Over the past few years, organizations are more focused on “being in control.” They are increasingly—often forced by regulations—building and implementing processes that underpin the company’s “In Control Statement.” The inevitable extra costs and efforts are often seen as a burden, distracting people from what they should focus on: doing business!

**Introduction**

At the same time, organizations are more aware than ever of the importance of managing risks. One reason is that financial disasters, which seem to occur on a regular basis, remind us of the perils of “not getting it right.” Creating value or doing business is impossible without taking risks. So how much risk can a business take? How much uncertainty is acceptable given the objective of creating value?

Enterprise Risk Management (ERM) helps organizations deal with these critical issues. It enables companies to identify events related to achieving a certain objective, which leads to identifying risks or opportunities. The disadvantage of “control” is combined with the benefits of new opportunities identified as part of the risk management process.

Effective ERM helps management to reliably achieve its objectives. But ERM, no matter how well designed and operated, does not ensure an organization’s success. Meeting objectives is also affected by limitations inherent in all business processes. ERM does not change an intrinsically poor process into a good one! Risk management means consciously balancing seemingly competing goals like minimal process cycle time and cost, with output quality and (regulatory) compliance. Therefore, it’s crucial to align ERM with business performance. Providing the up-to-date and comprehensive view on business performance (revenue driver) and compliance performance (cost driver) creates the transparency fundamental to good decision-making.
Why is it important to balance “being in business” with “being in control”?  

Recently the COO of the asset management division of a European insurance company wanted to weigh certain risks before making a business decision in the process “Request for Offer.”

In searching for and selecting a service provider that worked with shopping centers, the company could use an external person. But the company wanted to manage the risk of doing business with an unreliable business partner. Assuming the process “Request for Offer” takes two days, then the process costs are 350 euros. To further minimize risk, the company also included an independent expert opinion regarding the reliability of the selected business partner. This increased the process cycle time and costs by four days and 650 euros respectively, but on the other hand, this additional process step minimized risk.

It’s up to management to consider the matter, and here ARIS serves as a basis to do so. It allows the company to identify the operational costs, among other things, and make the organization transparent overall. Since the managers obtain a more accurate picture of the processes, they have an easier time when weighing the decision to improve business or stay out of trouble. Since ERM uses a company’s objectives as a starting point, it is of great help in deciding how to both make business better and keep it out of trouble. This white paper will help you understand the importance of relying on world’s most widely used standard approach of risk management and how to achieve a balance between being in business and being in control. You will learn how to implement effective ERM by building a sustainable Governance Risk & Compliance (GRC) solution.

**COSO II ERM framework**

The COSO II ERM Framework is widely accepted as a standard for implementing ERM. A well-designed and operated enterprise risk management framework can provide the management of organizations with reasonable assurance that:

- They understand the extent to which the entity’s strategic objectives are being achieved
- They understand the extent to which the entity’s operations objectives are being achieved
- The financial reporting is reliable
- Applicable laws and regulations are being complied with

The COSO II ERM Framework consists of eight related elements (see Figure 2). These elements are aligned to the way a company is managed and inseparably related to the management process.
How to Implement Effective Enterprise Risk Management

Internal environment
The internal environment describes the risk culture of an organization that defines how risk is viewed and addressed by the organization. It includes the risk management philosophy, risk appetite, integrity and ethical values, and the environment in which they operate.

Objective setting
Without defined objectives, it’s impossible to identify potential events affecting the achievement of objectives. ERM ensures that a process is in place to set objectives (aligned with the entity’s mission and consistent with its risk appetite).

Event identification
It is possible to define opportunities and threats by identifying internal and external events that influence the realization of the objectives. Opportunities are channeled back to management’s strategy or objective-setting processes.

Risk assessment
Risks are analyzed, considering likelihood and impact as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

Risk response
Several reactions are possible when a risk occurs. Risks can be avoided, accepted, reduced or shared. Management selects the correct risk response, developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.

Control activities
Procedures are established and implemented to help ensure the risk responses are effectively carried out. Here you can think about explicit control measures to mitigate the risk, management reviews, reporting, physical controls (such as assets, values and stock), controls based in performance indicators and/or segregation of duties.

Of course, it’s very important to keep in mind that the costs of the control activities are aligned to the potential loss of the risk which is reduced or mitigated.

Monitoring
The entirety of ERM is monitored and modifications are made as necessary.

Information and communication
Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.

Figure 2: COSO II Cube
How to Implement Effective Enterprise Risk Management

How Software AG supports the ERM framework

Software AG’s ARIS GRC Management Platform is fully aligned to the COSO Framework and supports ERM in all phases of the process. The solution combines ARIS software, Global Consulting Services and the proven Prime methodology as well as time-saving reference content based on industry knowledge and project success. Here’s how the solution supports the ERM framework.

Internal environment

The internal environment determines to a great extent how successful a company is at applying effective risk management. A good internal environment includes a number of required elements that are necessary to provide clarity concerning what is and what has not been permitted. These elements can include: how the organization behaves; which values and standards are important; how it handles risks; and how roles, responsibilities and authorizations have been assigned. As such, it can be seen as a prerequisite rather than a process that can be supported by tooling.

The GRC experts of Software AG’s Global Consulting Services support clients in fulfilling this prerequisite. They do this by providing guidance and consulting services that translate the company’s risk management philosophy and corresponding risk appetite into a practical approach for organizing and implementing the relevant activities and responsibilities. A commonly used model in this perspective is the model of the lines of defense.
Figures 4 and 5 demonstrate the different responsibilities of involved roles and related activities within a company. Since ERM affects many people within the organization from different areas of expertise and responsibility, it’s of upmost importance that the G (Governance) in GRC is in place. The responsibilities and roles are used later in the ERM process for allocation of tasks in a workflow and related authorizations in tooling. When the internal environment is arranged properly, fewer controls at the end are needed.

**Objective setting**

The starting point for the ERM process is the organization’s strategic objectives. These objectives can be defined on both company and business unit level. Without clearly defined objectives, it’s impossible to identify potential events affecting the achievement of these objectives. ERM ensures that a process is in place to set objectives, aligned with the entity’s mission and consistent with its risk appetite.

It’s not enough to define a mission, vision and strategic objectives though. The objectives should be defined very concrete and specific. In this perspective it’s important to think about the factors that are of upmost importance for success or failure (critical success factors) and executing these factors into measurable Key Performance Indicators (KPIs).

Using ARIS Business Strategy with its balanced scorecard functionality, strategic objectives can be defined and visualized in various perspectives (for example, from the customer perspective, financial perspective and internal perspective).

Taking ARIS Business Strategy as a starting point, the strategic objectives are made concrete and specific using objective diagrams, in which critical success factors and more specific (sub) objectives can be defined. The objective diagram also facilitates linkage of the business processes that support the achievement of the specific objective.

By assigning a KPI allocation diagram, the critical success factors/specific objectives are translated into KPIs. KPIs define the parameters (e.g., the process throughput time and number of complaints), which are used to measure the achievement of the objective. The definition of KPIs in ARIS not only includes information like the target value and tolerance range but also shows the exact measure points in the corresponding business processes.
This process demonstrates the close connection between performance management and risk management. In fact, risk management is not about managing risk but about managing the achievement of objectives. Performance management focuses on measuring and optimizing the defined indicator values while risk management focuses on measuring and managing the events that might prevent achieving the organization's strategic, tactical and operational objectives.

For this reason, it's crucial that both disciplines are closely aligned and cooperate. Using shared methodologies and working from a single repository containing all process relevant information, such as objectives, risks and KPIs, is an important prerequisite for success.

**Event identification**

Once objectives are clear, possible events that could influence these objectives can be defined. Events with a positive impact are defined as opportunities and channeled back to management's objective setting process. Events with a negative impact are defined as risks.

ARIS supports defining risks using risk diagrams, in which risks can be clustered into categories, and KPI allocation diagrams, in which governance structures ownership and responsibility are defined. Also risk attributes can be maintained like a risk description, risk type (strategic, operations, reporting, compliance), risk assessment instructions, affected laws and regulations.

**Risk assessment**

Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis. Inherent means that the mitigating measures are not taken into consideration. Residual value of a risk means that the mitigation of the risk is considered. The risk values can be assessed qualitatively (in categories such as low, medium, high) and quantitatively (in absolute percentages and euros).
**Risk assessment planning**
ARIS Risk & Compliance Manager automatically creates workflow-driven tasks based on the risk information defined in the previous step (event identification). The software will also automatically create a forecast concerning all the risk owners and the so-called annual risk assessment planning. Risk owners are notified by email when risk assessment tasks are to be performed.

Figure 7: Risk Assessment Planning in ARIS Risk & Compliance Manager

To make sure risk assessments are performed in a coherent way and the results are comparable over different business areas, it’s important to define and agree on some guidelines. One example of guidance relate to the qualitative values (low, average and high) of probability categories and the corresponding qualitative evaluations (absolute percentages or amount of euros).

**Example likelihood categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Appearance</th>
<th>Number of events, occurrence frequency</th>
</tr>
</thead>
</table>
| **Very low** | • Never heard of in industry, once happened in industry  
              • Has never taken place before                                           | < 0,01  
                                      |                                                                 | < 1%                           |
| **Low**     | • Took place once  
              • Takes possibly place in the future                                      | 0,01 – 0,10  
                                      |                                                          | 1% – 10%                     |
| **Average** | • Took place one or more times  
              • Is expected to take place in the near future                           | 0,10 – 1,00  
                                      |                                                          | 10% – 50%                    |
| **High**    | • Takes place one or more times a year  
              • Is expected to take place                                               | 1,00 – 10,00  
                                      |                                                          | 50% – 90%                    |
| **Very High** | • Takes place a few times a year  
              • Is almost unavoidable to happen                                           | 10,00  
                                 |                                                                 | > 90%                        |
### Example impact categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Health, Safety Environment</th>
<th>Reputation Regulatory</th>
<th>Financials % of BU Gross Margin (Corp. level)</th>
</tr>
</thead>
</table>
| Unimportant   | • First aid accident, no absence  
• Minor emission within limits | • Non-public commotion  
• Minor regulatory incident | < 0,02  
< €1,2 mio |
| Low           | • Small injury, temporary absence  
• Emission exceeds limits without permanent damage | • Local commotion  
• Argument with regulator(s) | 0,02 – 0,20  
€1,2 mio – 6 mio |
| Average       | • Serious injury, long-term absence  
• Emission causes temporary damage to surroundings | • Regional commotion  
• Major Argument with regulator(s) | 0,20 – 2,00  
€6 mio – 30 mio |
| High          | • Disabled or dead employee  
• Corrective measures needed in surroundings | • National commotion  
• Serious conflict with regulator(s) | 2,00 – 20,00  
€30 mio – 150 mio |
| Catastrophic  | • Several disabled or dead employees  
• Ecological effects at large scale | • International commotion  
• Major sanctions by regulator(s) | > 20,00  
> €150 mio |

Figure 8 shows both the qualitative and quantitative evaluations are maintained during the risk assessment.

![Software: ARIS Risk & Compliance Manager](image)

Figure 8: Performing Risk Assessments in a Qualitative and/or a Quantitative Way

After closure of the risk assessment, a reviewer will check the results and gives approval or rejection on the risk assessment results. All managed by the workflow in ARIS Risk & Compliance Manager. Clear dashboards represent all risk assessment results in heat maps and in text and can be reported in both Microsoft® Excel® and PDF formats.
For risk managers and the responsible line management, it is important to analyze the trend of risks. At the end it is important to learn if investments in risk response are worth it. In the following example, for the risk “Invalid Sales Order Processing,” it’s clear that in the risk assessment the residual/net risk has been decreased. Clicking on the dot in the graph representing a risk assessment gives insight into the reason behind the decreased expected losses. In this example, the reason was the implementation of a mitigating control. In this way the risk management function can demonstrate the impact of mitigating actions.
Risk response
Based on the risk assessment output, several responses are possible for the assessed risk. Risks can be avoided, accepted, reduced or shared. Often line management, supported by a business risk manager, decides on appropriate risk response. A response can also be a set of actions to align risks with the entity’s risk tolerances and risk appetite.

Some examples to explain the four possible risk responses:

- **Reduce**—for example, by implementing a mitigating process control of executing a screening on every new business partner
- **Share**—for example, by fire insurance on the building
- **Accept**—for example, because the costs of mitigating are not worth it, risk value is tolerated
- **Avoid**—for example, by shutting down one of the locations or termination

Control activities
Procedures are established and implemented to help ensure the risk responses are effectively carried out. Here you can think about explicit control measures to mitigate the risk, management reviews, reporting, physical controls (assets, values, stock), controls based in performance indicators and/or segregation of duties. Often, more than one control is needed to mitigate one risk.

It’s important to keep in mind that the costs of the control activities are aligned to the potential loss of the risk which is reduced or mitigated. Controls are defined in business control diagrams in and related to the risk that is mitigated by the control. Ownership is defined and the control is implemented as part of the actual business process execution. Based on the criticality of the control it’s decided and maintained if, when and how the control is tested/audited for design and/or effectiveness. Risks identified can be related to compliance with applicable law and regulations.
Dealing with law and regulations comprises these steps:

- **Defining compliance scope.** The first step is the definition of "where to comply to?" This step is about identifying relevant laws, regulations and standards.
- **Analyzing and interpreting.** All detailed sections of the defined laws and regulations are analyzed and interpreted. Based on this analysis, the translation/interpretation of the articles into company-specific integrated requirements/control objectives is made.
- **Integrating requirements into business processes.** The next step is to implement the requirements/control objectives into the company’s business processes.

This approach is based on the idea that laws, regulations and standards overlap quite a bit. Defining integrated requirements covering multiple articles from laws and regulations, and then implementing these requirements into the business processes/controls, reduces both implementation and audit effort. Instead of auditing for each regulation separately, only one audit is performed on the process/control in which the integrated requirement is implemented. The audit results are used to prove compliance to all related law and regulations. This is a very efficient way of meeting the requirements of several regulations simultaneously.

The impact on related controls, business processes and accountable roles is reported instantly. There is no need to start up a separate change project because all necessary information is already available in ARIS. In short, the benefits are time savings, cost reduction and quality improvement.
Monitoring

Monitoring is accomplished through ongoing management activities, separate evaluations or both. The aim of monitoring is ongoing quality assurance and improving the framework. A component of this is making a judgment concerning the set-up of the Risk and Control Framework (RCF), its existence and how it functions. Based on the information defined in the previous phase, ARIS Risk & Compliance Manager creates an audit or test plan automatically. According to this plan, testers are notified by email when test tasks are to be performed.

The judgment concerning the set-up is a pronouncement concerning the design and tells to what extent the RCF has been composed adequately. Questions include: Are all the risks identified? Have the risks been judged? Have adequate controls been defined? Do the controls effectively mitigate the risks? Does the cost of the controls outweigh the potential damage of the risks?

Monitoring is an important component of the ERM cycle. Ideally, monitoring takes place continuously. Because of changing circumstances, it might be necessary to check if the RFC is still adequate. Monitoring, therefore, also means that you can’t rely only on the relative certainty of the well-functioning framework but you also have to check the influence of changing circumstances that can have effect on the framework. Software AG’s ARIS GRC Management platform supports both automated monitoring of controls (continuous controls monitoring) as well as semi-automated monitoring via comprehensive workflows in ARIS Risk & Compliance Manager.
Figure 16 shows the task list of a tester. It encompasses all test tasks due for the tester role. ARIS Risk & Compliance Manager is a role-based system so users will only see the tasks that are relevant for the role they perform.

The test task contains all information needed to perform the test including clear instructions on what to do, details on the control that is subject to the test as well as a link to the corresponding process model. The test results are documented, documentation (evidence) is linked or uploaded and a final status is defined (effective/not effective). For controls that can be monitored automatically this is done by the GRC system notifying the control responsible on the results in real time.

For test results with the status “not effective,” the test reviewer role is notified. The reviewer checks the test results and decides whether the not effective test result is a deficiency or not.
If the test reviewer accepts that the control is not effective, he can define an appropriate measure. In most cases he will create an issue (remediation task), prioritize it and assign it to a responsible person. An overview of all the issues (role-based), including the due status, can be requested in a dashboard. This is a very comprehensive way of getting insight at any moment into all open issues. Separate action management systems are not necessary anymore; everything is stored in the same repository.

Figure 19: Overview of All the Issues That Are Assigned to This Role

Issues can be related to other assets in the repository such as applications, test cases, risk assessments, persons, etc.

The results of the tests are immediately visible in the dashboard. All dashboards are role-based. That means users see only the results of authorized areas. It’s possible to filter all results based on a certain time period, on certain departments and other criteria. It is also possible to generate reports from the dashboard (Microsoft Excel or PDF) to share for example with auditors.

Figure 20: Test Management Dashboard With All the Test Results
The test results can be aggregated by different views—test results per process, per department, per test group or per law and regulation. The view of law and regulation gives compliance officers insight in the successfulness of complying with specific requirements. It might be, for example, that the controls related to SAS70 are effective, but the controls related to Sarbanes Oxley are ineffective and lead even to several deficiencies. The evaluation helps to start up new initiatives and possibly the creation of new issues.

Information and communication

All roles involved in the ERM process are informed of the tasks they should execute based on the planning. Notifications/alerts are sent to when predefined thresholds are exceeded. It’s up to the administrator to (de)activate these kinds of triggers informing the different roles.

Besides the risk and control assessment reports and dashboards, ARIS offers a broad range of additional reports giving insight in the set up. For that purpose the flexible ARIS WYSIWYG (What You See Is What You Get) reports are helpful.

Transparency for end users, business managers, auditors and other roles is achieved by a process portal with risk and controls embedded in the process design, including business roles, application systems and segregation of duties.
Another way to communicate relevant information effectively is with MashZone. MashZone enables you to bridge the gap between static tables, evaluations, and rigid reports and the need for graphical, interactive, easy-to-understand presentations. You can create your own custom dashboards using a simple drag-and-drop interface. Drill down to detailed information via the interactive visualization options to display relationships between data. Since MashZone has role-based access, it is possible to create role-specific mashups. The source of the dashboard can be ARIS products and other sources, such as services on the Internet, Excel spreadsheets and feeds from ERP systems.

Figure 23: MashZone Dashboard for GRC

Figure 23 shows in one dashboard per process both the business performance (in blue) and risk and compliance performance (in orange). Often, more effort to increase control leads to a decrease of business performance. Think, for example, about implementing mitigating process controls. Additional controls decrease the process cycle time and increase the process costs. That’s why it is very valuable for the business to analyze both performance metrics in one dashboard.

**Best practices in implementing ERM**

**Prime for GRC**

Prime is a leading implementation methodology. It’s a core component of Software AG solutions and is built on our experience with enterprises the world over. The methodology is applied by Global Consulting Services to jump start your projects, assure long-term success and accelerate results with:

- Work packages that guide you step-by-step to achieve specific results
- Pre-configured questionnaires, reference processes and templates
- Tools equipped with required standards, guidelines and sample solutions
The Prime approach for ERM consists of several work packages. Figure 24 shows the main packages used to implement ERM. Best practices are the result of dozens of successful ERM implementations across several industries. The duration of the implementation project depends on several factors. With a limited scope, the set-up of the methodology and tooling for ERM can already be implemented in seven weeks. Embedding ERM completely in the enterprise is more time consuming and even can take several years, depending on the current and targeted maturity level.

**Preparation/strategy**

In the preparation/strategy phase, a project plan for implementation will be discussed, including all involved roles and the scope. Progress will be monitored regularly. Also, the development of a Business Governance Framework is started. In workshops, all the guidelines and phases of ERM will be discussed. For each phase, we define what should be done, why and how this will be achieved.

Predefined deliverables accelerate the process. The business governance framework forms the basis for the ERM implementation and continuation. The document is in that way never finished.

**Blueprint**

Based on the business governance framework defined in the strategy phase, the workflow in ARIS Risk & Compliance Manager is designed and the relevant roles are implemented. Furthermore, the decision must be made what and how the existing GRC master data is uploaded in the single repository of ARIS. After the upload in the implementation phase, other sources will be archived and not maintained anymore.

**Realization/roll out**

In the realization/roll out phase, all administrative tasks are done to generate the risk and control assessment cases. Models must be completed. Users will be trained for those activities that they will execute in their daily work. The first assessments can be executed, issues can be followed up and sign-off can be done by the process or department owners.

**Monitoring and optimization**

In the monitoring and optimization phase, both the ERM process itself and the outcomes will be monitored. Based on certain findings, issues and deficiencies can be initiated and monitored as well. Different roles can find their way in the methodology and tooling.
Top 10 reasons to use ARIS for ERM

The ARIS software is the foundation for Software AG’s ERM solution. Here’s why you’ll want to adopt ARIS GRC for ERM:

1. **Lower TCO**
   By maintaining business processes in ARIS, the process structure can be re-used for GRC activities. This means fewer sources of documentation, less administrative work and more consistent content.

2. **Better communication and alignment between different roles across the enterprise**
   Business managers, Quality Assurance (QA) managers, auditors and end users benefit. The business manager/process owner is responsible for the effectiveness of processes and all related risks. The structure of processes, risks and controls is the foundation for QA activities, compliance by linking the laws and regulations, work instructions for end users and so on. A single point of truth is in place. By clear ownership, methodology and release procedure, governance can be improved.

3. **Better change management, higher quality of work**
   By posting all company processes, risks, controls, organization and regulation in one repository with one methodology, impact analysis on changes is better supported. It’s easier to gain insight into the impact of changes to the business processes and the involved owners. This results in faster and better decision-making when changes are required.

4. **Work systematic on compliancy and certification as a continuous process**
   By the regulatory sections, such as the chapters of ISO, ARIS can support work systematically on translating the sections as guidelines and their impact on the company. The ISO sections can be maintained in ARIS. Per subsection, the requirements for the enterprise can be related. The requirements for the company processes and organization are then linked to controls within the business processes. The controls can be assessed during the year. The control assessment results are aggregated automatically in a dashboard to the ISO sections. This way, management can view daily to which ISO sections they do and do not comply. Reports can be generated at any time.

ARIS gives you fast insight into the impact of changed regulation on the business processes and organization. This results in faster adaptation to new/changed regulations.
5 More efficiency by lean control and test definitions
By using a structured way to translate regulations into company requirements and needed controls in the processes, very lean controls and test definitions can be defined covering more risks and regulations at the same time. Fewer controls and tests are needed. This results in less time and money to spend on compliance.

6 Reduce operational surprises and losses
By using a systematic approach of deriving risks and controls from the company objectives and the relevant regulation, there will be fewer unhappy surprises and losses. Negative trends in risks and controls can be detected much earlier by more transparency and can be triggered also automatically by the ARIS notification. The current individual decision-making must be replaced by choices of owners based on assessment results and trend analysis in ARIS Risk & Compliance Manager.

7 Optimal usage of economic capital
For financial institutions counts that the better the transparency and risk management system in place, the less capital they are required to hold. This sustainable risk management system is a perfect solution in today's solvability issues.

8 Reliable reporting on risks, controls, issues and deficiencies at any time
Reports can be generated at any time in different views like processes, organization, regulation or financial statements and tester hierarchy. This makes it possible for management to focus on those things that really need attention.

9 Issue management in one integrated system
Instead of sending action points by mail without any track and trace possibility, in ARIS Risk & Compliance Manager, you can view the status of workflow at any time. This results in more transparency and better insight in open issues to react on. This means management now has one process to monitor and control for all the issues.

10 Insight in the relation of strategy, risk management, compliance and process management
Management can use the risk information (results of risk and control assessments) to make decisions about strategy and related objectives. Risks can be identified based on the attempt to achieve all the enterprise objectives within a certain time period. One of the objectives can be to (remain to) comply to ISO. The relationship is in ARIS, established between strategy and regulation towards risks, mitigating controls and the responsible organization and executing processes.
How to Implement Effective Enterprise Risk Management

About the authors

Sven Roeleven is Vice President, Global Solutions at Software AG, responsible for developing new and deepening existing solutions in close collaboration with customers and partners. After graduating in Public Administration from Erasmus University Rotterdam, Sven joined Software AG in 2002. He gained extensive hands-on experience covering almost all Software AG’s products throughout the course of more than 150 projects. Sven has specialized in GRC management and business process analysis & management solutions, particularly in an SAP® environment. In addition, Sven is advisor and member of a dozen of risk and BPM committees in the private and public sector.

Michiel Jorna is Director, Global BPA & GRC Solutions at Software AG and responsible for the development and deepening of Software AG’s Business Process Analysis (BPA) and Governance, Risk & Compliance (GRC) solutions. Michiel holds a master’s degree in Business Administration from Radboud University Nijmegen and is an expert in the area of business process management, (enterprise) risk management and internal control with experience in a broad range of industries. Michiel has led many very innovative and successful implementation projects in international settings providing him credible background to support Software AG’s sales effort and thought leadership among customers.

ABOUT SOFTWARE AG

Software AG offers the world’s first Digital Business Platform. Recognized as a leader by the industry’s top analyst firms, Software AG helps you combine existing systems on premises and in the cloud into a single platform to optimize your business and delight your customers. With Software AG, you can rapidly build and deploy digital business applications to exploit real-time market opportunities. Get maximum value from big data, make better decisions with streaming analytics, achieve more with the Internet of Things, and respond faster to shifting regulations and threats with intelligent governance, risk and compliance. The world’s top brands trust Software AG to help them rapidly innovate, differentiate and win in the digital world. Learn more at www.SoftwareAG.com.

© 2016 Software AG. All rights reserved. Software AG and all Software AG products are either trademarks or registered trademarks of Software AG. Other product and company names mentioned herein may be the trademarks of their respective owners.