



# Enabling the governance around an ISMS through GRC Solutions

**Security-Congres 2010, Zeist**  
**Ir. David Janmaat CIA CISA EMITA**



# Agenda

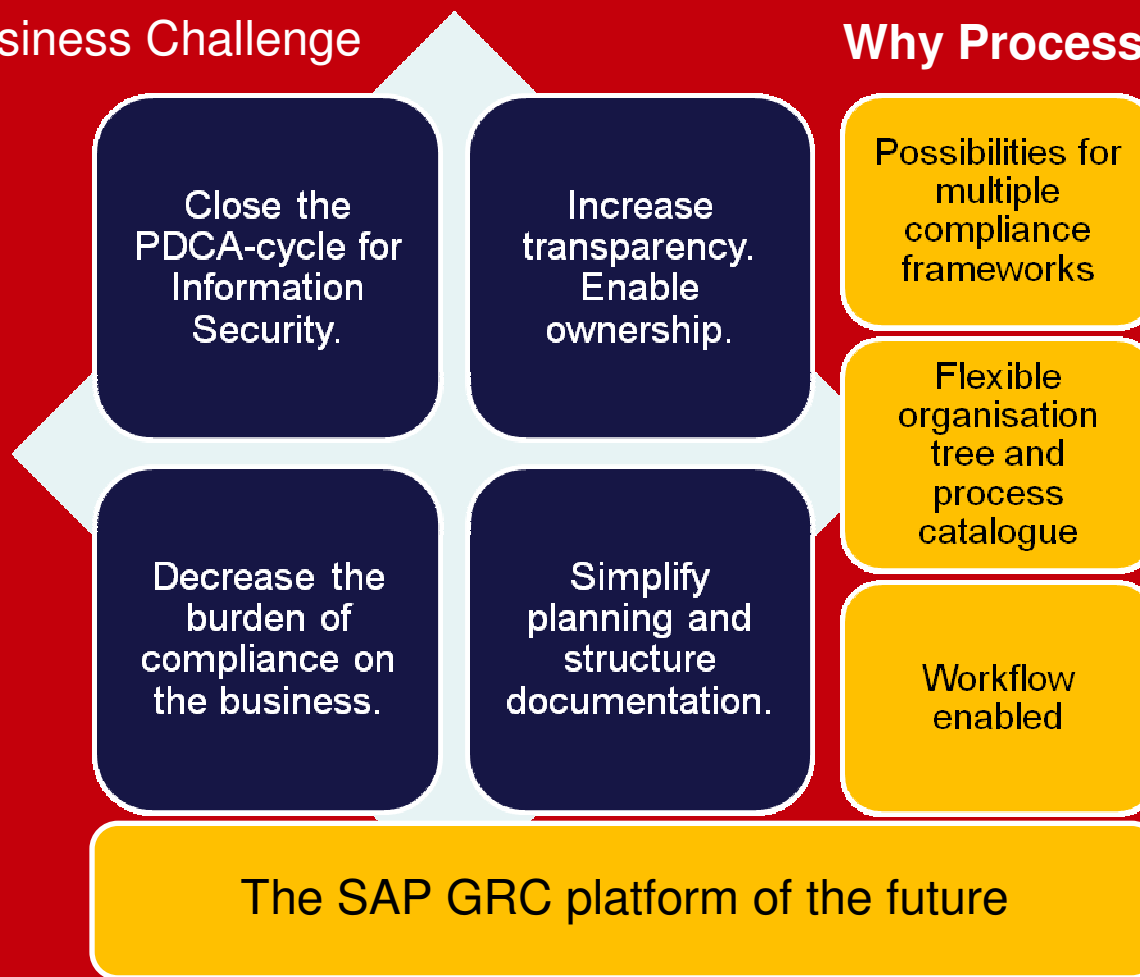
- Introduction
- Business Challenge
- Rapid Explanation of Process Controls
- Project Approach
- Project Challenges
- Lessons Learned
- Questions



# Business Challenge

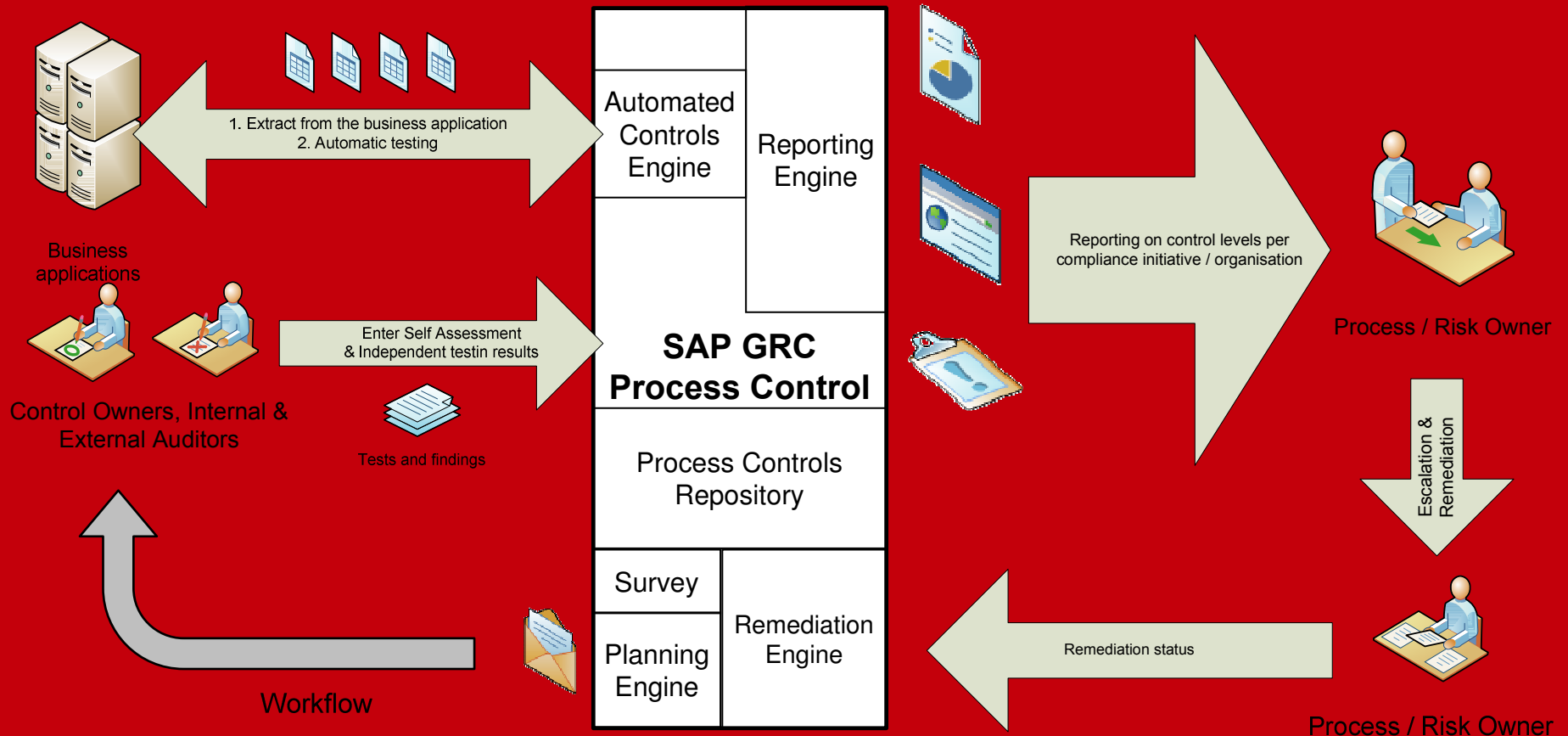
## Business Challenge

## Why Process Controls





# Rapid Explanation of Process Controls





# A shift in the use of GRC Technology

## FROM

SAP provides full GRC coverage for strategic applications throughout the enterprise

SAP Business User

SAP ERP

Composite Apps

SAP Netweaver

IT Foundation

## Other Applications

Enterprise Applications

LoB Applications

IT Applications

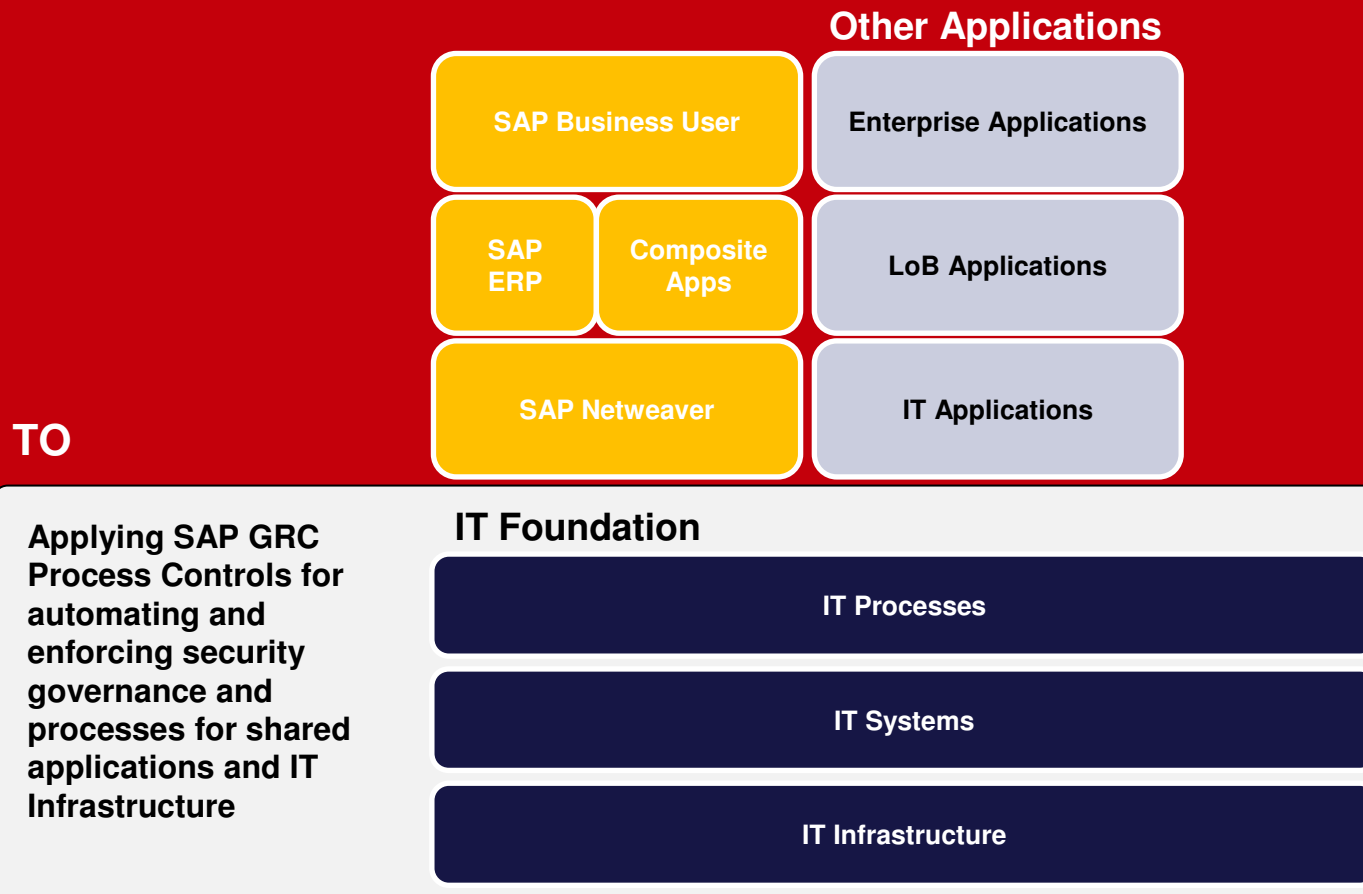
IT Processes

IT Systems

IT Infrastructure



# A shift in the use of GRC Technology





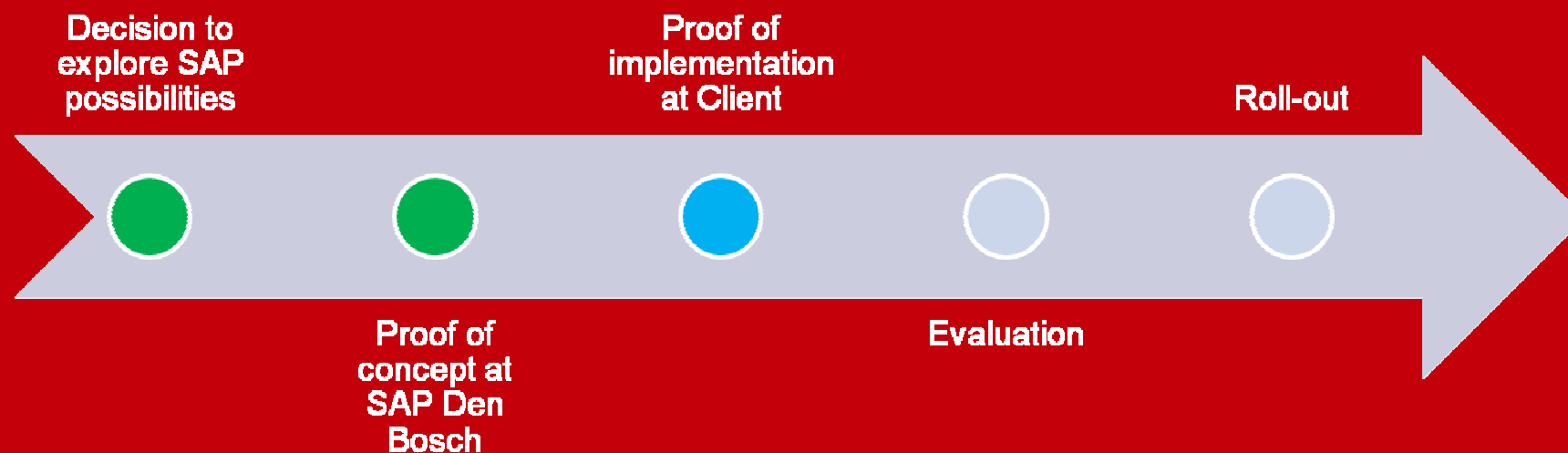
# Key project challenges

A somewhat special use of the software





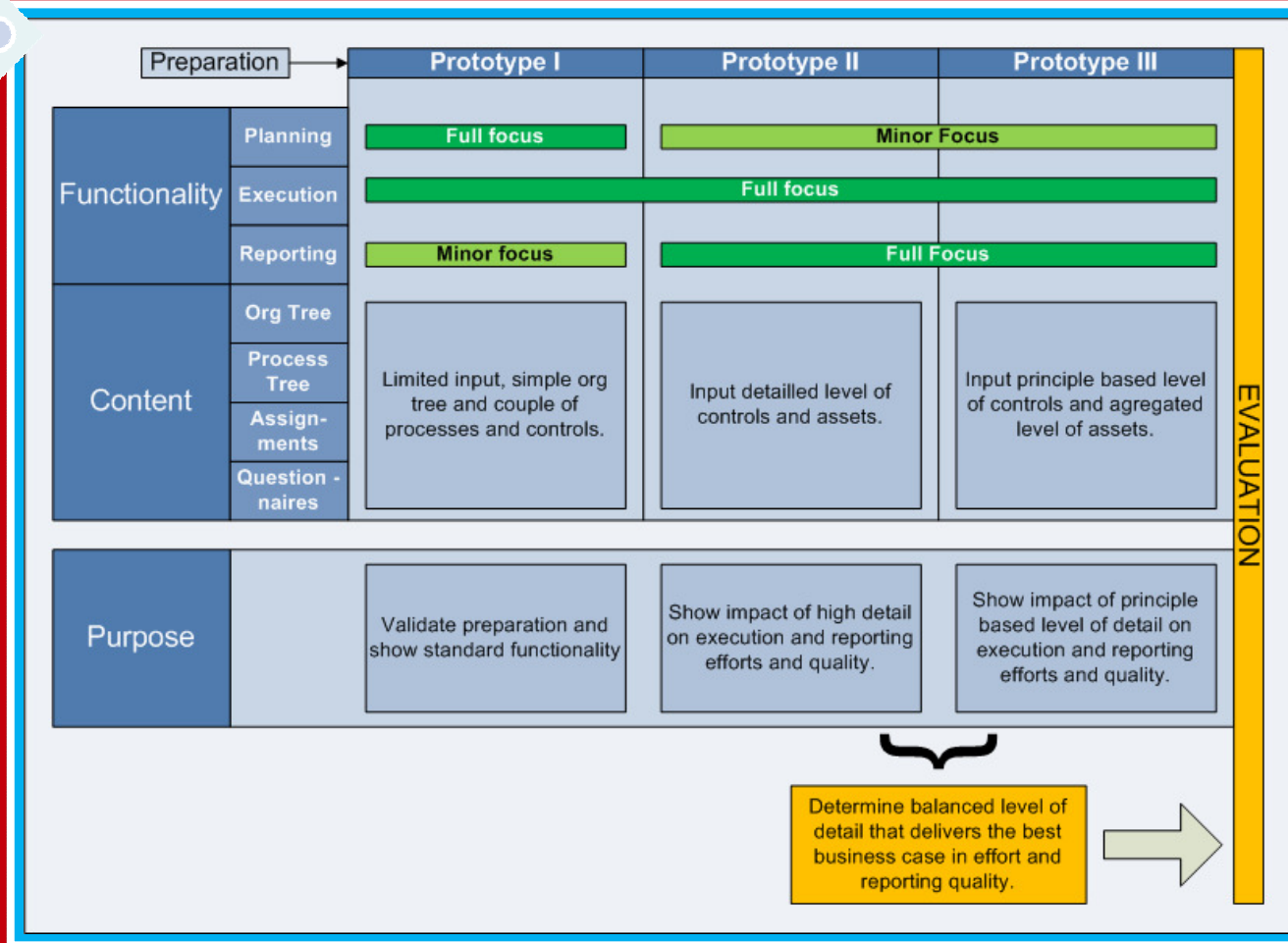
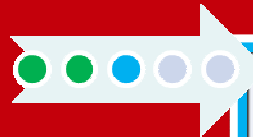
# Project timeline







# Prototyping focussed on the key project challenges





# Configuring process controls

**1**

Organizations

View: Standard Hierarchy

Show: September 2010

Apply Create

Name
Organization Hierarchy
ACME Co.
California Based Utility
Controllers
Tax
Information Technology
JB Trial 1
Test
Corporate Bank of America
Corporate Bank of America
Corporate Banking Entity
Global Aerospace and Defense Co.
Global Media and Consumer Products Co.
NASA
National Electric Utility

**Process Structure**

Show: September 2010

Apply Create Open Actions

Name	Type
Process Structure	
1. General Ledger	Process
1.1 Master Data	Subprocess
1.1 Control 1	Control
1.1 Control 2	Control
1.1 Control 3	Control
1.1 Control 4	Control
1.2 Transaction Proc Site Level	Subprocess
1.3 Transaction Proc Shared Svcs	Subprocess
1.4 Transaction Proc Site Level	Subprocess
1.5 Reporting Shared Services	Subprocess
10) Financial Reporting	Process
11) ERP System Controls (GCC)	Process
11) ERP System Controls (Process)	Process

**Control: 1.1 Control 4**

General Risks

Description: Monitors changes to bank mast

Valid From: 01.01.2009

Valid To: 31.12.9999

Control Automation: Automated

Trigger: Date

Operation Frequency: Monthly

Purpose: Detective

Significance: Key Control

Control or Process Step: Control

Control Category: Transactional-Level Control

Nature: Recording

To Be Tested: Yes

Testing Technique:

Test Automation: Semi-Automated

Documents: [u](#)

**Global - Assign Corporate and Organization Roles**

3 (=1+2)

1 Select Organizations 2 Assign Roles 3 Review 4 Confirmation

Timeframe: September 2010 Effective Date: 27.09.2010

Assign Users to Roles for the Selected Filter Criteria.

Assignments

Level	Object	Parent	Central Risk Manager	CEO/CFO	Internal Auditor	System Administrator	Organization Owner	Unit Risk Manager	Global Automated Rules Customi
Corporate	Global Media and Consumer Products Co.		David Janmaat	David Jan	David Janmaat	David Janmaat	Glen Holland	David Janmaat	David Janmaat
			Glen Holland	Glen Holla	Bruce Wayne	Glen Holland	David Janmaat	Glen Holland	Glen Holland
					Glen Holland				
	Global Aerospace and Defense Co.		David Janmaat	David Jan	Glen Holland	Glen Holland	Glen Holland	David Janmaat	David Janmaat
			Glen Holland	Glen Holla	David Janmaat	David Janmaat	David Janmaat	Glen Holland	Glen Holland

**Multiple compliance frameworks:**

- ICS,
- Solvency2
- ISO27001
- Operational,
- ...



## Lessons Learned

- Do not underestimate the importance of change management
- Start directly with the data gathering within the organization to improve timeliness and quality of information.
- Identify stakeholders and agree on reliance approaches
- External audit will gain a clear picture on the design of Internal Control
  
- Prototyping is a very suitable approach
- Challenge is to find the appropriate level of detail for implementation
- Automated controls in the early stages of development
- Time sensitive, clean install by prototyping
- Mass upload functionality



# Questions