

# SAP GRC

Governance Risk and Compliance



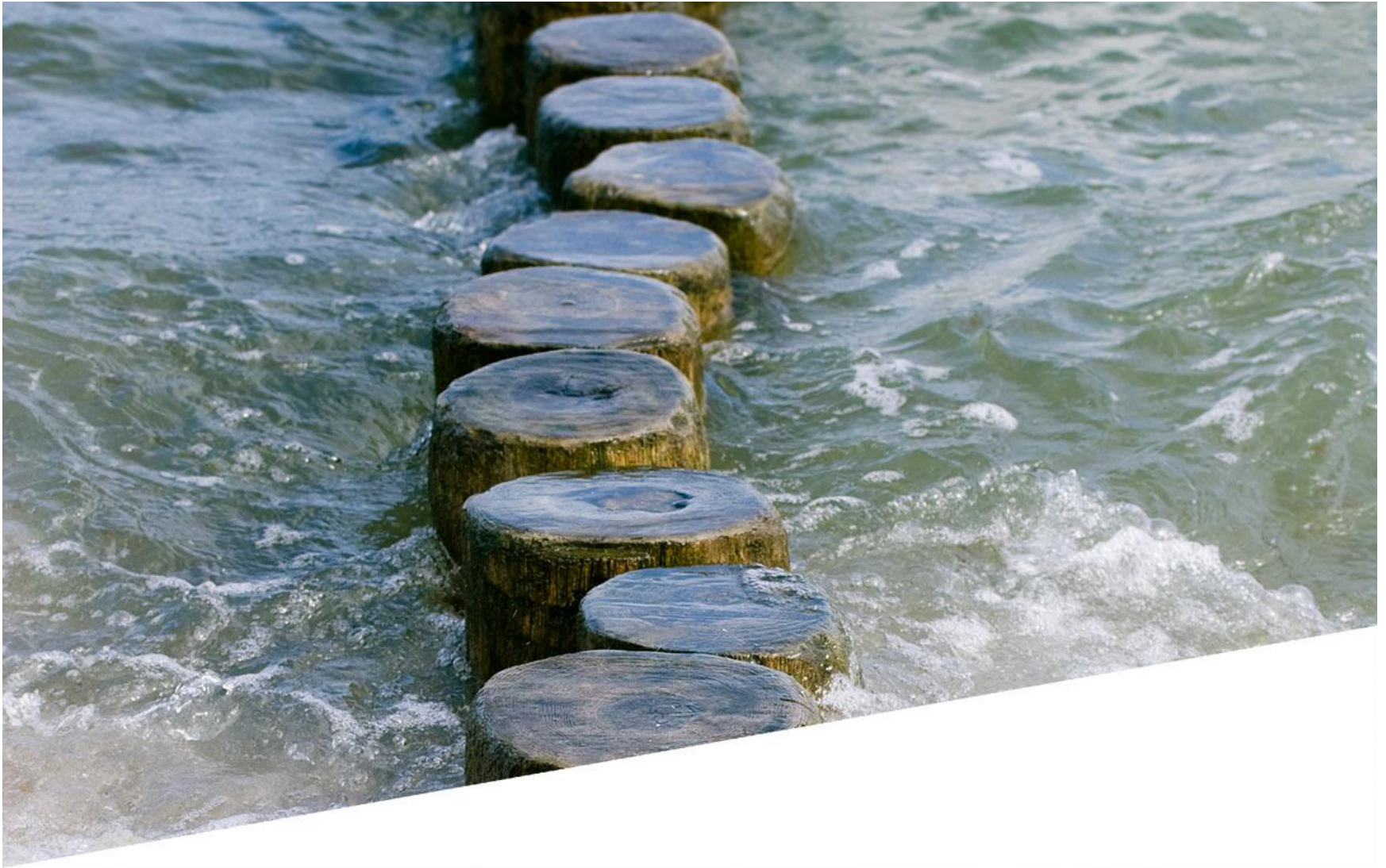
Building a better  
working world

# Agenda

---

- ▶ EY's Global Governance, Risk and Compliance Survey 2015
- ▶ Governance, Risk and Compliance Challenges
- ▶ SAP GRC Solutions
- ▶ An example

# EY's Global Governance Risk and Compliance Survey 2015



# Looking at Risk Differently

We believe that regardless of how they are organized, it is beneficial to consider risks in the context of your business and how best to respond to those risks

---

In this year's survey, we asked 1,196 participants, around the globe and across sectors, how well they are managing risk and what they need to do to **better manage** the risks that **drive performance**.

In this year's survey, we found that organizations are making progress in improving the way they manage risk in response to a changing risk landscape.

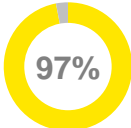
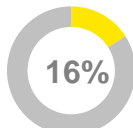
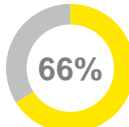
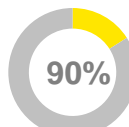
However, organizations also indicated that there is still further room for improvement and opportunities to be seized. However, this requires businesses to **change the way they work** and **how they capitalize** on it

- ▶ Organizations have primarily focused on risks that can be managed through the implementation of controls.
- ▶ However, **leading organizations** are now focusing more of their **time** and **efforts** on managing the risks that impact value creation.
- ▶ Our global GRC survey tells that organizations are looking for a more **comprehensive, coordinated** and **innovative** approach. But this requires **“building a risk-aware organization.”**

# What Our Clients Telling Us

In 2015 GRC survey; risk strategy, coordination, internal audit, technology topics were focused to gain better understanding of how well organizations are managing risk

While organizations demonstrated they are making progress, they indicated that **further opportunities** exist to improve the way that they identify, manage and respond to risk.

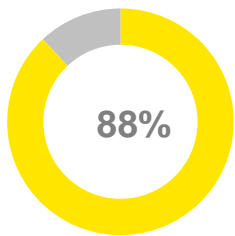
Survey Findings		Implications	Survey Findings		Implications
<b>Top five risks</b>	<b>Bottom five risks</b>	<ul style="list-style-type: none"><li>• While organizations have expanded their view of risk, they continue to primarily focus on preventable risks.</li><li>• Organizations that also focus on strategic and external risks are able to profit from the upside of risk.</li></ul>	<b>21%</b> of respondents indicated risk activities are well-coordinated today; whereas <b>67%</b> indicated they expect risk activities to be well-coordinated within three years.	<ul style="list-style-type: none"><li>• Organizations expect to see a significant improvement in the level of coordination of risk activities.</li></ul>	
<b>Links to the business</b>		<ul style="list-style-type: none"><li>• Organizations have made a significant amount of progress in bridging the gap between risk management objectives and business objectives.</li><li>• However, greater opportunity exists for organizations to achieve stronger alignment.</li></ul>	<b>Top internal audit skills or experience</b>	<ul style="list-style-type: none"><li>• Businesses clearly recognize that their Internal Audit functions require the appropriate skills and experience.</li><li>• Organizations must appropriately develop and align talent with the requisite skill sets.</li></ul>	
 <p><b>97%</b></p> <p>97% made progress in linking their risk management objectives and business objectives</p>	 <p><b>16%</b></p> <p>but only 16% of the 97% consider them to be closely linked today</p>		<div><div>Critical/analytical thinking</div><div>Analytics</div><div>Risk management</div><div>Audit</div><div>Business strategy</div></div>		
<b>Risk involvement</b>		<ul style="list-style-type: none"><li>• Organizations recognize the value of directly involving risk management in business decision-making.</li><li>• Organizations that directly involve risk management are better able to identify, manage and respond to the risks that impact their business.</li></ul>	<b>GRC technology</b>	<ul style="list-style-type: none"><li>• Many organizations adopt and leverage technology to better enable and sustain risk management activities.</li><li>• Organizations must view technology as a way to more efficiently and effectively execute, as well as sustain, their responses to risk.</li></ul>	
 <p><b>66%</b></p> <p>66% of organizations indicated that risk management has limited involvement</p>	 <p><b>90%</b></p> <p>but 90% expect to be directly involved or providing inputs within the next three years.</p>		<div><div>46%</div><div>49%</div><div>5%</div></div> <p>46% of respondents do not yet utilize a GRC technology, 49% utilize one or more technologies and 5% did not know.</p>		

# Robust Risk Aware Organisation

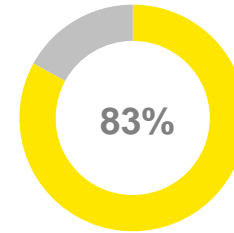
## Risk is a key part of strategic business planning

---

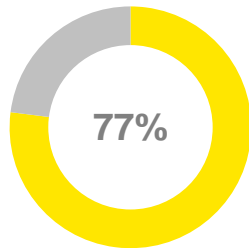
Risk is a key part of strategic business planning and top of mind of many boards today; however, the board's ability to provide oversight could be enhanced by more frequent evaluations of the organization's risk profile.



of respondents indicate that the board or a board committee provides oversight of the organization's risk management activities.



of respondents identify, assess and develop plans to address risks to all key initiatives (43%) or identify and discuss the risks (40%).



of respondents evaluate their organization's risk profile on an annual basis, limiting their ability to adjust their business strategy based on changes to their risk landscape.

# Building a Risk Aware Organisation

---

To build a risk aware organisation, a stepped approach to risk management is required:

## Advance Strategic Thinking

- Identify and assess risks that impact business strategy
- Design risk response to reduce the downside and take of upside potential

## Optimise Functions and Processes

- Optimally align functions to execute the organization's risk response plans/strategy
- Develop risk processes to facilitate better coordination, communication and reporting

## Embedded Solutions

- Design solutions that prevent, balance or limit risk
- Implement technologies to effectively execute and sustain the solutions

# The Governance Risk and Compliance Challenges



# The burning platform

Unprecedented focus on GRC post issues and the increasingly complex regulatory environment has put tremendous cost pressures on organizations.

- ▶ **Can't keep up** – The pace at which technology and innovation is driving change in the business and regulatory landscape is unprecedented. Chief compliance and operating officers cannot keep up with changing expectations and spiraling costs of compliance
- ▶ **Work smarter, not harder** – There is unprecedented focus to work smarter and coordinate GRC efforts versus the traditional 'pile-on' approach to add more controls for every new requirement

**#1**  
area of focus for  
Board of directors  
of Fortune 100  
companies

**\$200 billion**  
Cost of compliance  
in Fortune 500  
companies

**60%** of companies  
expect cost of  
compliance to  
significantly increase  
over the next 5 years

**How is it good business to let  
your cost of compliance outrun  
the business benefit?**  
- Fortune 100 CFO

**67%** of companies  
have **overlapping** risk  
coverage in two or  
more risk functions

**"Managing the cost  
of compliance has  
grown larger than  
I've anticipated"**

**Less than 15%**  
of Fortune  
200 companies have  
moderate to significant  
coordination in risk  
management activities

*Based on EY Global Surveys, Thompson Reuter Cost of Compliance survey 2014, and EY insights through industry roundtables and networking forums*

# SAP GRC Solutions



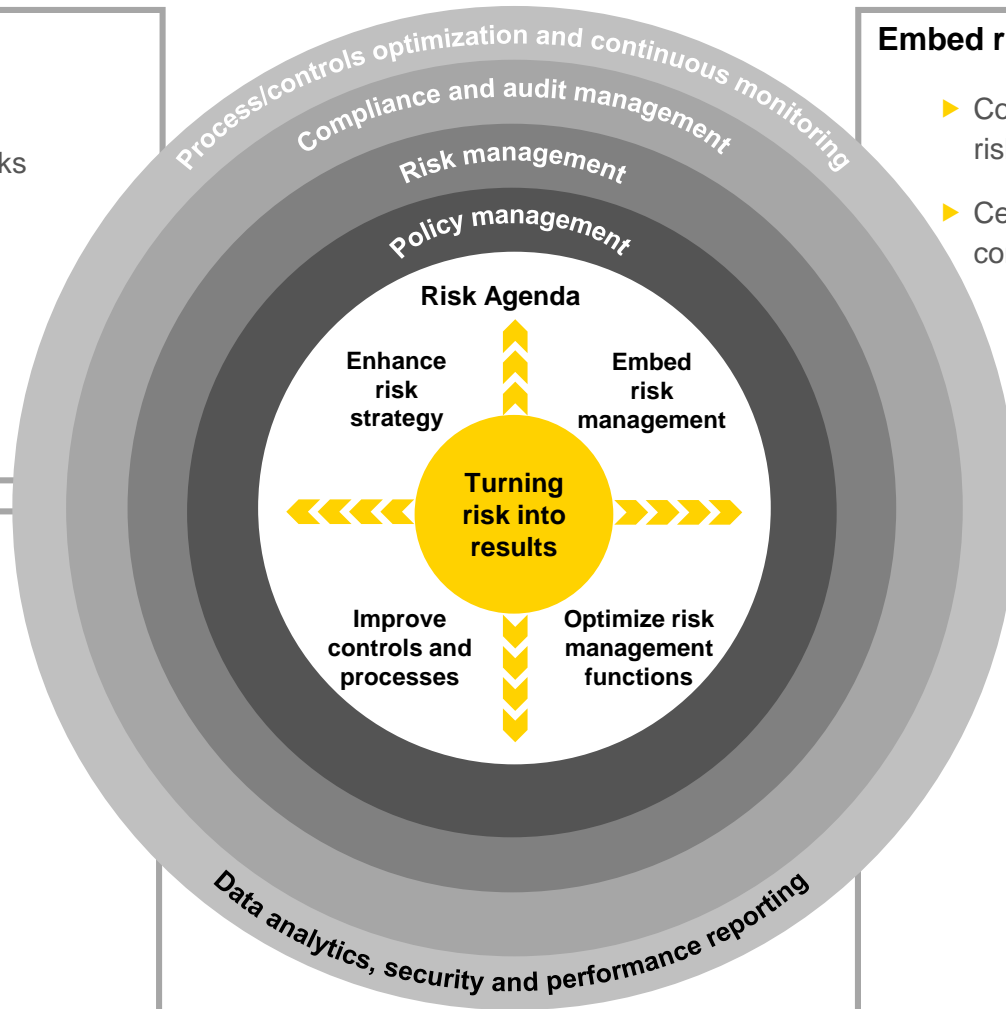
# SAP Governance, Risk and Compliance (GRC) Overview

## Enhance risk strategy

- ▶ Improved visibility
- ▶ Proactive identification of risks
- ▶ Enhanced decision making

## Improve controls and processes

- ▶ Better aligned risk coverage, including the identification of stronger, more pervasive controls
- ▶ Improved control mix that addresses key business risks while driving process efficiencies



## Embed risk management

- ▶ Comprehensive and continuous risk management and monitoring
- ▶ Central management of risks and controls across organization

## Optimize risk Management functions

- ▶ Consolidated risk management activities
- ▶ Increased integration among business, IT and compliance
- ▶ Effective top-down and bottom-up reporting

# Critical Considerations for Implementation

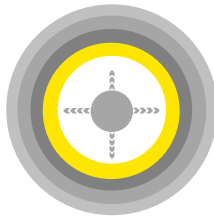
GRC integrates process, people and technology

## Defining the roadmap



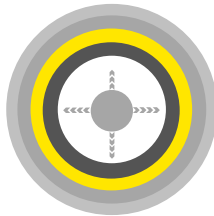
- Definition of GRC road map and consideration of prior work / requirements before implementing the tool (role design, controls improvement, improvement of risk management function)

## Business involvement



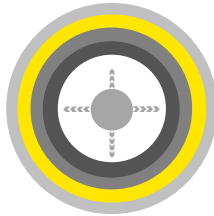
- GRC Projects are not technology projects but rather business projects

## Content



- Providing the right content to the tool is key for success

## Governance



- Governance model is critical for the sustainability of the solution

# GRC roadmap

Integrates process, people and technology

## Deliver GRC solutions for specific events or situations

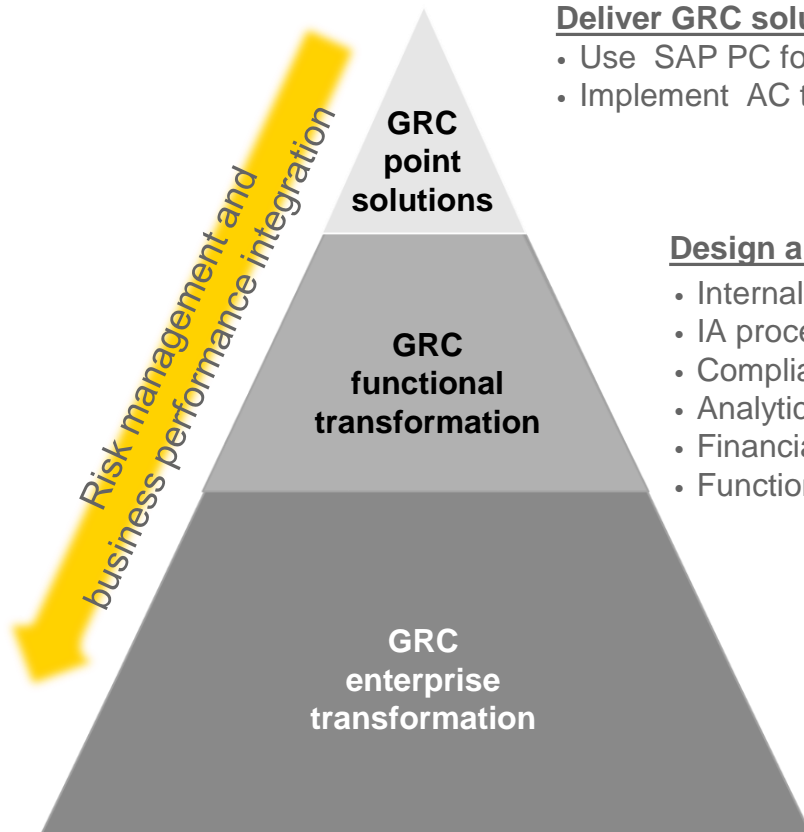
- Use SAP PC for Business/IT process and controls monitoring and testing
- Implement AC to manage segregation of duties

## Design and deliver specific GRC function/process

- Internal controls optimisation and monitoring
- IA process/technology transformation
- Compliance function enhancement
- Analytics enablement and fraud monitoring
- Financial close reconciliation automation
- Functional risk systems conversion

## Develop an enterprise-wide GRC program supporting strategic vision and objectives

- Risk management integration initiatives
- Risk and controls transformation initiatives
- Driver-based performance management integration
- Business intelligence integration
- Continuous monitoring

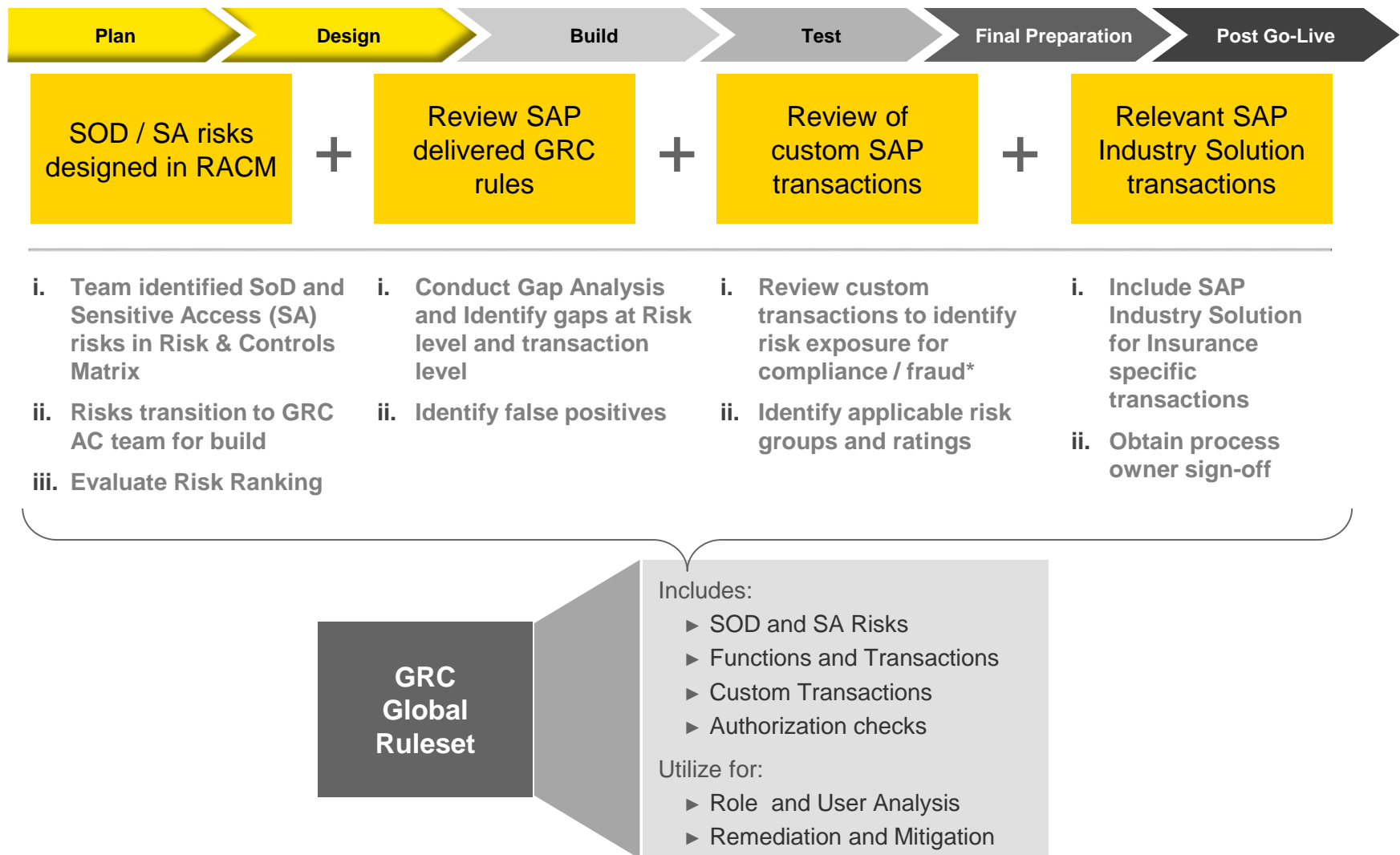
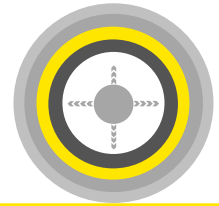


## Holistic enterprise-wide technology enablement



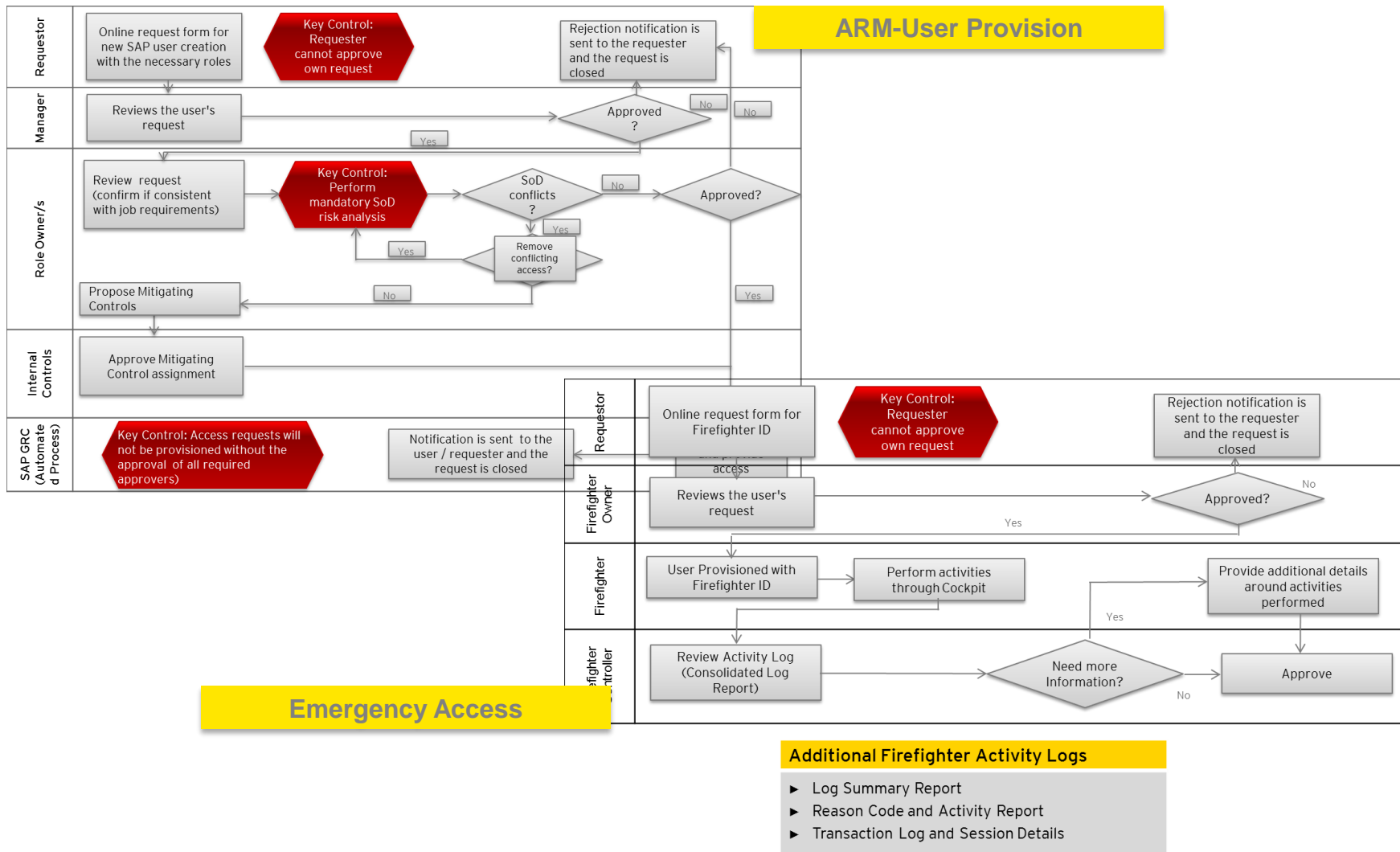
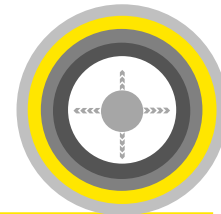
# Content

## SAP GRC Access Control – Rule Set



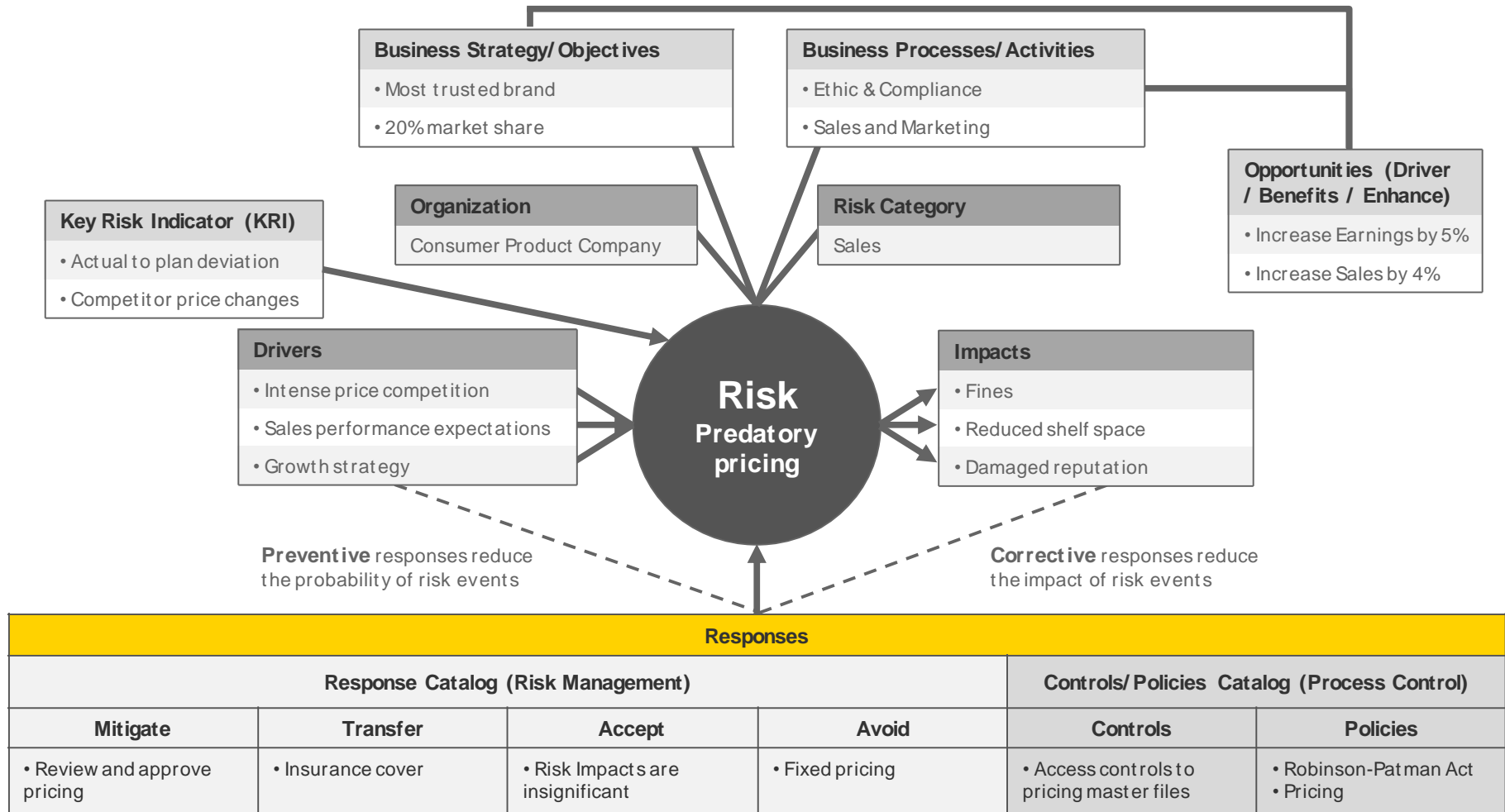
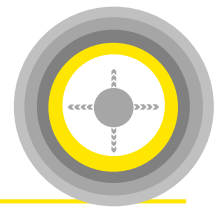
# Governance

## SAP GRC Access Control – Governance Structure



# Business involvement

## Risk management data objects and their relationships



# Project Examples



# SAP AC Re-implementation

## An holding company with many multinational operations in Consumer Products and Mill Products industries

The Client was struggling to use SAP GRC AC since the results in the reports were overwhelming, contain too much irrelevant data, and are reporting false positives. Also ARM approvers couldn't understand the access risks and access requests were approved unconsciously. So, the group decided to re-implement AC with proper content and methodology: The result is announced as **20% reduction** in access management operational costs, increased compliance and IT satisfaction results.

### Previous State

#### Too many rules

- ❑ 216 SoD rules were defined, company was getting run-time errors while running GRC ARM

#### Complex role structure

- ❑ Position based roles with wide access, no standardization
- ❑ Many unused transactions

#### No mitigating controls

- ❑ Mitigating controls were perceived as «no risk»

#### The responsibility was on IT

- ❑ The governance model was not defined including role and risk owners.

#### No use

- ❑ The tool was not accepted by the users
- ❑ There were many work-around

### Current State

#### Necessary rules

- ❑ Only real risks are defined as SoD or SA risks
- ❑ Total number of rules are 34.

#### Simple and sustainable role structure

- ❑ Task based roles based on functions
- ❑ Standard, adaptable, easy to monitor
- ❑ Sustainable

#### Relevant mitigating controls

- ❑ Relevant mitigating controls were defined to mitigate SoD and SA risks and risk owners are trained to assign proper controls

#### The responsibility in on Business

- ❑ Proper governance structure were defined
- ❑ Business owners take the responsibility and accountability with clearly defined roles

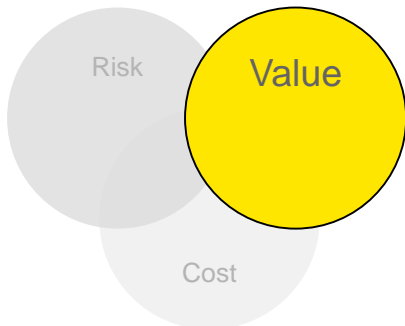
#### In use

- ❑ The tool is used company wide with immediate effect on costs and user satisfaction

# SAP RM Implementation

An holding company with many multinational operations in Consumer Products and Mill Products industries

- Outdated, unreliable and inconsistent risk information without focus on strategic risks
- Inability to meet corporate objectives and stakeholders' oversight expectations
- A lot of effort to aggregate and report risk information
- Risk management practices and tools in subsidiaries were not standardized – collaboration was impossible
- High cost of control – sub-optimal risk appetite, no use of analytics or continuous monitoring.



- ▶ Improved alignment to the objectives and strategy of the business
- ▶ Central management of financial, operational and compliance risks and controls across organization
- ▶ Increased integration and coordination among business, IT and compliance
- ▶ Sustainability of risk management process
- ▶ Effective top-down and bottom-up reporting



Thank you



Building a better  
working world