Unlocking the power of SAP's governance, risk and compliance technology
## Contents

- Introduction ........................................ 1
- Governance, risk and compliance defined ............... 2
- Value of GRC technology ................................. 6
- SAP GRC technology solutions ....................... 8
  - SAP GRC Risk Management ........................ 9
  - SAP GRC Process Control ............................ 10
  - SAP GRC Access Control ............................. 11
- Conclusion ............................................ 12
Introduction

Risk management is no longer an ad hoc activity; it is an integral part of the day-to-day operations of organizations. External and internal risk management requirements are becoming increasingly complex and intrusive, while the demand for more comprehensive and actionable governance, risk and compliance (GRC) information continues to increase. The historic approach of managing risk in silos across different functions, processes, methods and infrastructure cannot keep up with these requirements; and, in many cases, risk management has become a growing operational and financial burden, limiting the organizations' ability to keep pace with essential business growth and transformational initiatives.

In order to manage these challenges, leading organizations are driving technology-enabled GRC transformation programs that can:

• Create improved visibility of enterprise risks and how these are mitigated
• Lower the cost of risk management through the reduction of manual processes and controls
• Increase efficiencies through standardization, simplification, automation and end-to-end process centralization

In this paper we will consider the scope of GRC; elaborate on what value GRC technology can bring to the table; and demonstrate how SAP GRC software supports risk management, process control and access control.

A robust GRC technology solution can help embed cost-effective risk management practices into daily business activities.
What is GRC?

GRC is the umbrella term covering an organization's integrated approach to governance, risk and compliance. While interpreted differently in various organizations, GRC typically encompasses activities such as governance, enterprise risk management (ERM), internal controls, regulatory compliance and internal audit. GRC activities are increasingly being integrated and embedded into organizational structures, processes, systems and data structures in order to avoid redundancies, as well as identifying and closing gaps. In other words, acting as “assurance as a whole” for the entire organization.

Governance improves the alignment of risk activities to the strategic objectives of the business. The following governance activities enable clearer accountability and reporting, increase visibility of the risks that matter most to the organization, and enhance decision-making processes:

**Strategy related:**
- Setting the business strategy and objectives
- Establishing the organization’s culture and values

**Risk related:**
- Defining the roles and responsibilities of risk governance bodies
- Determining risk appetite
- Setting standards and policies

Risk management embeds risk activities into business functions and processes and helps to ensure optimization across the enterprise. The following activities allow the performance of predictive analytics to correlate driver-based performance management and identify trends and anomalies for rapid response:

- Identifying and assessing risk that affect the organizations’ ability to achieve business objectives
- Determining risk response strategies
- Defining control activities

Compliance facilitates controls and processes to meet regulatory and business requirements. The following activities integrate automated controls measures and continuous monitoring into the transactional processing cycle, resulting in transparency of risk and controls and the elimination of transactions “at risk”:

- Testing adherence to control activities, policies, standards and commitments
- Addressing issue management, tracking and remediation
The model below sets out Ernst & Young’s leading practice Risk Agenda. Its four components focus on increasing risk performance management and integrated GRC, providing an end-to-end GRC approach for an enterprise-wide scope.

**Governance**
- **Enhance risk strategy**
  - Improved alignment to the objectives and strategy of the business
  - Improved visibility of risks that matter most to the organization
  - Proactive identification of risks
  - Enhanced decision making

**Compliance**
- **Improve controls and processes**
  - Better aligned risk coverage, including the identification of stronger, more pervasive controls
  - Reduced level of effort associated with performing and testing controls
  - Increased control and process efficiencies enabled through automation and continuous monitoring
  - Improved control mix that addresses key business risks while driving process efficiencies
  - Reduced cost of control

**Risk**
- **Embed risk management**
  - Comprehensive and continuous risk management and monitoring
  - Central management of financial, operational and compliance risks and controls across organization

**Optimize risk management functions**
- **Optimize risk management functions**
  - Elimination of duplicate and fragmented risk management activities
  - Increased integration and coordination among business, IT and compliance
  - Sustainability of risk management process
  - Effective top-down and bottom-up reporting

---

**Global Fortune 100 food and beverage company**

Implemented a common risk and controls framework and centralized its process controls library across the organization to gain better visibility over its redundant control activities. Rationalized and automated the testing process for over 90 SAP automated business process controls.
Governance, risk and compliance defined

Why is GRC important now?
The world is constantly evolving, creating external pressures on organizations to drive performance and manage risk. A single negative risk event can destroy a company’s reputation.

External and internal risk management requirements are becoming increasingly complex and intrusive, while the demand for more comprehensive, consolidated and actionable GRC information is also increasing. The historic approach of managing risk in silos across different functions, processes, methods and infrastructure cannot keep up with these evolving requirements. Risk management has become a growing operational and financial burden limiting its ability to keep pace with business growth and transformational initiatives.

Audit, risk and control functions have grown organically and in isolation, leading to challenges in alignment and communication at all levels of the enterprise and the disintegration of risk planning and performance management. Companies are now being forced to align in order to close gaps and eliminate overlaps, while focusing on the risks that matter and create value. Also, cost pressures in the current economic environment call for enhanced GRC management in the identification of hidden costs, inefficiencies in control and compliance structures, and in reducing duplicative activities at corporate and business unit levels.

Historic GRC focus

- Risk managed in silos
  - Inconsistent approach to capture and assess risks across the organization
  - Segregation of duties violations
  - Lack of confidence in accuracy and precision of risks identification

- Fragmented activities
  - Fragmented, manual and ad-hoc reporting
  - Inability to produce a consolidated heat map
  - Focus on compliance over risk performance management

- Decentralized processes
  - Lack of process and control standardization
  - Multiple and manual risk activities
  - Significant cost impact on business

Future GRC focus

- Enterprise-wide
  - Risk activities are consistently covered across all business units
  - Centralized risk and risk assessment management
  - Top-down and bottom-up risk integration
  - Ability to manage risks at multiple organizational levels

- Integrated activities
  - Consistent and real-time reporting
  - Centralized and consolidated heat map
  - Drill-down capabilities
  - Significant work-flow automation
  - Compliant role design and user provisioning activities

- End-to-end processes
  - Centralized and consolidated views of end-to-end processes
  - Automated risk activities and processes
  - Significant work-flow automation
  - Reasonable cost impact on business
Technology-enabled GRC transformation

Companies increasingly recognize the business value that GRC technology-enabled transformation offers. Business functions that previously focused on their goals in isolation are moving toward the integration of business, risk, finance and capital planning management. This enables risk management to focus on forward-looking developments and on building competitive advantage. A risk-aware culture should be promoted as a key value-added activity through all levels of organizations, allowing a shifting focus from downside to upside risk management.

The following diagram shows the development from historical focus on risk and compliance functions in isolation through to a successful GRC transformation. The leading practice in GRC transformation enables organizations to achieve an integrated end-to-end and enterprise-wide GRC state of maturity. It focuses on high-performance levels of risk management that no longer only protects but creates business value.
Value of GRC technology

Traditional GRC technology solutions were aimed at providing organizations with a single issue solution, but nowadays leading companies utilize GRC technologies for multiple purposes. Whereas companies in the past focused on meeting a specific requirement, such as Sarbanes-Oxley compliance, leading organizations these days have other GRC activities to be considered, such as audit management, regulatory compliance, IT governance, performance improvement and policy management. Therefore integration, central databases and reusability are more important than in the past.

Organizations use GRC technology to enable, integrate and optimize their risk management functions and processes, while focusing on supporting strategic objectives and creating value. GRC technology is emerging rapidly and is being adopted by leading organizations. It provides one risk management language, consistency, integration, cost efficiency, innovation and effective work flows. GRC technology offers solutions to fully integrate governance, risk management, compliance and process improvement.

GRC technologies successfully transform risk performance levels by:

- Automating and standardizing processes and controls
- Embedding and maintaining one single version of risk and control data
- Managing holistic views of risk and compliance exposures
- Generating dynamic and real-time risk and control intelligence and reporting
- Analyzing risk-driven indicators and exception-based decision making
- Escalating via work flow through different levels of the organization

Global Fortune 500 medical technology company

Rationalized 2,000 global process controls down to a total of 300, resulting in considerable savings from automation and benchmarking of controls. This company also implemented SAP GRC Access Control globally, which greatly improved audit results and resulted in considerable reduction in ongoing testing efforts both internally and externally.
Selection process
Due to the increased importance of risk in driving shareholder value, information technology vendors are now providing more comprehensive and flexible GRC solutions, enabling companies to expand their risk management programs and reach a greater level of risk process maturity, while delivering quick wins in the short-term.

In order to select the right GRC technology that meets risk management objectives in line with the business’ strategy, please be guided by this checklist:

Global Fortune 500 oil and gas company
Strengthened its controls environment by standardizing its access management process globally and implementing SAP GRC Access Control across its 20 SAP strategic systems. This standardization drove efficiencies (20%–30%) around access management processes and improved the risk posture by relying more on preventive segregation of duties and sensitive access checks than on reactive, manual procedures.
In the current market, many information technology vendors offer GRC technology solutions. In this paper we focus on the GRC technology solutions of SAP:

- **SAP GRC Risk Management** offers a holistic risk visibility, key risk indicators and enterprise risk intelligence through dashboards and surveys.
- **SAP GRC Process Control** provides a central controls repository, self-assessments, automated process and work flow management, as well as configurable controls testing and real-time exception based reporting.
- **SAP GRC Access Control** enables sensitive access management and segregation of duties, critical and emergency access management, and compliant access provisioning.
- **SAP GRC Global Trade Services** demonstrate export/import compliance, customs e-filing and sanctioned party list screening in a global trade environment.

In the remaining part of this paper, we will focus on the first three components: SAP GRC Risk Management, SAP GRC Process Control and SAP GRC Access Control.
SAP GRC Risk Management

SAP GRC Risk Management provides an integrated approach to understand and manage all of the risks that an organization faces. Its main purpose is to improve the quality of decision making. Additionally, it provides management with the visibility to recognize the interdependency of risks, thereby decreasing the likelihood that the organization would be surprised by events that could have been predictable. The benefits are:

- **Plan** the integration of the management of risks and controls across the enterprise (strategic planning and business processes); this will unify the way the organization approaches strategic, financial, operational and compliance risks.
- **Identify**, in a proactive manner, risk and quantify exposure across the enterprise to improve transparency; automatically identifying and prioritizing risks through proactive alerts and escalations will provide additional security over regulatory compliance and prevent loss of reputation and resources.
- **Analyze** risks better and faster due to the improved decision-making process and the increased effectiveness and efficiency of the risk model.
- **Respond** quickly with risk implementation and mitigation activities to prevent risks from having negative impact.
- **Monitor** the impact of risk against performance in an accessible and visible way; this will provide an effective reporting workflow.

SAP GRC RM provides the following functionality:

- Common risk definition (risk profile, risk appetite, risk tolerances, strategy, objectives, etc.)
- Risk repository and classification
- Automated risk assessment process
- Centralized and consolidated risk heat map
- Risk correlation and simulation
- Automated and work-flow driven risk management end-to end process

SAP GRC Risk Management (SAP GRC RM) enables four major components of risk management model: risk governance, risk management, risk integration, and business process performance.
## SAP GRC technology solutions

**SAP GRC Process Control**

SAP GRC Process Control enables an organization to automate its internal control model (automatic and manual controls and testing/approval workflows) and compliance monitoring, thereby reducing the efforts taken by the organization and increasing the security in the operations for the directive committee.

- **Control repository centralization**: creates a repository that centralizes all the documentation processes and management of the internal control model. This allows an early detection of configuration and master data changes.
- **Integration**: increases integration and coordination among business, IT and compliance, allowing the embedding of internal controls into the business processes (functional areas take a more relevant role).
- **Automation**: ensures the compliance of the internal control model (continuous control monitoring (CCM)) and real-time control exception reporting, which increases the confidence in the effectiveness of controls by eliminating the “human error” factor and improves the efficiency of the internal control model. By reducing the cost of compliance (less time, less people) and increasing the effectiveness, the number of manual controls required in processes will be minimized.
- **Periodic and continuous monitoring**: manages real-time notification of potential control failures based on established business rules; identifies production change anomalies that may indicate fraud through alerts; improves test effectiveness through configured controls with 100% coverage; and increases operational efficiency through standardization and policy management. Processes associated with the preparation and analysis of configured controls show higher efficiencies. Costs associated with audit failure are avoided.
- **Cross-system visibility**: enables a unified repository of compliance information for efficient multi-initiative management and enhanced visibility to process-related risk exposure and controls testing throughout the enterprise.

SAP GRC Process Control enables organizations to execute coordinated, transparent and automated compliance and risk management activities.

<table>
<thead>
<tr>
<th>Key activities</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sign-off and report</strong></td>
<td>- Interactive, multi-format control, testing, exception and remediation status across processes, policies, geographies and accounts</td>
</tr>
<tr>
<td>Analytics and reports</td>
<td>- Policy and certification management</td>
</tr>
<tr>
<td>Certify, signoff and provide evidence</td>
<td>- Near real-time notifications of control exceptions and associated impact</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>- Workflow-enabled activity and response rules</td>
</tr>
<tr>
<td>Monitor exceptions</td>
<td>- User defined multi-step control effectiveness test plans</td>
</tr>
<tr>
<td>Remediate issues</td>
<td>- ERP integration through 120+ delivered scripts or customizable SAP queries/reports for continuous control monitoring</td>
</tr>
<tr>
<td><strong>Evaluate</strong></td>
<td>- Centralized entity, process and control maps</td>
</tr>
<tr>
<td>Test automated controls</td>
<td>- Risk assessment utilities and customizable testing strategies definitions</td>
</tr>
<tr>
<td>Test manual controls</td>
<td>- Compliance support for multiple mandates and for strategic, financial, operational and IT risks</td>
</tr>
<tr>
<td>Perform assessments</td>
<td></td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td></td>
</tr>
<tr>
<td>Materiality analysis</td>
<td></td>
</tr>
<tr>
<td>Risk assessments</td>
<td></td>
</tr>
<tr>
<td>Test strategies</td>
<td></td>
</tr>
<tr>
<td><strong>Set-up and manage</strong></td>
<td></td>
</tr>
<tr>
<td>Control environment</td>
<td></td>
</tr>
<tr>
<td>Regulations, policies and audits</td>
<td>- Centralized SAP queries/reports for continuous control monitoring</td>
</tr>
<tr>
<td>Enterprise integration</td>
<td>- Compliance support for multiple mandates and for strategic, financial, operational and IT risks</td>
</tr>
</tbody>
</table>
SAP GRC Access Control

This suite of solutions is made up of various tools that allow the automation of the access control model of the organization, through a dual system that initially allows the organization to detect and clean the segregation of duties (SoD) violations (“get clean”), and then keep it clean in the future (“stay clean”) by an automated process.

SAP Access Control enables the four major components of access management: risk analysis and remediation, enterprise role management, super-user privilege management and compliant user provisioning.

SAP GRC Access Control provides the following functionality:

- **Role centralization**: centralized and consolidated role design and definition that is business centered and compliance enabled; including a sensitive segregation-of-duties rule library.

- **Access monitoring and control**: automated emergency access management with integrated monitoring and reporting. Access anomalies indicating possible fraudulent activities are identified through alerts and access request scenarios; they can then be stimulated across business processes and applications.

- **Automation**: automated work flows that facilitate the access management end-to-end process, such as self-service user access request and related approval processes.

- **Compliance**: compliant continuous control of access (including authorization), helping to enable the segregation of duties (SoD) management across the enterprise.

- **Protection**: proactively helping to protect information and preventing fraud through automated access risk analysis and remediation.

SAP GRC Access Control (SAP GRC AC) enables four major components of access management: risk analysis and remediation, enterprise role management, superuser privilege management and compliant user provisioning.

- **Prevent**: Design roles and prevent violations, Provision regular access, Provision emergency access.

- **Detect**: Design roles and prevent violations, Provision emergency access, Identify and remediate violations.

- **Business role management**

- **Access request**

- **Emergency access management**

- **Access risk management**

SAP GRC Access Control (SAP GRC AC) provides:

- Business-centered and compliance-enabled role design and definition
- Emergency access management with integrated monitoring and reporting
- Self-service user access request and approval process
- Centralized and consolidated sensitive and segregation of duties rule library
- Rapid identification of access violations and ability to simulate access request scenarios
- Automated and workflow driven access management end-to-end process
Conclusion

GRC technology creates value, reduces costs and improves your risk performance. It enables your organization to automate, standardize, streamline processes, create holistic views of risk and compliance, and analyze real-time business intelligence, and it allows your decision making to really make a difference. The following model helps to assess your organization’s GRC technology maturity level.

GRC Risk Management

- Aligns and integrates the management of risks and controls across the enterprise (strategic planning and business processes)
- Unifies the management of strategic, financial, operational and compliance risks
- Increases the effectiveness and efficiency of risk model
- Increases visibility into the impact of risk against performance
- Provides an additional security over regulatory compliance and prevents reputation and resource loss
- Proactively identifies risk and quantify exposure across the enterprise to improve transparency
- Improves the decision making process and provides an effective reporting workflow

GRC Process Control

- Implements a real balanced scorecard over SAP enhancing automated controls and monitoring techniques
- Allows business areas to detect, prevent, monitor and approve unusual operations and transactions
- Real-time notification of predefined rule-based exceptions in order to obtain an effective response
- Control automation significantly reduces audit execution, documentation and tracking exception times
- Reduces the effort time to manage the internal control model in the whole organization
- Establishes a “cost-effective” combination of resources designated to perform internal control testing
- Changes the traditional and reactive internal control model to a proactive and dynamic model that is exception based
- Optimizes financial and operational processes to gain a higher internal control level (increase control confidence and effectiveness)

GRC Access Control

- Real-time diagnostic of segregation of duties risks over applications
- Real-time monitoring of critical t-codes and user activity
- Provides a centralized control repository and a monitoring risks dashboard
- Prevention of the risk of segregation of duties conflicts propagation
- Automatic and controlled approval of the accesses by the different data owners
- User management optimization in all the systems (granting/revoking/modifying user privileges)
- Compliance with the “best practices” in terms of roles and profiles management, ensuring their definition, documentation, creation, testing and maintenance in a consistent way throughout all the administration process
- Automatic management of the emergency access in a controlled and auditable environment

GRC solutions can help companies turn risk into results and improve financial performance by embedding consistent and sustainable risk management practices while improving management’s ability to make decisions. The value of GRC integration is outlined in the recent Ernst & Young article for the special report on GRC in SAPinsider, published December 2012: http://www.ey.com/Publication/vwLUAssets/10-2012_GRC/$FILE/10-2012_GRC_Ernst&Young.pdf
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page

Risk management

Turning risk into results: enabling risk management with SAP GRC
Ernst & Young’s GRC Risk Management (RM) solution paper focuses on enabling risk management. It highlights what we see in the market, opportunities, benefits and related next steps.

The future of internal audit is now: increasing relevance by turning risk into results
We explore actions internal audit can take to realize strategic alignment, increase business relevance and achieve a risk maturity that accelerates financial performance.

Process control

Turning risk into results: enabling compliance and process management with SAP GRC
Ernst & Young’s SAP GRC Process Control (PC) solution paper focuses on enabling compliance and process optimization. It covers the Rapid SAP process and control diagnostic which provides accelerated current state assessment of SAP processes, controls and technology.

Smart Control: transforming controls to reduce cost, enable growth and keep the business safe
Balancing value, cost and risk in processes and controls helps create a competitive advantage. Becoming streamlined helps you anticipate and respond to changes.

Access control

Turning risk into results: enabling access management with SAP GRC
Ernst & Young’s SAP GRC Access Control (AC) solution paper focuses on managing access risks. It looks at how you can lower cost and effectively sustain access management through centralization, standardization, automation and integration with other GRC modules.

A risk-based approach to segregation of duties
Read clear guidance on a sound risk-based methodology that integrates IT and financial controls, resulting in an approach that is both manageable and cost effective.
How Ernst & Young makes a difference

At Ernst & Young, our services focus on our clients’ specific business needs and issues because we recognize that these are unique to that business.

Effective risk management is critical to helping modern organizations achieve their goals and it offers the opportunity to accelerate performance while protecting against the uncertainties, barriers and pitfalls inherent in any business. Integrating sound risk management principles and practices throughout operational, financial and even cultural aspects of the organization can provide a competitive advantage in the market and drive cost-effective risk processes internally.

Our 15,000 Risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective support—wherever you are in the world. We work with you to develop an integrated, holistic approach to managing risk and can provide resources to address specific risk issues. We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It’s how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contact details of our leaders

Global

Paul van Kessel  +31 88 40 71271  paul.van.kessel@nl.ey.com
Randall J. Miller  +1 312 879 3536  randall.miller@ey.com

Americas

Michael L. Herrinton  +1 703 747 0935  michael.herrinton@ey.com
Bernard R. Wedge  +1 404 817 5120  bernard.wedge@ey.com

EMEIA

Jonathan Blackmore  +44 20 795 11616  jblackmore@uk.ey.com
Manuel Giralt Herrero  +34 91 572 7479  manuel.giraltherrero@es.ey.com

Asia-Pacific

Jenny S. Chan  +86 21 2228 2602  jenny.s.chan@cn.ey.com
Rob Perry  +61 3 9288 8639  rob.perry@au.ey.com

Japan

Yoshihiro Azuma  +81 3 3503 1100  azuma-yshhr@shinnihon.or.jp
Haruyoshi Yokokawa  +81 3 3503 2846  yokokawa-hrysh@shinnihon.or.jp

© 2013 EYGM Limited. All Rights Reserved.

FYI no. AU1488

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.