

**SAP Solutions for Governance,
Risk, and Compliance**

SAP NetWeaver®

**Providing the Building Blocks for Effective Governance,
Risk, and Compliance Management**

THE BEST-RUN BUSINESSES RUN SAP™



© Copyright 2006 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

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

CONTENTS

Executive Summary	4
The Need to Address Compliance and Beyond	6
Toward an Architecture that Supports GRC Management	7
SAP NetWeaver: The Building Blocks for Effective GRC Management	10
Step One: Understand	10
Step Two: Document	10
– User Productivity Enablement: Portals, Roles, and Profiles	11
– User Productivity Enablement: Duet Software	11
– User Productivity Enablement: SAP NetWeaver Mobile	12
– User Productivity Enablement: Knowledge Management	12
– Data Unification: Arriving at a Single Version of the Truth	12
Step Three: Guide and Monitor	13
– Business Event Management: Managing Business Tasks with Workflows	13
– Business Event Management: Automation and Monitoring	13
– Application Governance and Security Management: Enforcing Security	14
Step Four: Report	15
– The Future of Reporting: Toward Real-Time Compliance	16
Enabling Enterprise Services Architecture: Design and Deployment	16
– Unified Life-Cycle Management: Centralized Administration	16
– ESA: The Future Foundation of Embedded Compliance	17
– Custom Development: SAP NetWeaver Development Toolkit	17
SAP NetWeaver as a Foundation for GRC Management at SAP	18
Conclusion	19

EXECUTIVE SUMMARY

While some organizations are still focusing precious resources and management attention on specific regulatory mandates, leading organizations have started to take a broader, more integrated approach to managing interrelated risks through a holistic program of governance, risk, and compliance (GRC) management.

Today’s approach to managing a business is marked by fragmentation across multiple dimensions – for instance, organizational, technical, and regional dimensions – as well as across the separate disciplines of GRC management. This fragmentation compounds the cost of managing governance, risk, and compliance, and also potentially increases risk when interdependencies are not managed holistically.

Increased risk and regulatory pressures are propelling distributed organizations to craft strategies for centralizing GRC oversight. Business software is enabling this convergence of GRC management. By leveraging the information contained in enterprise systems and structuring the information in a GRC framework (see Figure 1), managers can move from reacting to business risks and events to proactively using GRC management to improve business predictability and performance.

This document does not discuss the GRC framework at large but instead focuses on the technical foundation – in other words, the **common software foundation** – of such a framework. A GRC framework must be firmly grounded in common, reusable technology components to avoid duplication and fragmentation of effort across the diverse GRC applications that are needed to build enterprise-wide risk awareness and risk response skills. What is called a common software foundation on a GRC conceptual level (in Figure 1) can be provided by the SAP NetWeaver® platform on a practical level.

Most CIOs may not be accustomed to thinking of SAP NetWeaver as a GRC foundation – even those who use SAP® applications extensively. SAP NetWeaver has been presented to the world primarily as a framework of interoperable technology functionality that helps integrate people, processes, and information across disparate systems and even organizational boundaries.

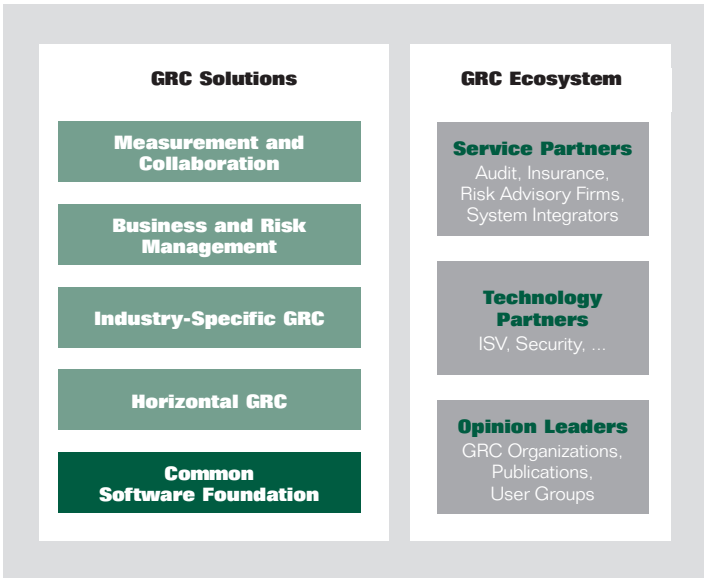


Figure 1: Framework for Governance, Risk, and Compliance Management

SAP NetWeaver supports a range of technologies that are integrated with each other, are integrated with mySAP™ Business Suite applications, and are based upon open standards that allow integration with third-party applications. This broad reach means that SAP NetWeaver can and should be viewed as a foundation that can help your organization with governance, risk, and compliance management.

SAP NetWeaver is unique because it provides the model-driven, flexible foundation for effective, organization-wide GRC management and because it offers the tools necessary to support organization-specific external regulatory and internal policy requirements both now and in the future. By connecting SAP and non-SAP applications and by composing compliance applications, your organization can contain and reduce the escalating costs associated with compliance. By overcoming the false dichotomy of build versus buy and achieving a more productive program of buy and extend, your organization can move closer to the ultimate goal of efficient and effective real-time GRC management.

SAP NetWeaver addresses GRC issues just as it addresses other challenges of integrating, adapting, and extending applications to meet new requirements. Because SAP NetWeaver was designed to be applied through model-driven methods, your organization can solve a number of issues by using its features. What is needed is support for business process flexibility, specifically, the ability to respond to and adopt regulatory changes quickly and effectively. Enterprise services architecture (ESA), a business-driven software architecture, amplifies the power of SAP NetWeaver by adding the ability to compose applications based on services that provide access to core business processes. As a result, you can adapt to regulatory changes faster with ESA.

By deliberately constructing its compliance-oriented architecture using SAP NetWeaver as its foundation, your organization can realize a number of wide-ranging benefits, including the following:

- The common components of the SAP NetWeaver platform reduce fragmentation and duplication of effort across multiple laws and multiple jurisdictions.
- Applications built with SAP NetWeaver can grow and change in response to changing regulatory requirements.
- Because of its integration with mySAP Business Suite, SAP NetWeaver provides ways to reach into appropriate applications to utilize their native functionality and their business context for compliance purposes.
- With SAP NetWeaver, you can fully resolve GRC events within the context of your business processes.
- SAP NetWeaver offers your organization the potential to automate processes and achieve a state of real-time compliance.
- The reuse and repurposing of SAP NetWeaver functionality makes maximum use of your investment in SAP and non-SAP applications for compliance purposes.
- Business process integration with SAP NetWeaver helps lower costs and eliminates human errors in compliance procedures.

That SAP NetWeaver can be applied to compliance problems is no surprise to anyone familiar with its functional scope. The question is: how can it be applied to solve pressing compliance issues? This document describes how SAP NetWeaver provides core functionality for each area of GRC management, specifically based on four key steps: **understand, document, guide and monitor**, and **report**. Some of the functionality of SAP NetWeaver is already widely in use; other functionality is just waiting to have its power unleashed in the context of GRC management.

THE NEED TO ADDRESS COMPLIANCE AND BEYOND

Try bringing up compliance in polite conversation among CIOs (or chief compliance officers or chief risk officers) these days. The issue, or rather the tangle of challenges it entails, is likely to elicit groans of mutual recognition and weariness. Organizations are under more pressure than ever before to hold themselves accountable to government agencies, shareholders, and other groups, so the stakes for an organization's IT executive could not be higher.

For most organizations, compliance remains largely ad hoc – a manual and costly process that diverts precious time and money from their core activities, offering competitors an opportunity to slip ahead. In addition, the associated and equally important concerns of effective governance and risk management do not receive the proper attention they deserve. While governance, risk, and compliance (GRC) management is clearly at the top of 21st-century management agendas in every industry, most organizations are still scrambling to meet regulatory requirements and deadlines using 20th century IT tactics. In other words, they are adding new applications and teams every time new compliance challenges arise.

Most CIOs and their peers are coming to realize, however, that GRC management requires more than adequate, narrowly focused tactics. Remaining in compliance is closer to a never-ending, ever-changing journey than a final destination. To embark on the journey of effective compliance, therefore, you can't view the effort involved as something apart from or on top of what your organization is or does. Combined with best practices for governance and risk management, compliance must be embedded into every business process and become part of your organization's day-to-day activities. Only a comprehensive

strategy with the right tools can put you on – and keep you on – the path from mere regulatory compliance to competitive advantage enabled through effective GRC management. “Organizations that choose individual solutions for each regulatory challenge they face will spend 10 times more on compliance projects than those that leverage each implementation for multiple requirements,” says French Caldwell, research VP at Gartner in a recent presentation.¹

What you need is a platform approach to GRC management, one in which you can reuse and repurpose common technology components within various GRC processes as often as possible to meet evolving and proliferating GRC requirements. Furthermore, that platform should also serve as a platform for your core business processes. This is the prerequisite for embedding compliance into core business processes on a common platform and automating these compliance subprocesses as part of your regular business processes. In other words, you need to merge your processes to address both business and compliance issues simultaneously using a common foundation.

The SAP NetWeaver® platform already provides the tools and infrastructure necessary for creating just such a platform approach to GRC management. This document explains how SAP NetWeaver can help your organization perform a variety of IT practices to address the compliance challenges facing it today.

1. “Technologies for Compliance: Automating Your Way Out of Confusion,” Gartner Symposium ITxpo, October 2005 (22J SYM15, 10/05, AE).

TOWARD AN ARCHITECTURE THAT SUPPORTS GRC MANAGEMENT

The best way to start exploring how SAP NetWeaver can support GRC management within your organization is to review the current thinking about what has become known as compliance management. This involves carving up both the world of compliance and the power of SAP NetWeaver into understandable chunks.

Starting at the highest level, there are three types of compliance:

- Vertical-industry regulatory issues, such as Basel II for the banking industry, the Restriction of Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE) directives for environmental compliance for high-tech manufacturers, and the U.S. Food and Drug Administration (FDA) Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11) for the life-sciences industry
- Horizontal legislation across industries, for example, the Sarbanes-Oxley Act and regulations for global trade, data privacy, document and record retention management, and supply chain traceability
- Internal process or policy frameworks within a single organization, including Six Sigma, ISO 9000 from the International Organization for Standardization, and voluntary standards, such as ethical norms governing minimum working conditions and wages worldwide

Each of these types of compliance has its distinguishing features, but it turns out that at a tactical level, compliance requirements in each of these categories can be satisfied through the four common steps shown in Figure 2.



Figure 2: Four Steps Toward Managing Governance, Risk, and Compliance

The steps are as follows:

- **Step One: Understand**
Laws and regulations must be interpreted and understood consistently to construct policies and procedures that ensure effective compliance.
- **Step Two: Document**
All business information, data, and documents need to be collected, harmonized, and logically grouped together to enable a comprehensive view throughout their entire life cycles. This single, consistent version of the truth needs to be shared to provide employees with the necessary business context to make informed and compliant decisions. This sharing includes the ability to deliver a compliance process with the widest possible reach and in the most suitable user interface, whether that be through a Web portal, Microsoft Office integration, mobile devices for constituents in the field, or even a voice recognition portal.

■ **Step Three: Guide and Monitor**

Your organization needs to create workflows that guide employees in their various roles through compliant processes and that automate these process steps where possible. These processes must be monitored and tied to alerts based on key risk indicators to avoid potential compliance violations.

■ **Step Four: Report**

Your organization must be able to perform detailed analyses of both structured and unstructured data to create a final report for regulators. Experts have examined the challenges posed by increased oversight of governmental and intergovernmental agencies, corporate boards, and other stakeholders within the context of the global organization from many different angles. A general consensus has emerged that today's tactic of approaching each compliance issue with silo systems – using one-off point solution and teams – is no longer viable. Figure 3 illustrates the trade-off. The onslaught of GRC mandates is poised to overwhelm the corporate agendas and IT budgets of even the most technologically advanced organizations.

What many in the compliance field have discerned is that most, if not all, compliance mandates share many common requirements. This commonality points a way out of the escalating impact of compliance on corporate financial and human resources. In short, effectively addressing the common requirements shared across disparate regulatory acts and internal policies does not require the wholesale adoption of entirely new systems and applications. Instead, by taking a deliberate asset and portfolio management approach, your organization can identify existing services that it can leverage for compliance purposes, as well as add new compliance-oriented services as needed using available technologies.

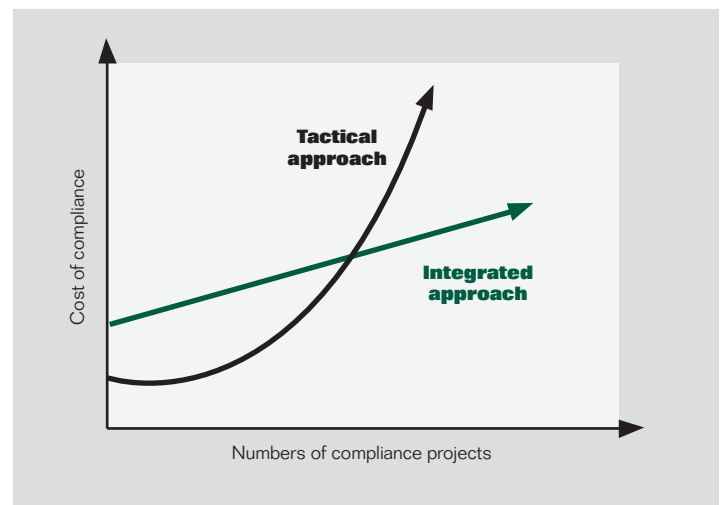


Figure 3: Cost of Compliance: Tactical Versus Integrated Approaches

User Productivity Enablement	Running an Enterprise Portal	Enabling User Collaboration	Business Task Management	Mobilizing Business Processes	Enterprise Knowledge Management	Enterprise Search
Data Unification	Master-Data Harmonization		Master-Data Consolidation	Central Master-Data Management		Enterprise Data Warehousing
Business Information Management	Enterprise Reporting, Query, and Analysis	Business Planning and Analytical Services	Enterprise Data Warehousing	Enterprise Knowledge Management	Enterprise Search	
Business Event Management	Business Analytics Monitoring			Business Task Management		
End-to-End Process Integration	Enabling Application-to-Application Processes	Enabling Business-to-Business Processes	Business Process Management	Enable Platform Interoperability	Business Task Management	
Custom Development	Developing, Configuring, and Adapting Applications			Enabling Platform Interoperability		
Unified Life-Cycle Management	Software Life-Cycle Management			SAP NetWeaver Operations		
Application Governance and Security Management	Authentication and Single Sign-On			Integrated User and Access Management		
Consolidation	Enabling Platform Interoperability	SAP NetWeaver Operations	Master-Data Consolidation	Enterprise Knowledge Management	Enterprise Data Warehousing	
ESA Design and Deployment	Enabling Enterprise Services					

Figure 4: Key IT Practices Supported by SAP NetWeaver®

The four steps mentioned at the beginning of this section – understand, document, guide and monitor, and report – help explain the variety of compliance requirements. SAP has created a technology map (shown in Figure 4) that shows how SAP NetWeaver can provide business value by supporting IT practices (shown in the left-hand column in Figure 4). This map helps you analyze on a more granular level how you can apply SAP NetWeaver to address GRC issues. For each project scenario, SAP NetWeaver supports a variety of key IT activities (as shown in the blocks in each row), all of which are easy to implement using the integrated components and tools of SAP NetWeaver. By exploring IT practices and the four steps together, you can gain a clearer view of exactly how SAP NetWeaver addresses GRC management through reusable services that can be shared across the organization and between GRC projects.

The next section explores not only how the core integration functionality of SAP NetWeaver satisfies these common requirements but also how SAP NetWeaver provides the GRC functionality necessary to help you meet typical future compliance challenges.

SAP NetWeaver: THE BUILDING BLOCKS FOR EFFECTIVE GRC MANAGEMENT

Our exploration of the ways that you can apply SAP NetWeaver to compliance issues uses the four compliance requirement steps defined earlier as an organizing principle. We'll discuss each step and describe the appropriate IT practices used in the step.

Step One: Understand

As a first step toward addressing GRC management, your organization must understand what it is expected to do. The understand step basically requires you to first translate laws and regulations into policies and procedures. Most organizations leverage management and audit consultancies to assist in interpreting the laws and regulations. But once your organization understands what must be done, it needs to determine where within its business processes to apply controls, to harvest information for monitoring risks, or to construct applications to support specific compliance needs and roles.

With SAP NetWeaver, you can perform the IT practice of **end-to-end process integration**, specifically business process management, for valuable modeling purposes. Using SAP NetWeaver, you can model business processes coherently on all necessary levels of abstraction: creating high-level business maps, modeling business processes and their interactions, and even modeling detailed process steps. Your IT team can use SAP NetWeaver to build compliance into these business process models.

Various tools bring this integrated modeling environment to life, including the ARIS for SAP NetWeaver joint application – which enables modeling of integration scenarios and process components at a business level – and the SAP® Solution Manager tool, which helps you to model on a technical level how business processes work within the context of SAP applications. For example, SAP Solution Manager provides you with centralized access to the business rules of implemented business processes within the SAP technology landscape.

Step Two: Document

The IT practices your organization can perform with SAP NetWeaver to support the document step are primarily concerned with capturing all business information, providing that business context to all stakeholders, and extending the reach of compliance mechanisms as far into the organization as possible to keep pace with users. These IT practices include **user productivity enablement, business information management, and data unification**.

Too often the people at the heart of the organization are forced to tailor their roles and responsibilities – the shape of the company itself – to the IT systems that support them rather than the other way around as it should be. SAP NetWeaver was created in part to deliver on the promise that business processes, and especially human interaction with those processes, should reflect and enhance the way people work in the real world.

Within the context of GRC management, that means helping you extend the reach of compliance procedures through a choice of interfaces, whether through portals or through the integration of productivity tools like Microsoft Office. It also means guaranteeing the consistency of data retrieved from a single back-end system through all of those interfaces. Together, these processes fall under the IT practice of user productivity enablement.

The next challenge is capturing all business information – structured and especially unstructured data – and creating a mechanism to store, search, and track any changes to it, including who modified the data and documents and when. In addition, this data and these documents must be shared across the organization. Customers and regulators do not want to hear about data formats; they want records – structured data combined with unstructured data (for example, documents, spreadsheets, PDFs, and Microsoft PowerPoint presentations) – to be properly managed from inception to disposition.

It has become apparent that most of the information generated by organizations is not being managed on an organization-wide level. At a recent symposium, Toby Bell and Kenneth Chin of Gartner pointed out that as much as 80% of an organization's data is unstructured, and 90% of unstructured information is not managed.² Information stored on local hard drives in Microsoft Word documents, Microsoft Excel spreadsheets, and PDF files are not accessible by others within the organization, leading to problems that range from uninformed decisions to difficulty in legal discovery during litigation to the inability to comply with data privacy requirements. Business information management is the IT practice concerned with consolidating and managing structured and unstructured sources of information, then preparing that information for consumption.

User Productivity Enablement: Portals, Roles, and Profiles

Within SAP NetWeaver, the document step toward compliance begins, for all intents and purposes, with an enterprise portal. Highly reliable and secured via single sign-on, portals provide access to data and functionality tailored to the needs of individuals. Any given window in the portal might include productivity tools, such as e-mail and search functions; collaboration tools for sharing and tracking changes to documents; and customized front ends to legacy applications and integrated applications, of which perhaps only a few aspects are relevant to the employee, partner, supplier, or contractor.

Portals proactively present only relevant and appropriate features. This is important for GRC purposes because portal-enabled environments are much less susceptible to accidental or even willful misuse by individuals who are forced to seek out the functionality they need. Portals are commonly configured using roles, which are standardized profiles with preconfigured settings that are specific to the person's role within the organi-

zation (a sales manager or customer service representative, for example). Through role-based settings, individuals are shown only what they are supposed to see and can perform only those tasks for which they are responsible.

One of the portal's most valuable attributes from a business process perspective is its ability to render processes as a step-by-step set of guided procedures narrowly tailored to the task at hand. This methodology – which will be discussed in more detail under the guide and monitor step below – is especially useful for a GRC approach because individuals can be guided through compliance-friendly practices without any obvious disruption to their day-to-day work.

User Productivity Enablement: Duet™ Software

Through a groundbreaking collaboration between SAP and Microsoft, Duet™ software promises to take this functionality a step further via the full-scale integration of Microsoft Office Professional 2003 with the mySAP™ ERP 2004 application. By leveraging the openness of enterprise services architecture (ESA) and the Microsoft .NET architecture, Duet exposes selected business processes and information from mySAP ERP 2004 through Microsoft Office Professional 2003. Alerts can be directly sent to your Microsoft Outlook in-box. Within Microsoft Outlook, you will be able to respond to events and drive real-time data management. Forms and other necessary data types can be rendered in Microsoft InfoPath and routed to individuals. Important Microsoft Office documents will be directly stored within mySAP ERP instead of on your local hard drive. In this way, it will soon be possible to bake business procedures, including those vital to GRC management, into the tools of everyday office life with minimal retraining and disruption of project workflow.

2. "Putting Content Into Context: Strategy, Integration, Analytics, and Valuation," Gartner Symposium ITxpo 2005, October 2005 (45F, SYM15, 10/05, AE).

User Productivity Enablement: SAP NetWeaver Mobile

Desktop portals are not the only interfaces that enable improved user productivity. The SAP NetWeaver Mobile component helps your organization integrate, synchronize, and secure mobile devices – not just online laptops and personal digital assistants (PDAs), but also offline, task-specific handheld devices – with enterprise systems. GRC-relevant information that was once captured after the fact in the form of paperwork can now be entered in real time as it is created. For example, envision emergency medical technicians (EMTs) arriving at an automobile accident scene, then rushing victims to a nearby hospital. Critical information about the victims' conditions – which otherwise might be captured on paper much later – could be entered on the spot into a device that is later synced with the hospital's systems. Guaranteeing the accuracy of this data while it is still fresh in the EMT's mind could make all the difference if it becomes necessary later to determine – in the discovery phase of a malpractice lawsuit, for instance – whether the EMTs acted properly and in compliance with certain requirements.

User Productivity Enablement: Knowledge Management

When used in tandem with knowledge management tools and data warehouses, portals become the setting in which individuals can share and search within documents and reports generated from both structured information and unstructured information (such as information within a multitude of documents and spreadsheets). The Knowledge Management component of SAP NetWeaver was designed specifically to track changes to dynamic documents that typically undergo numerous revisions, such as contracts and policies; SAP ArchiveLink® software links static documents to business data. All of this functionality comes into play during GRC situations, such as a patent application process or even a dispute – when questions of who made which decisions when are of paramount importance – to ensure that all the relevant information is captured and stored within the portal.

The data archiving functionality of SAP NetWeaver provides a robust mechanism for managing the life cycle of data. It allows your organization to extract historical data from online applications and to manage that information in accordance with legal retention statutes.

Data Unification: Arriving at a Single Version of the Truth

SAP NetWeaver also supports the document step through the IT practice of data unification. With this IT practice, your organization consolidates, harmonizes, and manages structured master data, which then can be processed in data warehouses for analysis and reporting.

One of the advantages of taking a platform approach to GRC management instead of using silo applications is the ability to capture, merge, and harmonize records from any database in your landscape as long as it resides on the platform. This is critical to eliminate duplicated records, such as ensuring that customers who request their names be added to the national Do Not Call directory are deleted from telemarketing lists even if their names appear in more than one entry. Another example is ensuring that hazardous material is defined with a unique, clear name and that all related product characteristics are standardized to enable fast and easy access, even if information is stored across multiple databases.

Step Three: Guide and Monitor

A desired goal for ensuring efficient and effective compliance processes is to automate as many process steps as possible and to only be alerted to situations that put your organization at risk of noncompliance.

With SAP NetWeaver you can perform the IT practice of **end-to-end process integration**, which addresses the activities needed to automate process steps in scenarios ranging from application-to-application to business-to-business integration. The IT practice of **business event management** is used to perform the activities that move you to the next level beyond plain automation – to intelligent management by exception. Business activity monitoring is the IT process within business event management that enables you to generate alerts when human intervention – in other words, a cognitive or discretionary decision – is required. And through the process of business task management, you can then guide employees through the correct procedures to ensure compliance with standards, regulations, and policies.

All of these interactions between people and IT systems need to be safeguarded with the IT practice of security so that you always know who has and who does not have access to your organization's systems.

Business Event Management: Managing Business Tasks with Workflows

Because the scope and complexity of regulatory mandates is expanding and changing so rapidly, it is nearly impossible for your employees to take responsibility for compliance on their own. The Sarbanes-Oxley Act alone has caused some organizations to define as many as 100,000 internal controls. And many organizations continue to aggregate the data corresponding to these controls in Microsoft Excel spreadsheets. The mind boggles at the associated labor costs, the potential for errors, the potential penalty for those errors, and the additional costs of double- and triple-checking those spreadsheets to head off penalties.

Where once ad hoc business processes were sufficient, from a GRC management standpoint, it is imperative that these processes become more structured and more verifiable. Business task management with SAP NetWeaver helps you address the guide step toward compliance by getting the right tasks to the right people and by providing the means to complete tasks on time and with the best results. With SAP NetWeaver, your organization can create workflows and guided procedures. In this way, you can ensure that business events propagate from a multitude of systems to the appropriate decision makers in the context of the relevant business processes and are optimally resolved. Akin to the software wizard that guides PC users through the setup of their home machines, guided procedures – or role-based procedures within a portal environment – can help your organization address the complexity associated with GRC management by walking individuals through occasional, but potentially complex, GRC tasks while minimizing the likelihood of human errors.

Business Event Management: Automation and Monitoring

The next evolution of automated process integration and human-machine interaction is management by exception, whereby multiple solutions are integrated and configured to run more or less automatically, notifying users only when an exceptional event demands immediate attention and resolution. In practice, this means using the portal, business activity monitoring, and end-to-end process integration features of SAP NetWeaver to address the monitor step and to determine relevant key performance indicators (KPIs). You also use these features to set rules to decide what is or is not an exceptional event when measuring those KPIs and to establish to whom in the organization alerts should be sent when an exception occurs, as well as when and to what interface (for example, portal or e-mail in-box).

The alert might take the form of a message – generated by the SAP NetWeaver Exchange Infrastructure (SAP NetWeaver XI) component – appearing in the chief compliance officer’s (CCO) digital dashboard as a flashing red light. This might be a warning of a security breach, such as when an individual has violated his or her access privileges or when an unusually high percentage of product returns over the past week is detected. Your CCO can then respond to these situations to determine whether the percentage indicates a product defect or if a product recall is necessary.

In this manner, your organization can mitigate risks by being alerted through continual monitoring routines, alerted instantly in the case of a pressing issue, and prompted to act before your organization ever falls out of compliance. In the long run, management by exception promises great savings through reduced headcount and fewer labor hours as an increasing number of once-manual tasks are integrated into automated processes.

Business event management is the combination of **guiding** people through a process and **automating** processes to the greatest extent possible (in cases where a process can be performed without human intervention). A good example of business event management is the provisioning of user identities and authorizations in a hire-to-rotate process. Clearly, the provisioning of identities and authorizations must be standardized and controlled throughout the employee life cycle. Only through such a process can your organization grant and revoke the appropriate access rights – from the time of someone’s hire until eventual departure – efficiently and in line with standing policies through all transitions and promotions of the employee.

A workflow guides HR, departmental managers, IT role and access managers, and others on how to request, cross-check, and approve new identities and authorizations in the proper

sequence (or workflow steps). Several steps in this workflow, including the check on proper segregation of duties (SoD), can be completely automated. (SoD is the concept of designating more than one person to a task in order to avoid fraud. SoD must be a central concept in any IT organization so that no single person is in a position to introduce fraudulent or malicious data, transactions, or other changes without detection.) The approver can then base a decision on the result of this automated check. A continuous health check on your IT systems can produce insight into whether any individuals have authorizations beyond the established policies and control objectives. In such cases, an alert is sent to the chief information security officer.

Application Governance and Security Management: Enforcing Security

With SAP NetWeaver, your IT organization can perform the IT practice of **application governance and security management**. You can maintain an appropriate level of security and quality in your intellectual property and information assets without compromising flexibility, user productivity, and collaboration with customers and partners. Your organization can manage security through integrated user and access management, as well as authentication and single sign-on to address the twin concerns of identity and access management. In this way, you can answer such questions as “Who is this user?” and “Which processes is this user permitted to access?”

On the identity management side, SAP NetWeaver supports central user administration, including integration with Lightweight Directory Access Protocol (LDAP) services for heterogeneous environments. On the access management side, SAP NetWeaver provides authorization controls that are uniquely granular to support even the most complex business processes. With SAP NetWeaver, your organization can define user roles and privileges down to a level that eliminates most possibilities for unauthorized internal and external access. And if an unauthorized access does occur, SAP NetWeaver can generate alerts.

The Virsa Compliance Calibrator application for SAP adds another level of security on top of the identity and access management controls described above. The software enables you to perform detailed risk analysis, detection, and remediation of access and authorization problems. It particularly helps enforce the required segregation of duties.

There is an obvious need to maintain the confidentiality, integrity, authentication, and nonrepudiation characteristics of messages that hop through applications, platforms, and often the entire organization. SAP NetWeaver contributes additional security functions, such as single sign-on. Using single sign-on is akin to granting individuals a security clearance. SAP NetWeaver authenticates users and takes responsibility for tracking their access rights to and progress through any and all of the business processes that rely on SAP NetWeaver as their platform. Rather than force users to reenter their credentials at every process step that invokes a new application, the platform sets and observes the rules assigned to each user or to more generic user roles to which individuals are then assigned.

Single sign-on can be implicitly audited if security logging is configured accordingly, for instance, so that every logon and logoff is recorded. And thanks to the framework provided by its audit information system and security audit log features, SAP NetWeaver can alert the administrator of any security violation, sending the alert to the systems management console. SAP NetWeaver also allows for structured analyses of user behavior in accordance with regulatory or policy requirements.

In this way, SAP NetWeaver provides a centralized, cost-effective, fully customizable security framework for all applications running on SAP NetWeaver. If needed, you can expand the security framework with partner products to cover unique needs (such as biometric authentication methods) or to protect certain data entry functions (for instance, running a virus check prior to document uploads).

Step Four: Report

In the end, every organization must still deliver proof to regulators that it is in full compliance with the millions of requirements it is grappling with in relation to the Sarbanes-Oxley Act, the Patriot Act, RoHS, WEEE, and the hundreds of other regulations it must adhere to. The question is: how will it deliver that proof in a form that is less costly and less resource intensive than the efforts of its competitors and is 100% accurate?

On its own, SAP NetWeaver cannot guarantee compliance with any regulation; you must still extend your core business applications with regulation-specific composite applications – whether custom-built or acquired from SAP or its partners. These composite applications provide at least a rudimentary solution for processing consolidated information into a report form acceptable to the GRC auditing body in question.

But the SAP NetWeaver platform approach does offer a radically different solution – in terms of scale, complexity, and cost – for addressing the report step. The SAP NetWeaver platform provides basic technology support for GRC solutions. Using the master-data management, data-warehousing, analytical tools, and document-management functionality of SAP NetWeaver performed primarily within the IT practices of **business information management and data unification**, your organization can quickly publish reports with the required information using a central repository of clean master data. The only regulatory-specific code needed is an “extension” for publishing the final report.

Consider the benefits of this approach against the niche solutions offered for each regulation, which redundantly attempt to harmonize, consolidate, and analyze data before generating their own respective reports. How much effort is wasted by using those applications? Is the resulting data more accurate? The answer is no.

The Future of Reporting: Toward Real-Time Compliance

It is important to understand that reporting does not necessarily have to end in a printed report. This year, for example, with the latest release of mySAP ERP, it will become possible to build enterprise services to interact with the SAP NetWeaver Master Data Management (SAP NetWeaver MDM) component. So, for example, rather than simply pump out another report on the RoHS and WEEE environmental compliance of a new high-tech product's components, a process enabled by SAP NetWeaver MDM might incorporate GRC checks into the heart of a product development process. Instead of checking compliance after the fact, the process could actually demand it as part of the procedure, refusing to allow development to continue should a batch of components fail to pass RoHS and WEEE compliance standards. In response to such an event, the service could send a flurry of SAP NetWeaver XI messages to the relevant systems, flipping switches that ensure product manufacturing is halted until full compliance is restored.

The convergence of end-to-end process integration, digital dashboards, and enterprise service enablement will lead inevitably to the types of services and workflows outlined above. Within the context of SAP NetWeaver, reporting will increasingly become less of an end state – in other words, the final report at the end of the fiscal year – and more of a real-time process. That central view on information comes alive, breathing proof of compliance, promising to drastically reduce the costs of post facto, year-end tallying. It also promises to minimize the potential for human error by removing individuals from as many day-to-day processes as possible.

Enabling Enterprise Services Architecture: Design and Deployment

Across all four GRC steps, SAP NetWeaver provides a comprehensive set of tools that support **unified life-cycle management** and **custom development** activities, which ensure business continuity at the heart of effective GRC management.

Unified Life-Cycle Management: Centralized Administration

Unified life-cycle management is the IT practice concerned with the centralized monitoring and administration of application performance, job scheduling, and data archiving. The overt aim of unified life-cycle management is to efficiently run and maintain all business processes (including compliance processes) and the IT resources underlying them. In the context of GRC management, unified life-cycle management tools log and archive every event in the life of the software – including every user login, every trigger of any automated process, and every job scheduled. These events are then reported within a single interface, in this case, the SAP NetWeaver Administrator tool. Other relevant features of SAP NetWeaver include central monitoring consoles and an audit information system.

That framework is critical because support for unified life-cycle management within SAP NetWeaver was not specifically designed with GRC issues in mind. However, SAP NetWeaver offers you the advantages of being able to monitor, administer, and archive in a holistic fashion – through a platform approach, as opposed to deploying stand-alone solutions to monitor for each compliance requirement. This will become more critical as ESA and other service-oriented environments lead to increasingly automated business processes spanning multiple applications. In this environment, being able to track cascading event triggers is key to understanding how decisions were made and what courses of action were taken.

Finally, the data archiving functionality of SAP NetWeaver supports comprehensive data life-cycle management activities across all application data. Your organization gains powerful tools to select certain sets of data and to define clear rules for retiring this online data. You can move the data first to nearline storage and then eventually dispose of it in accordance with the regulatory mandated retention periods.

ESA: The Future Foundation of Embedded Compliance

SAP is a pioneer and leader in ESA, a next-generation, business-driven software architecture in which applications are decomposed into services and objects that can be flexibly combined and recombined in almost limitless combinations with few development penalties. SAP NetWeaver is the foundation for ESA. SAP is actively working today to build enterprise services into its own applications, including the mySAP Business Suite family of business applications, which will offer organizations the ability to flexibly recombine and configure application and compliance solutions. SAP NetWeaver supports organizations' **ESA design and deployment** activities by allowing them to leverage existing IT investments to compose new, distinctive business processes flexibly and at low cost. It offers tools for rapid development and deployment of enterprise services and composite applications that can be configured and reconfigured at will for rapid risk response and to keep pace with regulatory changes.

By using enterprise services, your organization can create services capable of leveraging compliance procedures across its entire system landscapes. For example, it will become possible for a compliance application to automatically check internal controls simply by running checks using the relevant enterprise services within much larger business processes.

Custom Development:

SAP NetWeaver Development Toolkit

SAP NetWeaver was designed as a composition platform that enables IT departments to compose and support both packaged applications and custom-developed applications – and, more important, the recomposition of the former into the latter. The SAP NetWeaver platform supports both Java and the SAP ABAP™ programming language through the SAP NetWeaver Developer Studio tool. But SAP NetWeaver offers much more than a simple programming environment. SAP NetWeaver helps you manage the entire development life cycle – from initial coding, configuration, and testing to putting code into production and finally deployment of the application – all within a single controlled environment with support for authorizations and audit trails.

With SAP NetWeaver in place as their platform, compliance-focused organizations no longer face the dilemma of buying secure, dedicated compliance applications versus building custom solutions tailored to their unique business processes. Thanks to its support for ESA and its model-driven development tools, SAP NetWeaver makes it possible – through enterprise services – to recompose features of packaged applications for use in custom solutions.

The advantages of this approach are many. Rather than continually purchasing stand-alone applications for each and every GRC issue that arises and then attempting to weld them together using hard-coded, application-to-application integration techniques, you can use SAP NetWeaver to spearhead an alternative approach. With SAP NetWeaver, your organization can extend the functionality of off-the-shelf applications through code reuse and enterprise services to effectively build composite compliance applications.

SAP NetWeaver AS A FOUNDATION FOR GRC MANAGEMENT AT SAP

SAP itself is basing all of its governance, risk, and compliance execution on the SAP NetWeaver platform. As part of its global risk management initiative, SAP wanted to identify, evaluate, and monitor all relevant risk in the area of financial reporting. Using SAP NetWeaver, SAP was able to quickly leverage the contextual information contained within its various business applications and combine that information with its dedicated application for managing compliance with the Sarbanes-Oxley Act. SAP created analytical composite applications specifically designed to address these GRC issues. One of the first projects along these lines delivered six applications for monitoring compliance with Section 404 of the Sarbanes-Oxley Act.

It took SAP engineers just five weeks to create six analytical applications with SAP NetWeaver using the management of internal controls functionality in mySAP ERP. The applications were created to specifically create intuitive tools for visualizing data and to address the steep learning curve. These tools included an overview application for monitoring all Section 404 compliance tests and assessments being conducted at any given moment, a trio of tools for monitoring the progress of each assessment and their results to date, another tool for tracking the status and priority of any issues discovered during those assessments, and one more for monitoring the details of employee sign-offs from software managing compliance with the Sarbanes-Oxley Act.

All of these applications were then made accessible through SAP NetWeaver Portal. Users assigned to roles – including executive board members, the corporate Sarbanes-Oxley team, local Sarbanes-Oxley champions, organizational unit managers, and finance and administrative personnel – were able to see all of these analytical applications as portlets (called iViews) within their portal interfaces.

The final result was a solution that keeps executives updated on the status of internal controls and helps them track issue remediation under their direct responsibility. And – because they contain no programming language – any of these tools can easily be modified (or remodeled) to address individuals' future needs.

StrategicRISK magazine cited these applications when naming the SAP risk management team as European Risk Management Team of the Year in 2005. For more information on the award, go to www.strategicrisk.co.uk/awards/default.asp?id=Win05.

The SAP global risk management team also won awards for the most effective use of technology and for the best organization-wide risk program.

CONCLUSION

One thing SAP NetWeaver cannot do is prevent CIOs from groaning the next time you pepper them with questions about their GRC strategy. There are so many regulations already – and there will only be more to come – that they can't help but feel overwhelmed just thinking about it.

But a platform approach with SAP NetWeaver as the foundation can alleviate their concerns for a multitude of reasons. First, the rich native functionality of SAP NetWeaver, which includes – but is not limited to – a robust workflow engine; integrated document management, business intelligence, and portal features; and an XML-based messaging framework and a security framework, can easily be repurposed for simple GRC tasks. If establishing compliance is as simple as publishing a report, the publishing tools of the SAP NetWeaver Business Intelligence component can produce that report. If it only requires consolidating data in a warehouse, SAP NetWeaver offers any number of options for doing just that. The most basic toolset for performing simple GRC tasks is built right into the platform.

Second, the intrinsic integration of SAP NetWeaver with mySAP Business Suite and easy integration with third-party applications grants GRC tools a deeper reach into – and a greater semantic awareness of – the data and functionality residing within your organization's applications that are also deployed upon the platform. By embedding GRC tools in the platform, these tools can reach everywhere the platform goes, extending their scope far beyond the limits of stand-alone solutions.

Third, as the reach of the business platform extends and as the service enablement of enterprise software progresses, solving GRC issues will become a matter of composing composite applications that are tailor-made to the needs and business processes of your organization. SAP NetWeaver also provides the toolset for creating these composites and integrating them into the heart of business processes. This same toolset affords SAP NetWeaver the ability to incorporate stand-alone applications into the platform and to harness their unique GRC features while continuing to manage business process integration and other tasks.

To recap, the major business benefits SAP NetWeaver provides your organization in its governance, risk, and compliance management efforts include the following:

- The common components of the SAP NetWeaver platform reduce fragmentation and duplication of effort across multiple laws and multiple jurisdictions.
- Applications built with SAP NetWeaver can grow and change in response to changing regulatory requirements.
- Because of its integration with mySAP Business Suite, SAP NetWeaver provides ways to reach into appropriate applications to utilize their native functionality for compliance purposes.
- With SAP NetWeaver, you can fully resolve GRC events within the context of business processes.
- SAP NetWeaver offers your organization the potential to automate processes and achieve a state of real-time compliance.
- The reuse and repurposing of SAP NetWeaver functionality makes maximum use of your investment in SAP and non-SAP applications for compliance purposes.
- Business process integration with SAP NetWeaver helps lower costs and eliminate human errors in compliance procedures.

For more information about how SAP NetWeaver can help you manage governance, risk, and compliance in your organization, call your SAP representative today or visit us on the Web at www.sap.com/grc.

www.sap.com/contactsap

THE BEST-RUN BUSINESSES RUN SAP™



50 079 478 (06/05)

© 2006 by SAP AG. All rights reserved. SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary. Printed on environmentally friendly paper.

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