



Narina Sippy
Senior Vice President
SAP solutions for GRC

12 Risk Management Essentials Every SAP Customer Now Needs to Know

Business risk. The unknown. The unpredictable. The things that affect business outcomes but lie outside your managerial sphere of control. It's not just finance departments and risk managers who grapple with risk and uncertainty. We all do.

Risk possibilities are endless. Those responsible for the development, marketing, and sales of products and services know that a competitor can quickly overtake those products or services, or that new technologies can render them obsolete. A hurricane might disrupt the delivery of important materials from a supplier in Louisiana, a change in euro-to-dollar valuation might affect your ability to sell in France, evolving technology could stifle your online retail business, or a product safety issue could hit the press and mar your company's reputation. These are the risks of everyday business that should be part of your strategic and budgetary planning.

Inherent in every business decision we make are elements of risk and uncertainty. In fact, a 2006 Accenture global study — comprised of interviews with 436 senior executives at major companies in North America, Europe, and Asia — ranks managing risk at the top of executives' priority lists.¹

In this article, Narina Sippy, SAP Senior Vice President and General Manager of SAP solutions for governance, risk, and compliance (GRC), explains why companies are investing heavily in risk management — and what risk management essentials the SAP customer base now needs to understand.

The correlation is clear: Vigilant risk management leaves your business in good standing with shareholders and boosts potential profits. Ineffective risk management leaves your business exposed and hides potential opportunities. Executives are becoming acutely aware of this, and none want to be caught off guard.

But implementing limited-scope practices that address risk at only the highest levels — or assigning a department to identify risks in an ad hoc project — does very little to address your business exposure and lost opportunities.

Many executives don't understand how to approach risk management strategically. Others don't have risk management capabilities at their disposal; they lack tools and metrics to analyze risk/reward trade-offs and proceed accordingly.

Risk management does not happen only at the board level either. Risks and opportunities clearly exist throughout all levels of the organization, across all business processes. Consider the various internal teams and partners involved in your supply chain. Do they

Inside

- S-3 | **What Data Governance Model Is Right for Your Company?**
BackOffice Associates & CranSoft, Inc.
- S-5 | **Sustain Your GRC Strategy with Continuous Controls Monitoring**
Ernst & Young
- S-7 | **Use Master Data Management to Master Your Compliance Initiatives**
Siperian
- S-9 | **Do Your Testing Methods Work in Concert with Your Compliance Efforts?**
Worksoft, Inc.
- S-11 | **The 7 Pillars of Strong Internal Controls**
170 Systems, Inc.
- S-12 | **Atrion Helps EH&S Teams Stay Compliant in the Face of New REACH Regulations**
Atrion International Inc.
- S-13 | **Governance, Risk, and Compliance — Moving Beyond Integration to Enterprise Strategy**
BearingPoint
- S-14 | **Remaining Compliant**
CSI
- S-15 | **Why Change Management Should Be a Top Compliance Priority**
Revelation Software Concepts, Ltd.
- S-16 | **The Coming Revolution in Tax Reporting and Compliance**
Sabrix, Inc. & Deloitte
- S-17 | **Incorporate Security Intelligence into Business Intelligence**
SECUDE Global Consulting
- S-18 | **Tips for Building a Successful GRC Project Methodology**
Turnkey Consulting

¹ Accenture study (September 19, 2006). See www.accenture.com/Countries/Canada/About_Accenture/Newsroom/ManagingRiskRanks.htm for more information.

have collaborative indicators to apprise them of goods delays, outstanding duties or taxes, or import/export license renewals? Chances are, they don't. But implementing these types of controls to warn of actual or likely risk events can reduce the impact of the event. Once controls are in place, you not only minimize delays and penalties, you also realize strategic gains:

- Money previously lost to fines or production delays is now available for strategic investment
- The very same information used to assess risk and provide early warnings proves invaluable to logistics and inventory optimization
- Early warnings can help in managing customer expectations, thereby preserving your customer base

So it's not just risk mitigation that's driving the demand for risk management tools. These benefits of risk management also account for the strong demand.

Remember, all loss events negatively affect the bottom line. Plant managers, safety managers, product development teams, HR, customer service, and sales teams all have to contend with loss events – and all stand to benefit from a better understanding of risk factors in their planning and optimization activities.

The common challenge I see is that nearly all of these organizations are ill-equipped to evaluate and manage risk. And whatever measures *are* in place are often isolated from risk management initiatives across the company.

So I'm now seeing high demand, across the board, for risk management tools. At the same time, there's an awakening to the fact that risk doesn't confine itself to nice, neat silos. There are lots of interdependencies, and at the top of the corporate ladder there's a need for integrated risk management that spans all areas of the business – and for an understanding of the relationships that bind those areas.

Companies need a systematic way to identify, evaluate, and manage risks across all phases and facets of their business. That's why we're now working with so many customers, helping them forge a GRC initiative that provides a unified approach to corporate risk across their enterprise.

Risk Management Considerations Every SAP Customer Needs to Understand

1. **DO** openly support risk management at the executive level and make it a part of the company culture.

2. **DON'T** make risk management a one-time or theoretical exercise, one that's considered unimportant to executives.
3. **DO** look at the interplay between different types of risks: strategic, operational, financial, human capital, hazards, and natural disasters.
4. **DON'T** limit your risk management activities to reactive contingency plans.
5. **DO** establish a common infrastructure, a set of metrics, and even a language for your risk discussions.
6. **DON'T** overcomplicate the risk management process. For risk management to be adopted by everyone, it cannot be perceived as an experts-only function.
7. **DO** ensure that all key stakeholders collaboratively share the responsibility of identifying, mitigating, and managing risk across processes. It's better to have several thousand keeping an eye out for risk rather than a few dozen.
8. **DON'T** make risk management an isolated function or leave it to a single department.
9. **DO** look at risk as part of your strategic business planning and operations processes. Incorporate risk management in planning and budgeting by identifying key risk indicators that can be tracked as you implement strategy through your day-to-day activities.
10. **DON'T** separate risk from how you run the business.
11. **DO** make risk consideration a part of corporate performance management to understand the upside of business decisions and recognize the impact of poor risks.
12. **DON'T** leverage risk management tools only at the lowest operational level merely to mitigate risk.

3 Steps to Implement Risk Management

It's not an overstatement: The goal is to integrate risk management into the everyday lives of every manager to enable them to see and assess the company's complete risk profile. There is no question that this provides the most strategic benefit to an organization. So how does one transform risk management from a reactive process into a strategic weapon? I recommend a three-step approach:

1. Identify the wealth of risk management-related information already available to your company in SAP ERP and other ERP systems. Part of the evolution toward a more mature enterprise risk management framework incorporates existing business practices – reusing information

Article continues on page S-19

Even finance organizations, which tend to be among the most advanced in terms of risk management within a company, often don't have sufficient visibility into risk events that can impact profitability.



Tom Kennedy
Founder,
BackOffice Associates &
CEO, CranSoft, Inc.

What Data Governance Model Is Right for Your Company?

Sound GRC Initiatives Rely on Quality Data

An essential element of any successful corporate governance, risk, and compliance (GRC) initiative is quality data. The accuracy of all GRC-related analysis depends on the underlying quality of the transactional and master data within your ERP systems. And yet, while it would be unthinkable for a corporation to bypass quality control on the production floor, companies are still producing data with little or no quality control on a daily basis.

To ensure sustainable data quality, it is essential to consider a data governance initiative complete with remediation tools to establish metrics for data accountability. Companies implementing their first data governance initiative must understand the different levels of data governance and carefully decide which one is the right fit for their organization (see **Figure 1**).

4 Levels of Data Governance

Many companies are setting up departments or teams to take charge of and responsibility for data quality throughout their enterprise (see sidebar on the next page). To date, we have seen various levels at which data governance strategies are implemented:

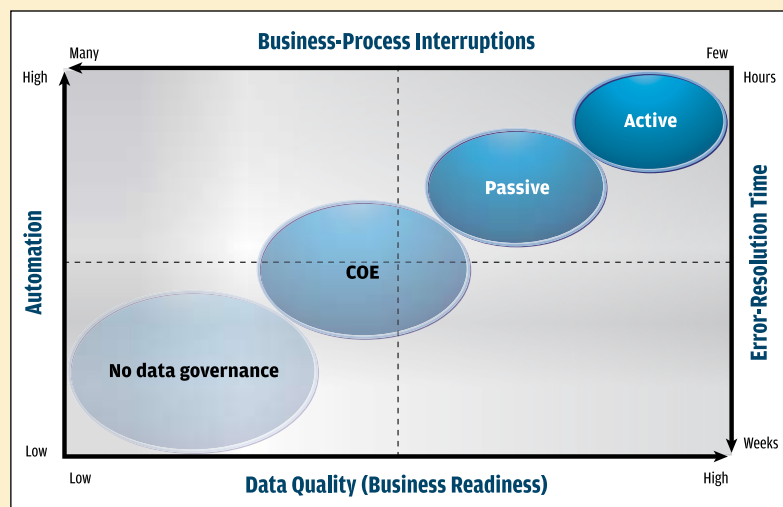
- **No data governance** – This is the “Wild West” model. Every user is trusted to enter in their data accurately and on time, all while minding corporate standard operating procedures and compliance statutes. The reality? Despite rigorous training, most users do not follow standard operating procedures. Based on the resulting lack of control and accountability, this is the least efficient and most risky model.
- **Center of Excellence (COE)** – This model tasks a central group with the responsibility of creating and verifying all data requests before posting them to the SAP system. The intention is to have a central core entering an agreed-upon “single version of the truth.” However, in many cases this model results in slow data-entry times and costly downstream effects.
- **Passive data governance** – Users enter data into the SAP system, and then a toolset or reporting mechanism iteratively identifies data-related errors within that system. Errors are automatically reported back to their authors for correction and quality metrics are delivered to management. This model enables a valuable, measurable process.
- **Active data governance** – All data required to support the configured SAP business processes is collected prior to posting into the SAP system and validated automatically through a collaborative environment. This eliminates the possibility of business-process interruptions due to omissions, duplicates, consistency and content errors, or a lack of standards.

As market forces drive GRC issues to the forefront of mainstream business processes, companies need to ask: Is our data ready to meet the goal of a sustainable GRC strategy?

Recommendation: Start with a Minimum of Passive Data Governance

The “no data governance” model is just too risky. And although the COE model may improve the quality of data, it also increases the time required to collect, validate, and enter that data into the SAP system. This model also proves difficult to scale with a growing SAP footprint. Accordingly, many companies implementing their first data governance

FIGURE 1 ▼ The four models of data governance; as automation increases, error resolution time and business process interruptions decrease



✓ NOTE!

Since both the passive and active models are business-critical, we recommend you use a solid passive solution as a roadmap for implementing an active model.

AMR Research reports that large companies can spend US\$250,000 to US\$500,000 on service-intensive engagements to find, fix, and prevent data governance problems.¹

strategy look to the passive data governance model to introduce automation and create accountability and data ownership at the user level.

We recommend that you start building your passive data governance strategy by acquiring a preconfigured toolset built for your unique data challenges. This toolset should include out-of-the-box functionality for workflow enablement, quality-metrics reporting, and duplicate detection. For global organizations, the tools should also be multilingual. Most importantly, the toolset should be easily configurable for business people, not just for IT. Enabling business users to control data and its quality is imperative to effectively encapsulating your specific business-process requirements.

Once you implement this toolset, you'll also need to build a business process repository based on your current data requirements. Over time, the configuration of this repository should be capable of iteratively reporting on all business-critical master and transactional data. BackOffice Associates has built our own passive governance solution, **DataDialysis** – specifically made for SAP systems – to fulfill all of these requirements.

Since the passive model's automation of data governance implements control while alleviating the bottlenecks associated with manual data entry, it is considered a great step forward. However, it does not always solve the entire data-governance conundrum.

For More Sophisticated Needs, Consider Active Data Governance

For some companies, including those operating in strictly regulated industries like pharmaceuticals, an active data governance initiative is necessary to control and validate data prior to entry into an SAP system.

Remember that the primary mission of data governance is to enhance bottom-line performance by eliminating business

¹ "MDM on a Single ERP Instance: Workflow and Data Quality," an article by Bill Swanton of AMR (www.amrresearch.com).

process interruptions related to incomplete, missing, or erroneous data, while fully complying with general business and industry-specific GRC regulations. The best way to accomplish this is to restrict any data that is not business-ready from ever reaching the SAP system. An active data governance model achieves this by implementing an automated system to manage the data collection and validation process – not just the remediation of existing data, as is the case with passive data governance.

The development team at BackOffice Associates provides a suite of collaborative applications – built specifically for SAP systems – that manages the data entry and change processes through a validated collaborative workflow environment. These applications, known as the *cApps suite*, act as firewalls for data. They use an automated and transparent process to ensure that only business-ready data reaches the SAP system.

The CranSoft cApps suite, which comprises cMat, cCust, and cVend, are active data governance applications designed specifically for materials, customer, and vendor data. Several Fortune 500 companies are already using these applications to govern their data management strategies.

These applications were created for the business user, so the technology skill level is based primarily on intuitive SQL statements. Once live, the solutions help our customers to mitigate risk and rid their SAP systems of low-quality data.

Conclusion

Implementing an automated data governance strategy – whether passive or active – is essential for sustaining a successful GRC strategy. The costs of implementing a holistic data governance solution greatly outweigh the risks involved with using manual data governance – or worse, not having a data governance strategy at all.

To learn more about BackOffice Associate's automated GRC data governance offerings, visit www.boaweb.com or contact us at info1@boaweb.com. ■

Data Governance Is Everyone's Responsibility

Many organizations are confused when it comes to who is responsible for the upkeep of data quality. When we ask project teams and leadership who owns the data's quality before, during, and after an SAP implementation, many are quick to say "the IT department." Our experience, however, shows that the answer should be "the business users." This is not to say that IT has no stake in ensuring data quality, merely that the business must also understand and be held accountable for the quality of their own data.

Companies that embrace this essential view of data quality responsibility and use it to drive their planning, organization, tool selection, and implementation processes will have the most successful data governance strategies.

Sustain Your GRC Strategy with Continuous Controls Monitoring

3 Key Considerations for Building a CCM Program

Increasing complexity and challenging new business risks pervade today's global environments. To address these risks and meet regulatory requirements, organizations must establish effective internal controls, along with processes to make sure these controls remain repeatable, sustainable, and cost-effective. Therefore, as part of their overall governance, risk, and compliance (GRC) strategies, organizations are building continuous controls monitoring (CCM) programs to improve efficiencies, avoid controls deficiencies, and focus resources on managing critical risks.

With an effective and sustainable CCM program that's designed, managed, and optimized to account for changes – such as regulatory shifts, mergers and acquisitions, and system upgrades – an organization can meet its compliance objectives, reduce risk exposures, and meet the expectations of key stakeholders. Over time, as their CCM processes mature, companies can transition from manual risk detection efforts to automated prevention measures.

Organizations considering CCM must first focus on their control objectives and establish sound processes. Ernst & Young has assisted many clients with their CCM programs, gleaned several key learning points from this experience.

1. Create a Foundation for Your CCM Program

A CCM program should include risk detection, prevention, remediation, and compliance components, all focusing on people, processes, and technology. Using CCM to evaluate and monitor key business processes against predetermined business rules enables an organization to identify patterns and anomalies to help minimize potential risk exposures.

When our clients embark on a CCM initiative, the automation or technical aspects often become their primary focus. Although automating the controls can be very beneficial to the organization, we recommend that clients focus initially on the following control objectives:

- *Application access controls and segregation of duties (SoD)* can reduce opportunities for fraud or for material

errors by ensuring that financial and operational transactions are properly authorized and approved. A CCM strategy should drive the development and enforcement of effective user and role governance processes, practical SoD rules, and sustainable access controls.

- *Business process controls* help users evaluate system configuration settings to identify events that occur outside of set control limits.
- *Master and transactional data controls* are used to analyze sensitive fields and transactional data against predefined control criteria. The analysis of this data supports the detection of potential controls violations, such as changes to vendor addresses or terms, duplicate payments, timing issues, and other anomalies. Additionally, the transactional data analysis can facilitate business efficiency improvements.

2. Manage the CCM Life Cycle

To create and sustain an effective CCM program, an organization must understand and manage the entire CCM life cycle (see **Figure 1** on the next page), which includes:

- *Process design* – This begins with a clear vision based on operational objectives (i.e., achieve compliance, reduce risk). It is impractical to monitor *all* of a company's controls, and therefore it's essential to first identify the controls most in need of monitoring, based on business objectives. We also recommend establishing a CCM governance body to lead the process design effort and to help ensure that business objectives are met.



Michael B. Brunenmeister
Executive Director
Global CCM Solutions Leader
Ernst & Young



Jason G. Glantz
Manager
ERP Advisory Services
Ernst & Young



Aman Joshi
Senior Associate
ERP Advisory Services
Ernst & Young

Failure to define a GRC strategy before automating CCM can result in significant losses of time and resources, or even the need to rebuild the CCM program.

Key Concept: Continuous Controls Monitoring

Continuous controls monitoring is a repeatable process in which specific control points can be continuously monitored against established thresholds to help determine business risk anomalies.

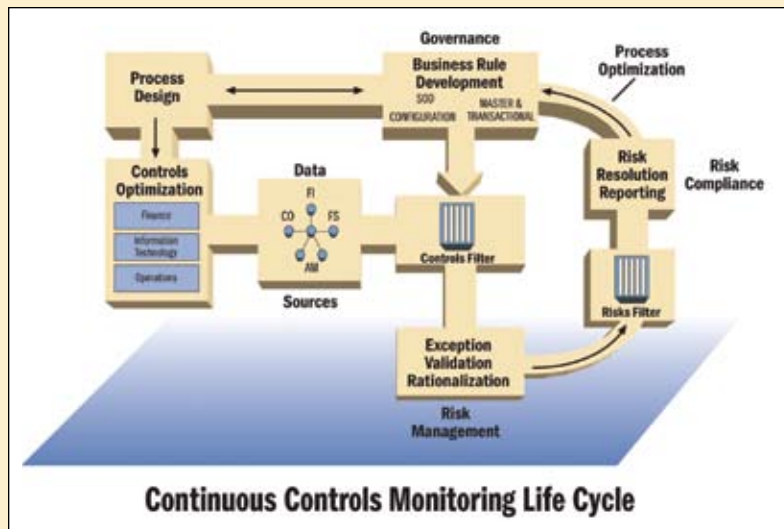


FIGURE 1 ▲ Building an effective CCM program means taking all aspects of the CCM life cycle into consideration

- **Business rule development** – A CCM program is only as effective as the business rules used to evaluate the control data. Business rules for SoD, master and transactional data, and automated application controls are used as filters and applied against data sources to identify potential control anomalies.
- **Controls optimization** – Once significant risks have been identified within business process areas, appropriate controls must be established to mitigate them. A vital step in achieving control optimization is establishing controls that cover multiple risk areas and eliminate redundant or ineffective controls.
- **Exception validation and rationalization** – Organizations often become overwhelmed by the volume of control exceptions. Since some exceptions are legitimate, organizations can manage risks and reduce the number of reported exceptions – and therefore the cost of compliance – by filtering out legitimate business exceptions.
- **Resolution reporting** – To successfully manage and mitigate business risk, and to ensure timely resolution of compliance violations, it is important to set up a process that allows your company to diligently review and resolve reported violations.
- **Process optimization** – The processes that make up your CCM program should be flexible and allow your company to dynamically react to change. They also should be continually adjusted to meet business needs and sustain your CCM investment.

Developing a process for handling exceptions with defined roles, responsibilities, and prioritized resolution procedures is critical to success.

3. Automate CCM with SAP Functionality

Organizations running SAP have a significant advantage when enabling and automating CCM because integrated business disciplines – such as financial accounting and asset management – can be built into a centralized CCM program. A CCM program that encompasses well-designed controls, appropriate business rules, and the diligent management of the CCM life cycle, allows organizations to focus on their enhancement and automation efforts, reducing time and resources that would otherwise be spent manually monitoring controls.

As companies move toward automation, they should make managing configurable controls through benchmarking a part of their testing strategy, since it is a mechanism that ensures configurable controls remain unchanged. SAP provides this capability through table logging, which can help reduce year-to-year control testing.

SAP also provides a number of tools embedded in its GRC solution suite, which can be used to automate the CCM process. These tools include SAP GRC Access Control, SAP GRC Process Control, and SAP GRC Global Trade Services. An organization can leverage these tools, combined with the functionality already embedded within SAP systems, to gain a clear advantage in creating an effective end-to-end solution for managing risk and compliance.

Conclusion: Make CCM a Priority

Having a GRC strategy and making an effective CCM program a priority can help organizations drive their compliance efforts, identify potential processing errors, and proactively detect fraud. It also is critical to design *practical processes* as you develop your GRC strategy and CCM program. Many companies hold the misconception that an automated controls solution will solve all compliance needs. However, an automated solution is only effective after a successful CCM program has been established based on well-designed controls, appropriate business rules, and ongoing management of the CCM program.

To learn more about how Ernst & Young can help your company build and sustain a CCM program, please email TSRS.ERP@ey.com or visit www.ey.com. ■



Ravi Shankar
Director of
Product Marketing
Siperian

Use Master Data Management to Master Your Compliance Initiatives

Companies in a wide range of industries are challenged to meet the often complex and always evolving requirements of regulatory governance, risk, and compliance (GRC).

But despite their attempts to establish internal controls to enforce this regulatory compliance, many companies have yet to be fully successful. Often, these businesses will try to enforce compliance by using existing back-office systems, only to find data and processes that are duplicated across the organization. Compliance-relevant data in one system is often incorrect or inconsistent in another system – and this can have serious consequences.

Consider a manufacturer with a marketing division that regularly mails flyers, brochures, and other marketing materials. This marketing team is required to manage opt-out compliance; failing to do so costs US\$11,000 for each violation. Even with such hefty fines, however, opt-out data often slips through the cracks.

Say a customer calls into customer service to opt out of all marketing campaigns. If a company has not ensured the consistency of its data, that customer's record may be updated in the customer service application but not in the marketing database. With customer records fragmented

and inconsistent across the organization, it is no surprise that companies may inadvertently violate privacy or other compliance regulations.

The bottom line? Companies are finding they cannot successfully enforce compliance without first addressing the underlying issue of master data. To unify data and ensure that all parts of an organization are working from the same source of information, companies need a solid master data management framework (see sidebar).

Find a Master Data Management Platform to Fit Your Compliance Goals

Companies can more easily and effectively manage regulatory compliance to reduce business risk with a master data management platform, such as **Siperian MDM Hub**. A master data management platform helps unify critical data about customers, products, and organizations across different systems, delivering reliable, complete views of this data to reduce operational costs, improve compliance, and drive operational effectiveness.

Siperian MDM Hub enables customers to create a reliable, centralized master data store. It includes integrated capabilities

Companies cannot successfully enforce compliance without first addressing the underlying issue of master data.

Use Master Data Management to Ensure Your Entire Organization Is Working from a Single Version of the Truth

Master data is a collection of common, core business data entities – including customers, products, organizations, as well as their attributes and values – that are considered critical to a company's business and are required for use in two or more systems or business processes. Master data management (MDM) is the controlled process by which master data is created and maintained as the system of record for the enterprise. This record can then be circulated for consumption by business processes, applications, or users. Ultimately, MDM should be deployed as part of a broader data governance program that involves a combination of technology, people, policy, and processes.

Typically, master data is widely distributed across different business functions and applications within the organization, leading to data duplication, inconsistencies, and incompleteness. By centralizing master data in one location and synchronizing a reliable, single version of truth with downstream applications that feed business processes, companies can uniformly enforce compliance across the organization. Additionally, by synchronizing the reliable version of truth with analytical systems, companies are able to more quickly provide reliable regulatory reporting.

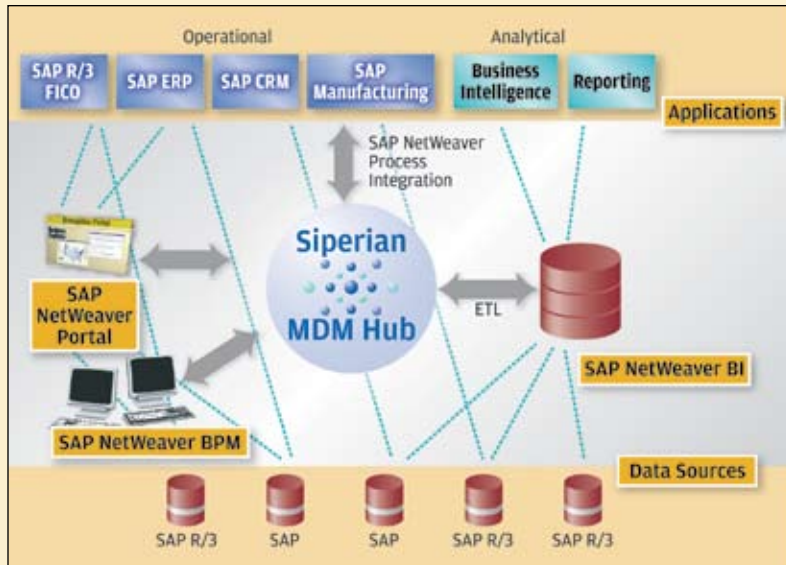


FIGURE 1 ▲ Siperian MDM Hub integrates with SAP systems to deliver an enterprise master data management solution that complements the capabilities of SAP NetWeaver MDM

to cleanse, match, and merge data to correct errors, identify duplicate records across systems, and create a single version of the truth to which all levels of the organization can adhere (see **Figure 1**).

Siperian MDM Hub also supports regulatory audit requirements for any given period by storing the complete history of all data changes, as well as a lineage of how data records have changed over a period of time. In addition, this master data management platform allows users to create reliable reports from analytical systems by synchronizing data from the centralized master data hub. It also enables customers to enforce strict, granular-level security regarding who is allowed to view and edit what data and when.

Using master data management as the foundation for successful data governance, Siperian has helped many

companies successfully address their compliance initiatives (see sidebar), as well as other business-critical areas including:

- Customer-centric marketing
- New product introduction
- Order-to-cash processes
- Contract management
- Physician spend management
- State license validation

And since Siperian MDM Hub is a complementary solution to SAP NetWeaver MDM and is certified for integration with SAP NetWeaver, SAP customers can integrate SAP master data sources, such as SAP CRM, into the Siperian MDM Hub.

Connect Your Compliance Strategy to a Master Data Governance Framework

Organizations often struggle to establish processes that will help govern their data assets and prevent the unauthorized creation, duplication, and deletion of key master data. Master data management platforms like Siperian MDM Hub can help customers establish overarching policies, define granular processes to enable these policies, enforce strict controls, and provide historical data needed for audit and regulatory reporting.

To learn more about data governance best practices, visit www.siperian.net/datagov and download a free white paper by Jill Dyché, co-founder of Baseline Consulting, entitled “A Data Governance Manifesto: Designing and Deploying Sustainable Data Governance.” ■

Global Pharmaceutical Company Successfully Manages Compliance Using Siperian MDM Hub

Several states have passed legislation requiring all pharmaceutical companies to establish firm caps on the amount of money they spend on each physician per year on direct promotion. One large pharmaceutical company found itself unable to proactively track and control spend on each physician by expense type based on state limits, causing different divisions within the company to continue paying physicians even after the spend limit had been reached.

This legislation violation was a direct result of inconsistent, incomplete, and inaccurate master data across

different data classes (such as physicians and hospitals) – inaccurate data that was then captured and stored in more than 40 different systems.

By using Siperian MDM Hub, this pharmaceutical company was able to create an authoritative view of master data across these different data classes to see the relationships among key business entities, such as physicians and hospitals. In addition, since the solution provided automatic notification and tracking of spend per physician, the company was finally able to fully comply with US and state physician spend requirements.

Do Your Testing Methods Work in Concert with Your Compliance Efforts?

Consider Automated Testing to Secure Your Audit Trail

A crucial advantage of SAP system architecture is that it allows organizations to easily modify application capabilities; they can quickly respond to competitive and market pressures with new functionality. Accordingly, it's important for IT teams to ensure that any custom upgrades or changes do not introduce risk to your organization.

IT typically addresses this with functional software testing. But traditional, manual testing strategies may be working at cross-purposes with your compliance efforts.

We encourage SAP customers to instead automate testing and to consider an innovative way to accelerate your delivery velocity, improve the productivity of your business experts, and assure the availability, accuracy, and compliance of your business processes after each and every change.

Manual Testing Can Compromise Compliance

The majority of software functional testing today is performed manually, primarily because of the deep subject matter expertise needed to understand all of a company's business process variations and rules. But there are several drawbacks to a manual approach:

- The most obvious is the sheer amount of time that manual testing takes. In a typical SAP business process, such as order-to-cash or procure-to-pay, testers must execute the same end-to-end activities hundreds of times in order to verify the varying types of orders, materials, delivery options, and pricing rules. Manually executing these variations not only takes valuable resources away from the business, but also delays the delivery of desired capabilities that may impact revenue or operating costs.
- Manual testing tends to be less formal and therefore subject to the skills and preferences of the tester. This makes coverage and quality unpredictable and not repeatable from one transport to the next.
- Manual testing is difficult to coordinate across end-to-end business processes that span various solution modules. Business process experts are usually organized around

functional areas, yet the risk of up and downstream impact from changes requires that processes be tested across departments and modules.

- Documentation – and in turn compliance – suffers because manual testing is so time-consuming that testers often do not have time to thoroughly or consistently document tests or results. Even if testers create documentation originally, they're usually strapped to keep it current with changes. This leads to a lack of management visibility and an inability to support compliance audits or regulatory requirements.

Because of these challenges, many companies have sought to automate their functional testing using tools commonly known as record/play.

Think Twice About Record/Play Tools

Record/play sounds easy and attractive: Simply perform a test manually and record the steps into a script that can be replayed multiple times. Unfortunately, this approach often produces poorly structured, undocumented, or unstable tests that are not reusable, maintainable, or auditable.

Recorded scripts are sensitive to the slightest changes. If an application is running more slowly at some times than others, the script can get out of synch and result in errors. Or if an unexpected condition arises, the script has no logic to recover and continue. Even changes in data can cause recorded scripts to fail.

Scripts also create a high maintenance overhead because they contain hard-coded data. This means that if you test a hundred different order variations, for example, your script must contain the same steps hundreds of times. If you make a change to the order process, the script will also have to be updated hundreds of times.

The lack of logic within these scripts also precludes making decisions or changing the workflow based on test results. For example, a particular material code may cause a window to appear that normally wouldn't with other material codes.



Linda Hayes
Founder
Worksoft, Inc.



Brian Anderson
Director of Product
Management
Worksoft, Inc.

Traditional, manual testing strategies may be working at cross-purposes with your compliance efforts.



Larry Concannon
Director of Product
Marketing
170 Systems, Inc.

The 7 Pillars of Strong Internal Controls

Discover the Compliance-Specific Benefits of Financial Process Automation

Finance departments are already working in a corporate environment that expects them to do more with less. Regulations like Sarbanes-Oxley and Basel II increase the pressure on these departments to strengthen internal compliance controls – without hampering everyday activities. The solution? Financial process automation, which helps strengthen these controls while improving visibility and efficiency.

Build Your Compliance Strategy on 7 Key Pillars

At 170 Systems, we encourage finance departments to leverage a strong financial process automation solution and structure internal controls according to seven key principles:

1. End-to-end visibility: In the typical accounts payable (AP) process, invoices sit in field offices waiting for coding and approval before being forwarded to the AP department for entry into an SAP system. This paper-based method lacks needed front-end visibility and creates a breeding ground for fraud. The best-practice approach is to receive and capture all invoices centrally by using financial process automation software integrated with SAP ERP to give management visibility into the entire review, approval, and payment process.

2. Strong approval framework: It is imperative for companies to maintain a robust, timely approval framework. Financial process automation software incorporates online approvals with full security controls, improving accuracy and ensuring the completion of key steps – such as signature verification – that are often neglected in manual, paper-based processes.

3. Segregation of duties (SoD): SoD activities are typically done at the role or responsibility levels. Well-designed financial process automation software, however, adds the ability to segregate controls by transaction and maintains an ongoing record of what action was performed by whom. This approach prevents a user from performing conflicting functions in the same transaction.

4. Policies and procedures enforcement: Even the most sophisticated compliance procedures are useless if they are

not followed. Financial process automation software enforces corporate policies by asserting incorruptible control over procedures; any attempt to bypass them triggers reminders and alerts.

5. Properly maintained transaction-level backup: The greatest risk for accounting fraud lies in the messy world of paper-based, transaction-level backup documentation. Best practice financial process automation software links source documents to the SAP financial record via capture technology, merging the paper trail into the digital world and making all backups easily accessible.

6. Internal and external audit support: It's important to do more than just verify that records are accurate; companies must also ensure that an auditor can easily access those records. Well-implemented financial process automation software gives auditors the complete transaction history of who accessed what document and when, as well as all backup documentation.

7. Error reduction: When finance uses manual, paper-based processes, even a minor error can trigger a cascade of time-consuming and expensive consequences. With financial process automation, however, automated controls and alerts can identify errors early on, before they become costly time-sinks.

Consider 170 MarkView for Your Financial Process Automation

The **170 MarkView Financial Suite** gives finance executives visibility and control over their core financial processes, such as accounts payable and expense management. With SAP-certified integration, 170 MarkView embeds best practices into the end-to-end automation of financial processes to help companies reduce costs, strengthen internal controls, and improve their visibility and service levels.

To learn more about how 170 Systems – an SAP software partner – can help you leverage your SAP investment, visit www.170systems.com/SAP. ■

The 170 MarkView Financial Suite gives finance executives visibility and control over their core financial processes.



David Lavoie
Executive Vice President
Marketing
Atrion International Inc.

Atrion Helps EH&S Teams Stay Compliant in the Face of New REACH Regulations

Europe has adopted an ambitious new framework – Registration, Evaluation, and Authorization of Chemicals (REACH) – to regulate the manufacture, import, marketing, and use of chemicals. REACH officially came into force on June 1, 2007, so environment, health, and safety (EH&S) departments are now gearing up to meet its requirements.

Keep Pace with REACH Requirements

Atrion International's products and content are fully integrated with SAP EH&S environments. Additionally, Atrion's consultants can help implement enhanced SAP EH&S functionalities, including the upcoming SAP International Uniform Chemical Information Database (IUCLID) 5 Interface and SAP REACH Portal – in line with progressive REACH legislation deadlines.

For example, in 2008 the pre-registration phase of REACH legislation requires companies to determine which chemicals they need to track. With the REACH substance volume tracking (SVT) capability within SAP EH&S, Atrion – and partner Linx/AS – can assist in SVT implementations.

Another REACH requirement will directly affect regulatory documents, such as the Safety Data Sheet (SDS). Atrion's REACH Solution for SAP EH&S Environments automatically updates SDSs – specifically for REACH specifications – within SAP EH&S environments. Atrion simplifies and ensures its up-to-date global content for SDS by monitoring regulatory changes and maintaining a validated database of rules through a network of regulatory, chemistry, and toxicology experts (see **Figure 1**).

Take Advantage of Atrion's REACH Expertise

Atrion's experienced consultants can help customers develop exposure scenarios and appropriate risk management measures; provide updated regulatory content to allow automated generation of Safety Data Sheets and Chemical Safety Reports; define collection and pre-registration requirements for documentation; and implement the SAP Document Management system and project management components of SAP EH&S and the REACH Portal. Atrion's offerings for SAP EH&S environments also have these key benefits:

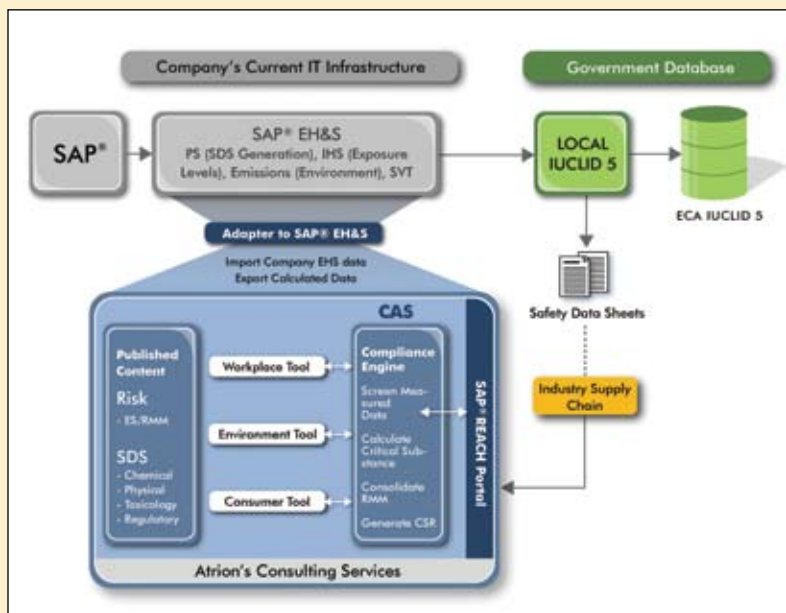
- Customers can produce compliance documents in more than 40 languages
- As soon as legislation changes, regulatory content is updated to keep clients compliant
- With Atrion's compliance engine, users can make audit reports based on rules used or regulatory classification

Conclusion

By leveraging their investments in SAP EH&S, enterprises can avoid increased operational costs associated with meeting REACH regulations. Atrion International offers products and services to ensure successful compliance measures.

For more information, call +1 888 8-ATRION (in North America) or +31 24 329 7420 (in the EU). Or visit us at www.atrionintl.com and www.linxas.com. ■

FIGURE 1 ▼ Atrion's REACH Solution for SAP EH&S environments



Governance, Risk, and Compliance – Moving Beyond Integration to Enterprise Strategy



David J. Evans
Managing Director
Technology Solutions
SAP Practice
BearingPoint

Governance. Risk. Compliance. There are substantial benefits to implementing an integrated solution to address these issues. Organizations can dramatically improve organizational transparency so that precise risks – and what can be done to mitigate them – are understood across multiple business units and functions. An integrated governance, risk, and compliance (GRC) strategy will also improve accountability and ownership for risk management throughout the enterprise. Further benefits can include reduced audit fees, lower cost of capital, and enhanced operational efficiency – all things that directly impact the bottom line.

Yet, there can be significant challenges to successfully establishing a GRC initiative:

- It can be very difficult to justify costs in the short term
- As GRC moves from being an organizationally siloed concern to an enterprise-wide one, it must be addressed in a much more holistic manner
- Companies must take a risk-based approach rather than indiscriminately documenting organizational activities

Technical and organizational complexities further complicate GRC efforts. These challenges can be specific to your company's industry requirements, reinforcing the need for solutions tailored to specific risk-management situations.

Understanding Your Exact GRC Needs

It's critical to comprehensively assess, plan, and design GRC requirements and processes – and then to identify which components of GRC technology you need to align those processes with overall corporate strategy (see sidebar). This upfront work shouldn't lead you to "analysis paralysis" but to a system implementation that's justified with a solid business case and benefits that meet your particular needs.

A Framework for Actionable Results

At BearingPoint, our approach to GRC (see **Figure 1**) goes beyond helping an organization formulate strategy and

establish processes. BearingPoint provides an end-to-end view of GRC that delivers an actionable, operational plan, moving from the initial requirements assessment and analysis through technology deployment.

BearingPoint has been named a leader in risk consulting services, according to *The Forrester Wave: Risk Consulting Services, Q2 June 2007 Report*. For more information, visit www.bearingpoint.com/sap. ■



J.R. Reagan
Managing Director and
Global Solution Leader
Risk, Compliance, and
Security
BearingPoint

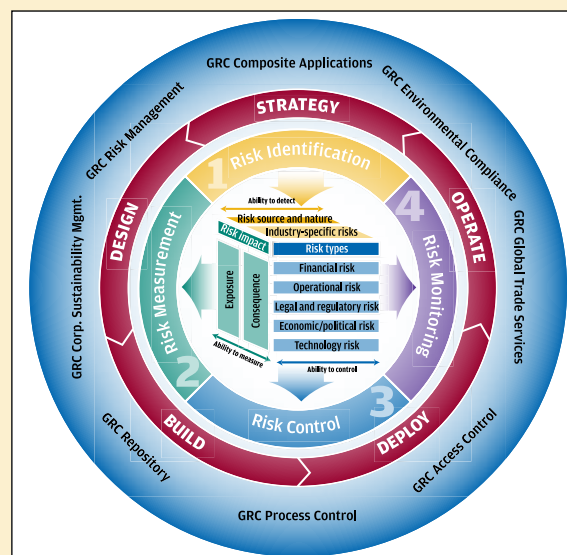


FIGURE 1 ◀
BearingPoint's
"big picture" GRC
framework for
security, risk, and
compliance

5 Questions to Reach GRC Readiness – and Success

To increase your chances of success, BearingPoint recommends that you ask yourself five questions before embarking on a GRC initiative:

- Why do we need a GRC framework?
- Why doesn't our current GRC strategy work for our organization?
- What should we improve within our current GRC strategy?
- What are the risks of *not* improving our GRC strategy?
- What benefits do we hope to gain as a result of a new GRC strategy?

Addressing these questions will help you implement a GRC strategy that results in *tangible benefits to your organization*.



Federico Pagiola
Partner
CSI Switzerland

Remaining Compliant

Use CSI KPIs to Identify and Analyze Weak Spots in Your Company's Governance



Werner van Haelst
Partner
CSI Netherlands

Following the introduction of legislation, such as the Sarbanes-Oxley Act, most companies have completed intensive projects to establish internal controls and ensure compliance. Now, companies face a new challenge: How do they maintain compliance and control levels, especially as their business processes fluctuate?

Many in the SAP user community are finding that remaining compliant requires an entirely new set of processes – and that these processes must seamlessly integrate into their SAP systems so as not to interrupt everyday business.

Unlike the bottom-up approach that many companies used to first implement compliance practices (using analysis tools for controls and security, such as CSI Accelerator, to pinpoint areas where remediation was needed), we recommend a top-down approach to remaining compliant. Give management a clear indication of control status and allow them to drill down and identify potential areas of concern through key performance indicators (KPIs).

Generate Intuitive, Automated KPIs

KPIs must be understood quickly and should be easy to set up and automate with the right tools. With some of our clients, for example, we set our *CSI Authorization Auditor* to

regularly collect and analyze information on access rights and segregation of duties (SoD) within a company's business processes. Using the *CSI Export to Excel* tool, we could then process the data into a radar chart that groups results by business domains for easy analysis (see **Figure 1**).

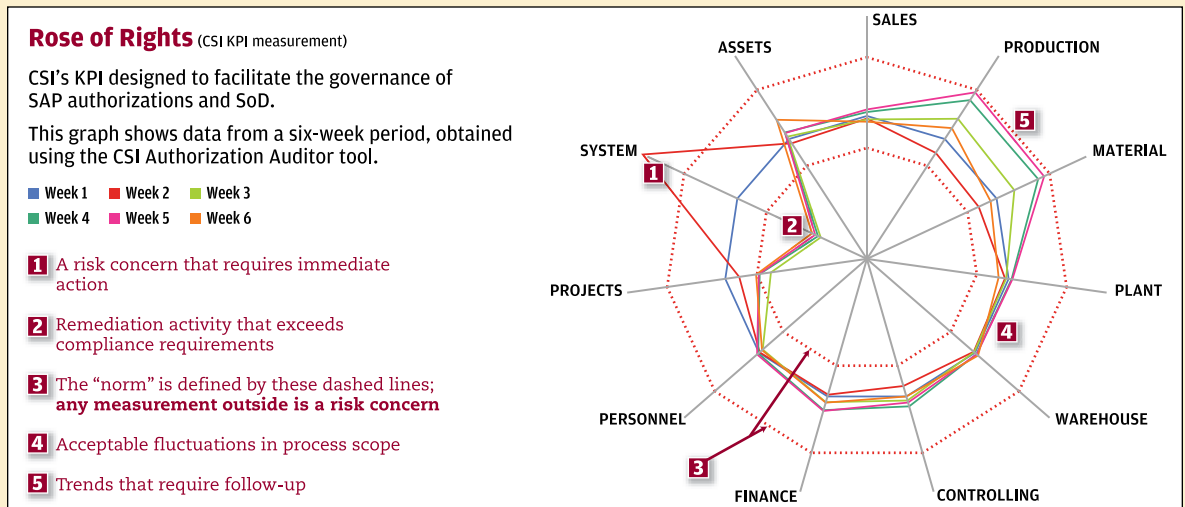
The resulting KPI, nicknamed the Rose of Rights, provides a powerful view of current control rights. It also indicates both good and bad compliance trends and triggers immediate alerts on control failures in the SAP system. With this KPI, decision makers can access analytics to focus on measuring risk. They can also see areas within the company that are successfully balancing compliance controls.

The Components of a Successful Compliance KPI

A successful compliance monitoring process is one that can quickly indicate potential problems, give early warnings of trends, and offer easy, intuitive analysis of compliance processes. With CSI's KPI-based approach to compliance management, business managers can view SAP authorizations in a simple, nontechnical way – this is key to a successful GRC strategy that extends far beyond implementation.

For more information on CSI's GRC consulting services and software solutions, please visit www.csi4grc.com. ■

FIGURE 1 ► CSI's Rose of Rights analytic KPI presents compliance of SAP authorizations and SoD; managers can quickly recognize any measurements beyond the outer dotted line as risk concerns that should be monitored closely, while areas of excessively strict controls are also visible in the center of the rose





David Drake
 Founder and
 Chief Executive Officer
 Revelation Software
 Concepts, Ltd.

Why Change Management Should Be a Top Compliance Priority

Ensure Compliance by Automating and Documenting Your Processes

The impact of the Sarbanes-Oxley Act continues to hit home as companies realize that its mandated audit capability is no simple order to fill – especially if they don't have strong change management processes in place. Even simple changes to an extensive business information system can have unanticipated consequences.

Say you're planning to enhance your visibility and reporting capabilities – which are key to maintaining compliance. These changes require auditable change management processes to ensure the revised reporting capability changes are approved and documented in accordance with a company's internal control processes. Change management is no longer just a technical issue – it is now business critical.

Automate to Ensure Compliance

You likely already have change management processes in place, perhaps based on widely accepted best practices from the Information Technology Infrastructure Library (ITIL).¹ The logical next step in using change management to ensure compliance is to automate these processes. Eliminating manual processes can help guarantee that deviations from the change control process won't go undetected – and that they don't happen in the first place!

Rev-Trac from Revelation Software Concepts is a solution that allows users to automate and enforce their change management processes, such as workflow, change control, transport migrations, electronic signature authorizations, and document referencing. This automation frees users to focus on managing changes rather than adhering to processes, ensures that they follow robust procedures, and assures change control teams that everyone who touches any aspect of change management within the organization is using a consistent and fully auditable process.

Additionally, Rev-Trac's process automation prevents accidental system disruptions by providing built-in extended object

and configuration locking – even across multiple landscapes – and incorporated overtake and overwrite prevention.

Leave a Fully Auditable Change Trail

Since compliance regulations require firm policies for processes, authorizations, and documentation, Rev-Trac is designed to enforce your policies so compliance is independent of everyday practices. With Rev-Trac, for example, you can always trace technical changes back to their specific change requests. Rev-Trac also prevents processes from progressing before all proper approvals are gained, necessary documents are completed, or test results are fully documented. Nothing falls through the cracks as it might have when using manual, paper-based processes.

Automating your change management processes also means that these processes will be enforced and that every change made in your system will be documented. This is key since, at its core, compliance is about proving the success of your internal controls and making them fully visible – to an auditor, for example. With Rev-Trac, you'll be able to approach compliance issues assured that all technical changes have been referenced. A full audit trail – including the process followed, approvals received, and approvers for each status – will also be generated for each change.

Rev-Trac makes all information available – complete with drill-down capabilities to key levels of detail – from the Rev-Trac console, where an auditor can easily identify changes requiring inspection and drill down into the audit trail to make certain compliance requirements were met.

Conclusion

Rev-Trac change control management ensures you can prove your compliance measures. There are no additional network security, disaster recovery plan, database administration, or desktop rollout requirements; if you're running SAP solutions, you've got all you need to run Rev-Trac. And since Rev-Trac lives in the SAP system, it comes with a low TCO. For more information, visit www.xrsc.com. ■

With Rev-Trac's automated signature verification processes, you'll no longer have to chase after signatures only to be told somebody just left for lunch...or for a conference in Hong Kong.

¹ For more information about ITIL best practices, see www.best-management-practice.com.



Mehrdad Talafar
Vice President
Partner Network
Sabrix, Inc.

The Coming Revolution in Tax Reporting and Compliance

Prepare for a Tax-Specific Workflow as Part of Your GRC Strategy



Mike Roberts
Director
Tax Management Consulting
Deloitte

Increased shareholder interest means that tax considerations are now high on the priority list when it comes to companies' governance, risk, and compliance (GRC) efforts – especially given the complexity of tax rules and the significant impact of tax on financial results. Imagine the level of risk involved when accurate tax liability has to be accounted for in every business transaction, on every invoice. What would happen if data quality and integrity is limited or poor?

- Lack of consistency and inadequate quality of data for tax reporting and compliance, often resulting in duplication of efforts and resources
- Difficulty obtaining data for tax reporting and compliance, resulting in labor-intensive tax reporting cycles
- The translation gap between client's own IT functions and tax departments in terms of identifying, mapping, and maintaining tax reporting and compliance requirements



Ainol Yaacob
Senior Manager
Tax Management Consulting
Deloitte

It's Critical to Know Where Your Tax Risk Lies

Tax departments are aware of ERP systems' limitations when it comes to determining and calculating various types of tax and providing reports to comply with numerous rules and regulations. Because of increased stakeholder interest, tax departments are required to understand limitations in systems and processes and must identify underlying tax risks within record to report (R2R) processes (see **Figure 1**).

There is also a greater push from fiscal authorities to undertake systems audits and electronic filing of tax returns. As a result, global businesses must now rethink their approach and investment in tax R2R processes.

These issues have the potential to create costly maintenance problems in traditional ERP systems. Organizations need to engage the appropriate tax experts and technologists to ensure that their ERP solution includes tax processes from beginning to end.

This is why the tax workstream within GRC is so important. The right transaction tax engine and implementation team can help tax functions mitigate and control tax risks within R2R processes. We've also found that fully integrated, bolt-on tax applications allow IT departments to focus on their core responsibilities while giving the tax department tools to effectively manage global transaction tax needs.

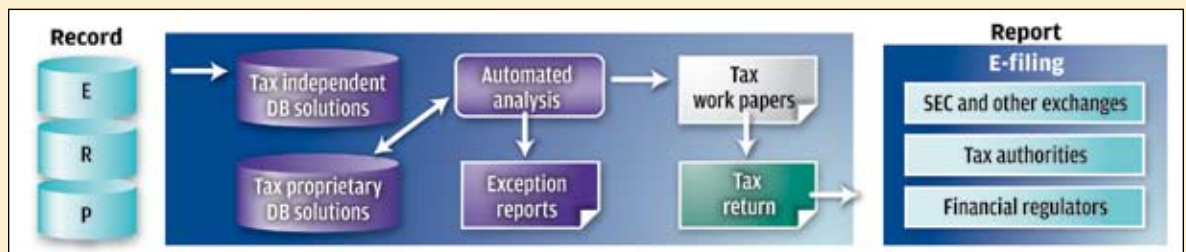
Big Changes in the World of Tax Management

Historically, tax professionals have built technology mostly in the report portion of the R2R cycle and in workflow management. However, the last year has heralded a revolution in this approach. Tax consultancies, which now commonly advise clients across the entire tax R2R process, have found several frequently encountered issues:

Additional benefits to having an automated and consolidated tax reporting and compliance solution include visibility to tax-specific information, a centralized repository of rules and policies, tax department control over tax policy enforcement, increased accuracy, consistency, and efficiency in tax data recording, and decreasing compliance efforts and costs.

For more detailed information, please visit www.sabrix.com and www.deloitte.com. ■

FIGURE 1 ▶ Tax risk can arise in any area within the R2R process



Incorporate Security Intelligence into Business Intelligence

Make Risk Management Part of Your Company's Overall Decision-Making Strategy

Successful companies use business intelligence (BI) systems like SAP NetWeaver BI and SAP SEM for their operational and strategic business management. So top managers are already accustomed to using BI to identify forecasting scenarios and key performance indicators (KPIs) to help them make the right strategic and operational decisions.

But on top of day-to-day BI, companies are seeing an increase in business risks that they must mitigate to remain competitive. Key business decisions must take into account KPIs that can control risks in an effective, compliant, and secure way. To do this, SECUDE Global Consulting (SGC) recommends building a *security intelligence framework*, based on SAP's solutions for governance, risk, and compliance (GRC), to infuse your BI strategy with knowledge from your previous experience in risk evaluation and mitigation.

Infuse Security Intelligence into BI Analytics

Security intelligence provides appropriate and comprehensive measures – both internal and external – for risk control and sustainability within a business environment. SGC's vision for a security intelligence framework is built on our model of enterprise risk management (ERM) – an internal methodology used to make security decisions.¹ But security intelligence takes ERM a step further to consider aspects like security incidents, noncompliance violations, and other security-related factors in major business decisions.

Think of security intelligence as a warehouse in which to record your experiences in building and implementing risk management procedures. You can then use your previous experiences to decide how to handle new risk mitigation challenges – and use those experiences to update your security information framework (see **Figure 1**).

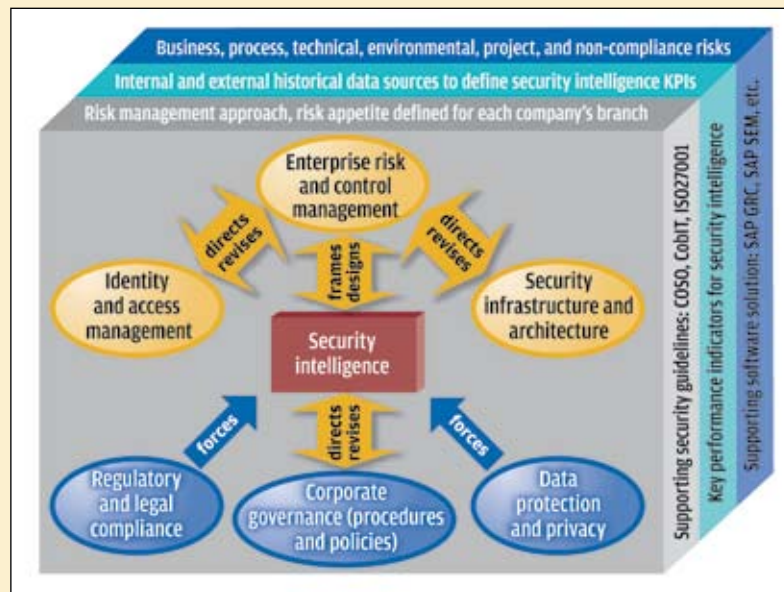
For example, consider a manager at a retail company who has to decide whether to introduce a new RFID-based logistics and payment system. Business KPIs such as cost reduction might make this transition look promising. But if

this manager has a security intelligence framework in place, he could notice that such an RFID system often results in fraud incidents and manipulation deficiencies. Because of these risks, the manager could decide to introduce RFID technology on a smaller scale, to get a better picture about the possible business risks before moving forward. And with the information gleaned from this trial RFID implementation, the company could further refine their security intelligence warehouse to help manage future risk situations.

Set up a Security Intelligence Warehouse to Help Make Risk Management Decisions

SECUDE Global Consulting can help you to set up an integrated security intelligence framework that fits your specific business needs. SGC's mission is to help enhance and sustain your business by identifying and limiting risks. For more information, visit us at www.secude-consulting.com. ■

FIGURE 1 ▼ The SECUDE Global Consulting security intelligence framework fosters a cyclical approach to security; the information in your security intelligence warehouse feeds into — and is fed by — risk management experience



Mario Linkies
Chief Executive Officer
SECUDE Global
Consulting AG



Dr. Frank Off
Chief Consulting Officer
SECUDE Global
Consulting AG



Eric Kang
Senior Vice President
SAP Security Technology
SECUDE Global
Consulting (US), LLC

¹ For more about building an ERM framework, see www.secude-consulting.com.



Paul Murray
SAP GRC Director
Turnkey Consulting

Tips for Building a Successful GRC Project Methodology

Complexity vs. Simplification in GRC Project Management

For companies implementing governance, risk, and compliance (GRC) projects, the first challenge is to build a successful project methodology to install GRC solutions – starting with SAP Compliance Calibrator by Virsa Systems¹ – that will allow them to identify, analyze, and mitigate risk.

We at Turnkey Consulting recommend that implementation teams focus on flexibility and simplicity when building these project plans.

Identify Your Project Resources

Generally, GRC implementation project plans allocate approximately 10% to 20% of their total implementation time to software deployment, 30% or more to risk identification and rules customization, around 20% to resulting risk mitigation, and the remaining 30% to 40% to security remediation. These plans also often go into great detail before go-ahead is even approved – based on the belief that a detailed project plan will minimize risk.

We recommend the opposite approach, having found that a light, adaptable project plan that focuses on a few critical deliverables is key. This approach allows you to flexibly refine project deliverables as you go – a hallmark of successful implementations, and something a heavily detailed project plan generally doesn't allow. This methodology also aligns well with extensive use of piloting, typically good for mitigating risks in GRC implementations.

Design Your Project Around 4 Key Standards

1. *Simplicity* – Where there is a higher-than-average degree of risk associated with a project, you should keep your project plan simple. Focus your core objectives on solving the simpler issues and gaining experience, and then move on to more complex areas. Frontloading effort into producing extensive documentation too often results in

wasted time and effort, while early testing and piloting provides early warning of potential issues.

2. *Flexibility* – Unexpected glitches will likely happen during any implementation – so build realistic buffers into your project milestones and flexibility into the project's links with other workstreams. Remember that you can best handle the unexpected by developing a framework that allows you to deal with such contingencies.
3. *Clarity in the project goals* – Project success should be defined by whether a number of critical goals are hit, a factor which often gets lost when dealing with ongoing issues. When core objectives are well defined and success factors are properly ranked prior to project start, there is a higher chance that these milestones will be met.
4. *Balance* – Project teams often concentrate on one specific area of expertise rather than on more holistic objectives. In practice, this often means that auditor-led projects tend to focus on risk recognition or documenting extensive controls mitigation, while security-led projects often focus primarily on creating complex SoD rules and remediation through security redesign. For successful compliance, you need a balance between the two approaches.

Overall, it is important not to overcomplicate the project and go for a big-bang approach – fine tuning it as you go will bring more immediate rewards and decrease a major risk for any GRC project: loss of momentum. ■

A light, adaptable GRC plan allows you to refine project deliverables as you go, a hallmark of successful implementations.

About Turnkey Consulting

Turnkey Consulting – a member of the SAP Global Security Alliance with offices in the UK, Australia, and the US – is a niche consultancy company focused on helping companies implement quality SAP solutions for security, portals, and GRC.

For more information about Turnkey Consulting's GRC services, contact paul.murray@turnkeyconsulting.co.uk or visit www.turnkeyconsulting.co.uk.

¹ For more information on SAP Compliance Calibrator by Virsa Systems, typically the first access control solution that companies implement, see www.sap.com/netherlands/solutions/business-suite/erp/financials/pdf/brochures/BWP_Compliance_Calibrator.pdf.

Article continued from page S-2

and expertise that has already been built up in the different lines of business. Set up and nurture a group of professionals who are responsible for delivering a consistent approach and methodology for risk management and yet who understand the intricacies of the business.

2. Automate your risk identification, monitoring, and notification activities, and establish a central risk repository for all of your risk-related data and best practices. Leverage existing investments in IT systems to automate operational processes. Reviewing the data and process flows in detail indicates potentially risky business transactions due to certain situations – like low inventory levels and lagging supplier delivery performance, customer credit risk, exchange rate fluctuations, and many more.
3. Put risk management tools and best practices at the disposal of all lines of business. This is best done by embedding risk management resources directly within the business applications they use day-in and day-out. Link risks to corporate performance management strategies and performance indicators, so that you can create new strategies with those risks in mind to quickly see whether you are meeting existing performance targets.

Not Risk vs. Reward, But Risk Generating Reward

Risk management is undergoing the same transformation that business planning went through several years ago. Today, everyone in an organization is expected to know the company's strategy and to align their activities to support it. Risk management is evolving in the same manner. More companies are incorporating risk management at the strategic level, rather than relying on the traditional approach of leaving it to a siloed department.

What enables this transformation is technology. Within every integrated business process, risk management is embedded into every step, regardless of whether you are in finance, human resources, the supply chain, or directly in the line of business. It is only when an organization can measure business opportunity against the financial, legal, and operational risks *at the desktop level* that risk management is no longer only a mitigator of business crisis, but instead a way to embrace business possibility. ■

Making Risk Strategic with SAP GRC Risk Management

To help companies mature their enterprise risk management processes, IT applications are critical. The right solution can help a company standardize its risk definitions and measurements, unify risk management across the enterprise, automate risk identification, and merge risk and performance management (see figure below).



▲ SAP GRC Risk Management enables risk management at all levels of the organization

With the SAP GRC Risk Management application, you can implement proactive, collaborative processes throughout the enterprise – enabling you to balance new business opportunities with financial, legal, and operational risks. SAP GRC Risk Management provides the functionality to:

- **Identify and monitor risk automatically** – Use role-based dashboards and alerts to prioritize corrective action. When risks exceed company thresholds, management receives alerts automatically.
- **Coordinate risk mitigation across lines of business** – Organize and share best-practice risk responses across the extended enterprise. Align risks with business policies and controls using the centrally managed GRC Repository to consolidate approaches and ensure consistency. Rely on risk self-assessments to capture, track, and address risk and loss events.
- **Acquire performance-based risk management strategies** – Address corporate risk strategically by balancing risk avoidance costs against new business opportunities. Analyze the overall risk portfolio, including cohesive, global profiles of operational and entity-level risks, in terms of severity and likelihood of impact based on early risk profile shifts.

See www.sap.com/solutions/grc/riskmanagement for more information.