


# 6 Key Tools for GRC Excellence





**Companies likely face enormous pressure** in an increasingly complex environment dominated by market globalization, shorter development cycles and constantly changing legal, political, cultural and technical requirements. In addition, local regulations, laws and business practices in other countries and cultures also impact how companies operate. This is forcing organizations to reconsider how their data is stored, accessed, secured and managed.

**The top business pressures driving investments in corporate governance are:**

- Increased regulatory standards
- Need for better risk and compliance transparency and traceability
- Elevated risk, potentially impacting profitability
- Lack of organizational accountability
- Higher customer expectations



**Corporate Governance, Risk and Compliance (GRC)** management can help companies manage these pressures. GRC offers driving mechanisms to control the way enterprises operate. Taking an integrated GRC approach enables companies to manage risks and compliance requirements related to environmental practices, processes, business partners and internal policies as well as financial, operational and IT controls.

GRC management is defined as the automation of the management, measurement, remediation and reporting of controls and risks against objectives, in accordance with rules, regulations, standards, policies and business decisions. Many enterprises typically consider a GRC application to satisfy a specific requirement, such as SOX compliance, an industry-specific regulation or risk management for a business process. However, enterprises often have other GRC activities in mind, such as audit management, additional regulations, IT governance, remediation management and policy management, which they may eventually integrate into a more consolidated GRC approach.

**Instead of acquiring separate solutions for finance, IT and other business units, many enterprises are choosing to use a single GRC platform integrating many points and functional solutions to satisfy specific GRC needs.**

The fundamental key functions to an integrated and automated GRC platform are:



## Risk management

All business activity involves risk resulting from uncertainty. But only those who are prepared to actively respond to risk can develop strategies for their companies that result in success. So, risks need to be managed.

Risk management involves systematic risk identification and assessment combined with the evaluation and management of potential events in response to the current situation. The risk management process describes the interaction between organizational units and their roles, therefore ensuring that risk management is properly coordinated. Risk management is typically established as a continuous control cycle. The control loop is embedded throughout key company departments and corporate processes, including value-adding business processes and support processes, such as IT.

A complete platform should support risk management professionals with the documentation, workflow, assessment and analysis, reporting, visualization and remediation of risks. This component focuses on general operational risk management, however, it may collect data from other sources and tools to provide a consolidated view of ERM (Enterprise Risk Management).

# Compliance and policy management

The objective of compliance management is adherence to external requirements, such as laws, and internal regulations, such as corporate policies and procedures. This includes both statutory regulations and other standards that organizations choose to apply for competitive or ethical reasons as defined by corporate strategy. Compliance management is made up of coordinated activities to stay within internally and externally mandated boundaries.

Faced with complex, dynamic, and distributed business operations, organizations are choosing a structured approach to corporate compliance to manage their business environments. This involves implementing a combined compliance organizational structure where enterprise compliance is aligned centrally with corporate governance and risk reporting but is distributed to business lines to assign ownership and accountability for risk and compliance.

A complete platform should support compliance professionals with the documentation, workflow, reporting and visualization of control objectives, controls and associated risks, surveys and self-assessments, attestation, testing, and remediation. At a minimum, compliance management will include financial reporting compliance (Sarbanes-Oxley [SOX] compliance), and also support other types of compliance, such as ISO 9000, industry-specific regulations, SLAs, and compliance with internal policies. This function includes document management capabilities that enable the policy lifecycle, from creation to review, change and archiving of policies, while also enabling distribution to and attestation by employees and business partners.





## Change management

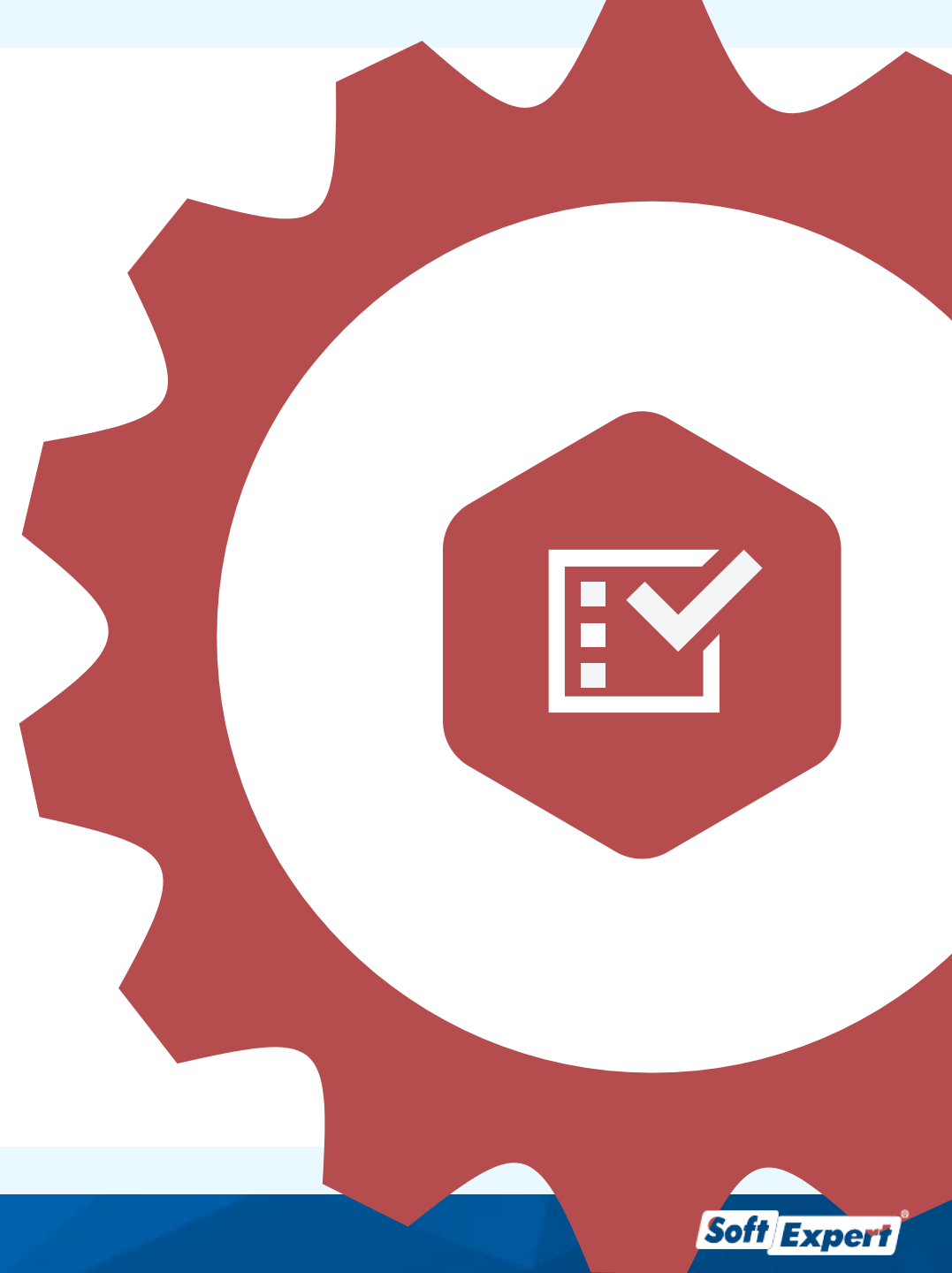
Managing change is hard. Change impacts risk and compliance requirements, policies and related procedures. It demands systems and assignments of responsibility to flag triggers for change, archive older versions of things undergoing change, and notify relevant parties of the changes that have occurred.

A complete platform should support the ability to respond to changes in processes. The goal should be a change management strategy that monitors change, alerts the organization to risk conditions, and enables accountability and collaboration around changes impacting the company. This requires a common process to deliver real-time accountability and transparency across regulatory areas with a common records system to monitor regulatory change, measure impact, and implement appropriate risk, policy, training, and control updates.

## Audit management

In an integrated GRC platform, effective risk management and compliance with regulations and policies pave the way for successful audit management. With the climbing in numbers and types of audits and the increasing complexity of business at companies, there is greater demand for an integrated GRC approach based on business processes.

Audit management within the context of GRC helps internal auditors to manage the complete audit lifecycle - from audit planning and scheduling to the development of standard audit plans and checklists, field data collection, the development of audit reports and recommendations, the review of audit recommendations and implementation of these recommendations. It is an essential function to secure consistent information throughout the enterprise along with content information relevant to GRC, such as policies, control test evidence and incident reports as well as previous audit findings.







## Strategy and performance management

Governance sets the tone at the top and establishes the culture of the organization, including attitudes toward risk management and compliance. The intention of GRC is to instill good governance, and the approach to its implementation requires strategy management and performance monitoring. A GRC platform has the benefit of:

- Setting business goals for the enterprise and validating enterprise strategy. It ensures vision enhancement with an appropriate amount of risk and provides focus for strategic initiatives.
- Setting the strategy to support business goals and planning for strategy implementation. It provides clarity and direction as to how business goals will be met, with coordination across the enterprise.
- Aligning spending with business goals. It ensures that spending for the implementation of enterprise initiatives is consistent with their priority level.
- Monitoring of business performance. It supports decision-making according to the most accurate information available.

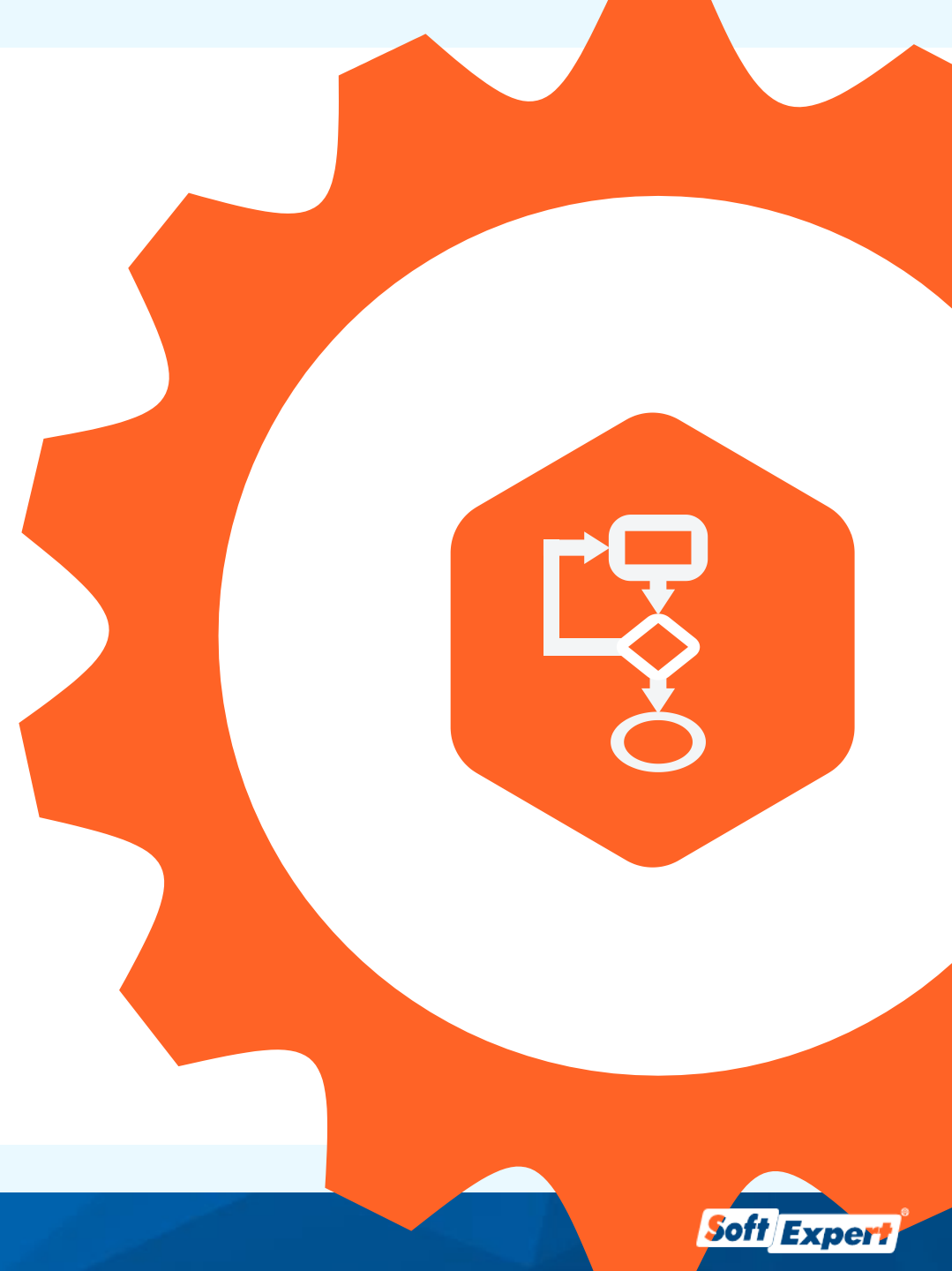
The mandate for risk and compliance is defined within these parameters.

## Business process management

GRC should be built on a consistent set of data and should have connectors for all relevant regulations, requirements, and risks. Processes are the perfect connectors. They allow for visualization of the relationship between assets, enabling impact analysis (which process is affected if a certain regulation changes) and mapping GRC from operations to monitoring.

Business Process Management is well known as an approach to improving an organization's processes by aligning all relevant aspects of an organization, promoting effectiveness and efficiency. Therefore, BPM has a large role to play in GRC, particularly within supply chain/vendor risk management, and in tracking compliance and incident management.

Using business process management to broaden the enterprise's risk management scope beyond traditional governance, risk and compliance practices helps detect unknown, critical risk exposures lurking in hidden or unstructured processes.



Now that you already know the **6 key tools for GRC excellence**, find out more about the most complete and innovative solution on the market for process automation and improvement, regulatory compliance and excellence in management.

## SoftExpert GRC

Effective and Sustainable Management.

SoftExpert GRC is a robust web-based software for supporting all governance, risk and compliance management processes in the organization. It enables organizations to effectively integrate business strategy execution with compliance and risk management practices. As a result, managers can accomplish organizational goals while managing risk and ensuring that operations stay compliant with corporate policies, laws and regulations, such as SOX, COSO, COBIT, and ISO 31000.



## Risk management

Soft Expert

Home Portals My tasks Components Shortcuts

File Document (DC003)

Search filters

Quick search

Saved searches

Type

SA-Sales Agreements

Including sub-levels

Advanced filters

Save SEARCH

Document

Category	ID #	Title	Revision	Date	Hits	Attribute
SA	SA000001	XYZ Company - Sales Agreement	00		1	17/01/2014
SA	SA000002	Sales agreement template	00		0	
SA	SA-100108	AGG Industrial International - Household Goods	01	11/02/2014	5	11/02/2014
SA	SA-100106	W2 All Trader Co. - Tool Box & Cutting Tools	00	23/10/2014	2	23/10/2014

Total records: 10

Display Preview

Scaling 100%

AGREEMENT TO PURCHASE REAL ESTATE

The undersigned (herein "Purchaser") hereby offers to purchase from the owner (herein "Seller") the real estate located at \_\_\_\_\_ in the city of \_\_\_\_\_, County of \_\_\_\_\_, State of \_\_\_\_\_, the legal description of which is: \_\_\_\_\_

upon the following terms and conditions:

Page 1 of 2

Soft Expert

Home Portals My tasks Components Shortcuts

Portals Risk Management 1 followers Private

Following

Purchase Process Financial Process Operational

Heat map

Vision Result

Probability

	Low	Medium	High	Very High
Low	10	13		
Medium	7			4
High		5	3	2
Very High	3		1	

Legend

Order	Sig	Risk	At
1		#00005 - Unauthorized or incorrect changes are made to the vendor master file	High
2		#00006 - Invoices are posted to accounts payable without proper authorization	High
3		#00007 - Unauthorized access is granted to individuals increasing the risk...	Moderate

Total records: 10

Risk and control plan

Plan	S	Actual
Purchase Process - Purchase Process		
P01 - Purchase Requisition		
#00001 - Unauthorized disbursements are made and recorded		Moderate
#00001 - The Supplier Maintenance Form must be signed by the buyer supervisor.		
#00003 - Application XYZ does not allow duplicate supplier names to reside in the system		
#00004 - Vendor maintenance is performed by the AP department and limited to supervisors.		
#00002 - Cash disbursements are not recorded accurately		Moderate
#00005 - All checks are processed through an integrated check-writing function in Application XYZ		
#00003 - Unauthorized access is granted to individuals increasing the risk...		Low
#00006 - All checks are processed through an integrated check-writing function in Application XYZ		



## Compliance and policy management



## Change management

**Soft Expert** Home Portals My tasks Components Shortcuts

File Process (PM022)

Search filters: change

Saved searches

Type: Select type

Advanced filters

Save SEARCH

F	B	S	T	Process type	ID #	Name
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	01	CR	Request for Change
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	07	PCR	Product changes request
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	04	04005	Change Management Process

Total records: 4

Display: Flowchart

Change Management Process

Change Requestor: Start, Request Change, Evaluate

Change Manager: Evaluate Change, Change Assignment

Change Advisory Board: Approves, Email to Requestor

Change Implementer: Implement Change, End

Audit criterion requirements > QA-RE000001 - SOX Compliance

SOX - SOX compliance Execution

Record Edit Browse View Tools

Save Add Associate Delete Previous Next Requirement basis Import Export Expand Collapse

Requirement: SOX - SOX compliance

Requirement	Weight	CL	AO	R
1.0 - Introduction	1			
1.1 - Are all board members familiar with the overall purpose and structure of the Sarbanes Oxley Act?	1			
1.2 - Are all Board members familiar with the purpose of a corporate governance framework?	1			
1.3 - Are all Board members familiar with the legal and regulatory framework governing the organization?	1			
1.4 - Are all Board members familiar with the need to achieve compliance with corporate governance policies?	1			
2.0 - Corporate Governance Policies	1			
2.1 - Are all Board members aware of the need to create, approve and disclose the organizations corporate governance	1			
2.2 - Are all Board members suitably financially literate and have good understanding of the organizations key risk and	1			
2.3 - Do all Directors meet the stringent 'independence' criteria specified by the regulatory authorities?	1			
3.0 - Internal Audit	1			
3.1 - Are the internal audit and external audit activities carefully coordinated to avoid omission or duplication?	1			
3.2 - Are Board members aware that internal audit has become mandatory for many public companies?	1			
3.3 - Does the internal audit function have full independence from all other operational units within the organization?	1			
3.4 - Does the internal audit function provide regular and ongoing comprehensive information to the audit committee?	1			
4.0 - Financial and other disclosures	1			
4.1 - Are Board members aware of the penalties under Sarbanes Oxley for not meeting disclosure requirements?	1			
4.2 - Are modern communication methods including websites used to disseminate information to the public?	1			
4.3 - Is the Audit Committee aware of its extensive reporting responsibilities?	1			
4.4 - Does the annual report contain a formal statement reporting on the adequacy or otherwise of the organizations int	1			
5.0 - Corporate Governance Committee	1			
5.1 - Is the board aware of the need for a separate committee to handle corporate governance issues?	1			
5.2 - Are the Corporate Governance committee members fully aware of their duties and responsibilities?	1			
5.3 - Does the Corporate Governance committee have access to external specialist resources?	1			
6.0 - Audit Committee	1			
6.1 - Do all Audit Committee members meet the required 'independence' criteria?	1			1
6.2 - Are all Audit Committee members financially literate and is one member suitably qualified to meet the criteria for a Y	1			

6.1 - Do all Audit Committee members meet the required 'independence' criteria?

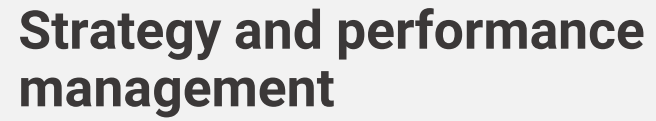
Requirement	Evaluation	Occurrence
Audit evidence		
Board member Mr. John Smith has official relationship with financial company as shareholder.		
Audit findings		
Conformity level		
Nonconformity - Nonconformity		
Comment		

Confirm Confirm & next



## Audit management





## Business process management



## SoftExpert Excellence Suite



SoftExpert Excellence Suite is the most comprehensive framework of independent yet united solutions to achieve business performance excellence, streamline corporate governance, risk and compliance programs, and ensure continuous business process improvement.

Companies may not need all applications at once, or may want to deploy one application module at a time, growing gradually as the need arises. Whatever the strategy chosen, only a fully shared environment allows its applications to fit together like puzzle pieces and work seamlessly.

## About SoftExpert

SoftExpert is a market leader in software and services for enterprise-wide business process improvement and compliance management, providing the most comprehensive application suite to empower organizations to increase business performance at all levels and to maximize industry-mandated compliance and corporate governance programs.

Founded in 1995 and currently with more than 2,000 customers and 300,000 users worldwide, SoftExpert solutions are used by leading corporations in all kinds of industries, including manufacturing, automotive, life sciences, food and beverage, mining and metals, oil and gas, high-tech and IT, energy and utilities, government and public sector, financial services, transportation and logistics, healthcare, and many others.

SoftExpert, along with its extensive network of international partners, provides hosting, implementation, post-sales support and validation services for all solutions to ensure that customers get the maximum value from their investments.



*Software for Performance Excellence*

Take your business to the next level

[www.softexpert.com](http://www.softexpert.com) | [sales@softexpert.com](mailto:sales@softexpert.com)

Disclaimer: The content of this publication may not, in whole or in part, be copied or reproduced without prior authorization from SoftExpert Software. This publication is provided by SoftExpert and/or its network of affiliates strictly for informational purposes, without any guarantee of any kind. The only guarantees related to SoftExpert products and services are those contained within a contract. Some product functionalities and characteristics presented herein may be optional or may depend on the makeup of the offer(s) acquired. The content of this material is subject to change without prior notice.