White Paper

Governance, Risk Management and Compliance: Sustainability and Integration supported by Technology

PRICEWATERHOUSECOOPERS

SAP

PRICEWATERHOUSECOOPERS

White Paper

Governance, Risk Management and Compliance: Sustainability and Integration supported by Technology

Published by PricewaterhouseCoopers AG

by:
Christof Menzies
Alan Martin
Michael Koch
Carsten Trebuth
Steffen Esche
Thomas Heinze
Christiane Roth
Christoph Schellhas
Philipp Stähle

Executive Summary

Growing transparency and increasingly complex stakeholder requirements have put Governance, Risk Management and Compliance (GRC) at the top of the Board agenda.

Today's businesses face more regulation, a wider range of stakeholder expectations and more public scrutiny than ever before. Global opportunities and growth bring global corporate governance responsibilities. Capital markets, consumers, pressure groups, employees and governments are a few of those who rightfully hold companies to account for the way in which they define and execute their corporate strategies. As a result, Governance, Risk Management and Compliance have never been higher on the Board's list of priorities.

A strategic and holistic approach to GRC provides competitive advantage and adds value to the company. The aim is to embed GRC initiatives into the daily business and to achieve synergies by integrating related GRC topics.

The successful, brand-defining corporate citizens of the future will be those that embed their response to key stakeholder demands into the fabric of their business. This can only be achieved by leaving behind the reactive, project-based approach to regulatory compliance that many companies have followed. By taking a strategic and holistic approach to Governance, Risk Management and Compliance (GRC), companies can achieve competitive advantage and add significant value to their organisation.

The paper lays out the vision for that holistic approach, showing how companies can integrate their Governance, Risk Management and Compliance initiatives and embed them into their daily business processes. The goal is to transform GRC activities from a costly burden into a strategic management tool, enabling the company to respond flexibly and effectively to changing stakeholder demands and lay a strong foundation for business success.

Technology is a key success factor in achieving holistic GRC management, allowing companies to attain immediate benefits and to drive long-term value growth.

Technology is a key enabler in achieving this vision. Using illustrations from existing solutions provided by the leading software producer SAP, this paper outlines how technology can support companies along each stage of the path towards integrated GRC. Both on the level of GRC management activities and on the business process level, it becomes clear how technology can provide immediate benefits – for example by updating the Board on the progress of various GRC initiatives by means of an integrated reporting functionality. Further quick wins can be achieved by integrating compliance requirements into workflows within the ERP system, or by using technology to support the development of an efficient and effective user authorisation management.

Technology is also a key driver in realising the strategic GRC vision, for example by providing an integrated platform for a range of key GRC information such as stakeholder requirements, mapped in turn to relevant risks, policies, procedures and controls. Equipped with the transparency provided by such a platform, companies are able to realise synergies between GRC activities, replacing the burden of duplicative compliance and reporting with a holistic GRC approach that directly supports performance objectives.

Contents

Figures

A Today's GRC Challenge

The growing number and complexity of regulatory requirements, the high expectations of stakeholders and increased supervision and reporting demonstrate today more clearly than ever the central importance of corporate governance, risk management and compliance (GRC). Most companies handle these topics in a reactive, fragmented way, focusing mainly on risk avoidance at an operational level in order to meet specific compliance requirements. Such companies are missing the opportunity to leverage their conformance investment by approaching GRC as a strategic tool to drive business performance.

90% of executives see Compliance as a top priority.[1]

A strategic and proactive approach to GRC contributes not only to an efficient and effective fulfilment of compliance requirements, but also enables companies to realise additional benefits. For example, they are enabled to respond earlier, more flexibly and more comprehensively to new or changed stakeholder requirements. This not only enhances their public image for corporate governance, but also helps them to obtain significant competitive advantage from GRC by demonstrating a firm foundation for the long-term profitability of their business.

Definitions of Governance, Risk Management and Compliance

Governance is seen as the processes and structures used to direct and manage the business and affairs of an organisation in a responsible and ethical manner, with the goal of ensuring financial viability and creating value.[2] Governance processes are therefore concerned with defining the company vision, strategy and objectives, defining appropriate organisational structures, directing the company using effective policies and procedures, monitoring performance, and communicating relevant information internally and externally.

Risk Management is defined as a process designed to identify and compensate for potential events that could prevent the fulfilment of the company's objectives.[3] An effective risk management process includes risk identification and documentation, risk analysis, definition and execution of risk management measures as well as the ongoing monitoring of their effectiveness.

Compliance is understood more broadly than mere regulatory conformance. It also involves understanding and delivering on the expectations of all internal and external stakeholders, taking both legal obligations and voluntary standards into consideration.[4] Compliance processes therefore ensure that the stakeholder requirements and associated measures are identified and prioritised, that the effectiveness of the measures is monitored, that weaknesses are addressed, and that appropriate reporting on compliance status is available. Figure 1 illustrates this broad view of compliance.

Figure 1 The broad view of compliance

Companies today are confronted with a growing risk of non-compliance as well as rising compliance costs. This results from the steadily increasing complexity and pervasiveness of stakeholder requirements and the multiple levels of conformance that are required to address them. Prominent examples of this in the regulatory field are the Sarbanes-Oxley Act, Basel II, and the Foreign Corrupt Practices Act. The compliance projects undertaken in recent years have shown that the initial implementation of a single compliance initiative

[1] University Hamburg: Umfrageergebnisse (2006).
[2] PwC/BDI (2005) and PwC/BDI (2002).
[3] COSO (2004).
[4] PwC (2004) and Menzies (2006).

can be a major challenge for a company and involves substantial commitment and effort. However, this does not guarantee ongoing fulfilment of the requirements.

Compliance initiatives are often isolated projects that are largely unconnected to structures already in place to satisfy other requirements.

Companies have typically undertaken compliance projects in response to a specific crisis, or in order to meet a legal deadline, and usually under severe time pressure. Consequently, management was often unable to establish sustainable organisational structures, processes, and technology support for the ongoing compliance effort. The focus was on meeting project deadlines rather than embedding compliance activities into existing business processes. As a result, many compliance initiatives have become isolated, discrete projects that are largely unconnected to structures already in place to satisfy other requirements. If this situation remains, companies will face higher recurring compliance costs coupled with limited involvement by those responsible for the affected business processes. This is likely to cause frustration in the organisation and stifle innovation and growth in the business.

In addition to a lack of integration between compliance initiatives, many companies also approach the topics of governance, risk management and compliance in an uncoordinated fashion.

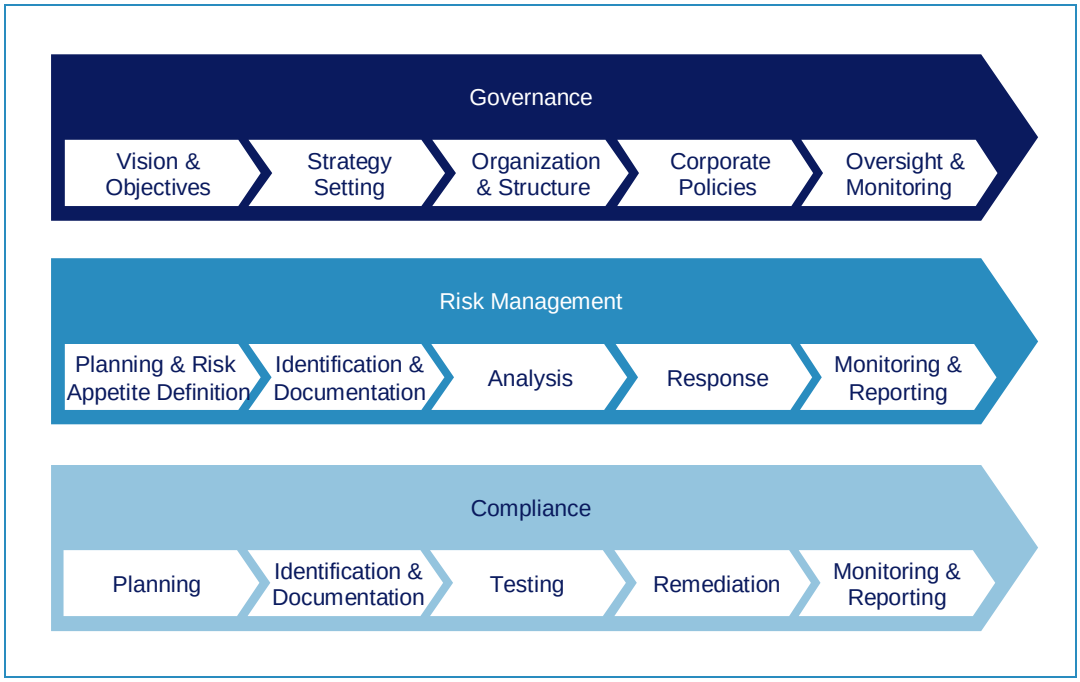

Figure 2 Isolated and fragmented view of Governance, Risk Management and Compliance

In addition to a lack of integration between compliance initiatives, many companies also approach governance, risk management and compliance in an uncoordinated and fragmented fashion (see Figure 2). This has significant consequences. For example, corporate governance is sometimes seen mainly as a formal response to requirements rather than an integral part of the company's management structures and processes. Risk management may also focus too heavily on operational risks, failing to support strategic decision processes. Compliance may be restricted to legal regulations, to the detriment of voluntary standards and obligations. Thus companies often fail to use risk management as an early-warning system with regard to possible weaknesses in corporate governance or within related compliance initiatives.[5] In short, much greater integration between all GRC activities[6] is required in order to gain the full benefit from them. Only then can companies begin to identify the potential synergies to be obtained by integrating various compliance initiatives, for example by standardising documentation standards or technology support.

[5] Note: The term "compliance initiative" refers to a programme aimed at fulfilling a specific stakeholder requirement, often as part of an isolated project unconnected to governance and risk management processes in the company. On the other hand, the term "GRC initiative" is used hereafter in reference to programmes that appropriately integrate and reflect relevant governance, risk management and compliance aspects.
[6] Note: Hereafter, all activities connected with governance, risk management and compliance are referred to as "GRC activities".

58% of companies interviewed consider their compliance approach to be inefficient.[7]

This lack of integration results in numerous silo approaches with regard to processes, organisation and technology. The consequences include:

- Increased complexity in the interfaces between the separate risk management and compliance initiatives, other GRC activities, and the related business processes;
- Insufficient technology integration, leading to a heterogeneous GRC IT landscape;
- Heterogeneous reporting structures based on differing reporting periods, data sources and reporting tools; and
- Lack of an integrated overview of the overall GRC status of the company.

Example : Heterogeneous reporting structures based on a fragmented approach to compliance initiatives

One of the consequences of a fragmented approach to various risk management and compliance initiatives is the emergence of heterogeneous reporting structures. This prevents management from obtaining a comprehensive overview of key compliance and risk indicators, so that an integrated view of the company's compliance and risk status is not available. This is particularly important for senior management, since inadequate reporting and monitoring of GRC activities increases the risk of non-compliance.

The heterogeneous reporting structures result not only from a lack of organisational integration but also due to the differing IT applications used to support the various risk management and compliance initiatives. These applications often have no interfaces with each other, so that considerable manual effort is required, leading to increased risk of error and higher costs. Heterogeneous systems thus lead to resource-intensive reporting processes that draw on diverse applications.

These systems also generally do not allow the use of comparable criteria, standards or methods to analyse risks and other compliance-relevant information across the whole company. As a consequence, the process of aggregating compliance and risk information and providing this to management in a structured and meaningful form becomes very complex and cumbersome.

In summary, it is clear that many companies face a significant challenge in meeting today's demands with regard to governance, risk management and compliance in an efficient and effective manner. The only way to meet this challenge successfully is to adopt a holistic approach to the management of GRC. Companies require an integrated, strategic view of GRC, supported by a sustainable operating model with the aims of:

- Optimal fulfilment of relevant stakeholder requirements in a dynamic and complex business environment, thereby minimising the risk of non-compliance;
- Ensuring the long-term effectiveness of GRC initiatives and reducing costs through increased efficiency;
- Exploiting synergy potential by reducing redundant efforts;
- Aligning the company's aims with the GRC objectives, so that compliance and risk management become integral, value-creating parts of the daily business.

The following section deals with the implications of a holistic approach to GRC management and explores how this can be used as a strategic tool to drive business value by ensuring sustainable compliance with key stakeholder requirements.

"As individual issues, governance, risk management, and compliance have always been fundamental concerns of business and its leaders. What is new is an emerging perception of GRC as an integrated set of concepts that, when applied holistically within an organisation, can add significant value and provide competitive advantage."

Samuel DiPiazza Jr., CEO PricewaterhouseCoopers[8]

[7] University Hamburg: Umfrageergebnisse (2006).
[8] PwC (2005).

B Holistic GRC Management

Holistic management of GRC encompasses sustainable design of relevant GRC initiatives as well as integration of methodologies and content.

The vision for holistic GRC management encompasses two key aspects:
- The sustainability of individual GRC initiatives that are implemented in a company; and
- The integration of GRC initiatives and activities.

Sustainability in this context refers to the merging of governance, risk management and compliance processes as well as to the embedding of GRC initiatives into the existing corporate structures and processes. GRC activities become sustainable when they no longer run in parallel to the business, but are part of the daily life of the organisation.

Integration in the context of holistic GRC management refers to the consolidation of the methodologies and content of different GRC initiatives. The importance of holistic GRC management is clear from the results of the 10th Annual Global CEO Survey organised by PricewaterhouseCoopers.[9] 40% of the CEOs participating in the survey consider overregulation as a fundamental business risk; 33% are very concerned in this regard. Holistic GRC management serves to counteract this risk through effective and efficient handling of compliance with current as well as future requirements.

In order to implement holistic GRC management, companies need to build on existing compliance approaches, gradually developing a holistic approach based on a company-wide and integrated view of Governance, Risk Management and Compliance. The following sections explain the benefits that companies can gain by implementing holistic GRC management, and go on to discuss what is meant by the sustainability and integration of GRC initiatives.

1 The Benefits of Holistic GRC Management

89% of the CEOs surveyed believe that effective handling of GRC can have a positive influence on the reputation or brand of the company.[10]

Transforming an individual GRC initiative into a sustainable process will, in itself, deliver substantial short and medium term benefits. However, in order to obtain the maximum benefit from governance, risk management and compliance, GRC initiatives must also be integrated into a holistic management approach. The short, medium and long term benefits offered by holistic GRC management include the following:
- The creation of flexible and sustainable structures and processes, supported by appropriate technology, in order to fulfil current stakeholder requirements effectively and to enable the company to respond to new requirements flexibly and efficiently;
- The reduction of costs related to governance, risk management and compliance initiatives and the internal control system;
- The establishment of a risk-based decision making process;
- The reduction of non-compliance risk, avoiding associated penalties and loss of reputation and enabling the company to increase its value over the long term;
- The creation of further value for the company through the realisation of synergy potential and organisational improvements prompted by the fulfilment of the stakeholder requirements; and
- The embedding of ethical values in the corporate culture and the creation of an opportunity and risk culture in the company.

Holistic GRC management can thereby become a strategic tool for top management to achieve competitive advantage and to differentiate the company from the competition.

[9] PwC (2007).
[10] PwC (2005).

2 Sustainability of GRC Initiatives

The prerequisites for sustainable GRC are the embedding of compliance initiatives in existing corporate organisational structures, business processes and systems and the close integration of governance, risk management and compliance processes.

For GRC initiatives to be sustainable, they must be embedded in the company's existing organisational structures, processes and systems. By doing so, companies can achieve sustained improvements in the effectiveness and efficiency of the initiatives, supporting their overall strategy and ensuring an optimal cost-benefit ratio. By embedding the controls, transparency will also be improved, and an increased sense of ownership and responsibility for GRC issues among the relevant process owners will result.

A further prerequisite for the sustainability of GRC initiatives is a close linkage and integrated view of governance, risk management and compliance processes in the company (see Figure 3). Closely linking these elements and embedding initiatives in existing corporate structures and processes are essential prerequisites for strategically successful, risk and value-oriented, ethical and compliant corporate management.

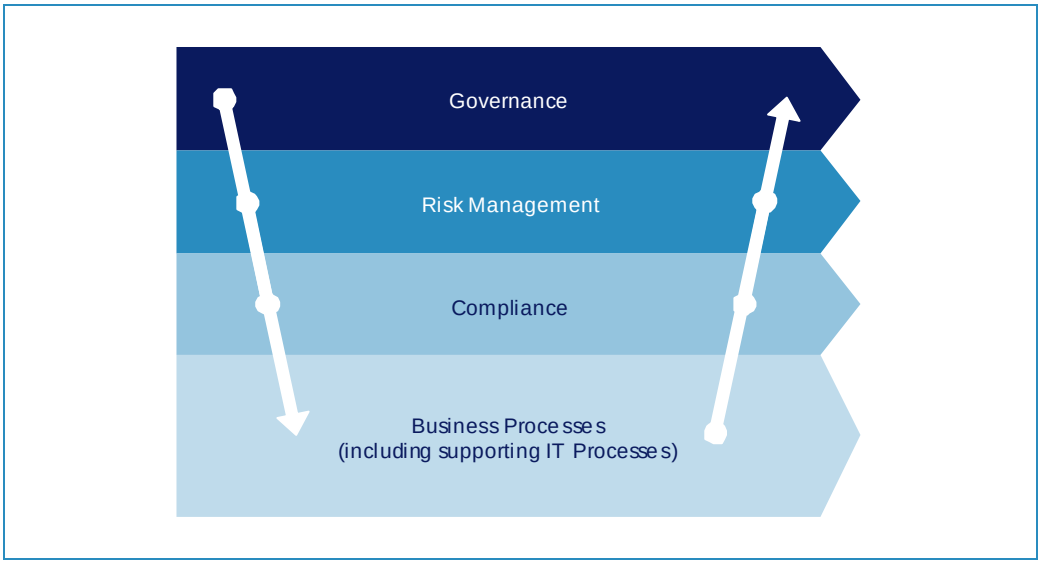

Figure 3 Integrated view of Governance, Risk Management and Compliance

Corporate governance sets the framework consisting of processes and structures for directing and managing a company. It determines the processes, roles and responsibilities for management and for measuring and monitoring performance. Effective governance balances the corporate strategy and objectives with the requirements of relevant stakeholders and the risk appetite of a corporation.

Thus, governance sets the general framework for enterprise-wide risk management. The goal of risk management is to minimise risks that can hinder the achievement of corporate objectives. The response to identified risks is influenced by the company's readiness to accept risk. One example is the risk of not meeting stakeholder expectations, or not fulfilling compliance requirements (non-compliance risk). Readiness to accept risk in terms of compliance with regulatory requirements is usually low, because compliance is often a prerequisite for doing business at all. On the other hand, readiness to accept market and currency risk may be higher. In this respect, companies have different options for dealing with the identified risks:

- Risk acceptance;
- Risk transfer (e.g. insurance);
- Risk elimination; and
- Risk reduction.

An effective integration of governance with risk management and compliance will enable companies to take better decisions on how to respond to a variety of risks, including that of non-compliance. By integrating their risk response into their existing structures and processes, companies will manage the risk of non-compliance as they do all other business risks. In this way, an isolated compliance initiative can become an integrated GRC activity that clearly supports the achievement of corporate objectives.

Example: Sustainability of GRC Initiatives

In the past years, SAP AG has taken a number of measures in order to ensure sustainable implementation of Sarbanes-Oxley Act (SOX) requirements in the company. The goal was to transform the project that had been running for numerous years into an established long term process. The SOX 404 process has been integrated into the Enterprise Risk Management of SAP. In order to achieve this goal, documentation and evaluation processes of the SOX project have been embedded in a uniform and integrated Enterprise Risk Management system.

The Sustainability Elements provide a framework in which to analyse the sustainability of GRC initiatives.

The sustainable design and implementation of GRC initiatives can be analysed using the **Sustainability Elements** (see Figure 4). At the level of individual GRC requirements, these elements reflect the degree to which the GRC activities have been implemented and embedded in the business processes as well as the extent to which governance, risk management and compliance are inter-linked. The analysis usually highlights opportunities for improvement in terms of individual initiatives, but also provides a basis for determining how to consolidate the methodologies and content of individual initiatives.

The purpose and content of the Sustainability Elements is explained below, followed by consideration of the possibilities for integrating different initiatives.

Figure 4 Sustainability Elements

1. GRC Framework

The GRC Framework creates a company-wide, uniform standard with respect to the content and implementation of diverse GRC initiatives. The framework is thus the basis for defining detailed guidelines and working instructions (e.g. for documenting processes and internal controls) and helps derive related actions. The GRC Framework includes, for instance, the GRC vision, strategy and goals of a corporation. Typically, the framework is based on the contents of stakeholder requirements (e.g. in the form of a Rule Base[11]) and describes centralised organisational and procedural standards that are related to compliance.

2. GRC Organisation

A sustainable GRC Organisation is characterised by a framework and management structure that clearly defines roles and responsibilities for GRC processes and activities within the company. This is often led by a business unit that coordinates and monitors company-wide GRC activities. The responsibility structure not only establishes roles and

[11] See section D for a definition of the Rule Base.

responsibilities for the business unit at a corporate level, but also at the operational level in the individual departments and processes. The framework and the responsibility structure is communicated and further integrated into the company through training, and employee development measures, job descriptions and performance target agreements.

3. Scoping and Risk Assessment

The applicability of GRC initiatives at corporate and business unit level is determined by a scoping and risk assessment process, which considers the significance and risk exposure of the company's various business units and areas. Periodic monitoring of the applicability of GRC initiatives ensures that internal and external changes (e.g. regulatory changes, new standards or contractual changes with business partners) are analysed and considered. Thus, the scoping and risk assessment process is a fundamental part of a GRC initiative, and will be even more effective if it is integrated with the strategic and operational risk management process.

4. Technology Support

Technology plays a key role in promoting the effectiveness and efficiency of GRC initiatives and thereby supports the implementation of the other Sustainability Elements. Technology is especially effective in automating the workflows supporting GRC activities, effective authorisation management and in supporting communication and reporting procedures. GRC technology should be integrated into the existing IT infrastructure and be aligned with corporate and IT strategies. The potential benefits of GRC technology are explored further in Section C.

5. Communication Processes

Structured, standardised communication processes that are supported by technology create transparency and increase the effectiveness and efficiency of a GRC initiative. Important synergies can be achieved by integrating GRC-related communication into the existing communication processes. For example the "tone at the top" that is set by top management should be reinforced by well-designed GRC communication processes, tailored to fit the needs of the audience and delivered to the right people at the right time.

6. Training and Human Resource Development Programs

The success of a GRC initiative depends, to a large extent, on the risk awareness and skill set of the employees involved. The development and implementation of suitable training and employee development programs takes this into account and reflects the roles, responsibilities and tasks laid down in the GRC Organisation. The training needs of the employees should be considered and appropriate qualifications should be integrated into the regular employee development and education programs of the company, including evaluation of training effectiveness (e.g. through tests or as part of a performance target agreement).

7. GRC Documentation Processes

The importance of documentation processes varies widely according to the requirements of each GRC initiative. The primary goal is to ensure sufficient documentation of guidelines, working instructions, business processes and the methods used to evaluate GRC effectiveness. Transparency and consistency of the documentation are important criteria in this context. Standards and guidelines, monitoring of changes, and quality assurance processes play a key role in ensuring that documentation remains up to date, complete, and accurate. Again, technology can provide substantial support in achieving this.

8. GRC Monitoring and Reporting

Sustainable GRC initiatives are also characterised by effective monitoring and reporting processes that are integrated into the existing operational structures. Monitoring, in this context, includes the process of continuously identifying weaknesses, gaps or other risks of non-compliance, as well as delays and budget overruns. For Sarbanes-Oxley compliance, this would include monitoring and reporting on control effectiveness assessments. Monitoring and reporting should be based on consistent key performance indicators that can be summarised in status reports for different management levels. This

provides the basis for appropriate escalation procedures for critical issues identified, such as compliance failures or risks.

9. Remediation Process

Failures to meet stakeholder requirements are identified not only through GRC monitoring and reporting but also as part of daily business. In the same way, business managers also initiate remediation measures to address identified issues. The process for defining, implementing and monitoring the effectiveness of these measures needs to be standardised for the relevant GRC initiative to ensure a consistent and sustainable approach to remediation.

The effective design and implementation of these Sustainability Elements creates the basis for fulfilling GRC initiatives as a part of the company's daily business. In this regard, technology plays an important role. However, the design and implementation of the elements is not a one-off effort. In order to pursue further benefits, a repeated analysis and optimisation of these aspects is necessary.

Looking beyond the immediate goal of achieving individually sustainable GRC initiatives, companies are looking to identify synergies that arise from integrating different GRC initiatives with each other. The analysis of the Sustainability Elements provides an excellent basis for this, by comparing how each element is addressed under different GRC initiatives. The integration of GRC initiatives is the theme of the following section.

"We take a holistic approach to fulfilling legal requirements and implementing internal control mechanisms. This ensures the greatest possible transparency and security across all areas and applications."

Dr. Werner Brandt, CFO, Member of the SAP Executive Board, SAP AG

3 Integration of GRC Initiatives

Companies are faced with a multitude of diverse stakeholder demands that are usually addressed using individual GRC initiatives. Although such initiatives may be individually sustainable (as defined by the Sustainability Elements above), they are often implemented in isolation, unconnected to related GRC topics. A number of negative consequences may result, for instance:

- The emergence of inefficient parallel structures, operating in a heterogeneous IT environment;
- An associated increase in cost and frustration among affected staff, characterised by "assessment fatigue";
- Ineffective overall monitoring of the company's GRC status, owing to the lack of comparable data; and
- As a result of the above, a higher risk of compliance issues "falling through the cracks", or going undetected.

Holistic GRC management ensures both the sustainability of individual GRC initiatives and the realisation of synergies achieved by integrating related initiatives.

In view of these drawbacks, it is clear that an isolated and fragmented approach to GRC exposes companies to unnecessary risks. It is therefore not enough to ensure that individual GRC initiatives are sustainable – rather, an integrated approach to related initiatives is needed to turn the effort invested in GRC into competitive advantage for the company. Based on the analysis of the Sustainability Elements suggested above, synergies can be realised and, at the same time, flexible structures and processes can be established, allowing new or changing stakeholder requirements to be fulfilled with less disruption to the daily business – for instance, by using integrated IT systems or by implementing standardised processes for meeting different requirements.

The Sustainability Elements described earlier form the basis for the identification of integration potential. The standardised implementation of these elements in the different GRC initiatives creates transparency and comparability, thereby allowing a systematic alignment of the different initiatives.

Full integration of all GRC activities is not usually the goal, if only because the differences in subject matter between some GRC initiatives are too great. The level of achievable integration can best be determined by viewing it at different levels, for example by distinguishing between methodology and content. Or, integration can begin by focusing on **GRC management processes**[12] and then extend deeper to the **business process** level. (See Figure 5)

The possibilities for the integration of GRC initiatives should be considered at different levels – methodology vs. content, and GRC management process vs. business process.

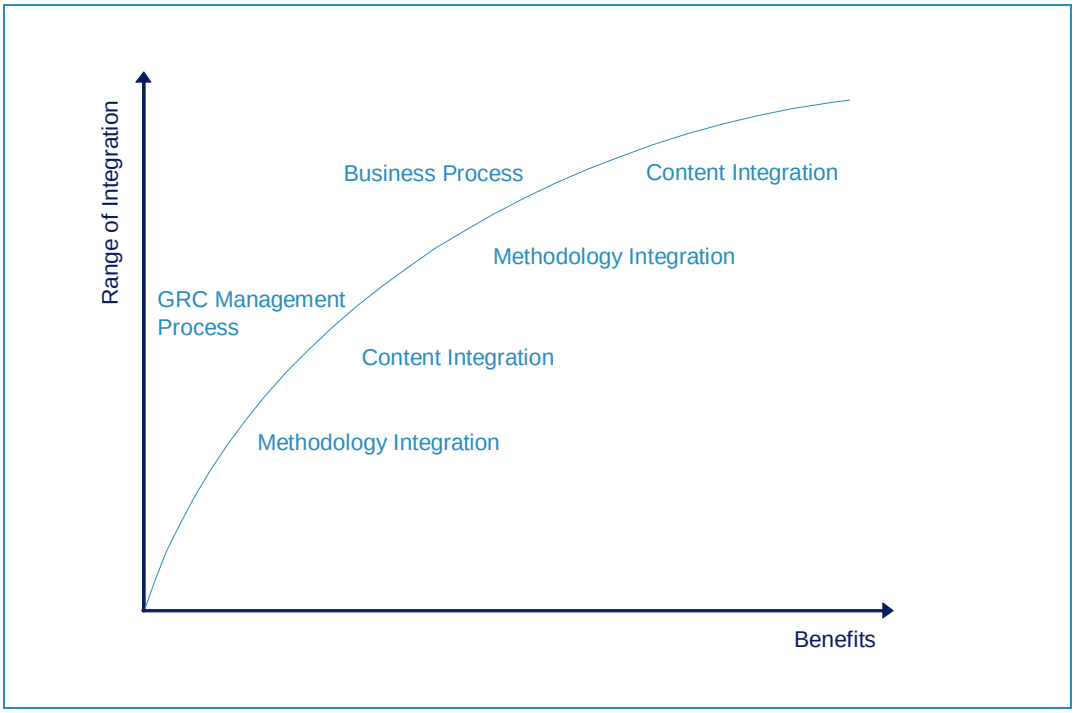

Figure 5 Levels of integration

At the methodology level, the main goal is to standardise the Sustainability Elements - or GRC management processes - for different GRC initiatives. An obvious example is the use of a common GRC technology solution to support multiple initiatives. Also, the approach to training and qualifications or the design of GRC frameworks can relatively easily be merged in terms of methodology.

[12] Note: GRC management processes include those activities performed “on top” of the business processes in order to achieve GRC-related objectives – e.g. compliance with a particular regulation.

Example: Integration of Reporting Methodology

Analysis of GRC monitoring and reporting processes has shown that in many companies, individual addressees – especially top management – are confronted with a wide variety of GRC-related reports. This makes it difficult or impossible to obtain a sensible overview of the company's compliance status or of key opportunities and risks. These reports are not only structured differently, they are also based on different terminology and are prepared with differing frequency. Moreover, there are often different escalation processes, which are not integrated or formalised for critical issues.

The different reporting processes also lead to uncertainty as to whether risks or compliance violations have been reported from different perspectives multiple times to the same addressees, or whether reported cases actually relate to different issues. Put simply, management may ask whether there is one problem or ten problems, and what does this mean for the company as a whole? Integration of monitoring and reporting processes can serve as the starting point on the journey to a stronger integration of diverse risk management and compliance topics. On this journey, the following points should be considered:

- Clear definition of scope;
- Formulation of uniform terminology;
- Definition of the addressees for GRC monitoring and reporting;
- Analysis of information needs and preferences with regard to efficient use of GRC-related information;
- Determination of the information needed, definition of the level of detail, frequency and the method of preparation and presentation of information;
- Definition of GRC monitoring and reporting processes as well as the definition of an escalation process;
- Implementation of suitable technological support (e.g. on the basis of SAP xApp Analytics/SAP NetWeaver BI); and
- Design and implementation of authorisation management to ensure that only authorised persons have access to confidential GRC information.

Standardisation achieved through the integration of methodologies can be used as a basis for the next level of integration, focusing on the subject matter or content addressed by the GRC management processes. Assuming that the initiatives concerned have a similar subject matter, overlapping content and as a result, potential synergies between the relevant GRC activities can be identified. An example of integrated content at the GRC management process level would be common controls testing for different regulatory requirements.

In addition to integration at the GRC management process level, methodology and content integration can also be achieved at the business process level. An example of content integration at this level would be the identification of redundant controls that each address different GRC requirements and are carried out independently of one another. These could be replaced with a common control activity that addresses both requirements at the same time.

Example: Integration of GRC initiatives related to the Sarbanes-Oxley and Foreign Corrupt Practices Acts

The potential for integration is well illustrated by considering two major compliance requirements faced by companies listed in the USA – the **Sarbanes-Oxley Act** (SOX) and the **Foreign Corrupt Practices Act** (FCPA). Both topics have a significant impact on many of the same business processes, and require similar levels of monitoring and control to achieve effective compliance. However, the two topics have nonetheless been treated separately in many companies, leading to the danger of risks "falling through the cracks".

The different compliance reporting requirements for SOX and FCPA have often led to a differing level of attention given by companies to each topic. Section 404 of SOX requires a specific, audited report on the ongoing effectiveness of internal control over financial reporting, leading companies to invest major effort to ensure a positive audit report. On the other hand, FCPA compliance becomes a public issue only when a possible breach of the law is suspected, meaning that some companies have not focused sufficiently on preventive controls.

An integrative approach can help companies avoid these pitfalls by leveraging the investment made in SOX compliance to ensure that adequate preventive measures are in place for FCPA as well.

Integration at the GRC Management Process Level and the Business Process Level

Since both SOX and FCPA affect similar operational processes, it makes sense to pursue integration at all levels. The integrative approach starts with a consideration of the common risks threatening compliance, followed by development of a common mitigation strategy. On this basis, standardised controls addressing these common risks can be integrated into the business processes, thereby increasing compliance effectiveness and allowing synergies to be achieved. The following opportunities for integrating SOX and FCPA initiatives are clear at the two different process levels:

Phase 1: Integration at the GRC Management Process Level:

- Define the GRC requirements and their impact on the company's processes;
- Develop a standardised risk assessment and compliance scoping approach (i.e. identify the organisational units, types of business, and operational processes most affected by both compliance requirements);
- Establish a common, risk-oriented, top-down approach to documenting, assessing and reporting on the control environment, covering especially the company-level controls and "softer" COSO components (Code of conduct, HR-related processes, tone at the top); process controls (e.g. extending the standard SOX risk and control templates to include FCPA-related topics); and compliance technology support (e.g. use of a common platform such as SAP GRC Process Control).

Phase 2: Integration at the Business Process Level

- Align and integrate relevant policies, procedures and operational controls with regard to financial reporting compliance and ethical business practices;
- Clarify operational roles and responsibilities with regard to SOX and FCPA compliance and ensure that these are equally reflected in recruitment guidelines and staff performance measurement;
- Incorporate compliance risks for both areas in the company's enterprise risk management program to ensure consistent risk evaluation, monitoring and reporting across all units and processes;
- Integrate the training and communication programs with regard to SOX and FCPA;
- Integrate control procedures to cover risks in both areas, especially in respect to procurement (e.g. payments to sales consultants), sales (e.g. pricing and discounts, contracting), cash and bank account management;
- Optimise the use of automated controls and the system user access concept to ensure adequate coverage of risks in both areas, e.g. with the support of SAP GRC Access Control.

C Technology as a key success factor illustrated by SAP solutions

As described earlier, companies often address new or changed compliance requirements with an ad-hoc approach and in an uncoordinated manner due to lack of time and high complexity. From a technology perspective, such an approach means that necessary activities will not or maybe even cannot be implemented in a fully integrated and sustainable manner. Experience shows that many companies implement various isolated applications to support compliance requirements in parallel to existing systems and applications. Over time these solutions lead to an increasingly heterogeneous and complex GRC IT landscape. The growing complexity of the emerging structures results in higher costs for controlling and monitoring of compliance.

Effective technological support contributes to the design of sustainable GRC initiatives and to the leveraging of synergies by integrating those initiatives.

Therefore, using appropriate technologies becomes a key success factor for the implementation of truly holistic GRC management. Effective technological support not only contributes to the sustainable design of GRC initiatives but also to leveraging synergies that arise from the integration of different initiatives. The technology used should support the design of the Sustainability Elements as described in section B.3. Further benefits are achieved when GRC technologies and ERP systems work in an integrated fashion and are closely linked to each other. This allows comprehensive, company-wide, reliable, and meaningful GRC monitoring and reporting.

The following section will demonstrate the extent to which existing GRC activities in companies can be supported by SAP solutions for GRC and how they can interact with ERP and legacy systems. Figure 6 shows the solutions within the SAP solution portfolio which are available at the moment or will be available in the near future. The individual functionalities of these applications aim to support governance, risk management, and business processes with an optimal degree of automation. The modules support the respective GRC activities within the processes and use data from the SAP GRC Repository.

The application SAP GRC Risk Management provides a global framework of risk management methodologies for processes in all business areas. Risks that are to be compensated by an effective and efficient internal control system are captured within the SAP GRC Risk Management solution and can be monitored in SAP GRC Process Control at the process execution and control level.

The solutions SAP GRC Global Trade Services and SAP Environment, Health & Safety provide special processes and procedures meeting the requirements of foreign trade as well as environmental protection, and health and safety in the workplace. By using these modules, a substantial control set is embedded into the business processes in order to ensure compliance with specific requirements.

Change and approval processes concerning access rights to ERP systems are supported by SAP GRC Access Control. This application contains processes and controls to reduce and to prevent risks with respect to segregation of duties and system authorisation.

SAP GRC Corporate Sustainability Management is another application within the GRC suite that enables companies to promote their brands and identify new opportunities for taking on increased social responsibility by issuing corporate sustainability reports. As an example, it enables the definition, measurement, and evaluation of economic, ecological, and social performance indicators.

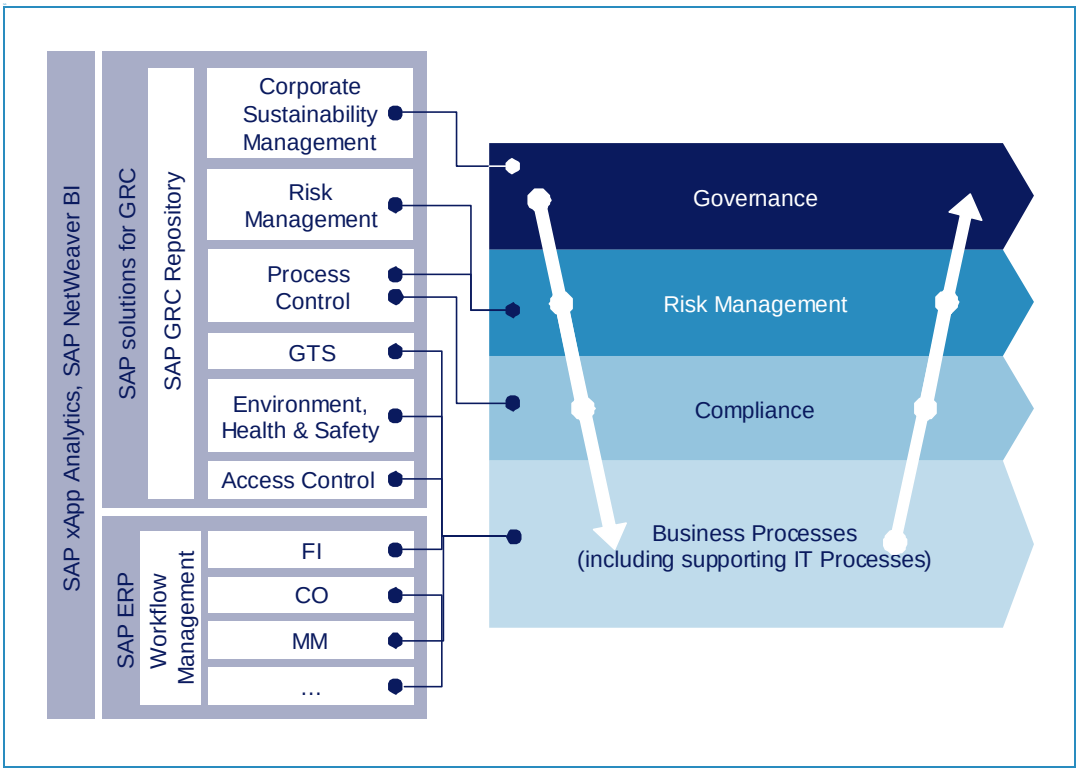

Figure 6 Applying technology as part of holistic GRC management

All applications of the SAP solutions for GRC have integrated reporting functionalities and provide Business Intelligence interfaces (BI-interfaces) so that information relevant to GRC can be made available in a consolidated and aggregated form.

In the following sections, the functionalities and possible fields of application of each solution will be examined. This analysis will be performed from the perspectives of GRC management and business processes (including supporting IT processes). In order to fully comprehend the possibilities for technology to play a supporting role, governance, risk management and compliance processes as well as business, authorisation, and IT processes will also be discussed .

Outlook: SAP GRC Technology Foundation

In the future, the SAP GRC Technology Foundation will function as the central integration platform for all GRC applications. It will be open to third party solutions addressing specific GRC topics. The foundation consists of the SAP GRC Repository, which allows for consistent storage of all GRC data as well as of tools and components for tailoring company specific GRC solutions. Thus, the SAP GRC Repository provides a single version of truth for all GRC data on top of which an integrated GRC monitoring and reporting system is set up. Likewise, the repository also allows for the integration of external data such as best practices or benchmarking information delivered by content providers. Further functions of the SAP GRC Technology Foundation are central authorisation management as well as a process modelling tool for the creation of GRC workflows.

1 IT support of Governance Processes

IT support of governance processes is particularly concerned with the central storage of relevant GRC information (single version of truth) as well as the monitoring and evaluation of this information. For example, one challenge within the governance process arises because relevant information is neither collected nor analysed, since the communication of policies and guidelines and the monitoring of compliance with these is, in most cases, not managed in a sustainable manner. The design and implementation of governance processes should ensure that such data are collected and stored, allowing the company to obtain a meaningful overview of relevant GRC information.

The solution within SAP's GRC portfolio to the problem of central data storage is the SAP GRC Repository. Additionally, the module SAP GRC Corporate Sustainability Management allows the evaluation of compliance with policies and guidelines. By using SAP NetWeaver Business Intelligence (SAP NetWeaver BI) and SAP xApp Analytics on top of the SAP solutions for GRC, sustainable support for GRC monitoring and reporting activities is provided.

SAP GRC Repository

The SAP GRC Repository will help to increase transparency, thereby enabling adequate oversight as stakeholder expectations grow. Strategic goals, risk management, and compliance activities will be aligned and supported in an integrated manner by using the repository. Primarily, this is achieved by using consistent definition of terms (consistent semantics) as well as standardised data structures for the storage of GRC-related data. All available data and documents, such as policies and guidelines, working instructions, process descriptions, risk and control libraries, test plans and evidence of compliance with guidelines can be stored centrally. Therefore, the SAP GRC Repository will take on an integrative function within the SAP solutions for GRC.[13] This function will assist in effective monitoring of GRC activities and systematic analysis of risks.

SAP GRC Corporate Sustainability Management

This application makes compliance with guidelines and working instructions measurable via appropriate performance indicators, thereby enabling the evaluation of compliance through reporting as well as internal and external benchmarking. SAP GRC Corporate Sustainability Management offers direct access to the other applications of the GRC solution portfolio, to ERP, and to third party systems. It also offers the functionality to manually enter relevant GRC information. This information is captured through a standardised process, which enables the collection, validation, consolidation, and evaluation of relevant data and information. Reporting units can be defined to enable customised analysis. Examples for reporting units include countries, regions, organisational units or divisions.

Integrated GRC monitoring and reporting provides a meaningful overview of GRC activities.

SAP NetWeaver Business Intelligence (SAP NetWeaver BI) and SAP xApp Analytics

All applications of the SAP solutions for GRC have built-in reporting functionality. Moreover, the modules provide interfaces for SAP NetWeaver BI integration, making it possible to use SAP NetWeaver BI for GRC monitoring and reporting. using this, management dashboards can be created directly using SAP NetWeaver BI or in combination with SAP xApp Analytics. With this functionality, those responsible for GRC such as the CEO, CFO or the Compliance Officer, obtain a timely and comprehensive overview of the compliance status of divisions as well as of the whole company. Management dashboards can be tailored to specific audiences and have drill-down capabilities, which make it possible to display information at various aggregation levels.

2 IT support of Risk Management and Compliance Processes

As risk management and compliance processes contribute directly to the fulfilment of stakeholder requirements, these processes should be closely linked in order to identify risks consistently and in a timely manner, and to address the risks with appropriate compliance activities. The information gathered in this context also supports the company's strategic and operational planning.

Generally, to take full advantage of the potential such a holistic approach offers, the responsible risk management function needs to take on a proactive role in the company. In practice, risk management and compliance are often handled reactively. Within the risk management process, risks are usually documented periodically. When implementing proactive risk management, companies face the challenge of identifying risks continuously

[13] Note: With the GRC Technology Foundation the SAP GRC Repository's importance is expected to grow through further integration.

and independently of the periodic risk documentation and to use consistent and objective criteria for evaluation.

Compliance processes are needed to address identified risks with appropriate risk elimination or reduction measures.[14] The support of compliance processes with technology is handled very differently in many companies. Even within one company, differences between the various compliance initiatives can be observed. The key challenges facing companies with regard to technology support for compliance processes are:

- A consistent understanding of compliance is needed across initiatives, based on common terminology and definitions (common semantics);
- When implementing individual GRC initiatives, technical support for the documentation should be considered right from the start in order to keep manual efforts to a minimum;
- Monitoring and testing of controls as well as management self-assessment should be automated and adequately supported by technology;
- The evaluation of the compliance status with appropriate GRC monitoring and reporting requires that relevant compliance information is made centrally available in electronic form.

Appropriate use of technology helps companies face these challenges and increase the effectiveness and efficiency of processes. For example, comprehensive technological support of risk and compliance processes facilitates the real time implementation of an early warning system for risks. Such a system reduces the risk of non-compliance and can be used as a strategic tool in the company. Furthermore, technology supports the integration of risk management and compliance processes as well as the creation and maintenance of consistent standards. With this support, compliance with standards becomes measurable and automation of controls and processes, such as approval procedures, is facilitated.

To technologically support risk management and compliance processes in an integrated manner, the SAP solutions for GRC include the applications SAP GRC Risk Management and SAP GRC Process Control. These will be further integrated in the course of the development of the SAP GRC Technology Foundation[15].

SAP GRC Risk Management

Comprehensive Risk Management: Risks are identified and assessed in order to derive measures for avoiding or reducing them.

The risk management application supports the implementation of company-wide proactive risk management. Important information can be made available to the risk manager on a timely basis, e.g. through specific dashboards and reports as well as in the form of personalised scorecards. With this information, risk indicators can be analysed and necessary measures can be initiated systematically. Further functionalities of SAP GRC Risk Management include for example:

- A framework concept with best practices and a predefined risk management process, which includes risk planning, risk identification, risk analysis, as well as derivation of measures to compensate for and monitor risks;
- Access to data and information from other SAP GRC modules and legacy systems;
- Support for the analysis of risk impact and the likelihood of occurrence, considering both financial and qualitative aspects;
- Monitoring of the entire risk portfolio using worldwide standardised risk profiles at the operational and the strategic level.

The integration to ERP systems helps to embed risk management into business processes. For instance, risks and thresholds can be assigned to customer orders. As soon as a sales order is created that exceeds this threshold, the salesperson is alerted that a risk analysis needs to be performed. The employee is informed about the identified risk automatically via e-mail. Additional risks can be added and other persons can be informed about the risk. In addition, the workflow functionality involves a risk manager or a risk owner in the whole process for evaluating and monitoring the risk.

[14] Alternatives for how identified risks can be handled are discussed in section B.1.
[15] See page 18 for an outlook on SAP GRC Technology Foundation.

SAP GRC Process Control

Increased automation of the internal control system: SAP GRC Process Control enables increased automation of the entire internal control system and reduces the need for costly manual controls

GRC Process Control provides technological support for compliance processes. The support comprises the documentation of controls for identified risks within business processes, the evaluation and testing of controls, as well as monitoring and coordinating the remediation of control weaknesses. The application helps to provide a comprehensive overview of compliance initiatives and their status.

By implementing automated controls in business processes[16], the number of time-intensive manual control activities can be reduced. SAP GRC Process Control supports companies in further automating control activities and associated workflows. Examples of SAP GRC Process Control functionalities include:

- Providing detailed instructions and approved templates, which testers can use to carry out their manual tests;
- Executing self-assessments for controls or other compliance indicators at different levels in a company and management certifications;
- Flexible survey functionality for the creation of compliance and risk questionnaires;
- Monitoring of configurations and transactions within processes such as procurement, order processing, and billing via automated control testing in order to reduce the effort necessary for monitoring controls;
- Forwarding of manual control tests to responsible employees through automated workflow;
- Integration with SAP GRC Access Control for automatic control of segregation of duties;
- Execution of an electronic bottom-up sign-off process across all relevant levels;
- Identification of violations of control instructions and prioritisation of remediation activities with a global heat map;
- Integrated reporting for monitoring the compliance status of relevant compliance initiatives (including interfaces for BI integration).

Systematic use of SAP's solutions for risk management and business process controls and the customisation of these applications to a company's GRC initiatives help to generate the following benefits:

- Comprehensive risk management enables risks to be identified and evaluated at an early stage so that effective measures to avoid or reduce the risks can be derived;
- By increasing transparency of risk management and compliance processes, the company's performance can be boosted and forecasting can be improved;
- Stronger automation as well as the analysis and monitoring of risks contribute to sustainability and reduce manual efforts and costs;
- A proactive approach allows effective management of operational risks and positively affects intangible assets such as brand and reputation;
- Technological support for risk management and compliance processes is a crucial prerequisite for sustainable GRC monitoring and reporting;
- An early warning system can be created by combining automated controls monitoring in ERP systems with risk management;
- With the survey functionality of SAP GRC Process Control, compliance and risk indicators can be gathered through questionnaires. The results can be used as evidence of control effectiveness, supporting the analysis of the company's overall GRC status.

3 IT Support of Compliance within Business Processes

Nearly all business processes in a company are supported by ERP systems such as SAP ERP. When optimising ERP systems, the focus usually lies on aspects relevant for performance, such as the reduction of processing time or process costs. The system's capabilities to support compliance are often not fully exploited. Manual controls are often implemented, even though the ERP system offers ways to automate these controls. The potential use and benefits of automated controls will be discussed below. In this respect, it is important to distinguish between preventive and detective controls.

[16] Automated controls in business processes are described in section C.3.

Detective controls are used to identify errors or violations of compliance standards that have already occurred. Subsequent counter measures correct or remediate the effects of such violations. Naturally, depending on the kind of violation and the time of its detection, there is a risk that not all the consequences can be corrected.

On the other hand, preventive controls help to prevent failures or compliance violations and their negative consequences from occurring at all. Thus, an increased use of preventive controls can increase the effectiveness of the internal control system. Furthermore, extensive remediation efforts can be avoided, increasing efficiency.

Additionally, controls are characterised by a varying degree of automation, which ranges from manual, to semi-automated, up to fully automated (see Figure 7).This characterisation is important with respect to the effectiveness and efficiency of preventive controls.

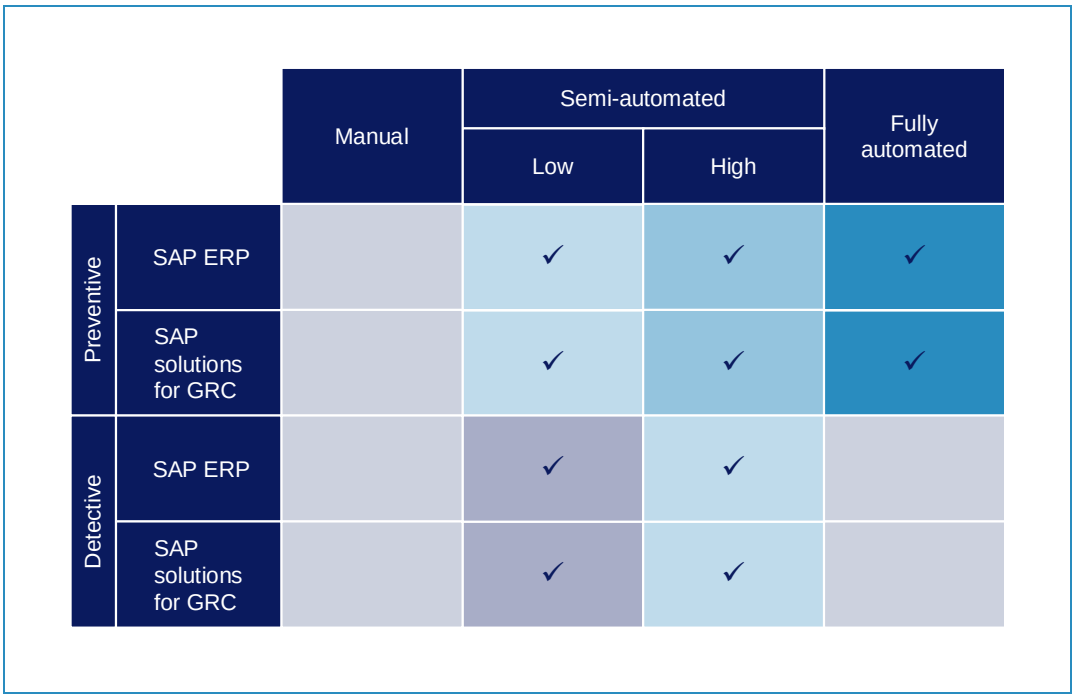

Figure 7 Classification of internal controls

Automation of controls means that control execution is at least partially supported by technology. Semi-automated controls can be preventive as well as detective, while fully automated controls are generally preventive.[17] Fully automated controls stop the process until the control can be carried out without disruption, thereby ensuring compliance.

Significant effects in terms of the sustainability and efficiency of the internal control system can be achieved by increasing technological support for controls and the number of preventive controls.

Automation of preventive controls has the following advantages:
- Reduction of resources necessary for control execution;
- Increased process throughput since control execution is accelerated (accepting the risk of process interruptions);
- Increased control effectiveness;
- Efficient administration of control evidence;
- Reduction of testing efforts, by reducing the necessary sample size and automated testing.

Automating preventive controls can also allow approval processes to be improved, for example by implementing a workflow within the system. Furthermore, automation has the

[17] See section C.2 regarding the increased automation of the internal control system.

effect that information especially relevant for the design and execution of controls in IT systems is stored comprehensively. This information can in turn ease control effectiveness testing, increase transparency of the status of an approval and reduce the efforts related to control execution. In this example, the usage of workflows represents only a minor automation as reports might be generated automatically, but evaluation and further processing mostly have to be carried out manually.

SAP's ERP system offers a large number of automated controls, which can be used to achieve compliance with relevant standards if the system is configured properly. These controls are already embedded into the business processes and not only have the advantage of increased efficiency because of their automation, but are also carried out preventively. They should be used in the best possible manner in order to increase efficiency of all GRC initiatives within business processes.

In addition to automated controls within SAP ERP, the SAP solutions for GRC provide other applications for specific business processes.[18] They support companies that have to comply with special requirements by providing automated controls for business processes relating to foreign trade as well as environmental protection and health and safety in the workplace.

SAP GRC Global Trade Services

Globalisation and the resulting cross border traffic of goods have drastically increased the complexity of transactions and associated risks. Foreign trade treaties, laws, and regulation as well as increased interaction with customs authorities especially contribute to this complexity. Companies face the challenge of having to react to relevant requirements flexibly and in a timely manner in order to ensure sustainable business success and compliance with country specific trade restrictions. By doing so, the increased risk of non-compliance and non-payment can be minimised. SAP GRC Global Trade Services helps companies to meet the challenge of global trade in a sustainable manner with an integrated solution.

By using SAP GRC Global Trade Services the following benefits can be achieved:

- Standardisation, automation, and optimisation of foreign trade processes, and safeguarding of compliance by integration of preventive controls into processes, for example by ensuring compliance with international trade restrictions through automated checks of embargo and boycott lists;
- Facilitation of interaction with responsible customs authorities by supporting the determination of tariff and customs values, and the preparation and printing of foreign trade documents, as well as support of communication with respective customs (e.g. NCTS, ATLAS), which will be a mandatory part of foreign trade in the future;
- Acceleration of the customer billing process through efficient cross-border goods and information routing, thus improving the structure of accounts receivables; and
- Automation and acceleration of reimbursements through efficient support of export reimbursements as well as preference processing and calculation.

SAP Environment, Health and Safety (SAP EH&S)

Those businesses operating internationally must comply with a variety of regulations concerning the environment and safety in the workplace. Requirements in the areas of environment, health and safety are subject to constant change, which constitutes an additional challenge.

As an integral part of the SAP solutions for GRC, SAP EH&S supports compliance by integrating legal requirements efficiently into business processes. Requirements arising from the Restriction of Hazardous Substances (ROHS) and from the Waste Electrical and Electronic Equipment (WEEE) Directive are incorporated as well as the Health and Safety at Work Acts. For example, it is possible to define special locations where hazardous substances are to be stored. If such a rule is violated, stockpiling can be stopped or the order can be blocked directly during the purchasing process. Furthermore, the solution supports the management of hazardous material, hazardous goods, and waste as well as

[18] Note: These were part of the SAP Business Suite.

safety at the workplace, occupational medicine and efficient environment and security management.

SAP EH&S helps to achieve the following benefits:
- Product safety of hazardous goods with central administration of all product data and provision of information exactly where it is needed within the processes;
- Flexible and quick response to changes in rules and regulation in the areas of safety at the workplace and product safety;
- Optimisation through standardisation of process flows, documentation, and communication by integration of hazardous material management processes, claim and accident management processes in the procurement, inventory, safety at the workplace, and security processes;
- Improvement of decision making processes by the provision of high quality and timely information created through aggregation and evaluation of data.

Sustainable compliance can be achieved if controls that are already available in today's SAP ERP modules are integrated into business processes. By using SAP GRC Global Trade Services, SAP EH&S and the other available SAP solutions for GRC, the effectiveness of the internal control system can be increased and service processes can be effectively monitored and secured.

4 IT Support of Compliance within Approval and IT Processes

Company-wide access and authorisation control: SAP software supports organisation, control, and auditing of a company's role and authorisation concept, thus avoiding segregation of duty risks. Unauthorised access and abuse of authorisations is prevented.

The growing complexity of IT and authorisation structures makes it difficult for companies to maintain effective oversight. The problem is aggravated when companies are not able to analyse existing authorisation structures. Furthermore, growing complexity increases the efforts necessary to secure compliance. For instance, companies face the challenge of having to implement standardised communication processes between departments, in order to ensure effective access rights management. Automated workflows and preventive controls help to meet the challenge. Nevertheless, appropriate implementation often proves to be difficult in practice.

An important part of an effective and sustainable internal control system is the implementation and monitoring of segregation of duties (SoD). Sensitive authorisations for all operational and administrative areas should be handled with caution. These rights need to be monitored carefully and granted restrictively. Furthermore, sustainable segregation of duties should be ensured by embedding it directly into the processes and the control environment. Future organisational changes, e.g. those resulting from market changes, should be monitored constantly. Within this context, companies face the following challenges:
- Identifying relevant segregation of duties risks and development of a standardised segregation of duties framework;
- Analysing risks within systems and evaluation of results;
- Handling of conflicts and violations within departments and development of solutions;
- Ensuring sustainable monitoring of these risks as well as constant expansion and improvement of the framework to keep pace with a dynamic environment; and
- Embedding segregation of duties into daily business operations and the control structure.

SAP GRC Access Control can contribute to meeting the challenge. The application supports process owners, data owners and IT managers during the entire process. SAP GRC Access Control contains the following capabilities:

Risk Analysis and Remediation

SAP GRC Access Control supports the identification, monitoring, and reduction of segregation of duties risks as well as individually critical rights. The integrated segregation of duties framework is the foundation for an automated risk analysis within the system and allows for continuous monitoring of risks. Systems relevant for accounting, finance, and reporting can be analysed and audited on the basis of this framework (SoD risk matrix).

Therefore, conflicts can be detected in a timely manner and solved proactively. Conflicts that occur can be evaluated and prioritised by using a risk classification. In case of exceptions, the responsible superiors are notified.

Compliant User Provisioning

Management of authorisation processes is automated with SAP GRC Access Control. Embedding this capability into IT management processes and integrated SoD risk analysis maximises the benefits of preventive controlling across all authorisations and tracking of changes within operational systems.

Enterprise Role Management

SAP GRC Access Control supports efficient role management with integrated SoD risk analysis and administration. Before roles are assigned, role conflicts are highlighted to the administrator. Saving is prevented until adequate adjustments are made. All of this is documented and managed in order to leave a clean audit trail.

Superuser Privilege Management

SAP GRC Access Control enables the monitoring and controlling of system access of super users with extensive access rights. A comprehensively documented audit trail enhances traceability and transparency of all activities that have been carried out.

SAP GRC Access Control facilitates cohesive and consistent monitoring of the authorisation management process. Risks and responsibilities are clearly assigned to business processes. SAP GRC Access Control is integrated into the organisation in the best possible manner and sustainable implementation is ensured.

The use of SAP GRC Access Control helps to effectively and efficiently operationalise guidelines that are defined in the compliance framework and linked to authorisation management within a company. The following benefits can be achieved:

- Significant reduction of efforts and costs for fulfilment of regulatory requirements concerning segregation of duties and simultaneous improvement of quality;
- Optimisation of the internal control system by automation; prevention and identification of organisational process weaknesses;
- Increased standardisation through a centrally defined framework and embedding of SAP GRC Access Control into existing control processes;
- Increased transparency of IT and authorisation structures as well as the status of compliance activities for process owners;
- Increased effectiveness of collaboration between business departments and IT departments through a consistent and well arranged platform, customised to meet individual needs of each user group;
- Increased process reliability and protection against malicious and unlawful acts within systems by minimising fraud risks;
- Sustainable support of internal audit as well as year-end processes.

Example: Experience of SAP GRC Access Control implementation

PwC has supported a leading supplier of high performance ceramics products with 13 factories worldwide in the implementation of the SAP GRC Access Control capabilities. The company is subject to the Sarbanes Oxley Act. PwC was engaged to support in the implementation of SAP GRC Access Control to manage segregation of duties as well as sensitive and critical access to systems and to improve the control structure in these areas. The primary goal of this project was to ensure SoD risk monitoring as well as to implement effective and efficient processes. Controls had to be automated in the best possible manner and sustainability had to be ensured. The following benefits were achieved:

- With the implementation of SAP GRC Access Control, SoD, risks can be monitored automatically, improving the security of processes;
- The discussion of several SoD conflicts led to the identification of an organisational weakness within the company's payment process. Instead of implementing a complex, time-consuming, and repetitive control, the department was restructured. This made it possible not only to reduce the identified SoD risks, but also to increase the process quality through clearly defined tasks and responsibilities and to reduce the resources required;
- Efforts for handling SoD conflicts that were identified via regular risk analysis were reduced with sustainable and preventive actions;
- The use of superuser privilege management capability has made it possible to do SAT and emergency user access without several previously necessary but mostly manual controls. According to the company, the control effort has been reduced to a fifth of what was necessary prior to the implementation;
- External auditor testing required by the Sarbanes-Oxley Act was carried out on the basis of SAP GRC Access Control results. This enabled efforts to be reduced, while quality and security were increased.

SAP's plans for the fourth quarter of 2007 include an application for Governance and Policy Development Management, SAP Analytics Dashboards and SEM integration for strategic planning. Further enhancements to SAP solutions for GRC and addition of new functionality are on the anvil.

With the SAP GRC Technology Foundation, each application can, in the future, be offered out of the box. Industry-specific solutions are also being planned. SAP's goal is to transform SAP solutions for GRC into an integrated solution, ensuring technological support for numerous initiatives aimed at securing compliance within the company.

D Implementation and Integration of GRC Management

As described in Section B, one of the goals of holistic GRC management is to ensure the sustainability of GRC initiatives. Moreover, synergies resulting from the integration of content and methodologies of the various GRC initiatives should be realised. The journey from fragmented GRC initiatives to sustainable, integrated GRC management is illustrated here by a proposed transformation process, providing a template for the practical implementation of the vision described in earlier sections of this paper.

A GRC strategy is fundamental to achieving a sustainable, risk and value-oriented, ethical and compliant corporate governance structure.

A prerequisite for the successful implementation of sustainable GRC management is the definition of a company-wide **GRC strategy**. This is the starting point for meeting stakeholders' requirements, as well as for achieving the company's objectives. The corporate vision, goals and values are important factors that influence the GRC strategy. Additional factors that should be considered when establishing a suitable strategy include:

- The size and structure of the company;
- The type of legal entity;
- The international markets in which the company operates;
- The countries in which the company's shares are listed;
- The industry specialisation of the company;
- The complexity of compliance requirements;
- The risk appetite of the company;
- The company's stance in relation to its competitors (with regard to GRC, whether the company aspires to market leadership or best practice among competitors); and
- The need to consider the compliance requirements of business partners (e.g. compliance with anti-corruption laws) and suppliers (e.g. compliance with environmental, employment or social standards).

Consequently, the GRC strategy is fundamental to achieving a sustainable, risk and value-oriented, ethical and compliant corporate governance structure, which considers long term corporate goals as well as essential stakeholder requirements. The strategy thereby determines the focus and scope of risk management and compliance activities. A change in the GRC strategy also leads to a change or reshaping of relevant processes, organisational structures and supporting technologies.

In order to obtain an integrated view of governance, risk management and compliance and also to establish a GRC strategy, it is essential to consider all relevant stakeholder requirements. A stakeholder needs analysis should not only identify, but also evaluate and prioritise these needs based on their importance to the corporation and to the achievement of corporate goals. For analysing and evaluating the various needs in the form of a central repository, the "Rule Base" plays an important role.[19]

A Rule Base can be used as a tool to set company-wide GRC strategies, prioritising stakeholder requirements and making the link to organisation, process and technology transparent.

The Rule Base is a tool to record, analyse and monitor all external and internal regulations, standards and agreements that have been determined to be relevant for a company from a materiality and risk point of view. A Rule Base can be a simple tabular listing of the requirements or a complex database or repository. The latter option enables the presentation and evaluation of detailed information regarding the effects of these regulations on the company's organisation, processes and technology. Consequently, a Rule Base contributes to effective and transparent corporate governance, while taking governance, risk management and compliance perspectives into account. In addition, the prioritisation shown in the Rule Base reflects the strategy, goals and risk appetite of the company.

On the basis of the GRC strategy that has been defined and the stakeholder needs that have been identified and analysed, a tailored and sustainable GRC management approach can be implemented with the help of the transformation process described below. Within the scope of the transformation process, the current GRC environment is analysed and measures to ensure sustainability of the GRC initiatives as well as measures

[19] Menzies (2006).

to take advantage of integration opportunities are extracted and implemented. The transformation process is divided into six steps, which are shown in Figure 8.

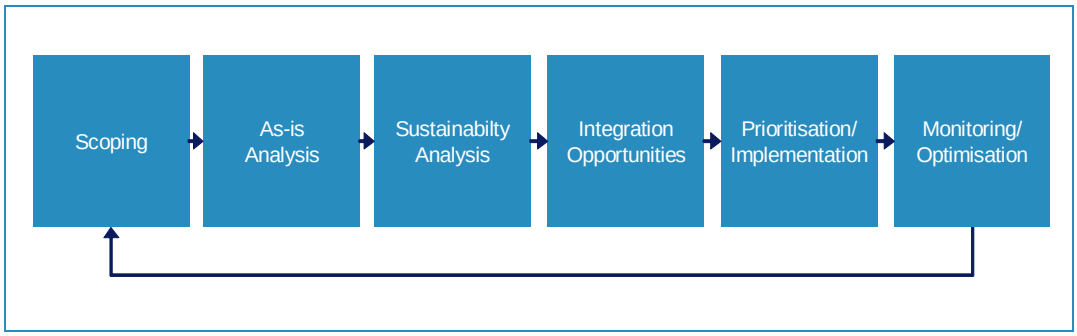

Figure 8 Transformation process for sustainable GRC management

Scoping

Scoping should be performed at the beginning of the transformation process. This will determine the areas in which the need for action is most critical in terms of implementing the GRC strategy and integrated GRC management. Scoping can be further detailed, rechecked and revised based on the information gathered in the course of the transformation process.

The result of the scoping exercise is a grouping of GRC-related topics, from which the GRC initiatives that are to be the subjects of the transformation process can be derived. The selection of the GRC initiatives depends on various criteria including:

- The perceived risk of non-compliance;
- Level of current compliance costs (Cost of Compliance Operations);
- Evaluation of the importance of GRC initiatives by management (with reference to company objectives);
- Time restrictions, interdependencies with other projects, availability of resources; and
- Potential constraints with regard to the extent that organisational structures, processes and technologies can be changed.

As-is Analysis

After the scope of GRC initiatives has been defined, the next step is to document the relevant company-specific GRC environment. The goal of the as-is analysis is to take stock of the GRC-relevant organisational structures, processes and technologies currently available. While the as-is analysis should be oriented towards the scope that was established, it may not be limited exclusively to the GRC initiatives that are in scope. The results of the as-is analysis, together with results from the sustainability analysis of specific GRC initiatives form the basis for prioritising and implementing the required measures.

Due to the various starting positions in which a company may find itself, it is important for the as-is analysis to examine the following:

- The corporate strategy and goals;
- The existing governance and risk management structures and processes;
- The existing compliance structures and initiatives; and
- The organisational structure, the relevant processes and the supporting technology related to the topics that are in scope.

Sustainability Analysis

The purpose of the sustainability analysis that follows the as-is analysis is to evaluate the extent to which the in-scope GRC initiatives are functioning as long-term embedded processes within the company. Thus the analysis seeks answers to the following questions:

- Whether governance, risk management and compliance processes have been linked, and how;
- To what extent GRC activities of the various initiatives have been effectively and efficiently embedded in daily operations; and
- How flexibly the company can respond to changes in the GRC environment.

The sustainability analysis should be oriented towards the Sustainability Elements introduced in Section B. This will ensure that the various GRC initiatives are analysed in a structured manner and that optimisation opportunities are identified.

As-is analysis and sustainability analysis can best be carried out in the form of topic specific workshops and interviews with management, the Compliance Officer and the control owner. Surveys or benchmarking studies are additional supporting tools that can be used to carry out a sustainability analysis.

Deriving Integration Opportunities

Based on the as-is analysis and the sustainability analysis and with help of the Sustainability Elements, integration opportunities relating to the separate GRC initiatives can be identified. Furthermore, analysing the different GRC initiatives also helps to identify opportunities to integrate content and methodology.[20] These integration opportunities become transparent through the structured and consistent approach of the analysis. While the identification of methodology integration opportunities is a natural by-product of standardising the differing Sustainability Elements, the opportunities to integrate GRC content depend on a holistic implementation of various GRC initiatives.[21]

Outlook: Rule Base

Depending on the level of detail, a Rule Base can also be used as a tool to identify integration opportunities. First of all, based on corporate and GRC strategies, the Rule Base can help in defining which compliance regulations [C] and risk management regulations [R]) are relevant to the different processes and where controls can be allocated. The following diagram illustrates the structure of a simplified Rule Base.

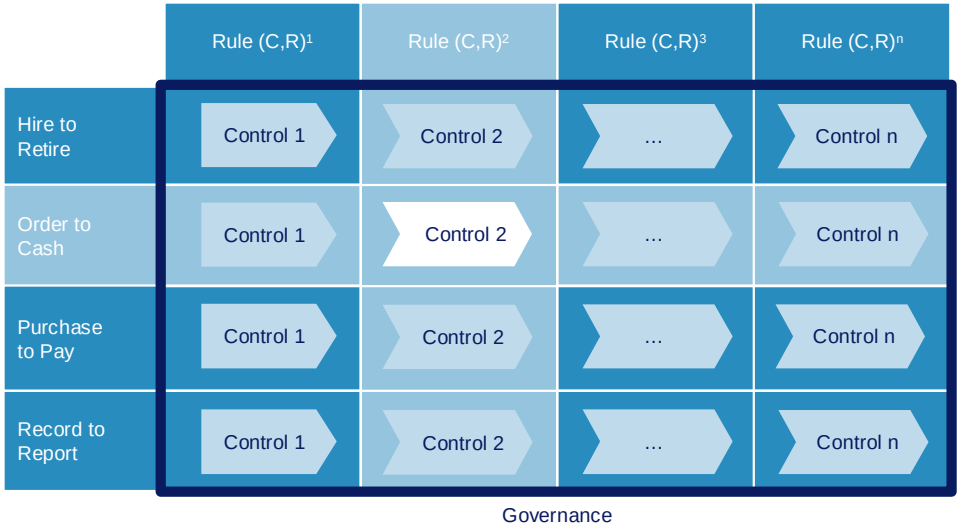

Figure 9 Diagram of a Rule Base

The diagrammatic allocation of business processes and the related departments to the different risk management and compliance regulations helps to identify controls that need to be implemented.

With respect to identifying integration opportunities, the Rule Base creates transparency and shows, for instance, which controls can be consolidated to address different compliance and risk management requirements.

Prioritisation/Implementation

Using the results of the as-is analysis, sustainability analysis and the identified integration opportunities as a foundation, measures for implementing a GRC strategy and for establishing sustainable GRC management can be derived. When deriving measures, it is important that the benefits of each of the measures can be identified and quantified, in terms of its contribution to achieving sustainable GRC management.

[20] See section B.2 for more detailed information regarding the methodology and content integration.
[21] See section B.2 for an example regarding the integration of a SOX and FCPA compliance initiative.

Companies may find themselves at different starting points and may pursue various goals in relation to GRC. In order to implement the transformation process successfully, it is especially important to define the desired future GRC status and to prioritise the derived measures accordingly, while also weighing costs and benefits. It also is to be noted that the transformation process is not static. Each of the phases successively builds upon and influences the others. For instance, the findings from the as-is analysis may impact the previously defined scope of the project. Additionally, a company may go through the transformation process multiple times in order to reach its defined goals.

In practice, due to the complexity of the topic, identified integration opportunities are often implemented successively. While making decisions on the sequence of implementation, it is recommended that companies focus on those GRC initiatives with the highest potential for creating synergies.

The implementation approach taken for integration measures can be influenced by numerous factors, which include for example:

- The scheduling and deadlines for the respective compliance requirements;
- The availability of sufficient resources;
- The interdependencies between existing corporate structures and processes;
- The impact of the changes that are related to the implementation; and
- The company's change management capability.

Monitoring/Optimisation

The phase "Monitoring/Optimisation" ensures that the measures that have been implemented remain effective. For this purpose, suitable project management must be performed and appropriate, predefined key performance indicators must be monitored. Monitoring not only ensures the ongoing effectiveness of implemented measures, it also helps to identify additional optimisation opportunities.

If variances from the desired future GRC status are noted, additional measures may be introduced. In this respect, the first steps of the transformation process may be re-performed. Even if the defined goals have been achieved, the transformation processes may still be reinitiated, for instance, in order to expand the original scope with further compliance initiatives.

E Conclusion

The only way that companies will be able to grasp the opportunities offered in an age of globalisation with any certainty of success is to adopt a holistic approach to GRC management. This demands the design of sustainable GRC initiatives that are both embedded into the daily business and also integrated with each other as far as possible.

Technology plays a key role in achieving this vision. It not only supports efficient and effective GRC initiatives on a process level, but also provides an integrated platform for the holistic direction and monitoring of all GRC activities across the organisation. Technology makes a significant contribution to ensuring that all GRC-relevant information is available to management when needed, to assist in defining and implementing the company's key objectives and strategy, thus playing a decisive role in securing the long-term success of the enterprise.

F Bibliography

COSO (2004) – Enterprise Risk Management - Integrated Framework, Executive Summary Framework, published by COSO - Committee of Sponsoring Organizations of the Treadway Commission, 2004

Menzies (2006) – Menzies, C. et al.: Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration, published by Schäffer-Poeschel Verlag, 1.Auflage, Stuttgart, 2006

PwC/BDI (2002) – Wolfram, J.: Corporate Governance in Deutschland, published by PricewaterhouseCoopers AG and Bundesverband der Deutschen Industrie e.V., Frankfurt, 2002, http://www.bdi-online.de/BDIONLINE_INEAASP/iFILE/X2FAFDEBD7B2542CD9A7822F2924E0109/2F252102116711D5A9C0009027D62C80/PDF/Corp%20Gov%20gesamt.PDF, accessed 20.02.2007

PwC (2004) – Integrity-Driven Performance: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management, A White Paper, published by PricewaterhouseCoopers, 2004, http://www.pwc.com/extweb/service.nsf/docid/c8753369ed2d193e85256e1b001c03d6, accessed 20.02.2007

PwC/BDI (2005) – Hönisch, H. et al.: Corporate Governance in Deutschland – Entwicklungen und Trends vor internationalem Hintergrund, published by PricewaterhouseCoopers AG and Bundesverband der Deutschen Industrie e.V., Berlin - Frankfurt, 2005, http://www.bdi-online.de/Dokumente/Recht-Wettbewerb-Versicherungen/BDI_PwC_Studie.pdf, accessed 20.02.2007

PwC (2005) – 8th Annual Global CEO Survey – Bold Ambitions, Careful Choices, published by: PricewaterhouseCoopers LLP, 2005, http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/8th_ceo_survey.pdf, accessed 20.02.2007

PwC (2007) – 10th Annual Global CEO Survey, published by PricewaterhouseCoopers LLP, 2007, http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/10th_ceo_survey.pdf, accessed 20.02.2007

University Hamburg: Umfrageergebnisse (2006) – Compliance kann Mehrwert für Unternehmen schaffen, published by Universität Hamburg, Hamburg, 2006, http://www.verwaltung.uni-hamburg.de/pr/2/21/pm/2006/pm25.html, accessed 20.02.2007

Local contacts

Jan Schreuder
Partner - GRC Technology
(p) +61 (2) 8266 1059
(e) jan.schreuder@au.pwc.com

Kevin Reilly
Partner - GRC Technology
(p) +61 (2) 8266 7202
(e) kevin.reilly@au.pwc.com

Andrew McPherson
Partner - Government
(p) +61 (2) 8266 3275
(e) andrew.mcpherson@au.pwc.com

Alan Hui
Director - Governance, Risk Management and Compliance
(p) +61 (2) 8266 7851
(e) alan.hui@au.pwc.com

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services for public and private clients. More than 142,000 people in 149 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

PricewaterhouseCoopers is acknowledged worldwide as a trusted advisor in the field of Governance, Risk Management and Compliance and supports companies in achieving holistic management of GRC. PricewaterhouseCoopers offers a proven and pragmatic approach to reducing compliance costs and realising the benefits related to GRC, helping clients ensure sustainable, risk and value-oriented corporate management.