Governance, Risk and Compliance

An Integrated Approach for Improving Oversight and Efficiency

Evelyn Uhlrich
Product Marketing, Software AG

Martin Kling
Business Development, Software AG

February, 2012

Business White Paper

CONTENTS

Evelyn Uhlrich is responsible for global marketing of Software AG's Governance, Risk and Compliance (GRC) Solution. Evelyn graduated in computer science from the University of Applied Science in Darmstadt, Germany, and her postgraduate studies were in business economics at the University of Applied Science in Berlin. She worked for multiple software vendors before joining Software AG in 2007.

Martin Kling has overall responsibility for Software AG's Governance, Risk and Compliance Solution. Besides driving the development of new capabilities to help customers increase their GRC maturity, Martin is actively involved in supervising customer projects during setup and delivery. Martin is also a well-known author on various GRC topics in books, articles and blogs.

ABSTRACT

Your company likely faces huge pressures in an increasingly complex environment that's dominated by market globalization, shrinking development cycles and constantly changing legal, political, cultural and technical requirements. In addition to local regulations, laws and business practices of other countries and cultures also impact how your company operates.[1] Once your enterprise enters a particular market, you generally have no choice but to meet the given requirements.

Corporate Governance, Risk and Compliance (GRC) management can help you manage these pressures. GRC offers steering mechanisms to control the way your enterprise operates. Taking an integrated GRC approach enables you to manage risks and compliance requirements related to environmental practices, processes, business partners and internal policies as well as financial, operational and IT controls.

An integrated approach is essential to sharing information and improving processes—thereby, increasing efficiency, improving oversight and optimizing strategic performance within a given set of boundaries.[2]

Read this white paper to find out:

- The elements of GRC
- The value of an integrated GRC framework
- How GRC improves efficiency and reduce costs
- How to calculate the value of GRC
- Why siloed GRC solutions won't work for the long term

This white paper also explains Software AG's proven GRC methodology called Prime. Read on to learn how ARIS tools can work with this methodology to assure compliance and deliver long-lasting business benefits.

FOUR ELEMENTS OF GOVERNANCE, RISK & COMPLIANCE

1. Governance

Governance focuses on defining codes of conduct and processes for organizations and their staff to ensure compliance.[3] Corporate governance defines the boundaries in which business will be running. Typical measures resulting from corporate governance are guidelines or policies.

A governance framework may comprise organizational measures, such as: security policies; instructions and signatory policies; and the documentation of governance processes, such as risk assessment, the way orders are approved and requesting/approving system access authorization. In addition to being implemented at the organizational level, many of these policies and processes are supported by IT systems.

As part of corporate governance, IT governance seeks to create organizational structures and processes that align IT with corporate strategy and support value-adding business processes.[4]

2. Risk management

All business activity involves risk resulting from uncertainty. But only those who are prepared to actively take on risk can develop strategies for their companies that result in success.[5] Therefore, risks need to be managed.

Risk management involves systematic risk identification and assessment combined with the evaluation and management of potential courses of action in response to the current situation.[6] Responsibility for enterprise risk management lies with senior executives, who are supported by the internal audit and financial controlling functions. Business unit managers and the head of IT are responsible for risk in their respective areas.

The risk management process describes the interaction between organizational units and their roles, thus ensuring that risk management is properly coordinated. Risk management is typically established as a continuous control loop.[7] The control loop is embedded throughout key company departments and corporate processes, including the value-adding business processes and supporting processes, such as IT processes.[8] The risk management process comprises risk analysis, risk assessment and risk handling.

Risk are typically categorized as:[9]

- Market risk
- Credit risk
- Operational risk originating from
  - Processes
  - Human behavior
  - Systems
  - External events that may lead to legal risk
- Residual risk (strategic, reputational)

Risk evaluation should also include opportunities for a company to develop and grow.

Figure 1: Classification of risk

3. Compliance management

The objective of compliance management is adherence to external requirements, such as laws, and internal regulations, such as corporate policies. This includes both statutory regulations and de facto or other standards that organizations choose to apply for competitive or ethical reasons as defined by corporate strategy.

Risk management is considered as the driver of compliance management. Risks arise from non-compliance with legal requirements and de facto standards or corporate risks arising in the daily working routines.[10]

4. Audit management

In an integrated GRC system, effective risk management and compliancy to regulations and policies pave the way for successful audit management. With the climbing numbers and types of audits and the increasing business complexity that apply to companies, the demand of an integrated GRC system based on business processes increases.

Existing silos and point solutions are of little help when addressing the needs of audit managers. The Software AG GRC Solution helps internal auditors manage papers, schedule audit-related tasks time management and reporting. To secure consistent information throughout the enterprise, content information relevant to GRC, such as policies, control test evidences, incident reports as well as previous audit findings, are all managed within the GRC platform.

IT CHALLENGES RELATED TO THE GRC FRAMEWORK

An organization's strategy is implemented in its value-adding business processes. These processes are supported by IT services that represent the output of IT production and management processes (derived from IT strategy) and are designed to meet business requirements. IT services for business and IT are based on the relevant applications (see Figure 2).

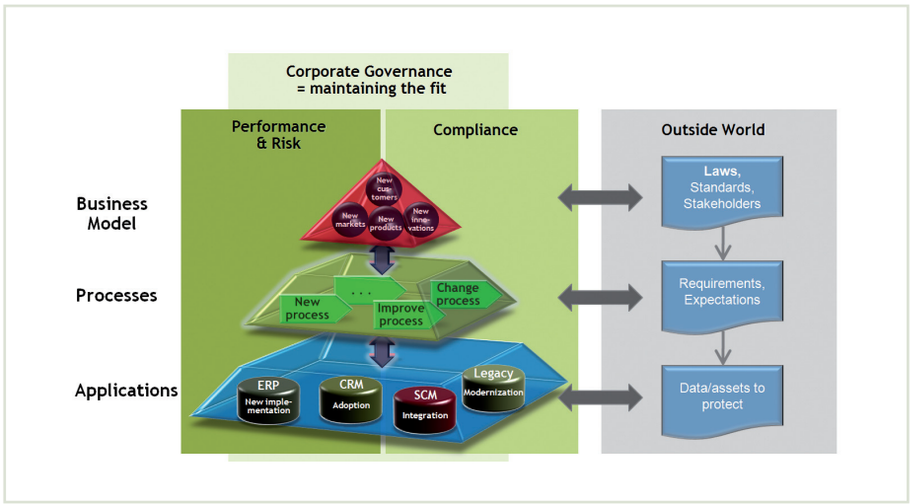

Figure 2: GRC related requirements to a company

A company-specific governance framework comprising governance processes, such as risk management and emergency management, and associated policies and rules, such as security policies, signatory policy, escalation plans and contingency plans, has been put in place to mitigate these risks.

Because a large number of different stakeholders and various country-specific issues are involved, the governance, risk and compliance framework needs to meet a range of highly complex requirements[11]. Since business processes are increasingly dependent on IT systems, virtually every risk and compliance management requirement has an IT dimension.

Just-in-time production in the auto industry, for example, involves a highly synchronized delivery schedule for materials and parts, which is calculated using sophisticated Enterprise Resource Planning (ERP) and supply chain management systems. Clearly, these processes are highly dependent on IT.

Other requirements, such as segregation of duties in accordance with the Sarbanes-Oxley Act (SOX)[12], also necessitate the implementation of identity and access management. They impact the user application and user approval process, as well as the definition of business user roles and IT user roles.

Experience shows that efficient introduction of a GRC framework is only possible if business and IT are involved. Sponsorship at the board or senior management level serves to accelerate the process.

Reasons to implement a GRC framework include:

- Legal
- Economic (business continuity management)
- Operational (IT savings realized by reorganizing in accordance with ITIL, for example)

The opportunities resulting from new-found transparency between business processes and business continuity management are usually overlooked. Along with benefiting from the efficiency and effectiveness provided by business continuity management, cost savings can easily be achieved in this particular case—that is, by rightsizing Service Level Agreements (SLAs) based on the relevance of individual IT systems.

PRIME FOR GRC: PRIMED FOR BETTER TIME-TO-VALUE

Software AG offers a flexible and proven methodology for GRC called Process Improvement Methodology (Prime). Prime provides a process-driven guide to implementing a GRC platform. You can implement GRC as a standalone solution or one that's combined with any other Software AG solution. Individual methodologies from hundreds of projects can be customized or combined to support new solutions, services and individual customizations.

Prime incorporates:

- A framework consisting of an implementation and deployment process for the entire solution
- A project lifecycle that's composed of phases, work packages, processes and procedures
- An inventory of accelerators in the form of best practices, guidelines, tools and templates to support the execution of detailed work steps and generate predefined deliverables
- Integration between the solution methodology and a proven project management methodology to ensure project success and the timely and qualitative creation of the promised deliverables
- A library of content based on leading industry reference architectures

All of these elements work together to guarantee project success with predictable delivery dates.

Figure 3 shows Prime for GRC in the form of a low-granularity value chain. The strategy, design, realization, operation and control phases are described along with the core activities and results of each phase.

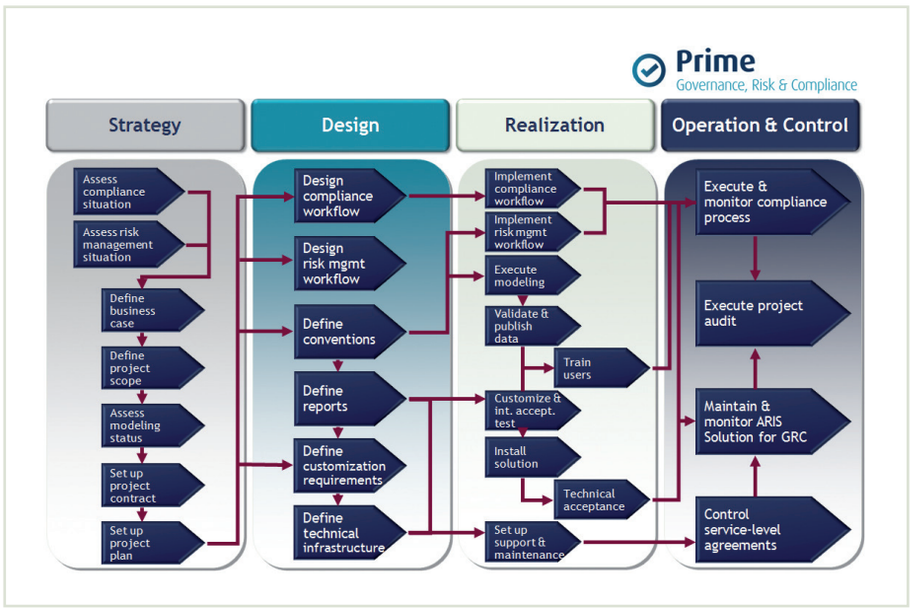

Figure 3: Compliance Management Roadmap

The following text describes each phase with its working steps and goal achievements in more detail.

Phase 1: Strategy

The strategy phase involves analyzing an organization's existing compliance and risk situation. The results of this analysis can include:

- An objective in the form of outcomes to be achieved by the project
- A set of compliance requirements that may be relevant to the company
- The impact of compliance requirements on business, IT and governance processes
- A risk matrix categorizing the risks identified in a risk catalog
- A catalog of measures for handling risk

Defining the project scope and establishing the documentation or modelling status enables a business case to be constructed that sets out the anticipated benefits of the project. Creating the project plan enables a proper project setup.

Phase 2: Design

The design phase is where the requirements from the strategy phase are mapped into the value-adding and IT processes. This may involve assigning critical tasks to multiple users (dual-control principle), incorporating additional approval mechanisms or establishing risk controls. Governance processes, such as compliance management and risk management, are designed and documented in line with defined requirements. Reports are defined for the various stakeholders. Requirements are defined for implementing software support of risk management or compliance processes—for example, via workflow systems.

The design phase results in a comprehensive business concept in documented form that can be used for system and organizational implementation. If new software is required for system support, the business concept is a valuable source of information for preparing and evaluating RFQ documents.

Phase 3: Realization

In this phase, the content from the design phase is translated into an IT concept and the selected software is installed and configured accordingly. Any in-house development work also takes place during the realization phase. Potential users of the systems and employees impacted by organizational changes are trained and prepared for their role in operating the GRC framework.

User feedback options are created, and performance and acceptance tests are designed and implemented. At the end of this phase, the GRC framework is up and running.

Phase 4: Operation & Control

This phase is about supporting operational use of the GRC framework. Progress toward defined objectives is continuously measured and documented. The results are used as input for further optimization, thereby enabling continuous process improvement. Action taken might include executing and monitoring compliance and risk management processes.

Other activities include performing audits, plus executing risk controls and monitoring their effectiveness. Regular reports are generated for the various stakeholders and can be used as proof of compliance. The results of the controlling phase serve as input for strategic fine-tuning as part of continuous business improvement.

ARIS AT WORK WITH PRIME: A REAL-WORLD EXAMPLE

Prime for GRC doesn't require any tool support. However, deploying ARIS tools with Prime significantly boosts efficiency. Software AG consultants have enriched ARIS tools with predefined content, such as reference models and best practice methods, to make projects faster to implement and more cost effective than when starting from scratch.

The intent of Software AG's Prime for GRC is to assure all needed stakeholders within the company are involved in the setup of the GRC framework. Prime also leverages experience gained from previous projects and assures all groups address risks, controls and issues the same way.

A company can use ARIS to implement operational workflows for risk management and create reports. ARIS can automate project steps, such as publishing role-based models and documentation on the corporate intranet or any content that's essential when establishing emergency management.

Figure 4 illustrates how ARIS tools were used in various Prime phases in an SAS 70 [13] project at Software AG. In its data centers, Software AG runs SAP® applications, ARIS and custom-tailored systems for customers, many of whom need to comply with the Sarbanes-Oxley Act. A Sarbanes-Oxley audit requires inclusion of companies that operate systems for the complying organization. A SAS 70 certificate makes it easier to include such external companies in an audit and, hence, was requested by Software AG customers. Software AG is certified for SAS 70 report types I and II.

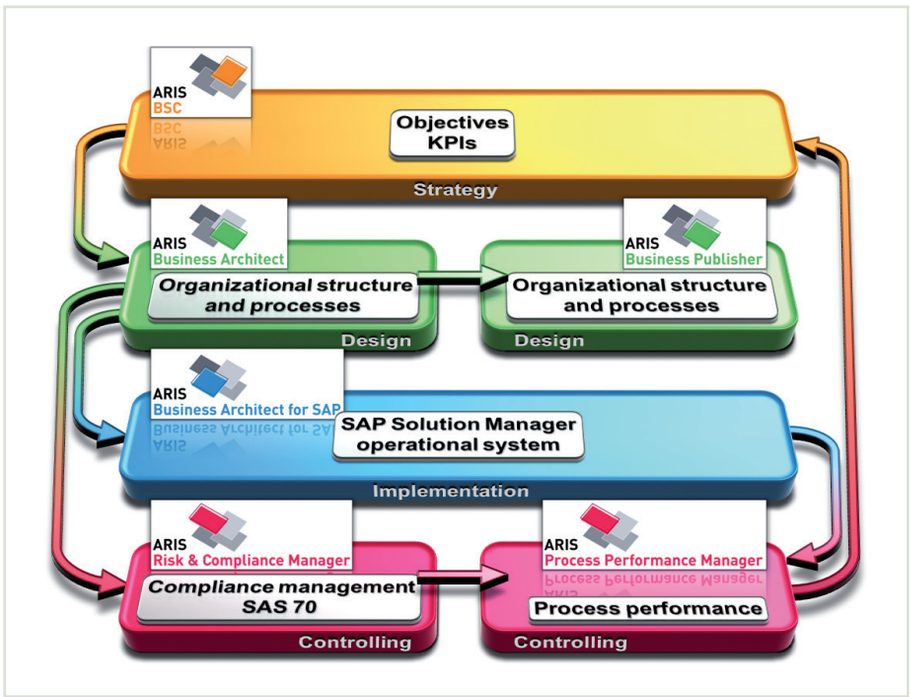

Figure 4: SAS 70 solution from Software AG

At the beginning, Software AG used the balanced scorecard method developed by Norton and Kaplan to define the project strategy. Standard perspectives, including those for financial, customers, processes, and learning and growth, were used. (As a side note, other customer projects have shown that instead of learning and growth, separate employee and infrastructure perspectives can be useful. For example, any involvement of the works council is facilitated by adding the employee perspective.) Additionally, ITIL[14] and COBIT[15] standards were used to define Key Performance Indicators (KPIs) during the strategy phase.

Target diagram and KPI assignment diagrams were modelled using ARIS strategy tools. KPI assignment diagrams contained targets and KPIs for measuring target achievement along with information on organizational responsibility.

The strategic results were used to define the organizational structure (such as organizational charts and role diagrams) and process organization (including process models for value chains and event-driven process chains with differing levels of granularity).

Software AG's ITIL V3-based reference model was used as the foundation. This model contains a predefined organizational structure and process organization as well as KPIs for various processes and a data model and can be used by organizations of all sizes in a wide range of industries.

Using this reference model meant there was no need to start from scratch, which saved time and money because only the models had to be adapted to this unique situation. The Software AG-specific models are part of Software AG's quality management system and were also used as the basis for ISO 9000:2000 certification. In addition, the models are published on a role-specific basis on the intranet and are accessed by users for training and task description purposes.

SAP Solution Manager was chosen as the implementation platform and operational system for service management. Customizing information and documentation were transferred automatically from ARIS design tools to SAP Solution Manager via a bidirectional interface, thus raising certain elements of customizing to the model level. Governance processes ensured consistency of the system and model levels.

In the operation & control phase, ARIS Process Performance Manager was used to manage process performance—for example, throughput times and SLA compliance. Personalized reports were created for each stakeholder. Alert and escalation management procedures were also established.

ARIS Risk & Compliance Manager was deployed to implement risk management and audit management and to provide proof of the effectiveness of risk controls.

Because strategy, design, realization and operation and control activities share the same repository, a wealth of transparent, consistent information is available for process improvement purposes. This also applies to the internal control system and quality management system. Significant savings in process costs and resource requirements for operational processes and GRC processes were achieved in the first year. Many Software AG customers who have implemented comparable solutions have experienced similar results.[16]

CALCULATING THE VALUE OF GRC

The ultimate goal for companies doing GRC is to become a high-performing, well-governed and well-controlled organization. This chart explains the key benefits you can expect from GRC and how to calculate their value.[17]

KEY BENEFIT	BUSINESS IMPACT	HOW TO CALCULATE THE VALUE
Higher Business Efficiency & Cost Savings	• Policy and control management: faster development, review, update, approval, distribution, access and attestation • Risk management: faster risk identification, analysis, evaluation and monitoring • Audit management: improved scoping, scheduling, data collection and reporting • Compliance management: easier control assessments, aggregation of date and reporting • Action management and escalation: faster event identification, notification, escalation, remediation, review and approval • Process improvement: every GRC project optimizes business processes	• Reduced costs of temporary staff like auditors; less alignment needed • Hours saved per function multiplied by the average rate for fully burdened risk, compliance or audit professionals
Risk Reduction & Transparent Compliance Status	• Unified repository across different risk and compliance areas • Common approach for risk assessment and control testing • Transparent ownership of risk and controls • Delivery of "in control" statement	• Reduced incident response costs • Reduced fines and penalties • Reduced capital risks • Increase in risk exposure mitigated per euro/hour spend • Increased customer trust (intangible)
Increased Business Agility	• Risk and controls are linked to processes • Hierarchy of risk and controls creates relations • Transparency, hierarchy and relations are required for business intelligence • Fact-based decisions related to development, procurement and investments • Smoother integration of business partners, acquired entities and new employees	• Numbers of hours/days of reduced compliance training and ramp-up time multiplied by productive output of new employees, partner or acquired entity • Decreased missed opportunities because of lack of compliance or risk insights
Higher Business Effectiveness	• Merger of overlapping laws and regulations into a common set of business requirements • Re-use of business processes, compliance requirements and reports through one single platform • Faster adaption to new regulations	• Payroll savings from avoidance or delay of staff increases • Reduced external audit and risk assessment costs

LOOKING AHEAD: WHAT'S NEXT FOR GRC

Scrutiny of the banking industry has increased the awareness of the importance of a sustainable GRC system. Before that, GRC projects were driven primarily by external regulations or compliance requirements, focused on providing evidence of compliance. The business case was either to comply at any cost or face the negative impact and costs of non-compliancy.

Although an increasing number of software vendors are entering the GRC market, closer inspection reveals that few of them cover the full range of GRC activities. Such solutions are best suited to remove or relieve an existing pain point in the enterprise. Unfortunately, these GRC approaches are siloed, which means that compliance is the only business benefit.

If a second "silo" is adopted, it soon becomes apparent that sharing the same data requires a more sophisticated concept and implementation of the associated interfaces. The majority of solutions are not end-to-end in terms of strategy, design, realization, and operation and control. Without an integrated repository, it is hard to implement a consistent KPI system across all levels or to incorporate a solution into the internal control system or quality management system.

To properly execute a sustainable GRC framework, your company needs to combine best practices, skills, methodologies and technologies to create a seamless body of risks, controls and issues throughout the organization and its business processes. Software AG offers that in a GRC solution that combines the benefits of Prime and also ARIS tools as your needs require.

ARIS, for example, offers a governance engine that can create a workflow instance and execute it using the information stored in the repository.

In the future, more companies will look for operational support of governance processes based on governance rules and using data held in a shared repository—ultimately moving to real-time monitoring and GRC management. This will allow managers to bring regulatory intelligence into GRC dashboards accessible via mobile devices or via online cloud-based services.

For more information on the Software AG GRC Solution, visit www.softwareag.com.

For more details on how Software AG can help with your specific GRC requirements, contact your local Software AG representative.

BIBLIOGRAPHY

[1] C f. Tarantino, A. (editor): Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance: Best Practices. Hoboken, New Jersey 2008, p. 781 ff.

[2] Forrester Research 2010: Market Overview: GRC Platforms, For Security & Risk Professionals, Chris McClean

[3] C f. Schewe, G.: Corporate Governance – Reconciling Management, Control, and Representation of Interests. Berlin 2005

[4] C f. Marx Gómez, J., Junker, H., Odebrecht, S.: IT Controlling – Strategies, Tools, Practice, Berlin 2009

[5] C f. Keitsch, D.: Risk Management, Second Edition, Schäffer-Poeschel, 2004

[6] C f. http://de.wikipedia.org/wiki/Risikomanagement, December 22, 2008

[7] C f. http://de.wikipedia.org/wiki/Demingkreis, December 22, 2008

[8] C f. Königs, Hans-Peter: System-Supported IT Risk Management, Second Edition, Wiesbaden, 2006, p. 2 ff., p. 28 ff.

[9] C f. Keitsch, D.: Risk Management, Second Edition, Schäffer-Poeschel, 2004

[10] C f. BITKOM (publisher): IT Risk and Opportunity Management in the Enterprise, Berlin 2005, p. 6

[11] C f. BITKOM (publisher): IT Risk and Opportunity Management in the Enterprise, Berlin 2005, p. 4

[12] C f. Hagerty, John: ProcessWorld presentation, Berlin 2008

[13] C f. http://www.sas70.com/, January 12, 2009

[14] C f. http://www.ogc.gov.uk/guidance_itil.asp vom, January 12, 2009

[15] C f. http://www.isaca.org/Template.cfm?Section=CO BIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981, January 12, 2009

[16] C f. Wood, D., Business Continuity Management – Keeping the Wheels Turning. In: Oprisk and Compliance 8, 2008 8, p. 18 ff.

[17] "How To Measure The ROI Of A GRC Platform for Security & Risk Professionals" by Chris McClean

TO FIND THE SOFTWARE AG OFFICE NEAREST YOU,

PLEASE VISIT WWW.SOFTWAREAG.COM

Take the next step to get there – faster.

ABOUT SOFTWARE AG

Software AG is the global leader in Business Process Excellence. Our 40 years of innovation include the invention of the first high-performance transactional database, Adabas; the first business process analysis platform, ARIS; and the first B2B server and SOA-based integration platform, webMethods.

We offer our customers end-to-end Business Process Management (BPM) solutions delivering low Total-Cost-of-Ownership and high ease of use. Our industry-leading brands, ARIS, webMethods, Adabas, Natural, CentraSite, Terracotta and IDS Scheer Consulting, represent a unique portfolio encompassing: process strategy, design, integration and control; SOA-based integration and data management; process-driven SAP implementation; and strategic process consulting and services.

Software AG – Get There Faster

SAG_GRC_Audit_Management_WP_Feb12