

## Dr. Werner Brandt

Member of the Executive Board / Chief Financial Officer



### Enterprise Risk Management

The Sarbanes-Oxley Act (SOX) of 2002 and similar legislation in other countries have rewritten the rules for corporate governance, disclosure, and reporting. Compliance with a growing variety of laws, regulations, or standards has become one of the most dominant business challenges for corporations today. Failure to comply could have a serious detrimental effect on a firm's reputation and financial health. SAP is faced with various national and international regulations in the field of risk management that go beyond the pure internal control perspective. There are, for example, special requirements for internal risk management in a German stock corporation and commercial law that apply to SAP. At the same time, SAP has to comply with various international corporate governance standards, such as the German Code of Corporate Governance and the respective rules of the New York Stock Exchange.

One of the key questions for me is how management can turn such legal necessities into a source of competitive advantage that ultimately helps us to compete more successfully in the marketplace.

In my point of view, a good answer to this question lies in the recommendations of the Enterprise Risk Management – Integrated Framework (“COSO II”) standard developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The standard expands on internal controls by providing a focus on firmwide risks beyond those relating to internal controls for financial reporting. In 2003, SAP's executive board made the decision to adopt an integrated, corporate-wide risk management approach based on this framework, which led to the establishment of our central Global Risk Management (GRM) department. It has a uniform method for coordinating, standardizing, and optimizing our global risk-related activities.

What we mean by a uniform method is that every identified risk is categorized using the same criteria, regardless of where it arises in the company. At group level, they are all assessed using the same company-wide probability and impact matrix. As a result, we now have a globally consistent base for both consolidated prioritization and risk reporting throughout the company. The method is applied by dedicated risk managers in every line of business to a variety of “risk-relevant” activities across our organization, such as development programs, implementation projects, M&A activities, and many more. Supported by a growing risk management maturity in the organization, the role of risk managers has evolved from pure subject matter experts supporting transparency to business partners providing strategic decision support.

In terms of IT support, we rely on our own expertise in using SAP Operational Risk Management (SAP ORM) and SAP Management of Internal Controls (SAP MIC). The SAP MIC system supports the implementation of the SOX and comparable international requirements for documenting processes and controls and assessing internal controls. The SAP ORM system supports the continuous recording of risks, their assessment, and the tracking of response measures. It also supports real-time risk analysis and reporting in individual organizational and management units across the company.

Through the software tool, our Global Risk Management department has complete visibility into detailed risk assessment results and also into the total risk exposure at all levels of our organization at all times. This risk assessment is also provided to SAP's management on local, regional, executive board, and supervisory board level through a cascading risk reporting process. Thus, risk management information is delivered at the level of detail required by the addressee. This enables the respective organizational units to more easily embed risk management information into their business and decision processes.

Looking at our above efforts to achieve global compliance with a variety of laws, regulations, and standards, within a very short time frame we have created a business benefit beyond mere compliance by establishing a risk management organization, value-adding software tools, and processes that all support decision making.

Our approach is also highly rated by others. In 2005, SAP was nominated in three categories at the annual Strategic Risk European Risk Management Awards and won two: “European Risk Management Team of the Year” and “Most Effective Use of Technology for Risk Management.” Leveraging the existing, award-winning technology, we decided to offer our internal enterprise risk management solution also to our customers as part of the new SAP solutions for governance, risk, and compliance (SAP solutions for GRC).

My next point of view will deal with the question how a business benefit can be derived from SOX-related compliance activities.