mandates independently.

Capturing the Value of Integrated GRC

Organizations that have moved to an integrated approach have been able to realize a new level of confidence and transparency regarding compliance. In addition, businesses have realized significant benefits:

- Optimized risk-return portfolio
- Reduced GRC costs
- Improved business performance and predictability
- Business sustainability
- Greater business agility

TAKING A COMMON AND INTEGRATED APPROACH TO GRC

FROM SILOS TO COHESIVE STRATEGY

In September 2006 the Americas' SAP Users' Group (ASUG) and SAP launched a benchmarking survey focused on GRC. Their findings indicate that GRC initiatives today are largely driven by government mandates and reactive in nature. In other words, these initiatives are primarily focused on addressing the latest compliance issues, with minimal attention on risk and governance, and are usually executed and managed in "silos" by individual departments (see Figure 1). This approach typically results in fragmented GRC activities and data that drive up costs and hinder visibility into business risks. The following survey results point to the consequences of this approach:

- Compliance-focused GRC investments are starting to generate value. In fact, more than 85% of survey respondents believed that their GRC investments helped them reduce the number of significant deficiencies and material weaknesses, and control violations within their businesses.
- However, more than 75% of respondents said that the associated costs still outweigh the benefits.
- More than 48% indicated that they had increased their GRC investments the year prior.

In reality, governance, risk, and compliance are interdependent and must be managed holistically in an integrated approach. A single set of applications deployed together support a cohesive strategy for ensuring compliance and monitoring, identifying, and managing risk across the enterprise. Ideally, all applications operate using a single, shared GRC data repository that pro-

vides complete visibility across the organization and automates manual tasks. This approach eliminates fragmentation and dramatically simplifies management and execution of GRC initiatives. Companies should also define their governance strategy before dealing with purely compliance issues.

Embedded GRC Applications

As illustrated in Figure 2, an integrated approach also assumes that GRC management is built into all core business processes, not treated as a separate process. This means that GRC applications are embedded in day-to-day activities, drive the automation of routine activities, and ensure information and process consistency across the business. This makes it easy to compile data for a comprehensive perspective on overall risk exposure, monitor compliance and risk, and adjust business

processes in response to new opportunities and regulatory mandates.

GRC Challenges	Rating
Necessary information is contained in complex and heterogeneous IT landscapes.	3.88
Governance, risk, and compliance management is fragmented at a departmental, divisional, or regional level, making it difficult to attain enterprise-wide business transparency.	4.00
Control activities are manual and take too much time.	4.18
Collaboration between IT, business process managers, finance, and auditors is weak.	4.31
Governance, risk, and compliance management effectiveness is difficult to quantify and measure.	4.53

1 = Most Challenging; 10 = Least Challenging

Figure 1: GRC Challenges
(Source: ASUG/SAP Benchmarking)

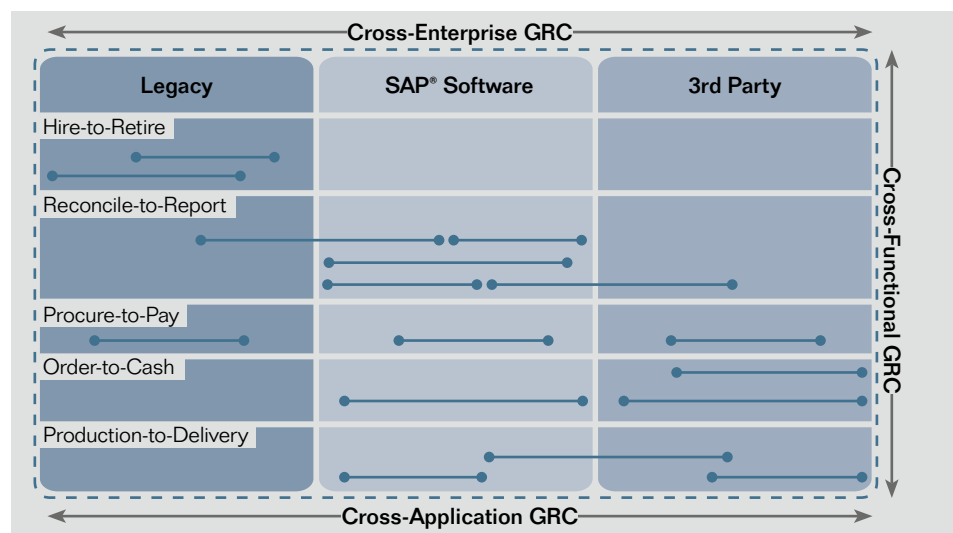


Figure 2: Supply Chain Benchmarks for Semiconductor Companies
(Source: ASUG 2007 Semico Benchmarks)

A CLEAR PATH TO GRC MATURITY

FOUR PHASES TO OPERATIONAL EXCELLENCE

Each organization needs to chart its own GRC course. Figure 3 illustrates the typical phases of GRC maturity and the types of activities that organizations in each phase typically engage in.

- Phase I: Blissful unawareness
 - Organization is unaware of GRC interdependencies and focuses only on the obvious and most critical (or mandatory) compliance issues.
 - Limited investment is made in tools and policies to support GRC.
- Phase II: Reactive, fragmented implementation
 - Organization responds to local regulatory compliance issues by engaging in disjointed, tactical GRC approaches.
 - A large number of independent teams deals with specific regulation, risk, or other governance issues.
- There is a limited understanding of the real cost of compliance, current risk exposures, and lost opportunities.
- Phase III: Consolidation
 - Organization is ready to initiate a strategic change based on one consistent, enterprise-wide GRC framework.
 - Successful pilot initiatives validate the GRC framework approach.
 - Executives have a well-balanced enterprise-wide view of all compliance and risk issues and know where the “hot spots” are.
- Phase IV: Operational excellence
 - Managers have a balanced GRC view across all processes and projects.
 - GRC is absorbed at all organizational levels across the enterprise.
 - A common language and set of metrics are in place for use with all initiatives.

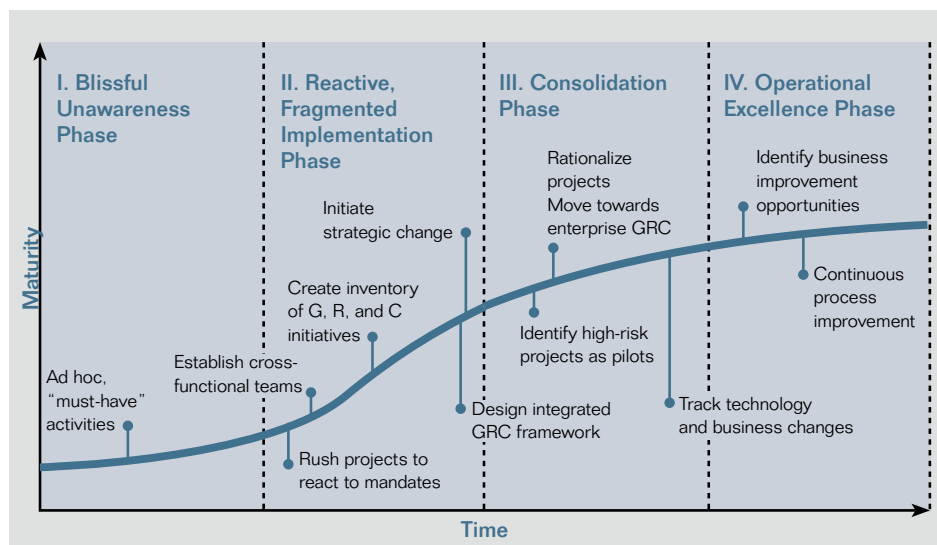


Figure 3: SAP Supply Chain Benchmarks for Semiconductor Companies

(Source: ASUG 2007 Semico Benchmarks)

Rohm and Haas

Industry: Chemicals

Summary

Rohm and Haas Company is a global manufacturer of specialty materials used in industries such as paint and coatings, electronics, water treatment, and plastics. Rohm and Haas needed to establish a global approach to comply with regional volume-based restrictions such as the European Union’s Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) regulation.

Results with SAP® Software

- Positioned company for long-term compliance with volume-based regulations
- Improved accuracy and quality of compositional data
- Improved ability to identify the regulation-defined volume bands for the company’s substances

REALIZING THE BENEFITS

TRANSPARENCY AND AGILITY

Regardless of the current level of GRC maturity, there are four cornerstones involved in laying the foundation of an effective GRC strategy:

- Get buy-in from the entire management team, including the board of directors and the executive team.
- Ingrain GRC at every level of the company, as mandated by the senior team.
- Drive the adoption of the GRC framework with select, high-priority initiatives.
- Leverage GRC as a proactive business optimization instrument. GRC is leveraged to effectively drive competitive advantage, based on business transparency and predictability.

An integrated GRC approach offers many benefits. First, it provides a new level of transparency and confidence regarding compliance across the business and beyond – delivering value to the board, line-of-business management, and external stakeholders. In addition, businesses realize the following benefits:

- **Optimized risk-return portfolios:** An effective GRC approach provides the transparency and insight that business executives need to make decisions based on risk impact and probability relative to potential return.

- **Reduced GRC costs:** Transitioning to an integrated GRC approach significantly reduces the number of people – and the amount of time – required to control and address risk.
- **Improved business performance and predictability:** This approach enables transparency across the enterprise and beyond, giving management a systematic way to anticipate and control risks. Managers have tools to determine actions and critical tasks that will reduce business performance variability.
- **Business sustainability:** An integrated GRC approach provides a clear path to sustainable compliance and risk management, even as mandates increase and business models and processes become more complex.
- **Greater business agility:** An integrated approach to GRC increases business agility by helping organizations accelerate decision making and identify associated business risks and their interdependencies.

GRUMA

Industry: Consumer products

Summary

GRUMA is the worldwide leading producer of corn flour and tortillas and sells its products in over 50 countries. GRUMA required a process and tool to ensure that its end users had the right access privileges to perform day-to-day business operations without exposing the business to risk. Governance regulations and increased internal controls are necessary for GRUMA.

Results with SAP® Software

- Greater ability to track compliance with auditors' recommendations and measure improvements
 - Better compliance with regulations
 - Internal IT audit revision time now 90% faster and external IT audit revision time now 50% faster
-

THE ROAD AHEAD

ACT NOW

Companies should take a broader, more proactive approach to managing interrelated strategic planning activities and business risks by developing an integrated GRC management strategy and thinking beyond just compliance with the Sarbanes-Oxley Act. This involves deploying a single set of integrated applications that ensure compliance and proactively monitor, identify, and manage risk across the enterprise. These applications should operate using a single, shared GRC data repository – the key to gaining complete visibility across the organization and automating manual tasks. Once deployed, companies can eliminate fragmentation, reduce compliance costs, make risk-informed plans and decisions, and dramatically simplify management and execution of GRC initiatives.

Benchmarking Services From SAP

The ASUG/SAP Benchmarking and Best Practices program provides a forum for SAP customers to track trends, share best practices, and measure value based upon key performance drivers. To date, more than 35 companies have participated in the GRC study. The GRC Benchmarking initiative addresses the drivers, benefits, investment levels, staffing, challenges, and general characteristics of GRC management. In addition to GRC, ASUG/SAP Benchmarking programs exist for several additional operational areas, including finance, human capital management, supplier relationship management and procurement, supply chain and manufacturing, new product development and introduction, customer contact centers, total cost of ownership, and business intelligence. For more information about the ASUG/SAP Benchmarking program, visit www.asug.com/benchmarking or contact benchmarking@asug.com.



Further Reading

To learn more, please visit www.sap.com/usa or contact your SAP representative about the following:

SAP® White Papers

- *Governance, Risk, and Compliance Management: Realizing the Value of Cross-Enterprise Solutions*
- *An Integrated Approach to Managing Governance, Risk, and Compliance*

SAP Customer Stories and Profiles

- *Bacardi*
- *Canadian Pacific Railways*
- *GlobalSantaFe Corporation*
- *Molex*
- *NVIDIA Corporation*
- *Synopsys*
- *The Coleman Company*
- *Wolverine World Wide Inc.*
- *Xerox Europe*

50 093 054 (08/12)

©2008 by SAP AG. All rights reserved. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in several other countries all over the world. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

www.sap.com/contactsap

THE BEST-RUN BUSINESSES RUN SAP™

