Silvano Palazzi
IBM – Risk & Analytics Leader

Governare il rischio e gestire i processi di controllo.

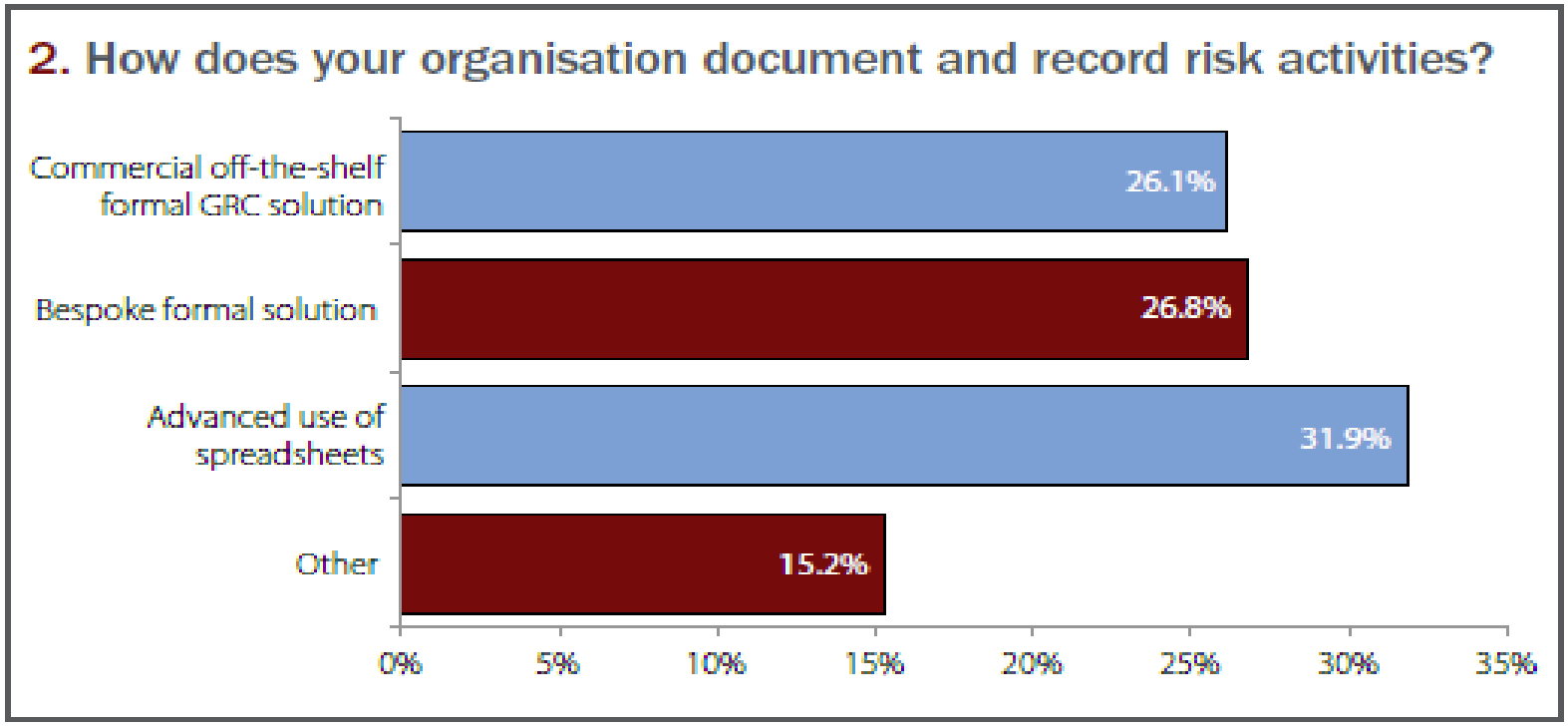
Aspetti di collaborazione tra efficienza ed efficacia.

Governance Risk and Compliance - IBM survey 2014

✓From 135 responses to the question it was revealed that **implementing regulatory demands,** improving risk management and **modelling**, and **aligning** the risk function **with the firm's overall business strategy** are top priorities.

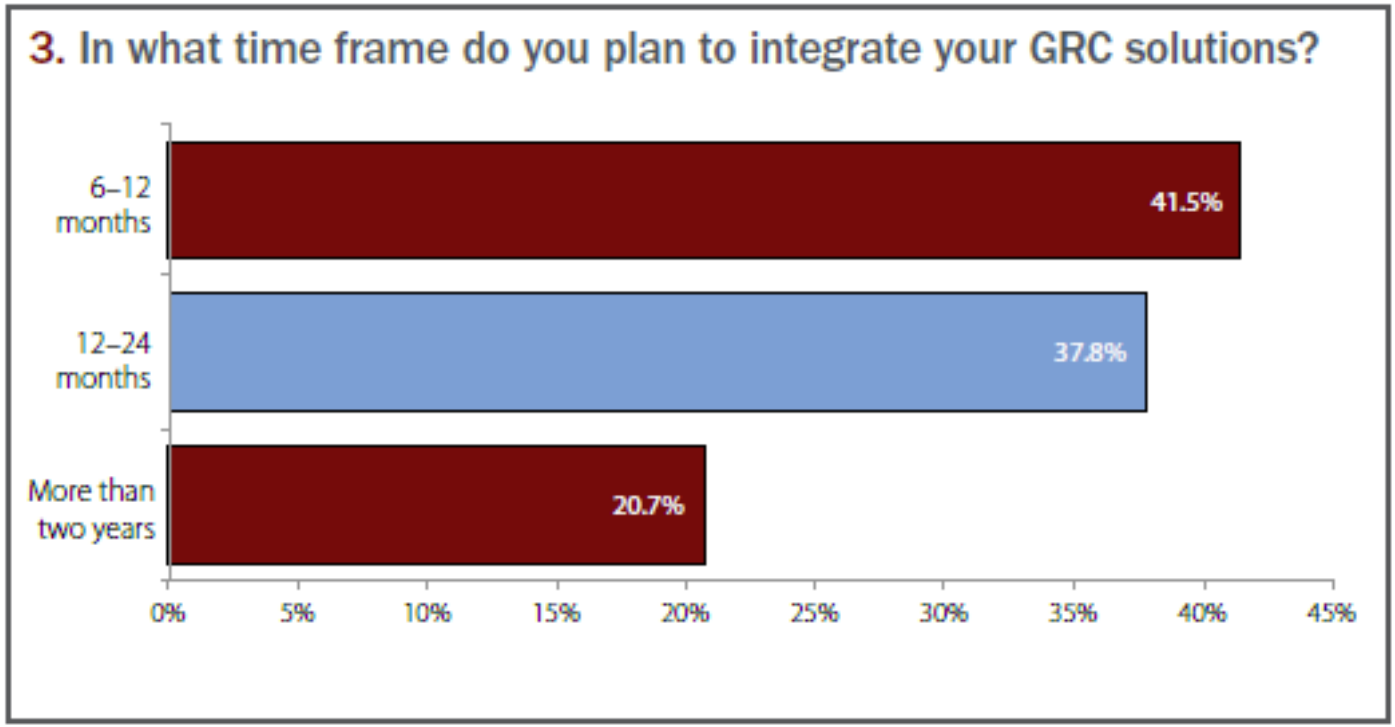
Governance Risk and Compliance - IBM survey 2014

✓The survey reveals that, out of 141 firms, almost **one-third still rely on spreadsheets** for their risk recording and documentation.



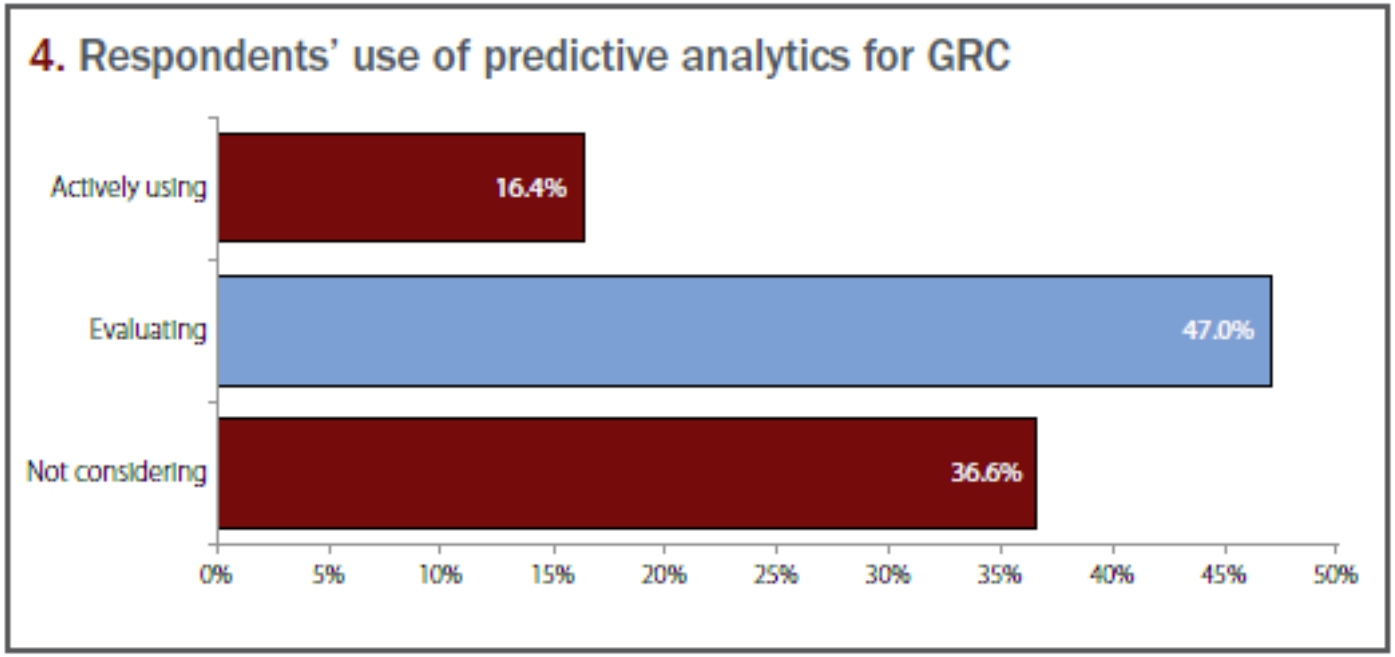
Governance Risk and Compliance - IBM survey 2014

- ✓Where a GRC solution can really **add value is through integration** of line-of-defense and business-as-usual (BAU) systems.
- ✓Understandably, **integrating GRC is a priority for many firms**. Of those saying they are planning on integrating, 41.5% intend to do so within 12 months, with a further 38% scheduling it sometime in the next two years



Governance Risk and Compliance - IBM survey 2014

- ✓Arguably the most **valuable benefit, however, lies** in the suite of **predictive analytics** offered through an advanced integrated GRC architecture.
- ✓The survey reveals that only 16% of firms are actively using predictive analytics, with more than 36% not considering their use at all.
- ✓These percentages may reflect firms' level of engagement with their GRC projects and the level of maturity of their GRC Architecture



The following is a summary of the key principles of highly effective GRC programs across a sample of 350 projects.

The 8 Principles of GRC Convergence

8. Principles of GRC Convergence

"Where a GRC solution can really add value is through integration of line-of-defense and business-as-usual (BAU) systems."

Operational Risk Management
Identify, manage, monitor, and analyze operational risk across the enterprise in a single integrated solution

IT Governance
Build and maintain a sustainable IT risk and compliance approach to meet the challenges posed by sensitive data, managing technology assets, and evolving regulatory requirements

Policy and Compliance Management
Consolidate the policy and compliance management process in a single solution and manage regulatory change and regulator interaction

Financial Controls Management
Provide transparency into the state of financial controls and assurance that compliance demands are being met

Internal Audit Management
Enable internal auditors to automate and manage intraorganizational audits and leverage broader risk and compliance management activities

8. Principles of GRC Convergence

Principle 1: Resist "one size fits all" approach

✓GRC, similar to most business functions, is not a "one-size-fits-all" solution. It has to be tailored adapted for each firm and each business unit.

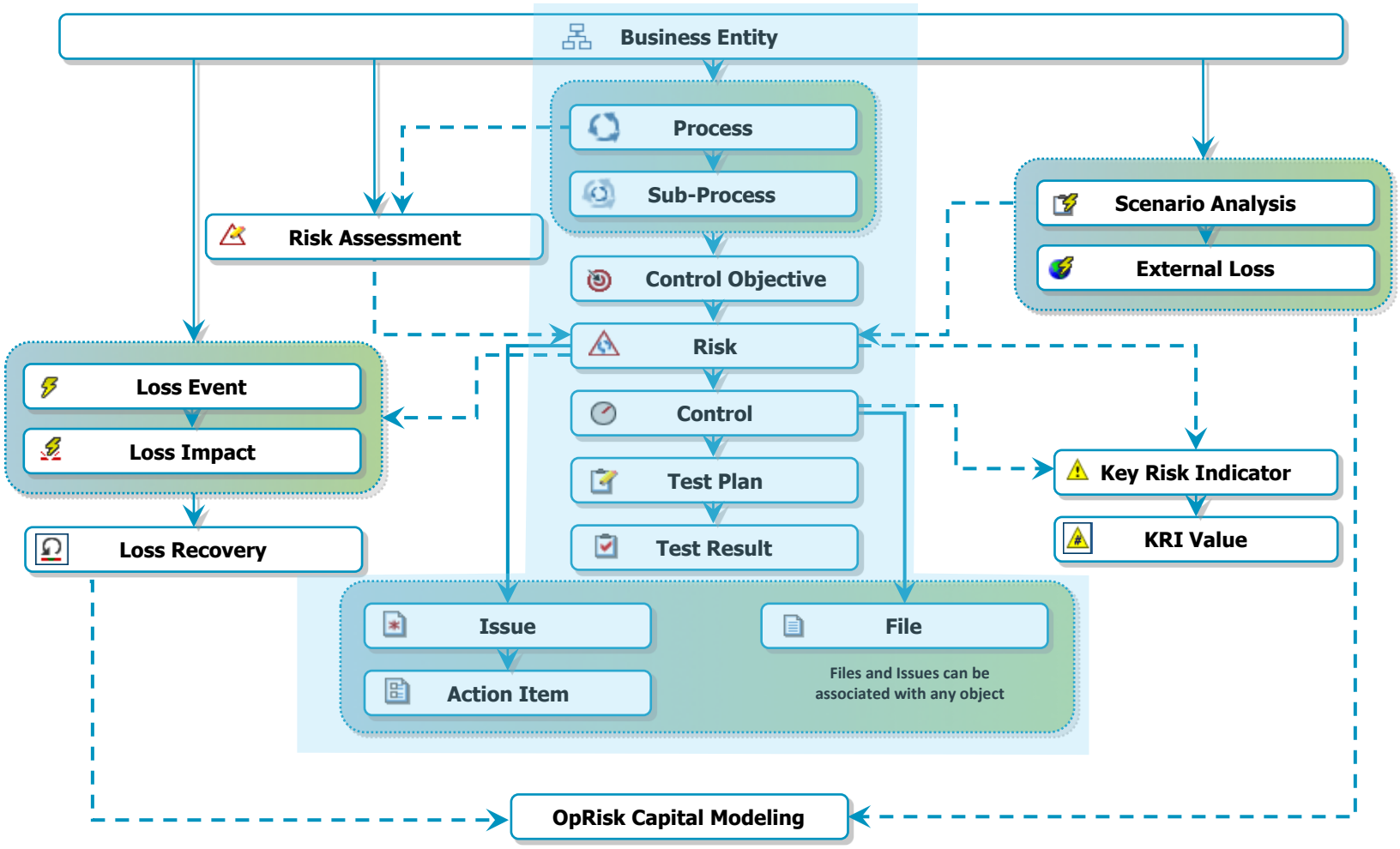
✓While most leading companies have tailored their risk methodologies to match their business operations, it is imperative to select a solution architecture that can easily **adapt to your firm's unique risk and compliance methodology** and evolve gracefully over time.

✓The key business benefits include:

- **Lower costs** much easier to maintain and extend over time.
- **Time to deployment** and support rapid implementation
- **Future proofing** will allow you to quickly adapt your risk framework to meet changing requirements while minimizing the impact on your business operations.

8. Principles of GRC Convergence:

1. Resist "one size fits all" approach: Operational Risk - Object Model



8. Principles of GRC Convergence

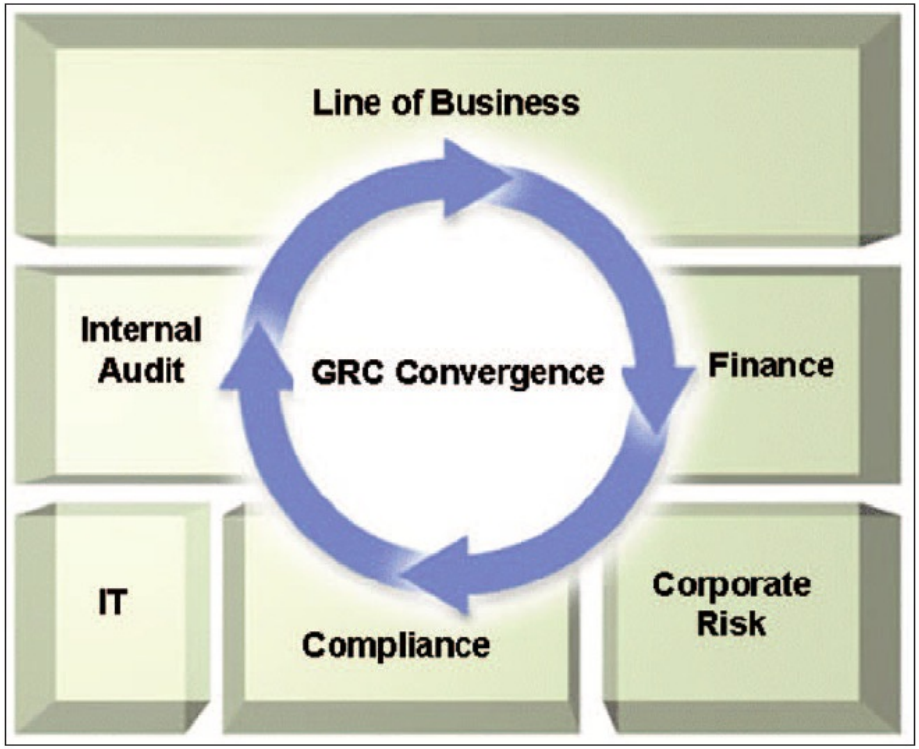
Principle 2: Converge should enable you to "Assess once and satisfy many"

- ✓By **eliminating risk and compliance management silos** and harmonizing risk and compliance activities you can reduce the burden on the business lines, avoid "assessment fatigue" and free up resources to focus on business goals.
- ✓To achieve a holistic view of risk across the business your firm will need to **establish a "common language"** for risk activities, which involves creating a rating methodology for all risk data, such as loss events, risk assessments, and key risk indicators (KRIs).
- ✓The approach should be **based on a common repository for all GRC elements** including frameworks, risk and control libraries, policies and procedures, and other elements of your risk rating methodology.
- ✓By implementing a single assessment and sign-off process you can **eliminate duplicated and redundant activities.**

8. Principles of GRC Convergence

Principle 3: Convergence requires collaboration and coordination

- ✓This comprehensive approach requires **integrating risk** and compliance management processes **across the different functional and business groups.** The key players are shown in the figure.
- ✓The technology solution should enable the unification of your GRC initiatives within a "single vision of the truth" (**"common language"**)
- ✓**Workflow** is a critical factor in helping **to coordinate the activities** of the different functions.



8. Principles of GRC Convergence

Principle 4: Convergence requires a cultural change

✓Successful GRC convergence requires a culture change that is driven by leadership from the top, and technology can be an important lever.

✓Some of the key goals for cultural change should include:

- Making risk management a part of **everyday business activities**
- **Empowering people** by making everyone in the company a risk manager
- Providing **risk information that is actionable**

✓Technology can help to build **accountability** and distribute **GRC ownership** into lower levels of the organization.

✓Automated risk processes can facilitate training and **awareness** and help to engage business users by **providing actionable information**

8. Principles of GRC Convergence

Principle 5: Risk management must be actionable

✓GRC information should be communicated up, down and across the organization, so reporting is a critical component for making risk data actionable.

✓To support decision making and action, communication needs to be timely, accurate and flexible

✓It key to shift the paradigm:

From “user has to navigate through the system to find the relevant data” vs “user can easily pull together the right data into a single view that supports the activity **prescribed**.”

✓The approach should be able to:

- Route risk and compliance activities to the right people at the right time.
- Monitor risk and compliance activities and track subsequent actions.
- Establish triggers and points of escalation so that responsible managers are notified and aware when action is required.
- Notify managers when identified action is not taken.

8. Principles of GRC Convergence

Principle 6: Assume risk is everywhere and make it the focal point

✓To adequately understand risk within multiple disciplines you need to be able to **assess risk to multiple GRC elements**.

- Does the framework force a single view of risk; for example, is it process-centric in that it associates risk only to processes?
- Can risk be associated to multiple GRC elements such as entities, processes, policies, accounts and regulations?
- Can risk be categorized at multiple levels using multiple taxonomies, for example Basel II (3 levels), COSO, or your own categorization scheme?
- Can risk be assessed at the different levels of granularity, for example multiple levels in the business entity or process hierarchy?
- Can losses be linked to risks to determine how risk exposure is trending versus actual losses?.

8. Principles of GRC Convergence

Principle 7: Risk convergence is evolutionary not revolutionary

- ✓Your risk and compliance **methodologies will change over time** as your GRC framework evolves and best practices mature.
- ✓ In addition, **your organization will change** due to reorganizations, mergers, acquisitions and divestitures.
- ✓You should **expect to evolve your best practices** and change your risk management methodology over time.
- ✓If your GRC architecture cannot respond quickly to changes in best practices or changes in your business, you will end up with a solution that does not reflect the realities of your business practices and does not meet the requirements of your users.

8. Principles of GRC Convergence

Principle 8: Make business process management a priority

✓Good risk management is a natural outcome of good process management. An organization with well-managed business processes will be less subject to breakdowns, errors, and other forms of GRC risk.

✓BPM is a relatively mature discipline, with proven tools to ensure effective management and control, but it requires an appropriate degree of rigor. The key elements to focus on include:

- Clear accountabilities
- Process objectives/requirements
- Control design and improvement
- Monitoring and measurement

✓Firms should also focus on standardization of key processes This can streamline GRC activities since risk and control frameworks will not have to be re-invented for key processes in every organization.

✓ This will simplify risk assessments and the aggregation of risk measurement

Opportunity for Efficiency through Convergence

	Compliance	ORM	Strategic Risk	Sox	Policy	Audit	IT Risk	Spreadsheets	Other
Governance									
Strategic Oversight			X						X
Internal Policy Development			X		X				X
Policy Management					X				X
Requirements Management	X			X					
Mapping Regulations to Policy	X			X					
Training					X				X
Risk Management									
Risk Identification	X	X		X		X	X	X	
Risk Assessment	X	X	X	X		X	X	X	
Risk Mitigation/Response	X	X		X			X	X	
Mapping Requirements to Risks	X			X				X	
Key Controls, Testing	X			X		X	X	X	X
Loss events	X	X					X	X	X
Issues Management		X				X	X	X	X
Capital Modeling		X						X	
Compliance									
Compliance & Policy Reporting	X	X		X	X		X	X	X
Risk Tracking, Monitoring & Reporting	X	X		X			X	X	X
Control Tracking, Monitoring & Reporting	X			X		X	X	X	X
Metrics/KRIs	X	X		X	X	X	X	X	X
Board Level Reporting	X	X	X	X	X	X	X	X	X

Multiple x's = possible optimization

Control optimization benefit calculation example

Number of controls tested in organization	1,200
Time per control (hours)	6
Percentage overlap in control testing	25%
FTE cost per hour	$96 (Based on $192,000 fully loaded /2000 hours)
Productivity correction factor	.7
Total Savings	$120,960

- ✓Many regulation have common requirements. An integrated approach reduces redundancies in control testing, assessments and audit.
- ✓Remove dependency on Excel to manage controls it could be assessed once and complying many times.
- ✓"With integrated approach we moved from having 1,400 SOX controls to 750 by identifying key controls."

It's the Analytics that drives Business Value to GRC

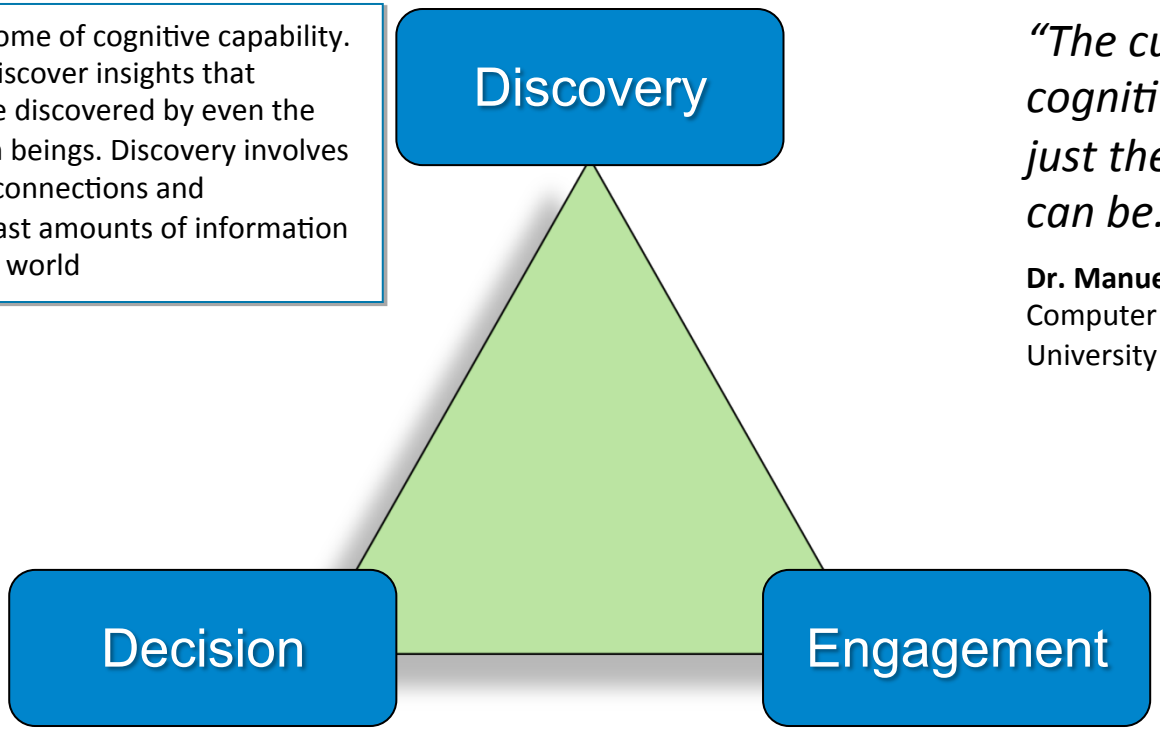
While data has become the new natural resource..

Cognitive	*Cross correlation of regulations against common requirements*	Cognitive
Stochastic Optimization	*Hedging risk for corporate bond holdings*	Prescriptive
Optimization	*Optimized investment allocation for portfolio*	
Modeling	*Highest returning portfolio based on risk appetite*	Predictive
Simulation	*Impact on new regulation or process reengineering*	
Forecasting	*Risk trending analysis vs benchmark*	
Alerts	*Unusual Loss Events , KRI breaches*	
Analysis	*Risk concentration and dependencies*	Descriptive
Discovery	*Suspicious risk trends comparing current vs previous month*	
Reporting	*Periodic Risk results*	

Cognitive computing capabilities

There are three emerging capability areas for cognitive computing ..

Discovery is the epitome of cognitive capability. These systems can discover insights that perhaps could not be discovered by even the most brilliant human beings. Discovery involves finding insights and connections and understanding the vast amounts of information available around the world



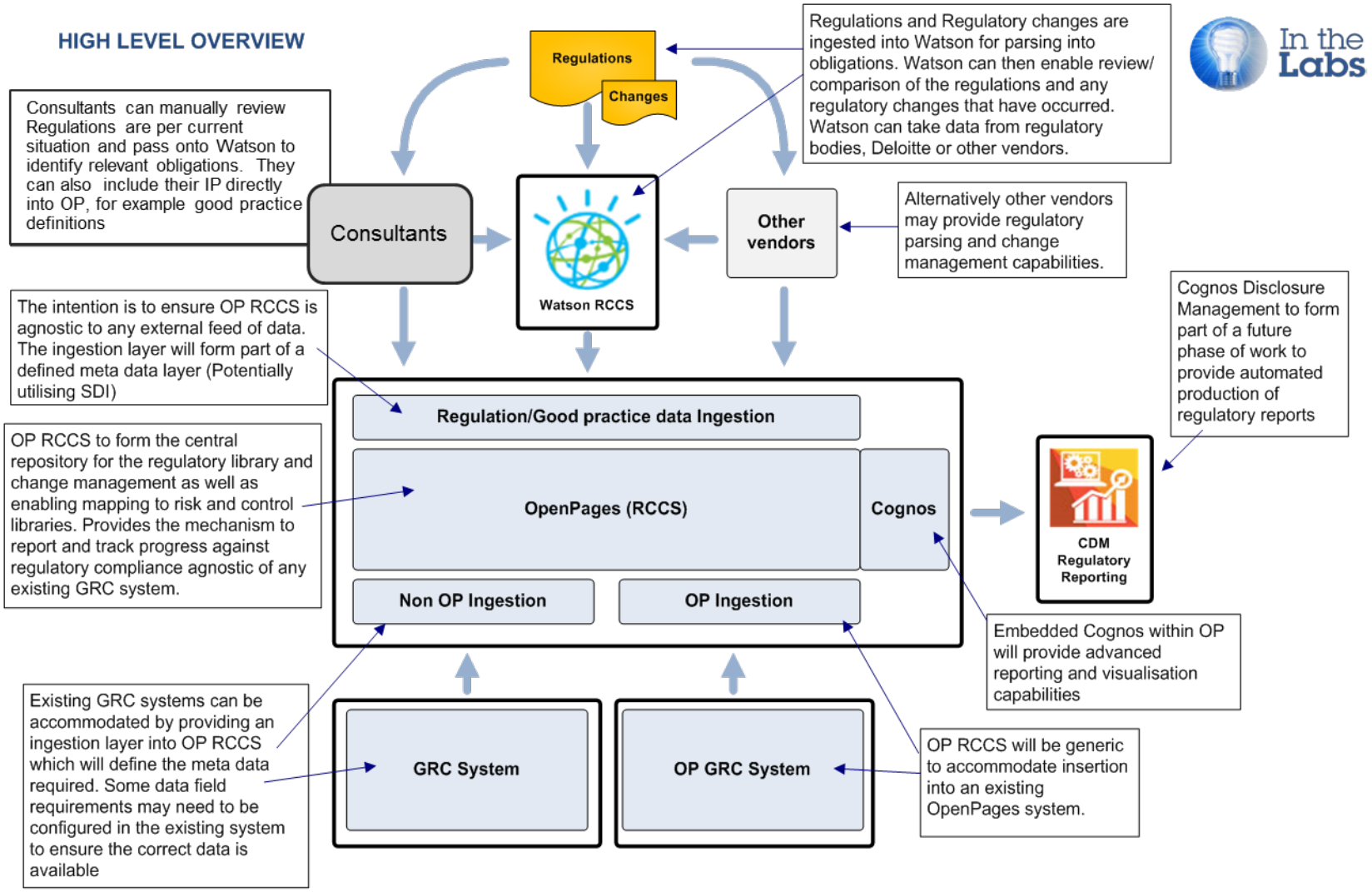
"The current capabilities of cognitive computing are just the beginning of what can be."

Dr. Manuela Veloso, Professor of Computer Science, Carnegie Mellon University

Decisions made by cognitive systems are evidence-based and continually evolve based on new information, outcomes and actions. Decisions made by these systems are also bias free; however, certain standards are required for humans to fully trust their decisions.

These systems fundamentally change the way humans and systems interact and significantly extend the capabilities of humans by leveraging their ability to provide expert assistance and to understand.

Discovery capabilities applied to GRC - high level overview



Silvano Palazzi
mail: s.palazzi@it.ibm.com