

SAP Forum

Looking for compliance with performance

Edgar R. P. D'Andrea, *CGEIT, CISA, CISM*



Março 2010

Today's Agenda

Understanding the GRC Market

ERM & Continuous Control and GRC

GRC Imperatives

PwC Vision – Integrated GRC

Final Considerations – GRC 2010 Opportunities

GRC Market Overview

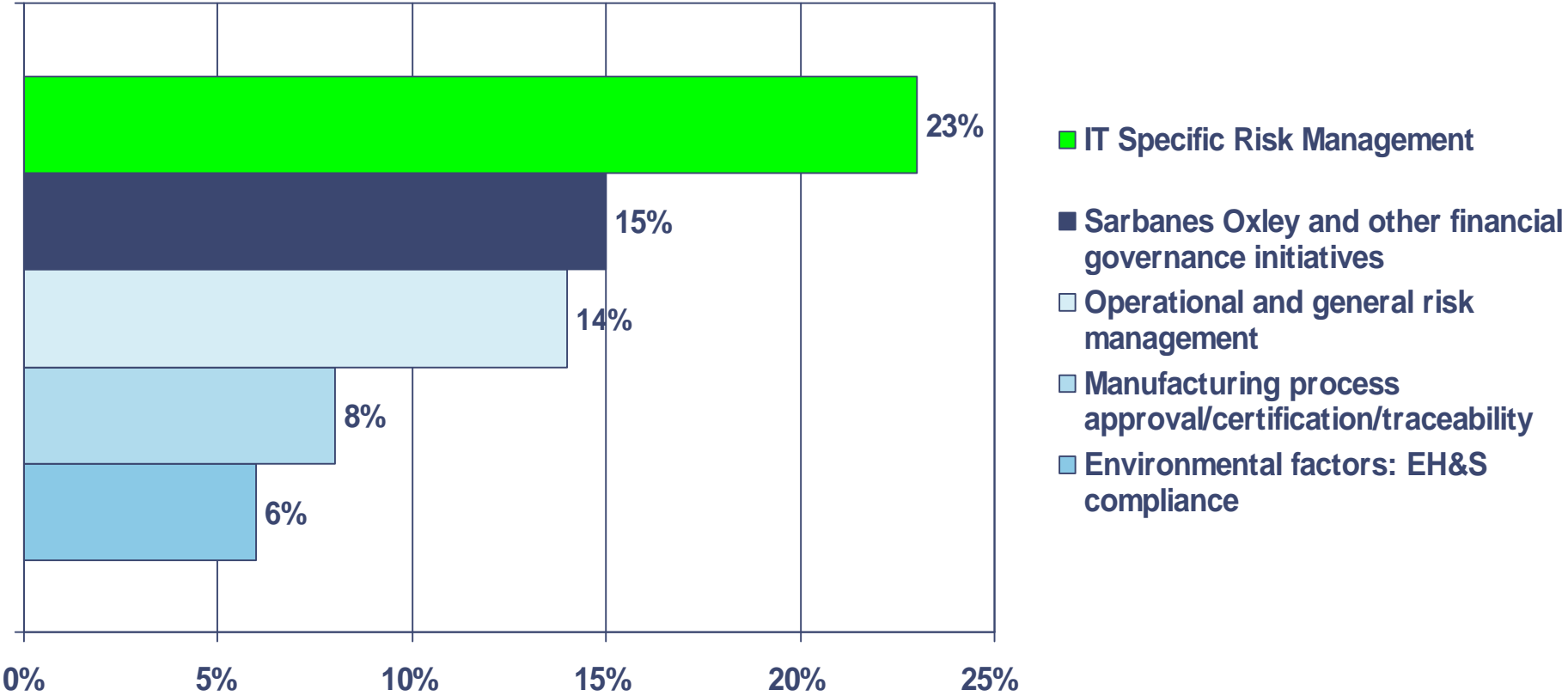
Key Market Messages

A shift is occurring in GRC with an emphasis from compliance to risk, this has changed the spending dynamic considerably. Firms report moving beyond specific initiative to more broad-based support for risk, especially in the IT arena.

S&P Credit Rating Impact on companies' business.

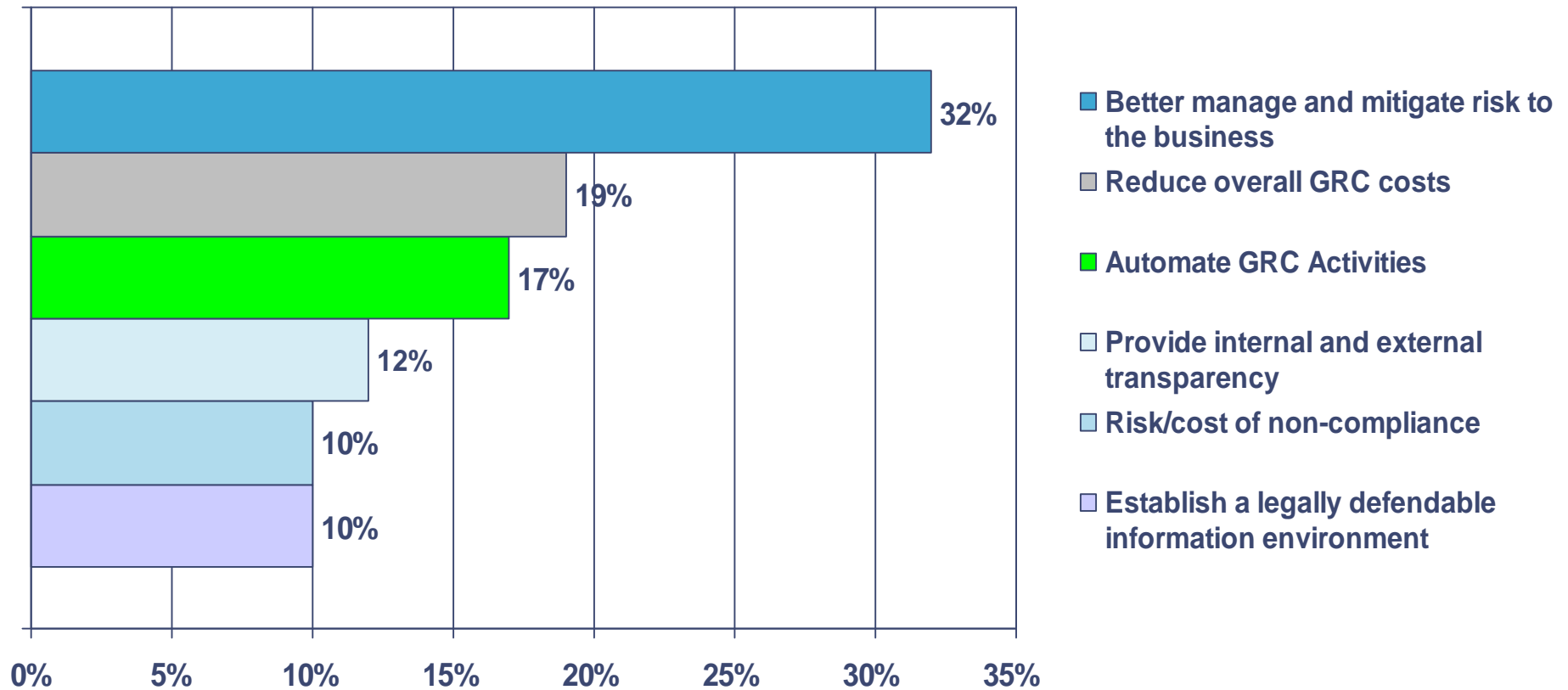
GRC spending is still on the increase in accordance with an AMR Research.

Five largest single GRC investment for all countries and buyers



Source: AMR Research, 2008

Management issues driving GRC spending



Source: AMR Research, 2008

Annual Report IT GRC

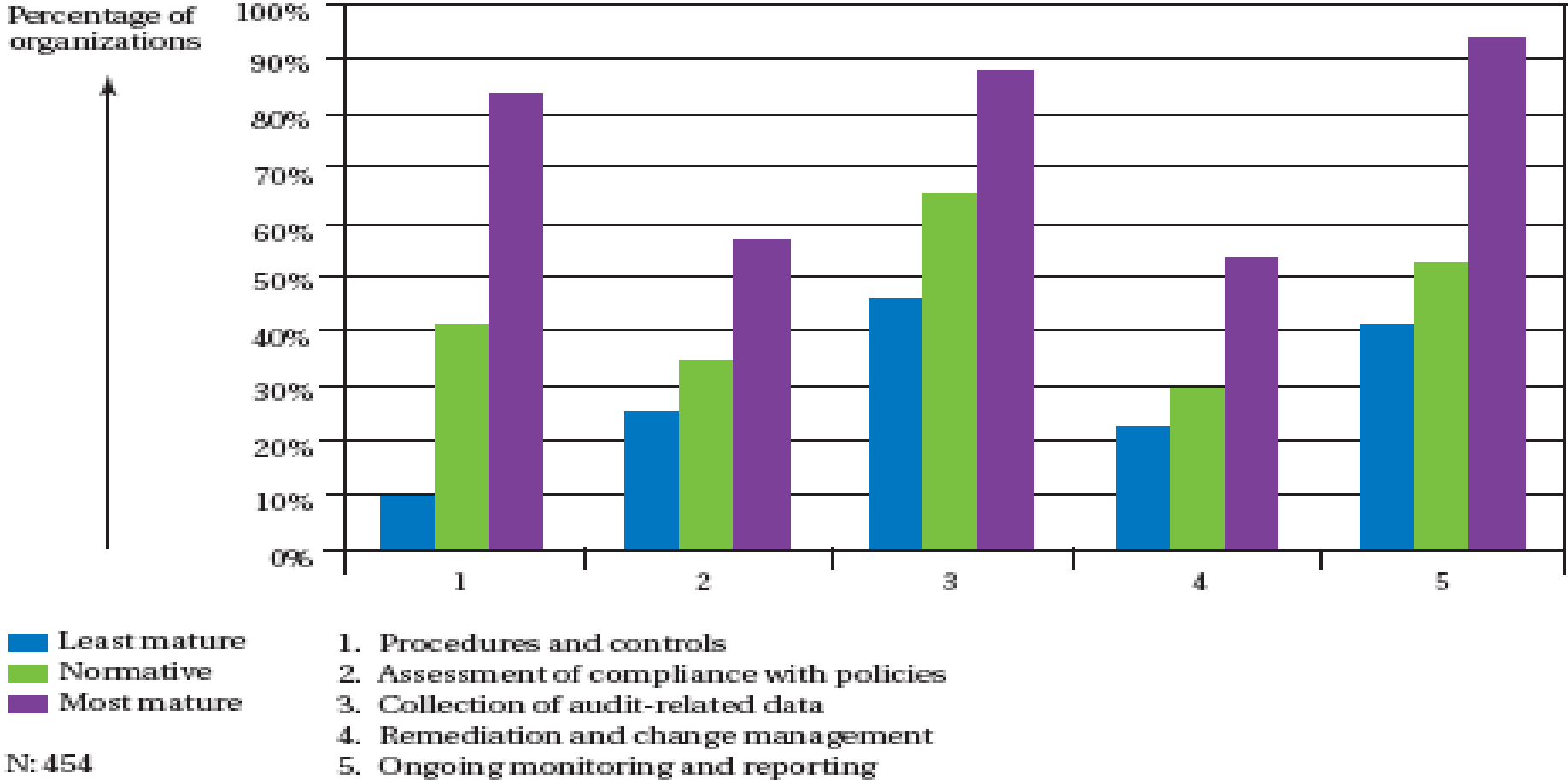


Figure 35. Automation of activities
Source: IT Policy Compliance Group, 2008

Key Market Messages

Agility and Flexibility - Accelerating rate of change

Rapid technological advances in recent years

Requires management to be more anticipatory

Requires a GRC approach that effectively aligns risk and rewards

Greater complexity

Accelerated rate and volume of change demands increased flexibility

Extended business models and increased geographic diversity increase the complexity of managing the business

Increased number of regulatory regimes

Increased transparency

Stakeholders learn about unmanaged risk almost immediately (sub-prime crisis, Derivativos, etc)

Management has little time to remedy the impact of a risk management failure

Places a premium on the ability to identify, evaluate and manage risks

Most C-level executives face a dilemma which can be characterized by cost minimization, regulatory oversight, and transparency.

Accelerating rate of change and complexity

- Sophisticated products, **unfamiliar markets and unprecedented volatility**
- **Rapid technological advances**
- **Accelerated rate and volume of change** demands increased flexibility and anticipation
- New risk and accounting standards (Basel 2, fair value accounting), IFRS, NF-e

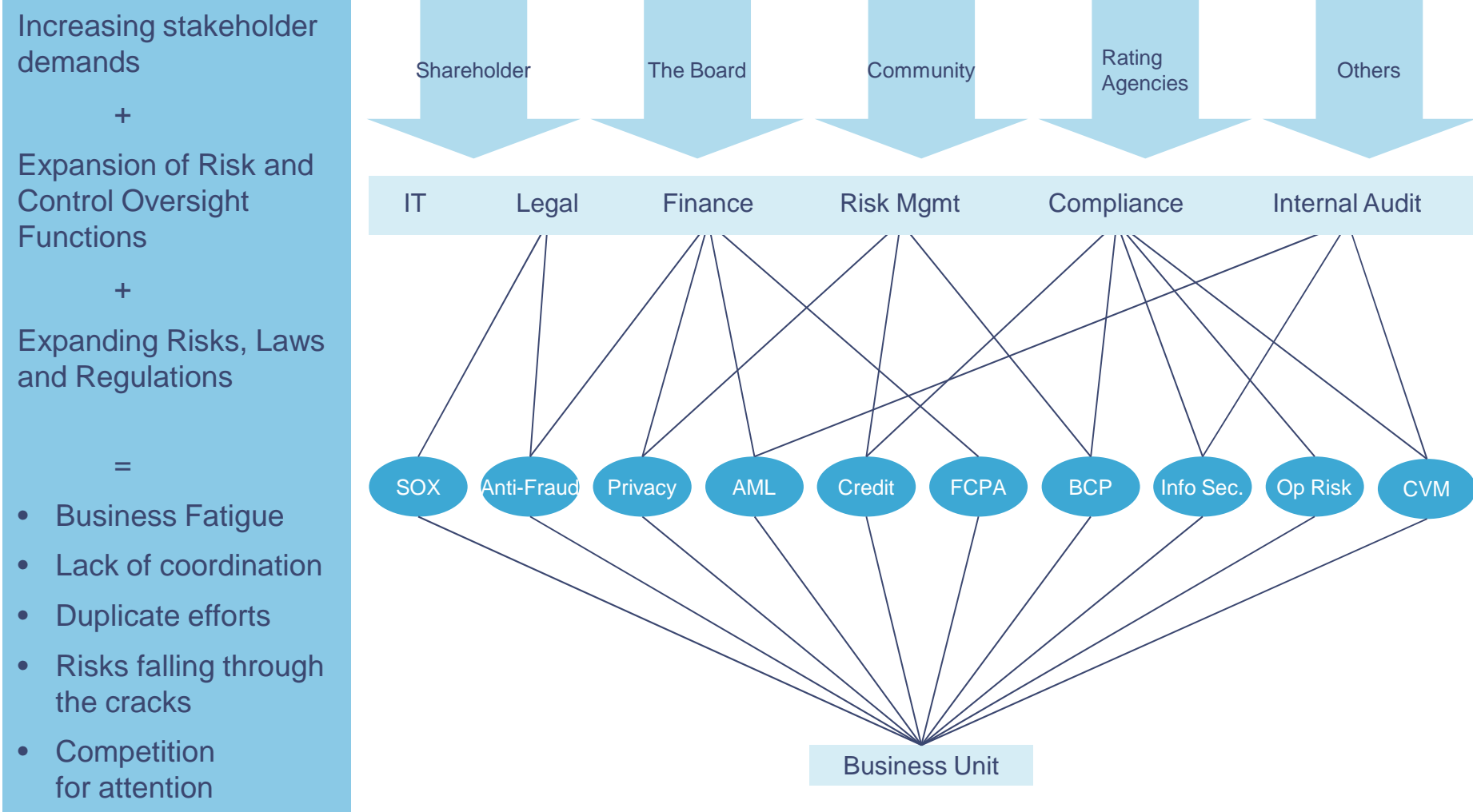
Increased regulatory oversight and uncertainty coupled with increased visibility and transparency demands

- Regulatory implications stemming from the Senior Supervisors Group observations on the **financial markets disruptions of 2007-8**, and the 2008 Treasury Blueprint
- Uncertainty on how to effectively relate to the 3 core **regulatory objectives- market stability, safety and soundness, customer protection**
- **Big focus on managing liquidity risk** more completely and effectively
- **Fed regulation of investment banks, potential of additional regulation**
- Focus on trading **markets exposure** and the possibility of **internal fraud**
- **Increased number of relevant regulatory** regimes for global institutions
- Likelihood of rise in **enforcement activities and litigation**
- Greater visibility requirements and disclosure needs to the market relative to practices places a premium on the ability to **proactively identify, evaluate and manage risks**

Cost reduction initiatives

- **Headcount freezes and/or reductions with the increased regulatory and business pressure create a fertile environment for Cost Reduction projects. GRC Technology Solutions** are a proven method to bring about automation, increase efficiency and lower operating costs

Companies have historically responded by instituting independent governance risk & compliance (GRC) oversight functions and committees.



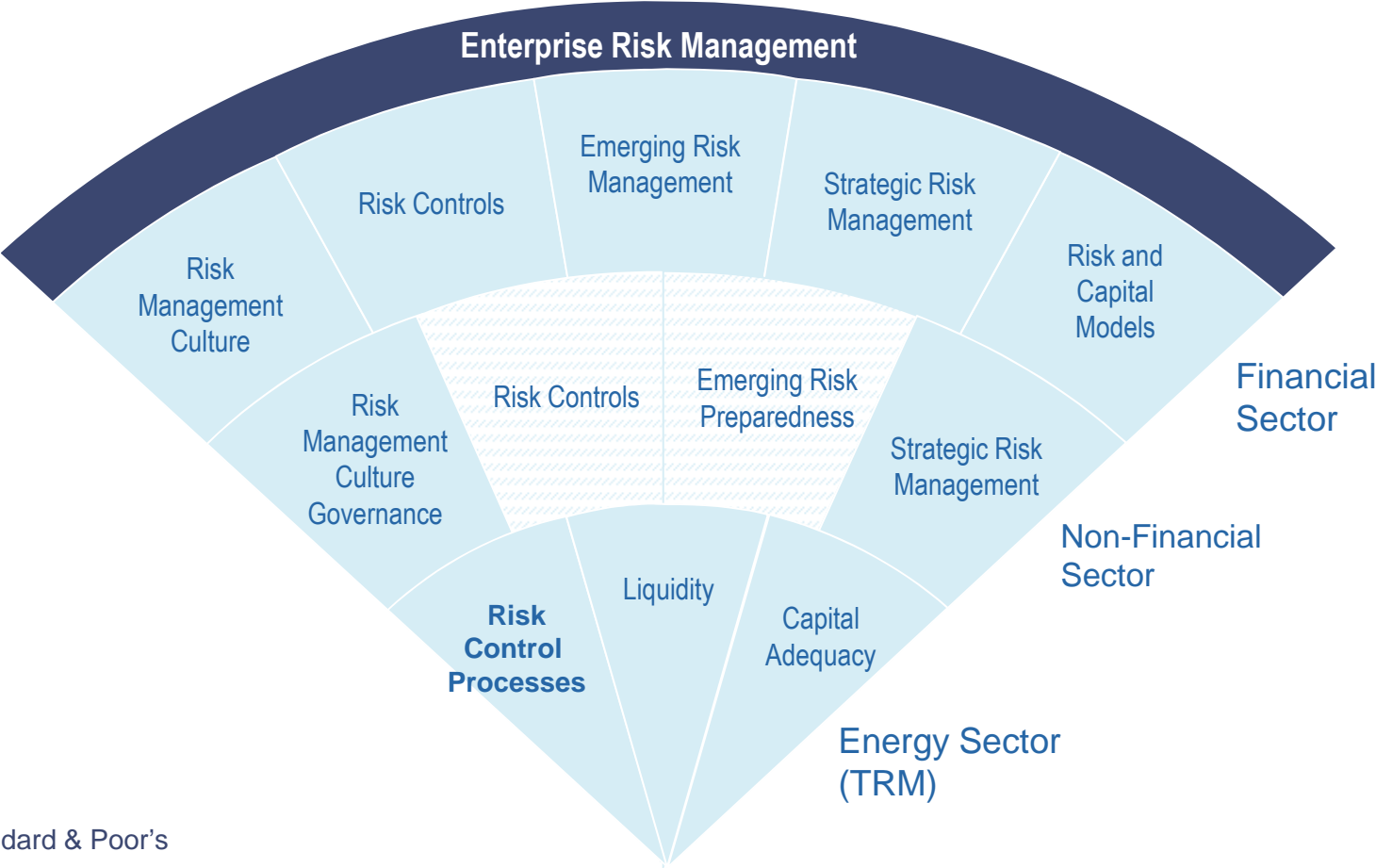
GRC



Enterprise Risk Management and Continuous Controls & GRC



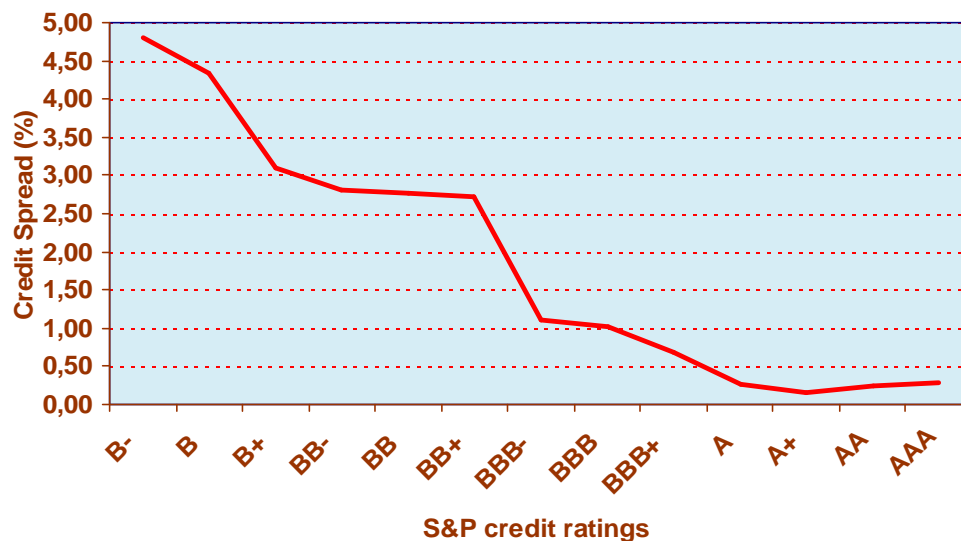
Standard & Poor's - S&P's approach to ERM by industry



Fonte: Standard & Poor's

Value Proposition: Better ERM assessments → better credit ratings → lower cost of capital → enhanced reputation

Higher credit ratings lead to a more favorable cost of capital



1 year credit spread for Industrial Products companies

This applies to all sectors:

- Industrial Products
- Retail & Consumer
- Technology
- Automotive
- Entertainment and Media
- Financial Services
- Others

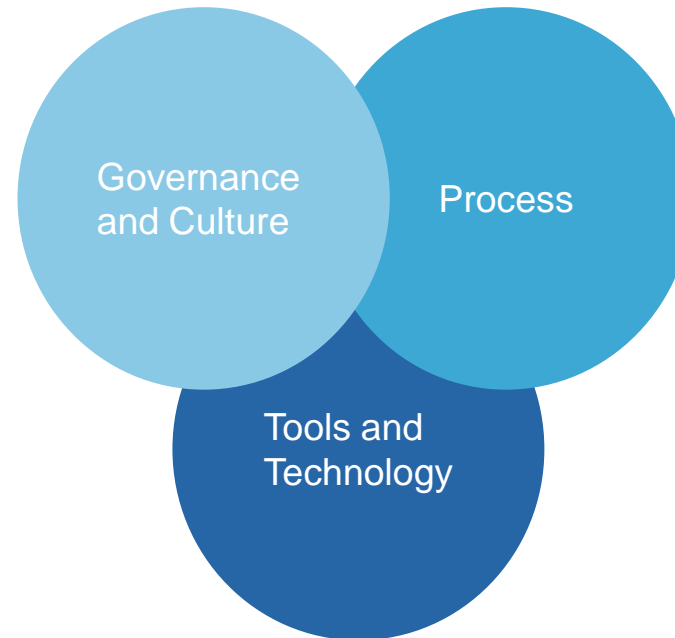
A company's cost of capital is driven by its credit rating and cost of debt capital – a higher credit rating enables a company to maintain lower borrowing costs.

Fonte: Standard & Poor's

PwC Vision

Successful ERM programs are enabled by three core elements

- Governance framework
- Organizational structure
- Roles and responsibilities
- Dispersed Accountabilities
- Performance metrics
- Risk culture/Training



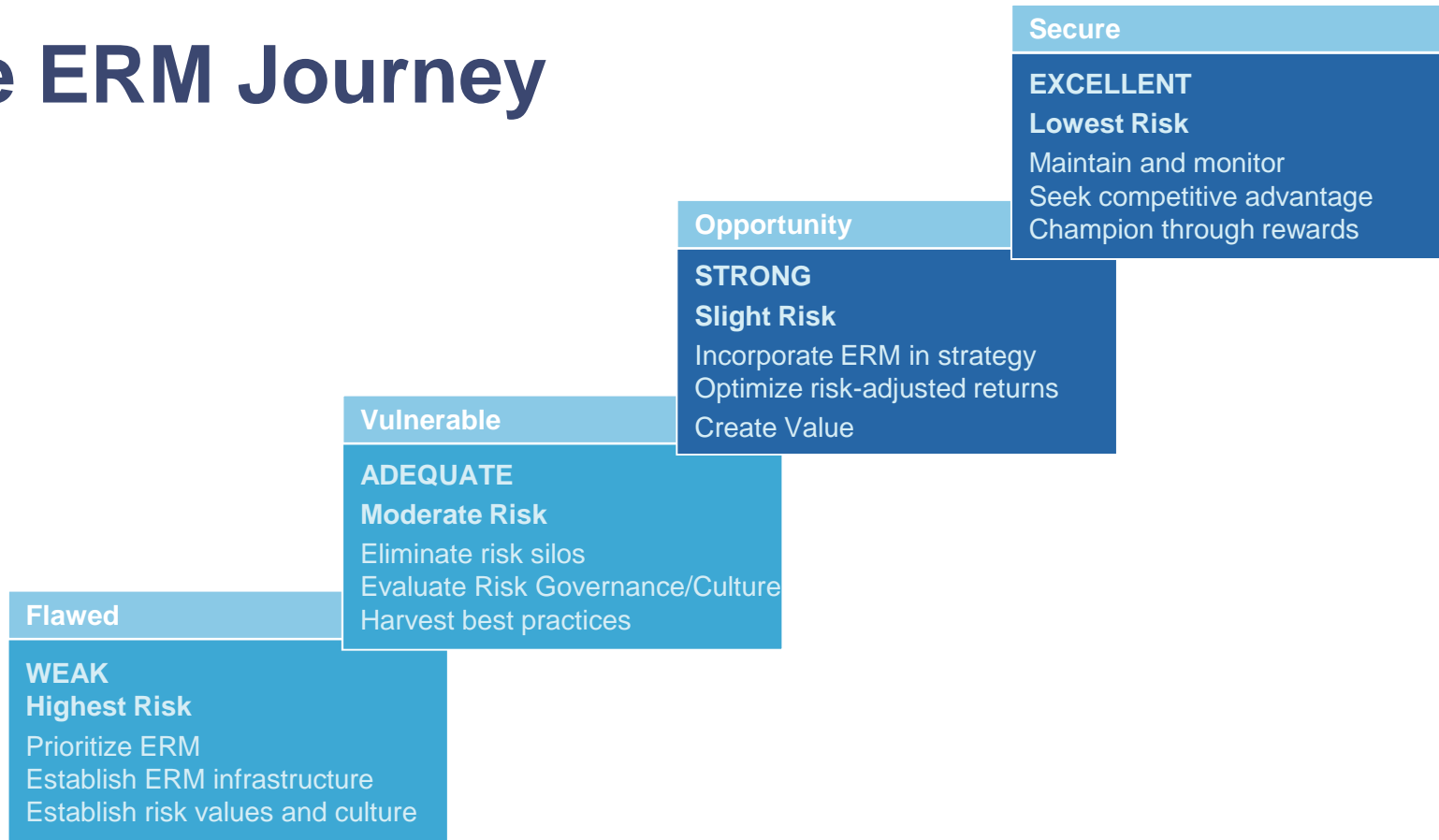
- Identifies potential risk events
- Gathers, aggregates and analyzes risk information
- Develops appropriate responses
- Monitors effectiveness and efficiency of risk responses
- Takes corrective action, as necessary
- Routinely update risk profile

- Data sourced from internal and third-parties
- Gathering and aggregation templates
- Reporting framework
- Analytical tools and techniques
- Presentation layer (e.g., dashboard, portfolio view of risk, etc.)

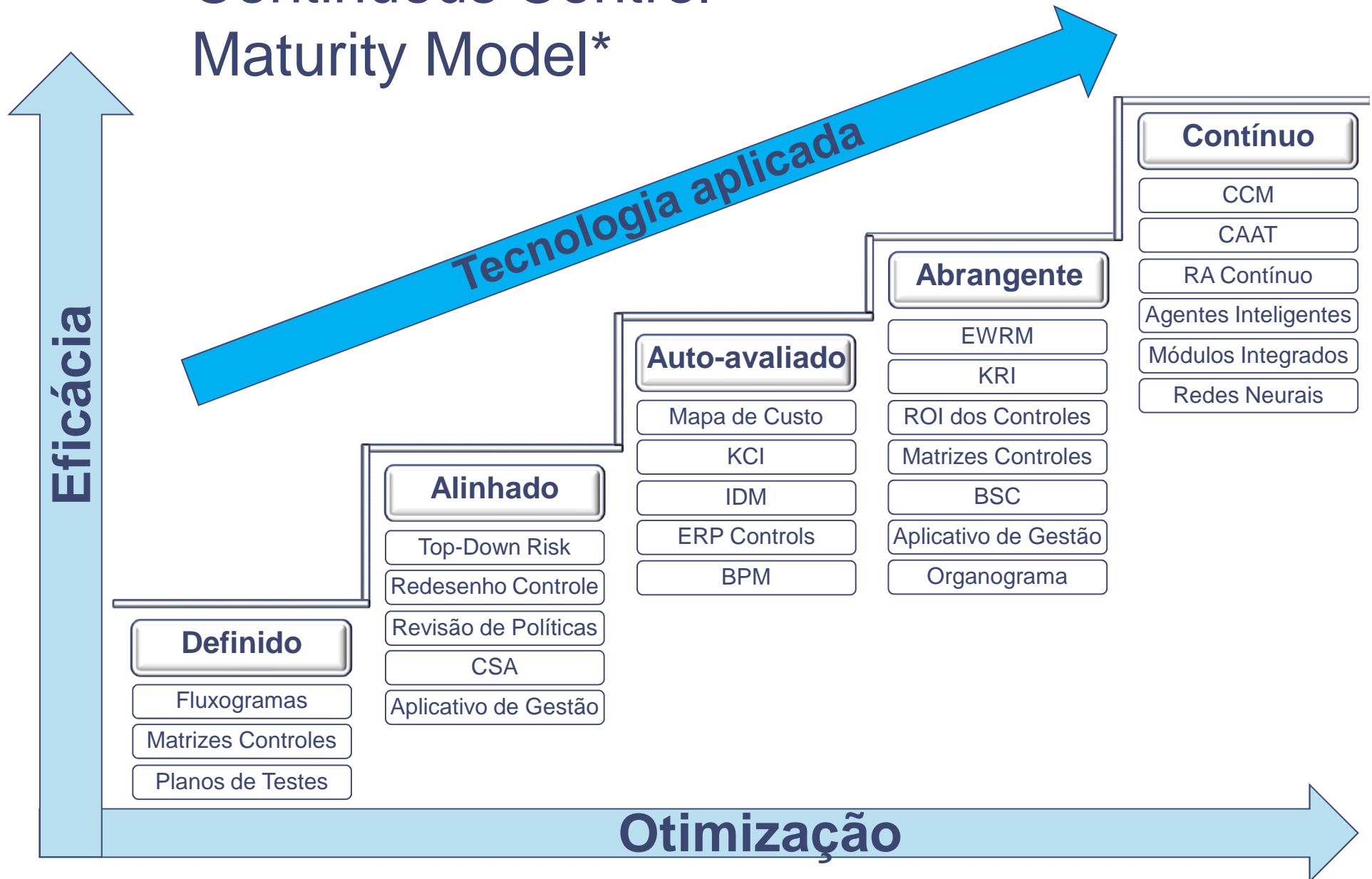
PwC Vision

Taking Stock - Evaluating the Current State of ERM

The ERM Journey

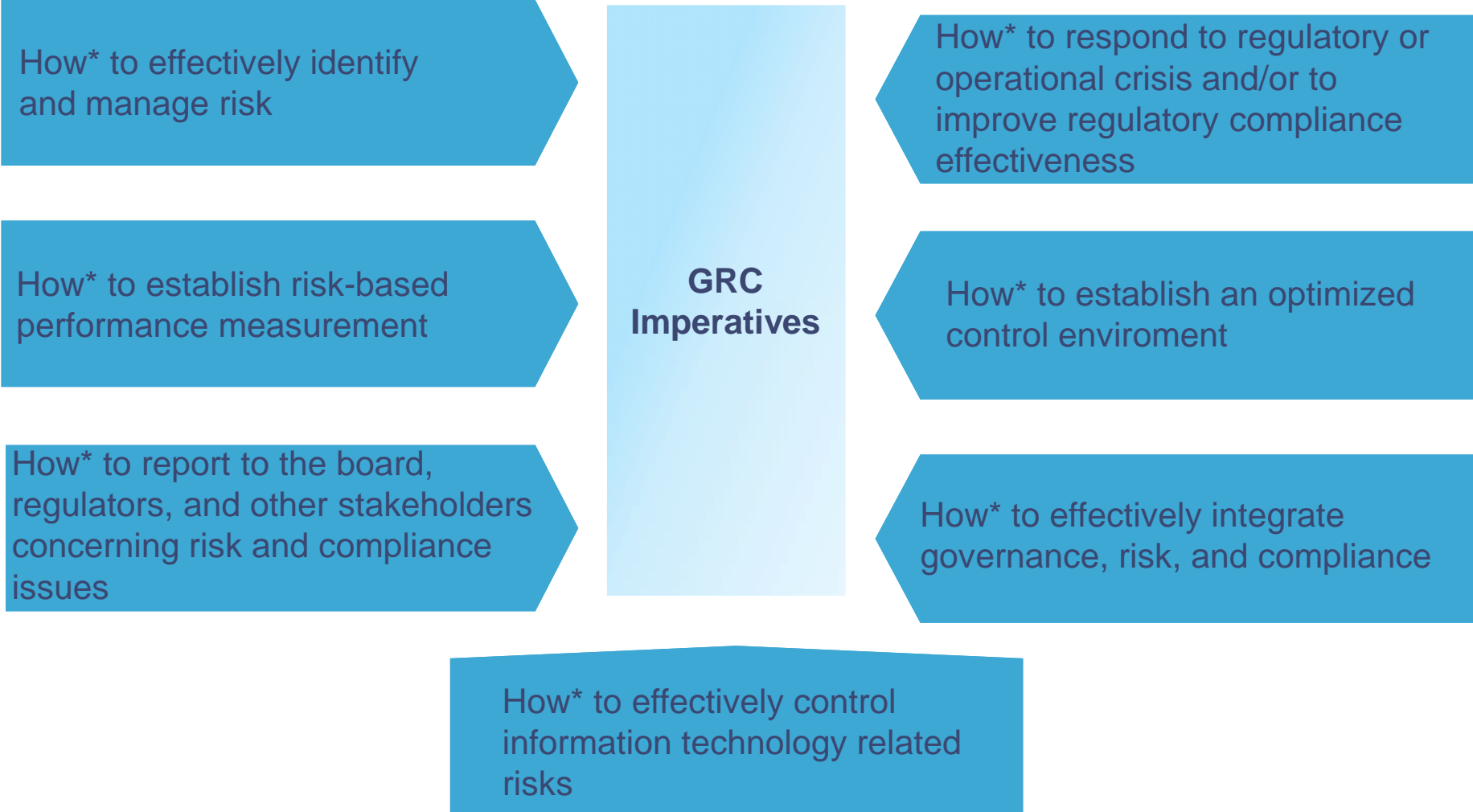


Continuous Control Maturity Model*



GRC Imperatives

GRC Imperatives



These imperatives encompass issues across an organization's value chain.

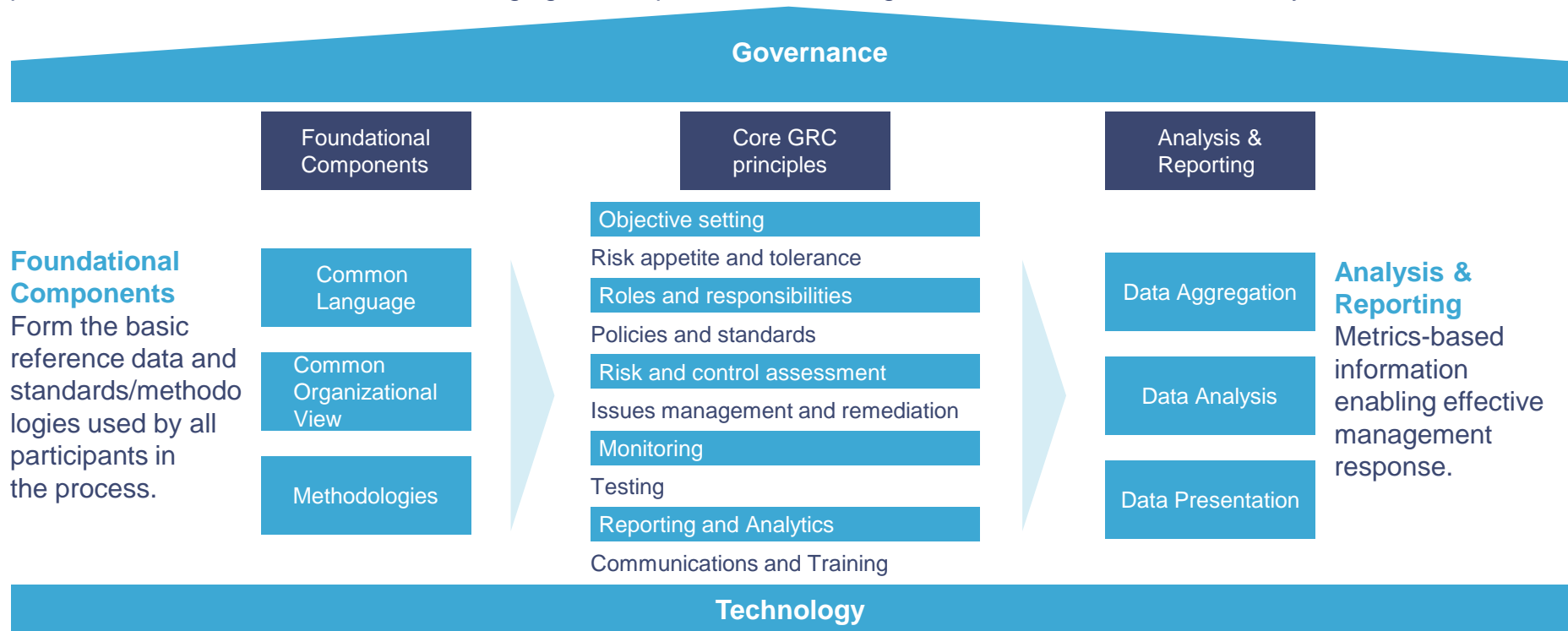
PwC Vision Integrated GRC (iGRC)



What is GRC?

An incremental, pragmatic approach to identifying improvement within an integrated framework that is enabled through technology

Governance – Provides leadership, consistency and accountability over the entire process. Critical roles (e.g. Internal Audit) are preserved as centers of excellence leveraging shared processes to drive greater effectiveness and efficiency.

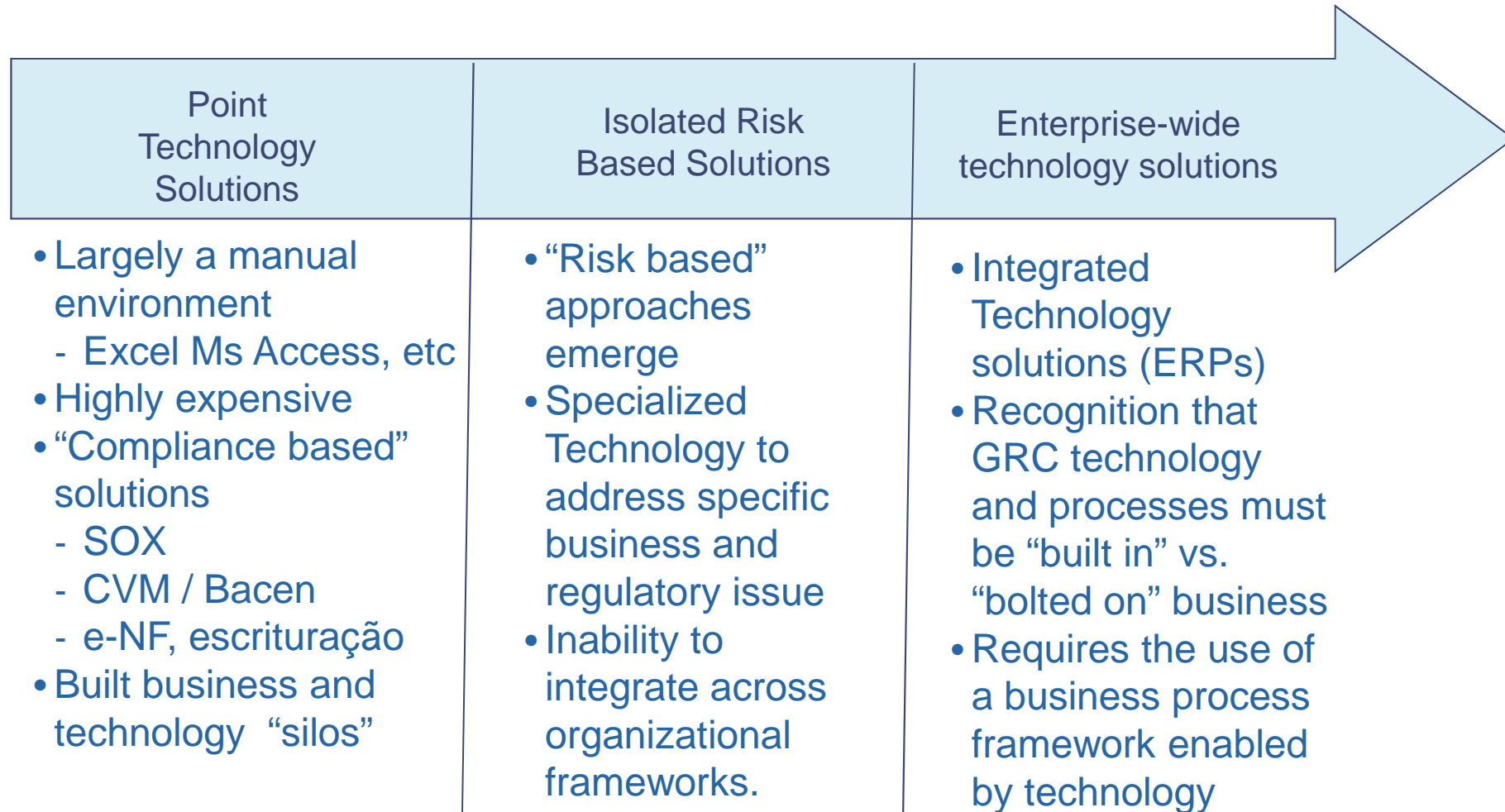


Technology – Supports the entire framework, creating process efficiency and more effective data management and reporting.

The enablement of GRC through technology

Example GRC Principles	Technology Enablement
Roles & Responsibilities	Automated access control to critical business applications and enforcement of access policies for effective segregation of duties management
Monitoring	Automate continuous monitoring of policies, controls, process and transactions to detect suspicious business activities in real time
Policies & Standards	Provide a common repository to bring together the enormous volume of documentation (GRC policies, standards, testing plans, etc.)
Testing	Provide a workflow capability to document, test, and review the design and operating effectiveness of process & controls that mitigate risk

The evolution of GRC Technology closely aligns to the integration of GRC principles and activities



CASE PwC

Final Considerations 2010 GRC Opportunities

Thank U*