

Klemen Koselj – Business Analytics Specialty Architect, Risk Analytics for CEE

09 May 2012

Using an Enterprise Governance, Risk & Compliance (GRC) Platform to Improve Risk and Compliance Initiatives



The stakes are enormous...

UBS share price tumbles after trader loses \$2bn

15/09/2011



UBS rogue trader loses \$2bn



As they always were...

The New York Times
nytimes.com

January 24, 2008

\$7.1 Billion Fraud Uncovered at Société Générale

By DAVID JOLEY

PARIS — The French bank Société Générale said Thursday that it had uncovered "an exceptional fraud" by a trader that would cost it €4.9 billion, or about \$7.1 billion, and that it would seek new capital of about \$8 billion.

The company, the second-largest listed bank in France, said in a statement that the fraud had been committed by a trader in charge of "plain vanilla" hedging on European index futures.

The trader, who was not identified, "had taken massive fraudulent directional positions in 2007 and 2008 far beyond his limited authority," the bank said. "Aided by his in-depth knowledge of the control procedures resulting from his former employment in the middle-office, he managed to conceal these positions..."




The bank said the fraudulent positions... to be a case of "isolated fraud."

...highly investigated and found

“Aided by his in-depth knowledge of the controls procedures resulting in his former employment in the middle-office...”

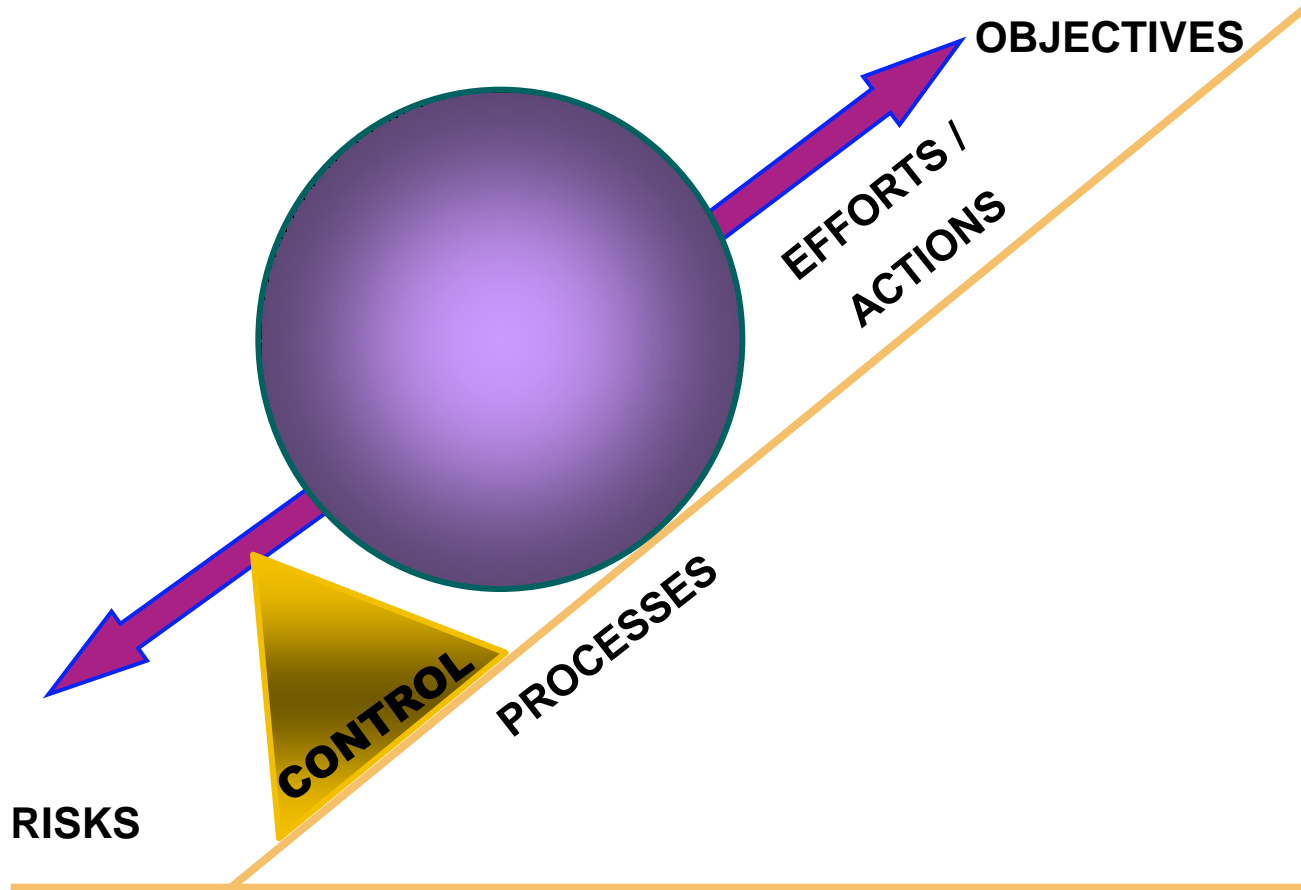
Growing need to manage risks that can impact business performance

Insider threats, cyber-crime and fraud cost billions and affect reputation

Network Security	Data Privacy	Access Control
 <p>Theft of information related to SecurID tokens affected 40 million people who use the tokens to access the internal computer networks of 25,000 corporations, including defense contractor Lockheed Martin.</p>	 <p>SONY ONLINE ENTERTAINMENT</p> <p>Personal information including credit and debit card numbers was stolen from over 100 million PlayStation accounts.</p>	 <p>SOCIETE GENERALE</p> <p>A trader familiar with access controls from years spent in its compliance department cost Société Générale over \$7 billion.</p>



“Operational” Risk Management Concept (day to day business)

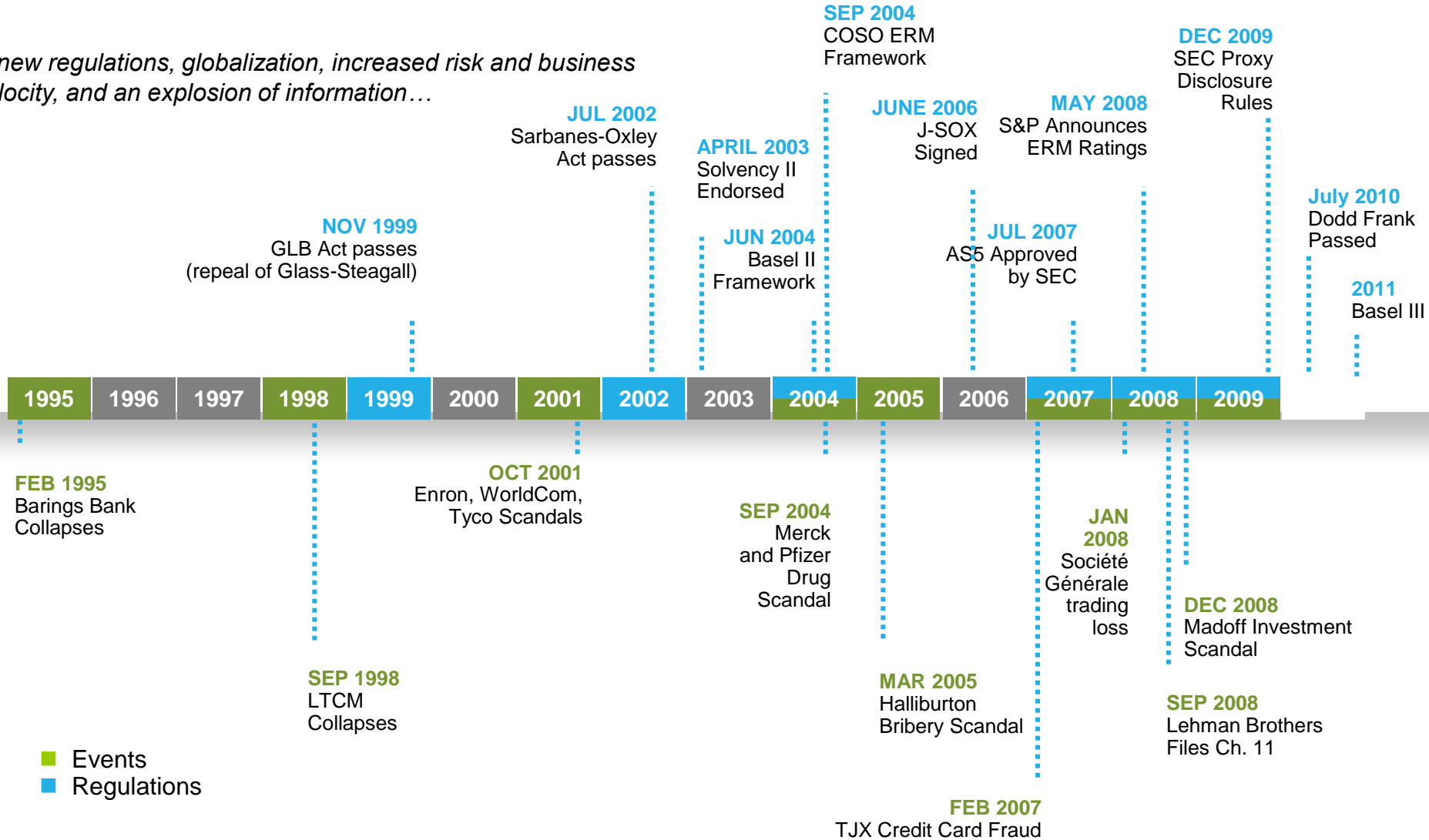


Operational Risk – Control activities



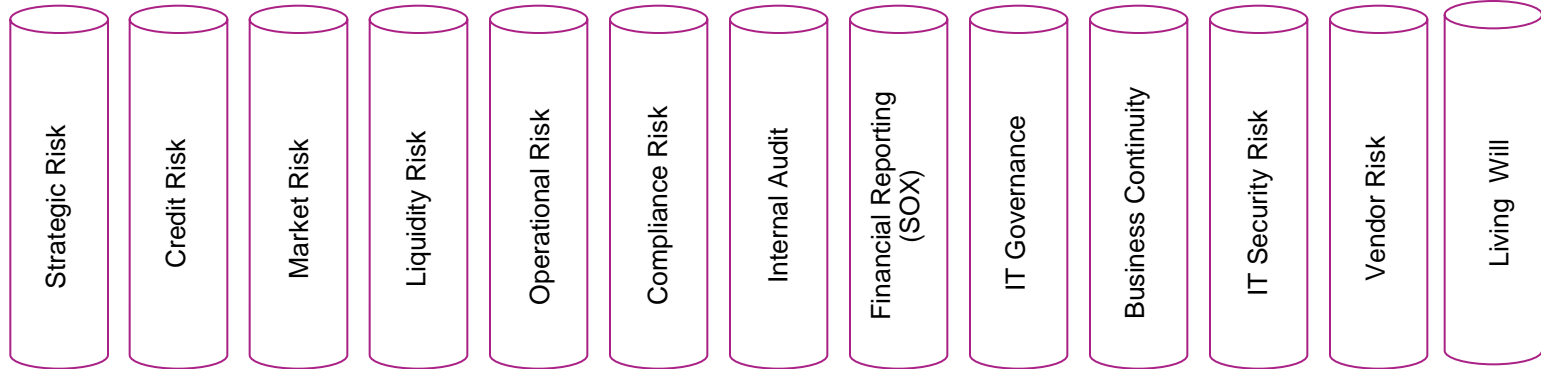
Risk has never been a bigger challenge than in today's business environment

...new regulations, globalization, increased risk and business velocity, and an explosion of information...

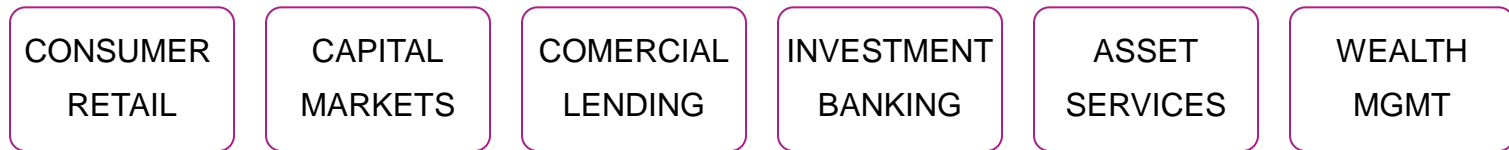


Most risk and compliance programs are fragmented

1.) Managed independently and in functional SILO's



2.) Managed independently in LOB's



3.) Managed independently of operational systems



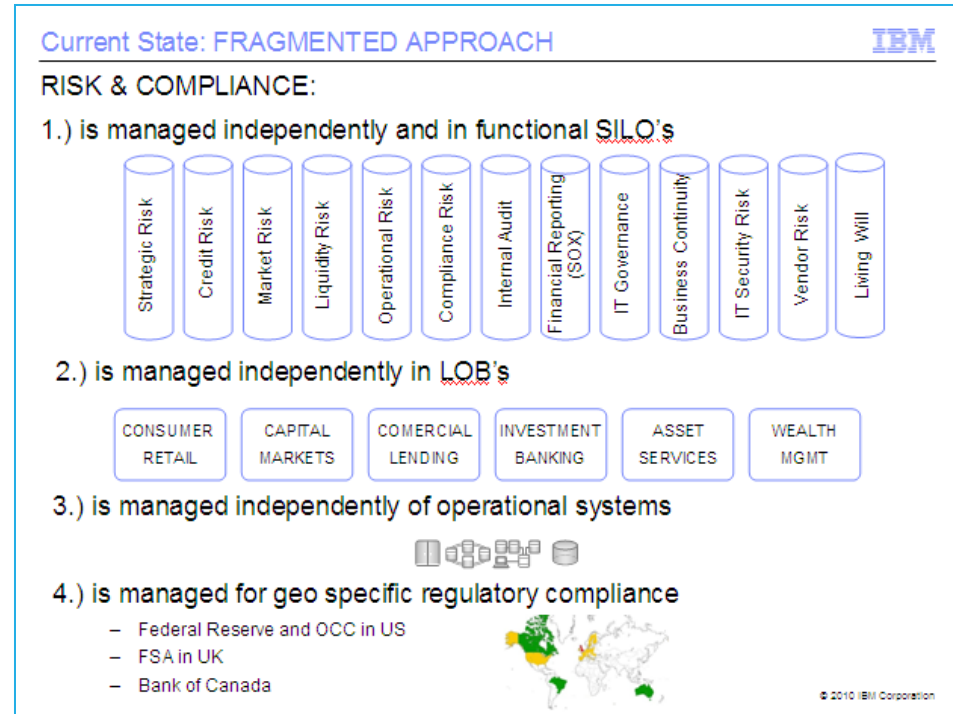
4.) Managed for geo specific regulatory compliance

- Federal Reserve and OCC in US
- FSA in UK
- Bank of Canada



Challenges

- Expensive
 - Costs of compliance exceeding \$100M annually and growing
- Cost of Non-compliance
 - Business disruption, fees, penalties, legal and settlement costs. Typically 3x the cost of compliance.
- SILO approach to management
 - Cost of duplicate efforts
 - Leaves significant risk of control weaknesses “falling through the cracks” resulting in reputational risk damage
- Difficult to respond to regulatory inquiries with accurate data
- New regulations doubling every six years
- Reactionary response today – inefficient & contradictory



Example: Many regulations have common requirements

Sarbanes Oxley

- Conduct risk, threat and **security vulnerability assessments**
- Design, implement and audit appropriate **security controls**

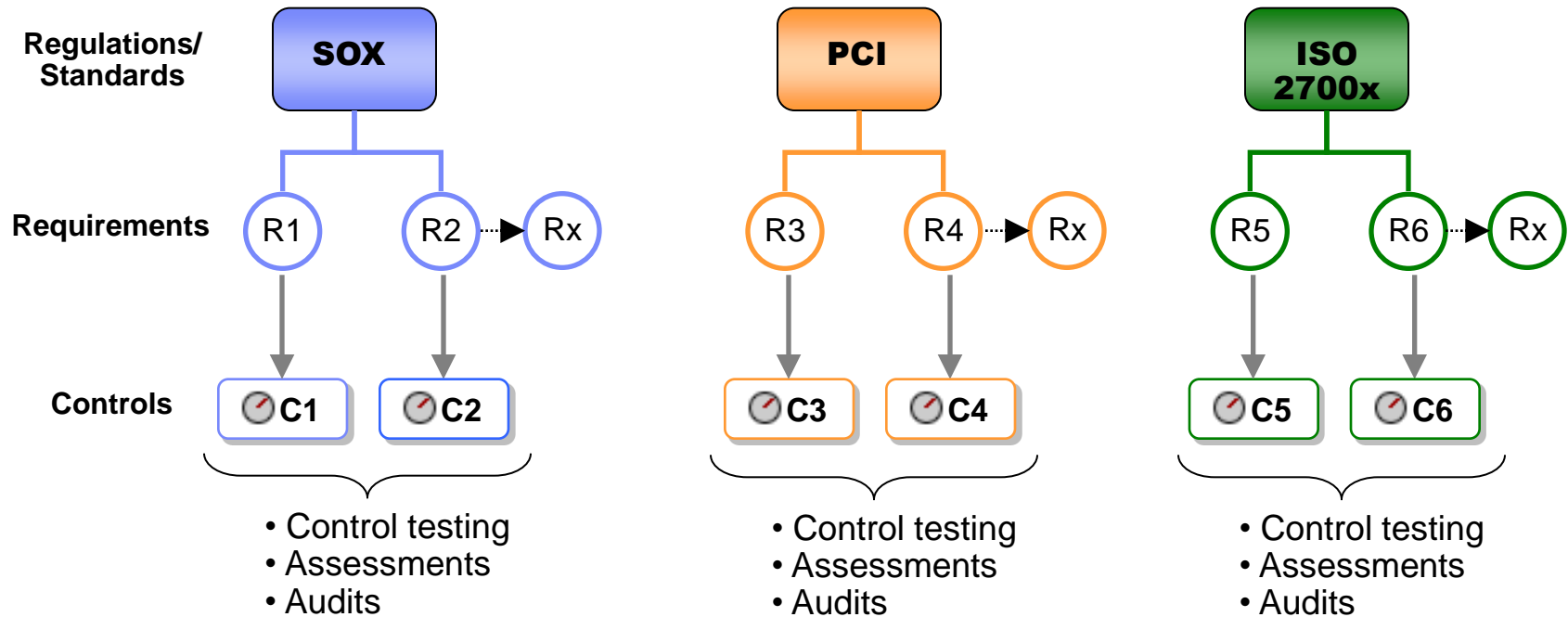
PCI DSS Requirement 6.6

- Ensure that all web-facing applications are **protected against known attacks**
- Have all custom application code reviewed for common **vulnerabilities**
- Install an **application layer firewall** in front of web-facing applications

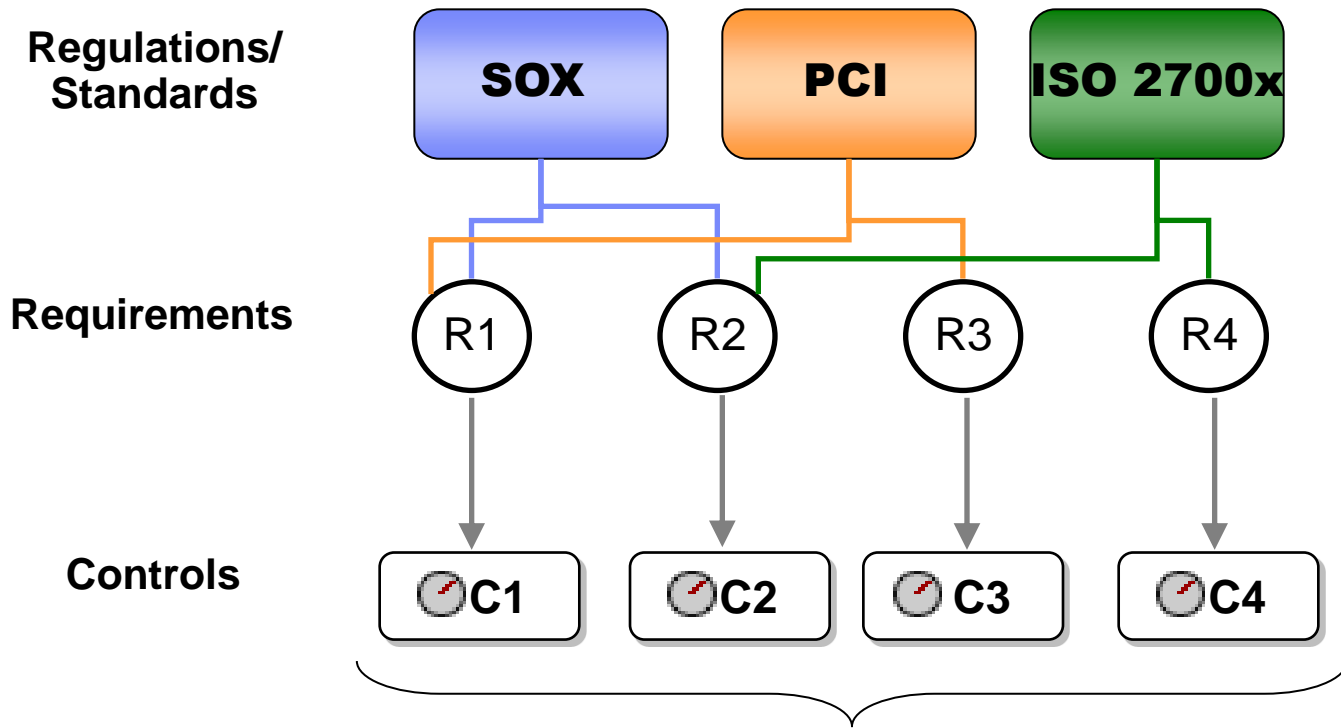
HIPAA Security Rule

- Implement appropriate **security measures** to address the risks identified in the risk analysis;
- Maintain continuous, reasonable, and appropriate **security protections.**

Example: Managing regulatory requirements in a silo

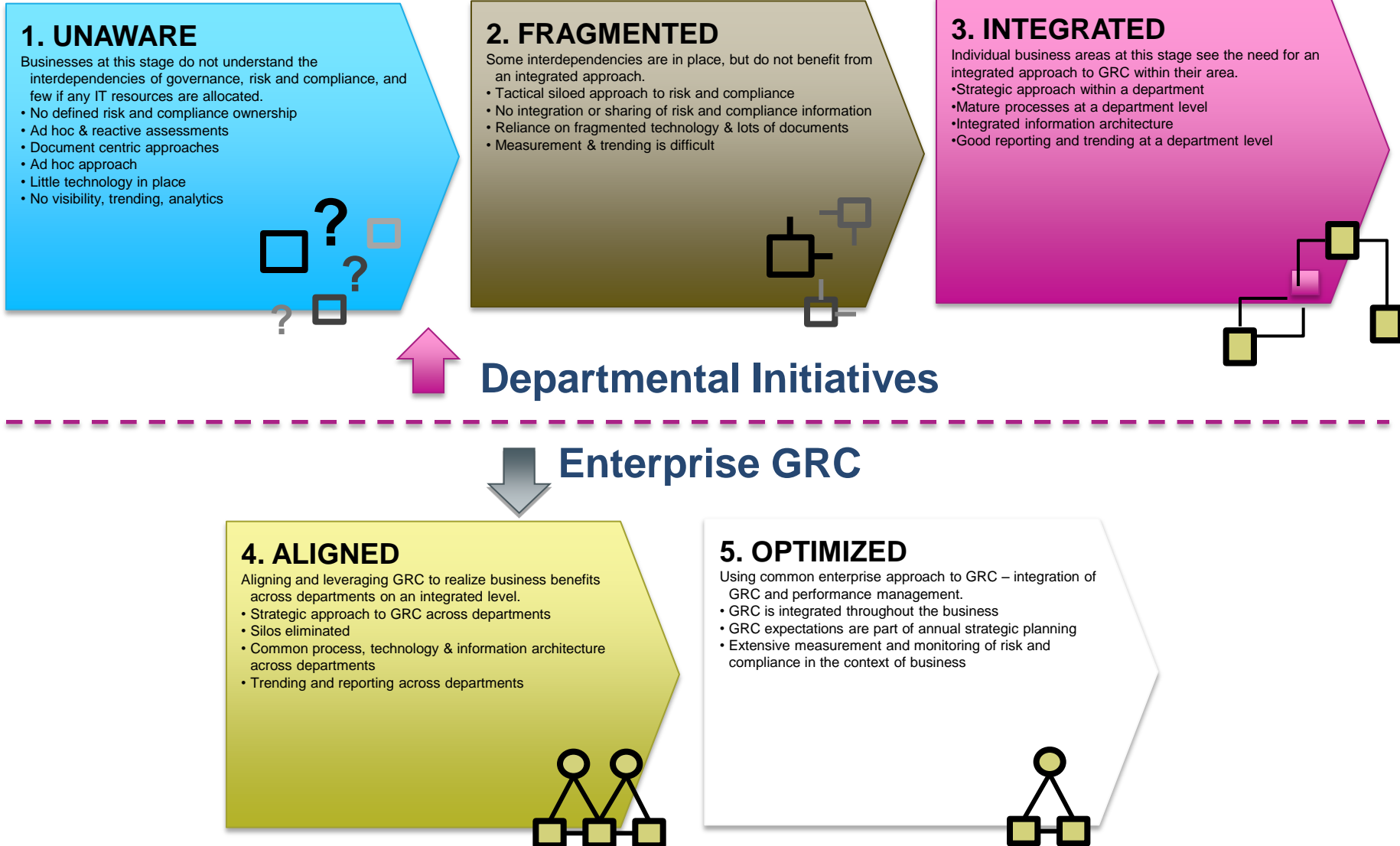


An integrated approach reduces redundancies in control testing, assessments and audits

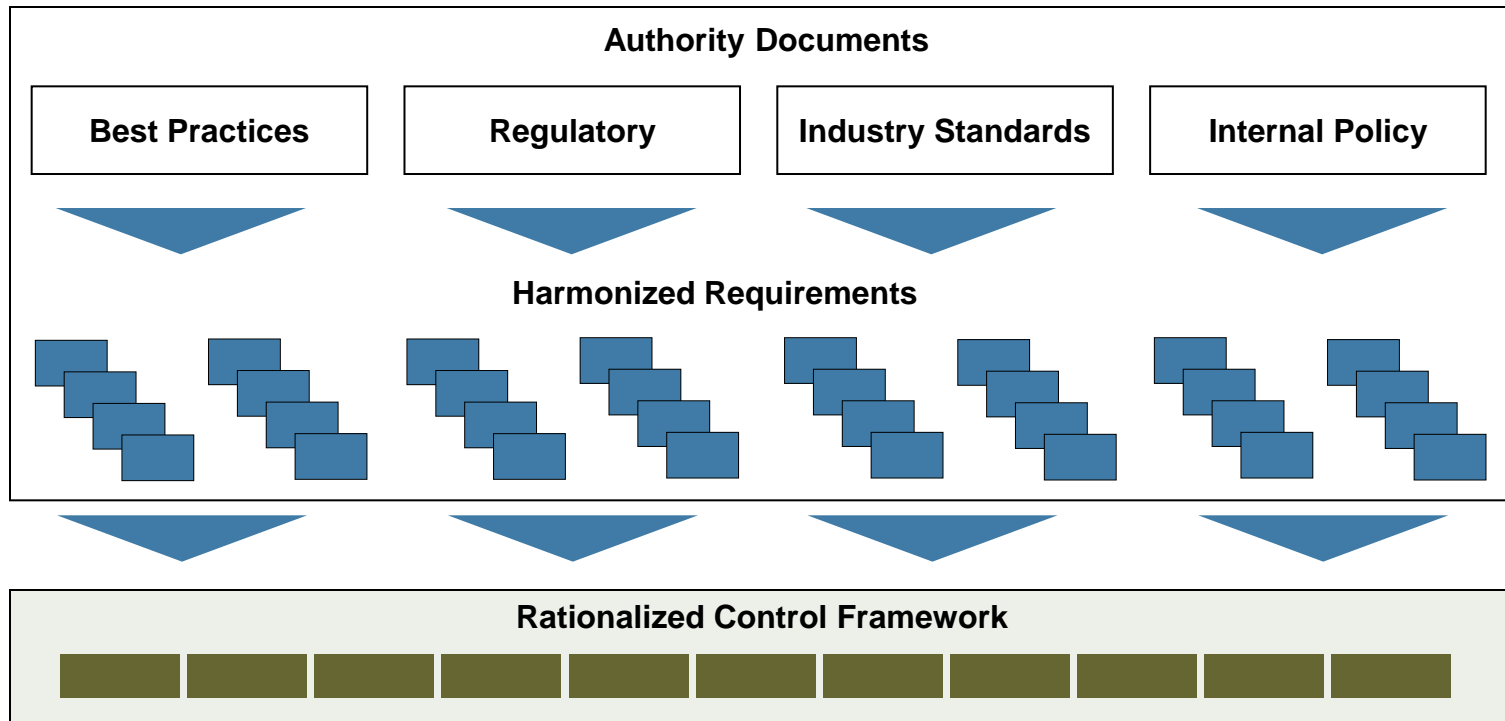


- Control testing
- Assessments
- Audits

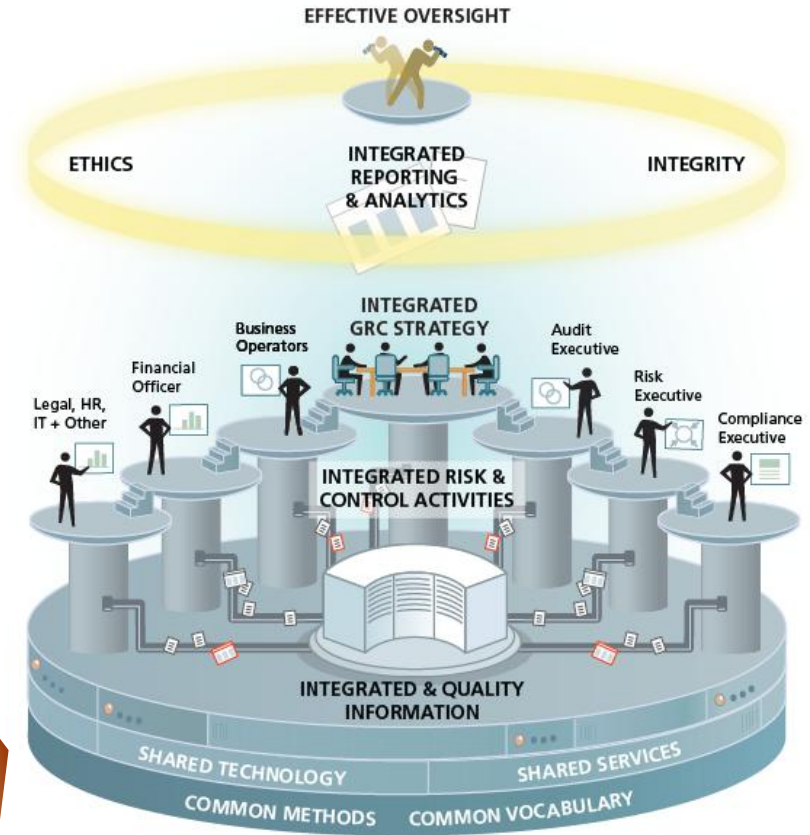
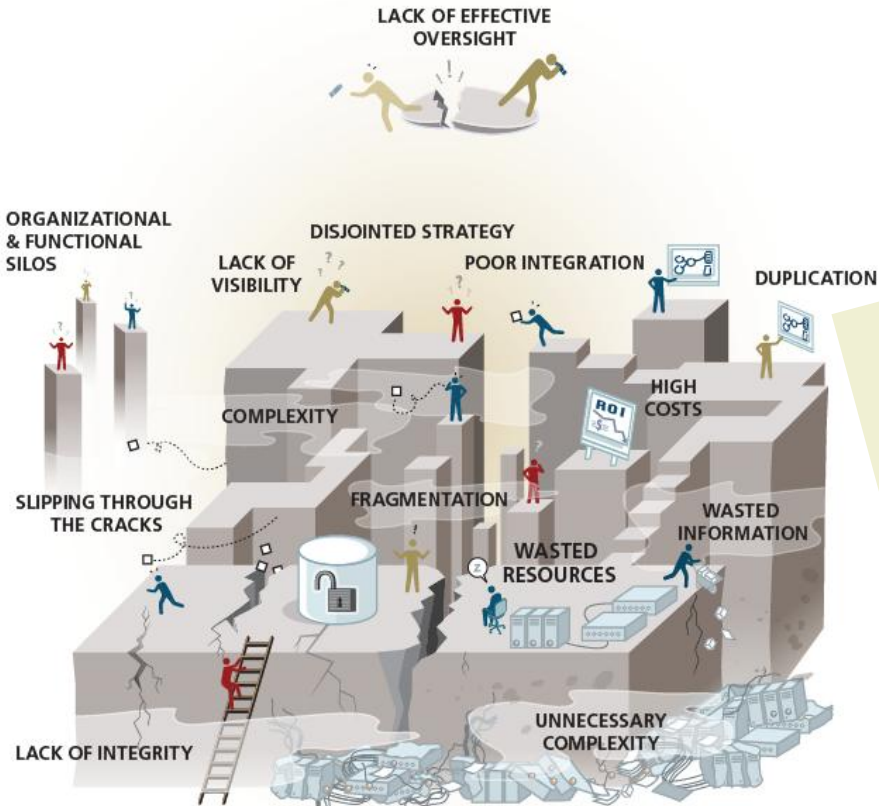
GRC Maturity Model – What Level is Your GRC Program?



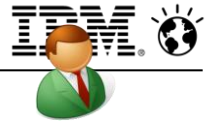
The integrated approach harmonized directives, best practices and policies for a rationalized control framework



GRC is a transformational opportunity



¹⁰ Source: *GRC Maturity: From Disorganized to Integrated Risk and Performance*, Corporate Integrity, 03/12

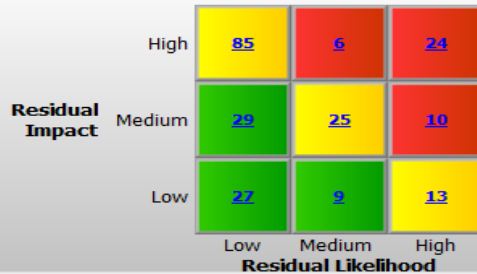


Executive View: ERM Dashboard

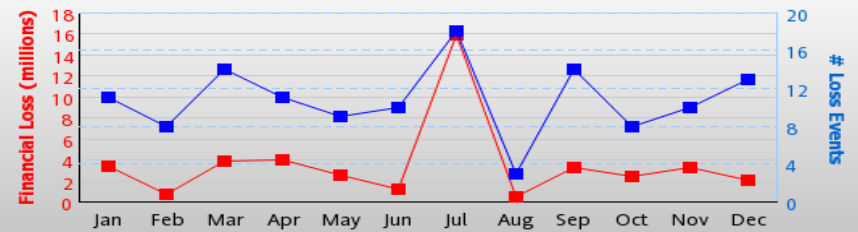
Key Risks

Name	Description	Residual Risk					Control Env	Open Critical Issues	Audit Rating
		10 Q1	10 Q2	10 Q3	10 Q4	Trend			
NA-CB-ERM-RSK-01	Failure to implement core client conversion (onboarding)	Medium	Medium	Medium	High		Needs Improvement	> 5	Medium
NA-CB-ERM-RSK-02	Failure to deliver services that meet the low risk tolerance of clients	Medium	Medium	Low	Low		Satisfactory	> 5	Low
NA-CB-ERM-RSK-03	Failure to establish robust internal control and governance structure	Medium	Medium	Low	Low		Satisfactory	> 5	Low
NA-CB-ERM-RSK-04	Failure to properly diversify product offerings and client base	Medium	Medium	Medium	High		Needs Improvement	> 5	Medium
NA-CB-ERM-RSK-05	Failure to retain and develop talented employees	Low	Low	Medium	Medium		Satisfactory	> 5	Medium

Risk Heat Map



2010 Internal Loss Amount & Count



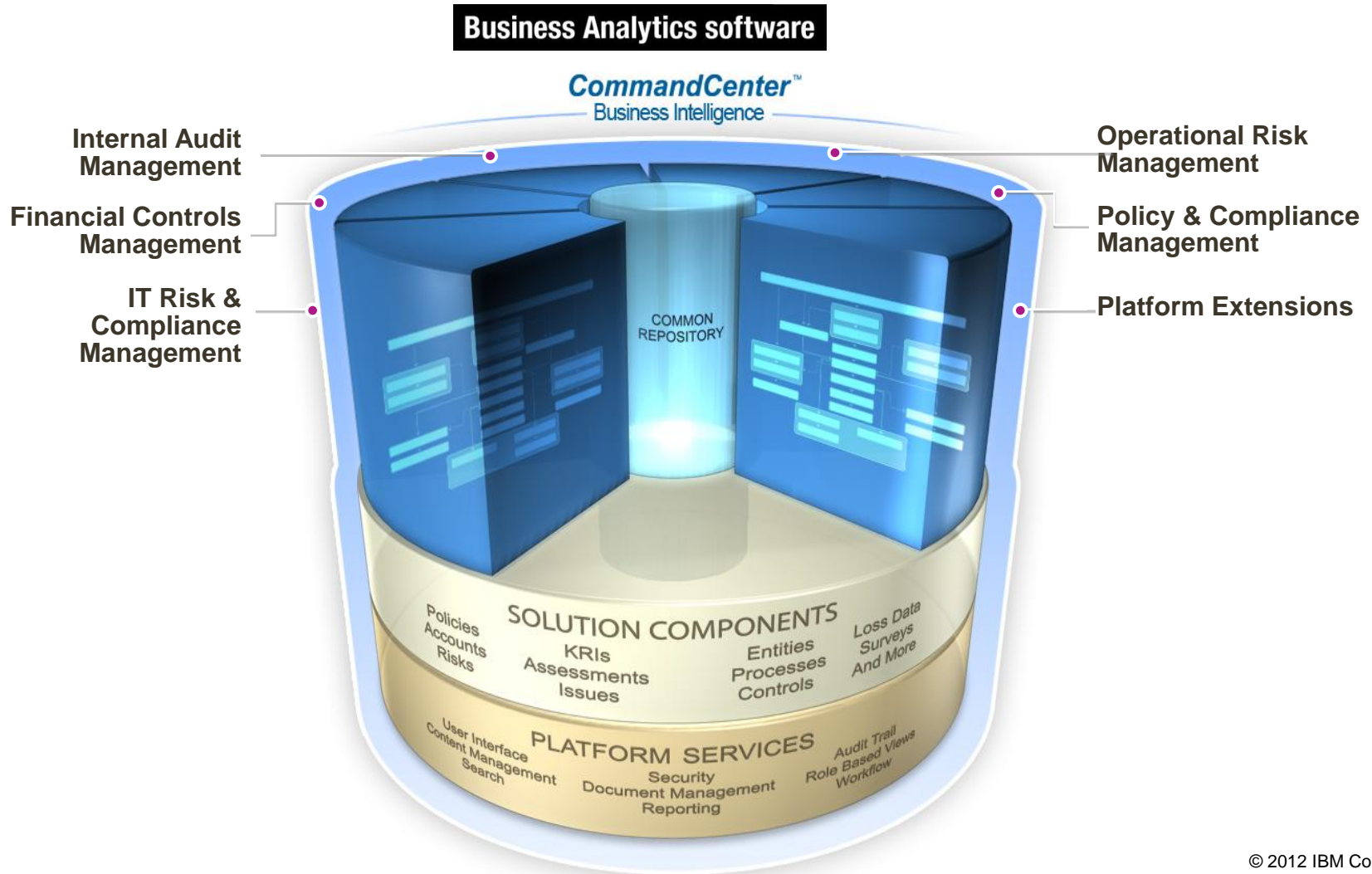
Mandate Control Effectiveness



Issue Status

		High	Medium	Low	Not Determined
Asia Pac	Closed	0	1	2	1
	Open	0	2	0	0
Corporate	Closed	0	1	1	0
	Open	2	2	1	3
EMEA	Closed	3	5	3	1
	Open	0	0	0	2
North America	Closed	1	4	4	4
	Open	11	2	0	3

IBM OpenPages GRC Platform integrates key operational risk and compliance functions



Proven by the World's Leading Companies

Financial Services



Insurance



Manufacturing



Retail/Consumer



Energy and Power



Telecommunications



Health Services / Pharmaceuticals



Allianz case study

Reducing complexity while improving communication and governance around risk



Business Challenge

- Allianz has 22 operating companies in 70 countries reporting directly into the risk function in Munich
- Need to prepare for compliance with Solvency II but also to look beyond this to best practice in the industry
- Need to satisfy regulatory requirements from multiple countries made it difficult to implement an operational risk framework
- Need to standardize methodology and processes to reduce complexity

Solution

- Allianz implemented a single, integrated solution for operational risk including scenario analysis, KRI's and capture evidence

Outcome

- Improved standardization of processes across the group
- Reduced the regulatory burden
- Better depth of information
- Audit trail and documentary evidence, less frequent audits
- Better and easier consolidation of information

Barclays case study

Integrated Operational Risk and Financial Controls Management



Business Challenge

- Barclays operates in over 50 countries, employs 147,000 people, and serves over 42 million customers and clients worldwide
- The company had multiple assessments and reports for risks and controls in Operational Risk and Sarbanes-Oxley, which limited reporting options and resulted in high operating costs
- The company was also looking to align their systems to a common risk management framework, a strategic goal for the company

Solution

- Barclays implemented a single, integrated solution for operational risk and financial controls management, which was highly configurable to meet needs of business
- Implemented across UK, Continental Europe, United States Africa, Asia—Over 10,000 users worldwide

Outcome

- Having access to this kind of data on one platform allows the firm to gain a better overall picture of where the risks lie in the entire organization
- Added benefit of saving time and resources in the individual business lines

Analysts...

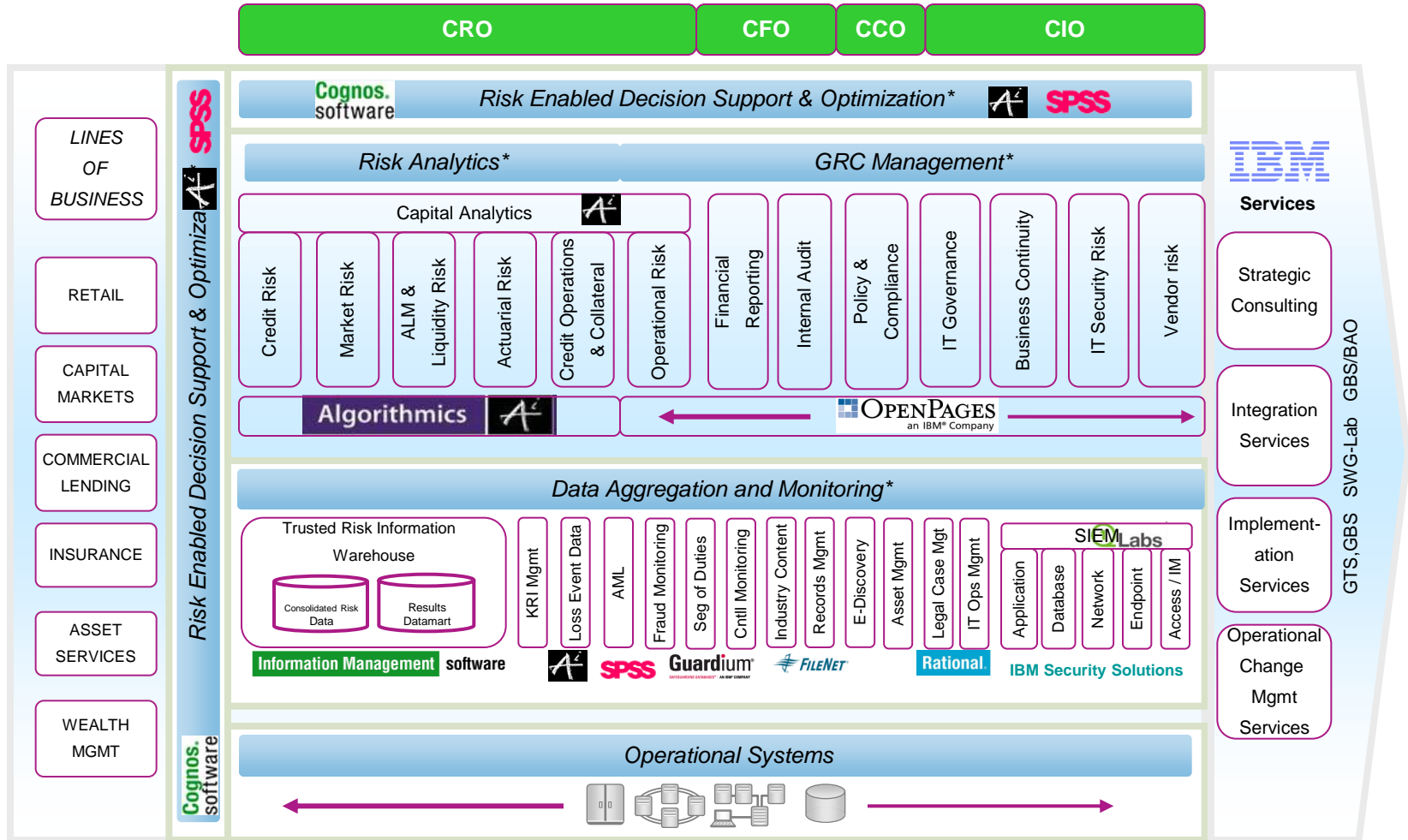


RiskTech100[®] 2011

Rank 2011	Rank 2010	Company	HQ	Total Score	Functionality	Core Technology	Organizational Strength	Customer Satisfaction	Market Presence	Innovation
1	7	IBM	US	69.8%	79%	73%	65%	63%	72%	67%
2	1	SunGard	US	66.8%	76%	63%	70%	60%	71%	61%
3	2	SAS	US	65.8%	77%	74%	63%	58%	62%	61%
4	9	Oracle	US	63.3%	70%	72%	61%	57%	60%	60%
5	6	Moody's Analytics	US	62.5%	61%	64%	64%	62%	62%	62%
6	8	Wolters Kluwer FS	US	62.0%	63%	56%	69%	61%	63%	60%
7	17	Misys	UK	61.7%	68%	59%	62%	59%	62%	60%
8	4	Fiserv	US	61.3%	62%	58%	69%	63%	61%	55%
9	5	MSCI	US	61.3%	59%	53%	69%	63%	63%	61%
10	12	NICE Actimize	US	60.3%	60%	59%	62%	58%	61%	62%

IBM Risk Management, C-Suite Solution Domain Summary

Financial Services Industry View



* representative solutions

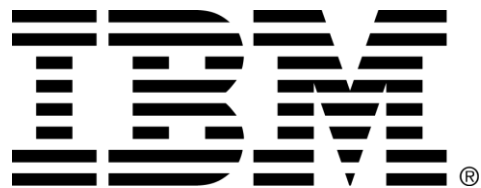
Better Business Outcomes with GRC

Lower costs, reduce redundancy and improve efficiencies by rationalizing your information architecture

Deliver **consistent** and **accurate** information about the state of risk and compliance initiatives to assess exposure

Improve **decision making** and **business performance** through increased insight and business intelligence





Trademarks and notes

IBM Corporation 2012

- IBM, the IBM logo, ibm.com, OpenPages, are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), these symbols indicate US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)” at www.ibm.com/legal/copytrade.shtml.
- Other company, product, and service names may be trademarks or service marks of others.
- References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.