



XBRL & GRC

Future opportunities?

Suzanne Janse – Deloitte NL

Paul Hulst – Deloitte /
Said Tabet – EMC

STILL HAVEN'T FOUND WHAT
YOU'RE LOOKING FOR?
HARNESS THE POWER OF
JOINED UP BUSINESS REPORTING

HOSTED BY XBRL IRELAND

Presenters



Suzanne Janse

- Deloitte Netherlands – Director
- ERP (SAP, Oracle) Risk Management
- GRC software



Paul Hulst

- Deloitte Innovation – Manager
- Senior XBRL expert



Content

- What is GRC (Governance, Risk & Compliance)?
 - GRC context & challenges
 - GRC automation with software
- GRC-XML: What is it?
 - Business Case for XBRL
 - The taxonomy
 - Specific areas of focus and use cases



Governance, Risk and Compliance (GRC)



Content

- What is GRC (Governance, Risk & Compliance)?
 - GRC context & challenges
 - GRC automation with software
- GRC-XML: What is it?
 - Business Case for XBRL
 - The taxonomy
 - Specific areas of focus and use cases

Definition GRC



Governance, Risk management and Compliance is the umbrella term covering an organization's approach across these three areas.

i.e. activities such as corporate governance, Enterprise Risk Management (ERM), Internal Control and Compliance with applicable laws and regulations.

Management challenges – Compliance

- Meeting regulation and legislative requirements (e.g. SOX, PCI DSS, DPA, FDA etc.)
- Demonstrating adoption of common practices (e.g. ISO, ITIL, COBIT, etc.)
- Tackling a variety of internal practices (e.g. policies, procedures, standards etc.)
- Interacting with internal compliance and assurance functions
- Interacting with third party assurance providers

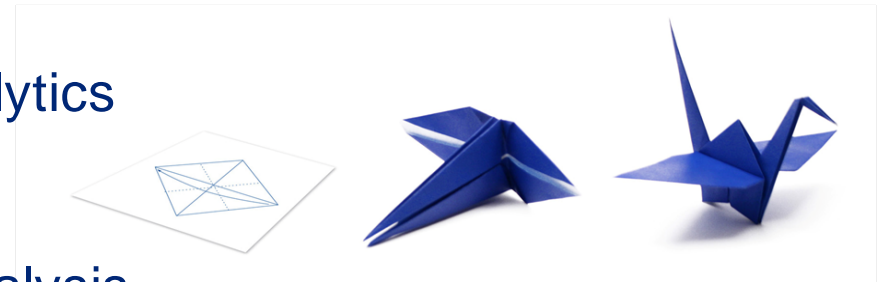


Management challenges – Excessive costs

- Duplication of effort due to a lack of a single source of business risk and control requirements
- More cost and time are required to de-conflict the standalone processes, tools and data
- Managing to worst case scenario; no credit for compensating controls
- Higher costs and extra work required for compliance – What is minimum necessary and why?

Management challenges – Poor Quality & Ineffectiveness

- Organizational functions view the requirements, operating environment, risks and controls differently
- Audit, Compliance, Security, Privacy, Business Continuity, IT Risk and third-parties use different processes and tools that produce different results
- “Compliance” is often confused with “Risk”
- Compliance is arbitrary and businesses are not provided risk-based options
- Inconsistent reporting of risk
- Inability to perform trending and analytics
- Inconsistent metrics and criteria
- Lagging indicators, not predictive analysis



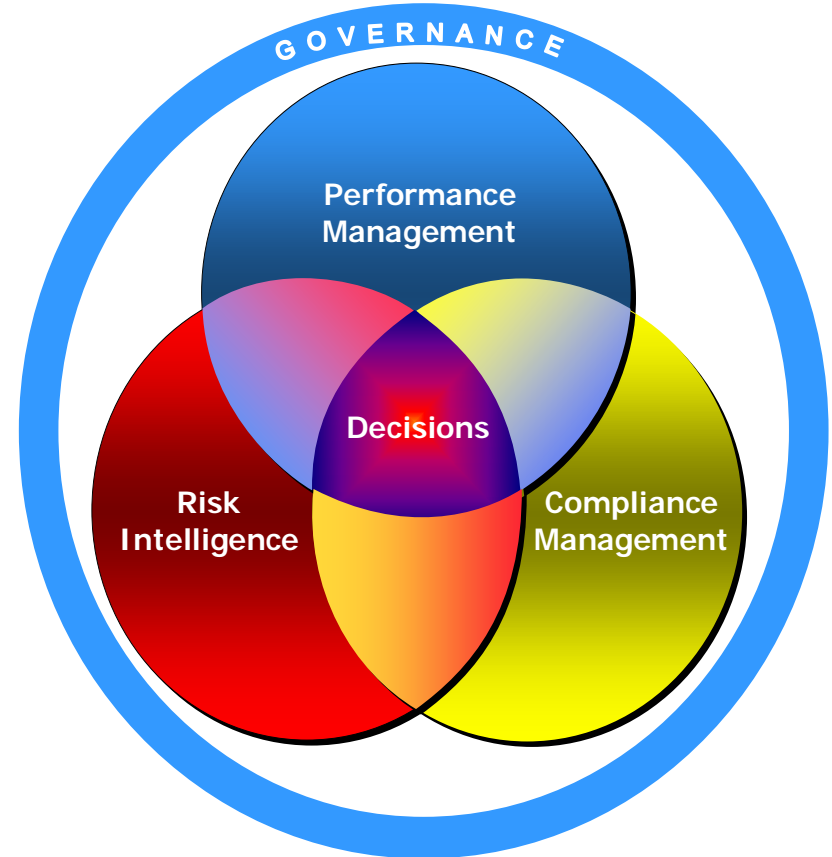
Market drivers

- Need to drive consistency of approach to compliance
- Increase the efficiency in achieving compliance
- Provide sustainability in a changing environment
- Demonstrate transparency on risk and control decisions made
- Reduction in costs related to testing and compliance
- Reduce reliance on spreadsheets for tracking compliance programs



GRC enables integration of company silo's

- The fundamental idea – GRC must be viewed comprehensively and integrated with performance management
- GRC no longer be separate from other strategic objectives
- Common information, processes, controls, and systems must be leveraged to simultaneously improve the effectiveness of decisions and produce significant efficiencies and cost savings
- Overcome disparate data and the inertia of “silos”




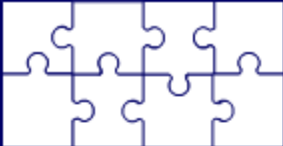
Linking pin between control initiatives



Enabling..

- Consistent and clear roles and responsibilities
- Integral part of planning and control cycle
- Central risk and control repository
- Integration of management reporting
- One “all comprehensive” framework

GRC benefits – Potential operating improvements

Before 	Operating Improvement	 After
847 reporting entities	Reduced Complexity	162 reporting entities
10's of profiles per configuration item	Consistent Risk & Controls	1 profile per configuration item
100's of hours – spreadsheets	Automated Workflow	10's of hours – technology platform
No trending and slow reporting	Streamlined Reporting	Trending and rapid reporting
100% control testing	Optimized Sampling	Country level sampling
Multiple approaches	Formal Risk Method	Single approach
Best Practices “Piling On”	Traceable Requirements	Linked to Authoritative Sources

GRC software

- Facilitates
- Streamlines processes
- Supports integrated reporting
- Enables automated testing
- Introduced the concept of continuous monitoring



ERPScan
Security Scanner for SAP

approva.

ControlPanel **GRC**

onapsis **x1**
The ERP Security Suite

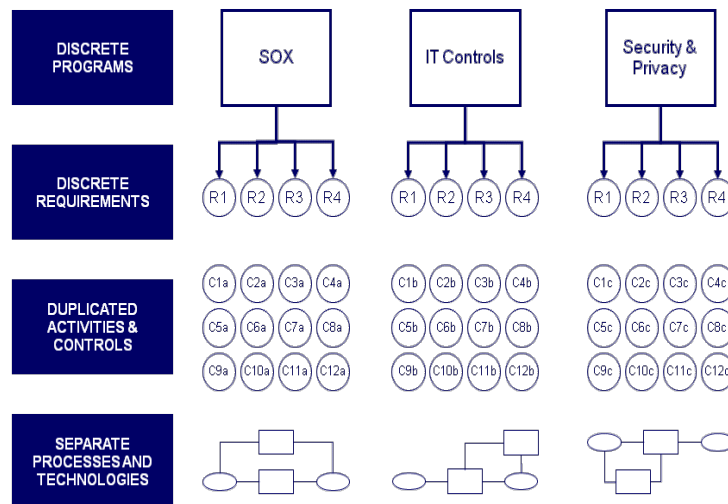


THOMSON REUTERS

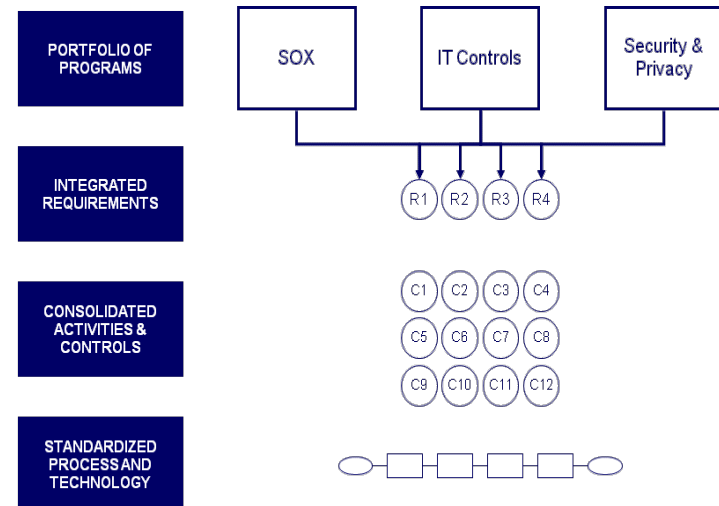
Value Driver 1: Enterprise Compliance

The integration of multiple compliance frameworks allows for a single control to serve multiple regulatory or policy demands

Overlap



Harmonized



Value Driver 2: End-to-End Risk Management



Better Efficiency

- Automate manual and fragmented risk and control activities across all lines of business
- Align risk management activities with corporate planning and strategy

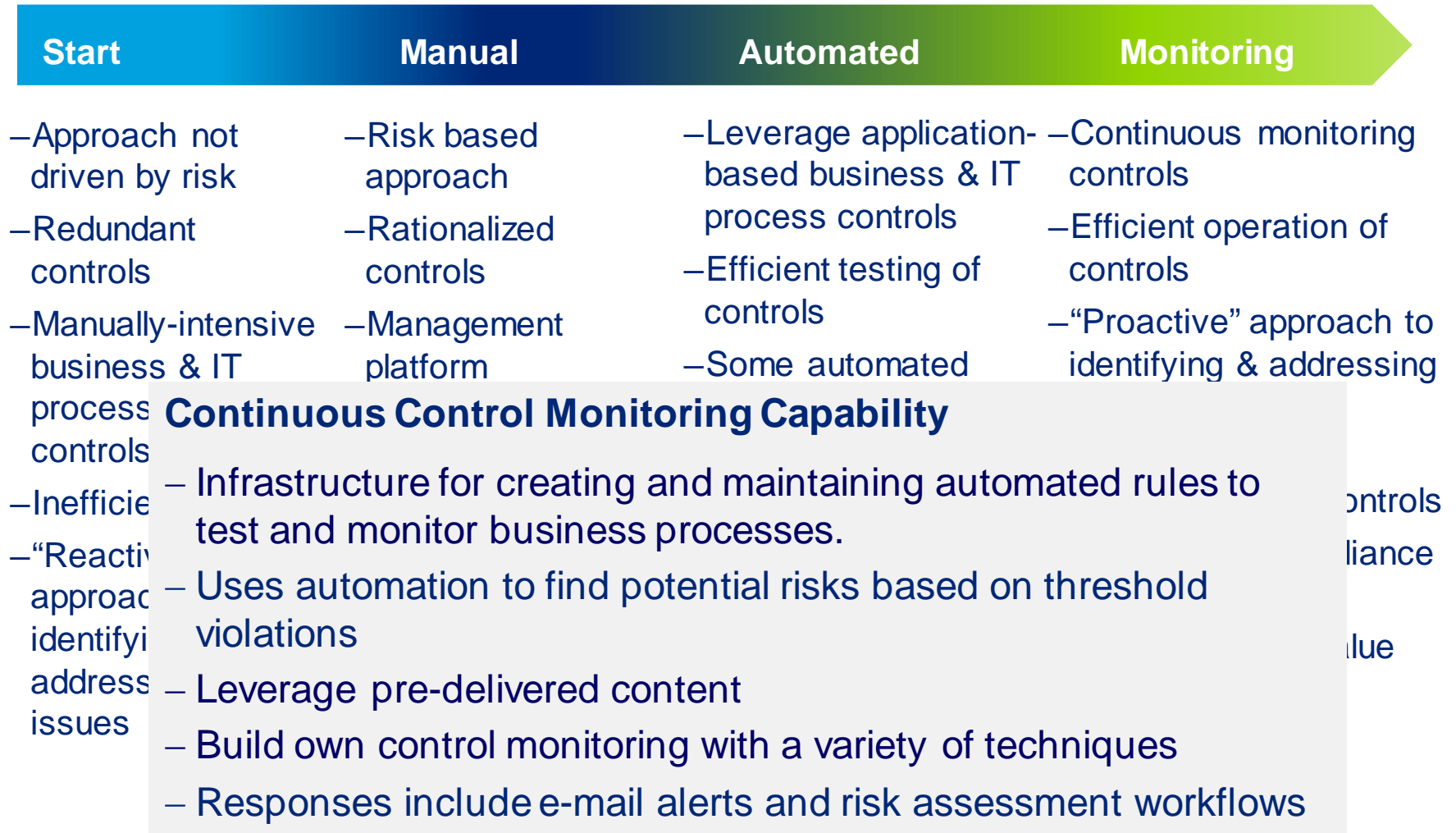
Higher Effectiveness

- Continuously monitor risks to proactively identify **and** respond to potential risks before they occur
- Implement risk response and mitigation activities to prevent risks from having negative impact

Maximized Visibility

- Align and integrate the management of risks across the enterprise
- Automatically identify and prioritize risks through proactive alerts and escalations

Value Driver 3: Continuous Controls Monitoring



Value Driver 4: Proactive Management of Access Risks

	Advantage of GRC Tools
Security	Increase of security and protection of critical data
Transparency	Immediate overview of user access rights and analysis of critical access violations
Administration	Efficient and reliable processes for user- and authorization administration
Audit	Increase of trust , that your system fulfill the requirements of audit
Segregation of Duties (SoD)	Automated monitoring and implementation of access- and SoD- controls
Costs	Low operative IT costs because of reduced complexity

Outlook: The Role of Analytics Technologies in addressing the strategic opportunities before us

- **Risk sensing**, which monitors websites and social media channels to identify "early warning signals" relevant to a particular risk.
- **Project predictive analytics**, which assesses the chance of large project success or failure and, hence, the need for intervention in project execution.
- **Risk-adjusted forecasting and planning**, which enables a more sophisticated approach for CFOs to integrate multi-factor perspectives into financial planning and evaluating risk/return.
- **Aggregated risk on demand services**, which will enable financial institutions to monitor risk exposures in near real-time.

Source: riskwire March 2013 - *Henry Ristuccia Global ERS Platform Leader – Governance, Regulatory & Risk*

GRC meets XBRL

Content

- What is GRC (Governance, Risk & Compliance)?
 - GRC context & challenges
 - GRC automation with software
- GRC-XML: What is it?
 - Business Case for XBRL
 - The taxonomy
 - Specific areas of focus and use cases

Examples of GRC issues



- **HSBC**: \$1.92b for Money Laundering
- **Barclays** was fined £290m, CEO forfeits bonus, quits (Libor): controls failures, etc.
- **Aviva** fined more than €2.4m by the Central Bank after it breached regulations at two of its **subsidiaries**

GRC & XML

- XBRL is a functional technology for enabling systems to communicate business and financial reporting information
- So
 - XBRL can also be effectively leveraged to enable information systems to communicate information on Risks, Controls and Test information: (GRC information)
 - Deliver consistency of GRC reporting

GRC-XML is a framework for the exchange and sharing of Governance, Risk, and Compliance Information

Some use cases for GRC-XML

1) Inside the organization

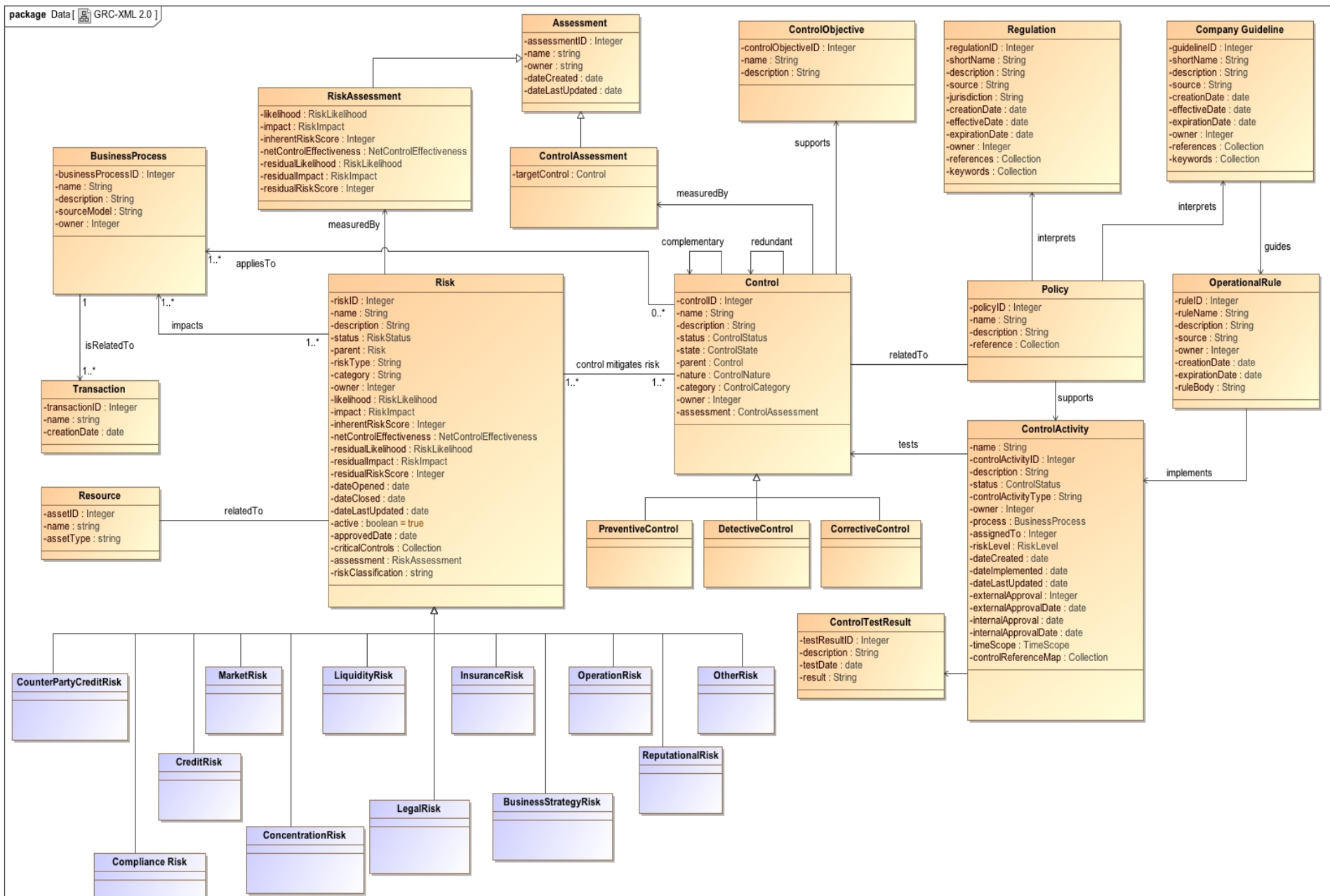
- Internal Risk assessments (e.g. IT risk assessment)
- Internal assessment of controls
- With standards, we can automate.
This lead to continuous monitoring and auditing

2) External auditors (and other inspectors)

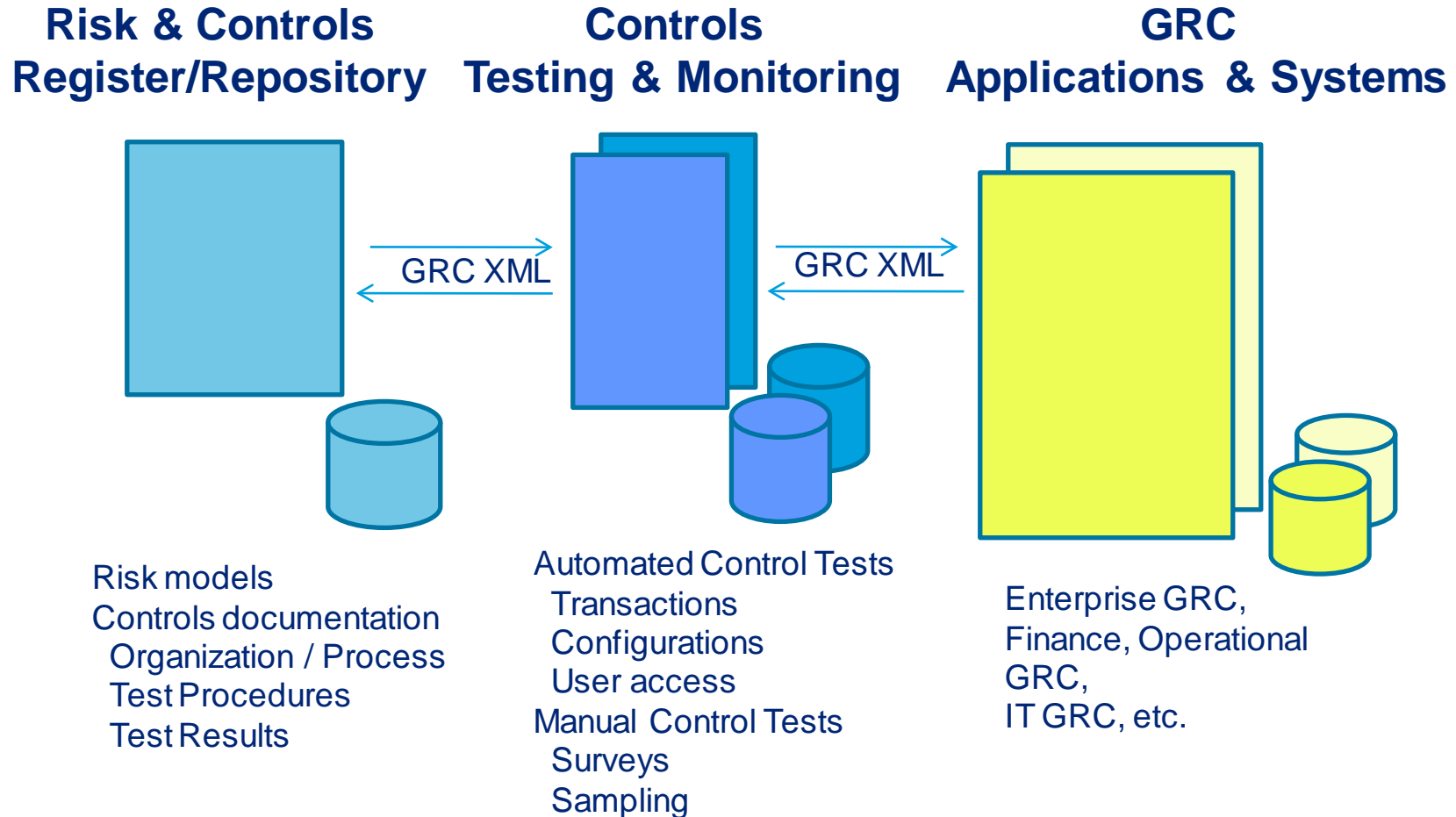
3) External reporting

- Solvency II directive
 - Pillar 2 Own Risk and Solvency Assessment (ORSA)
 - Pillar 3 Disclosure / Regulatory / Public

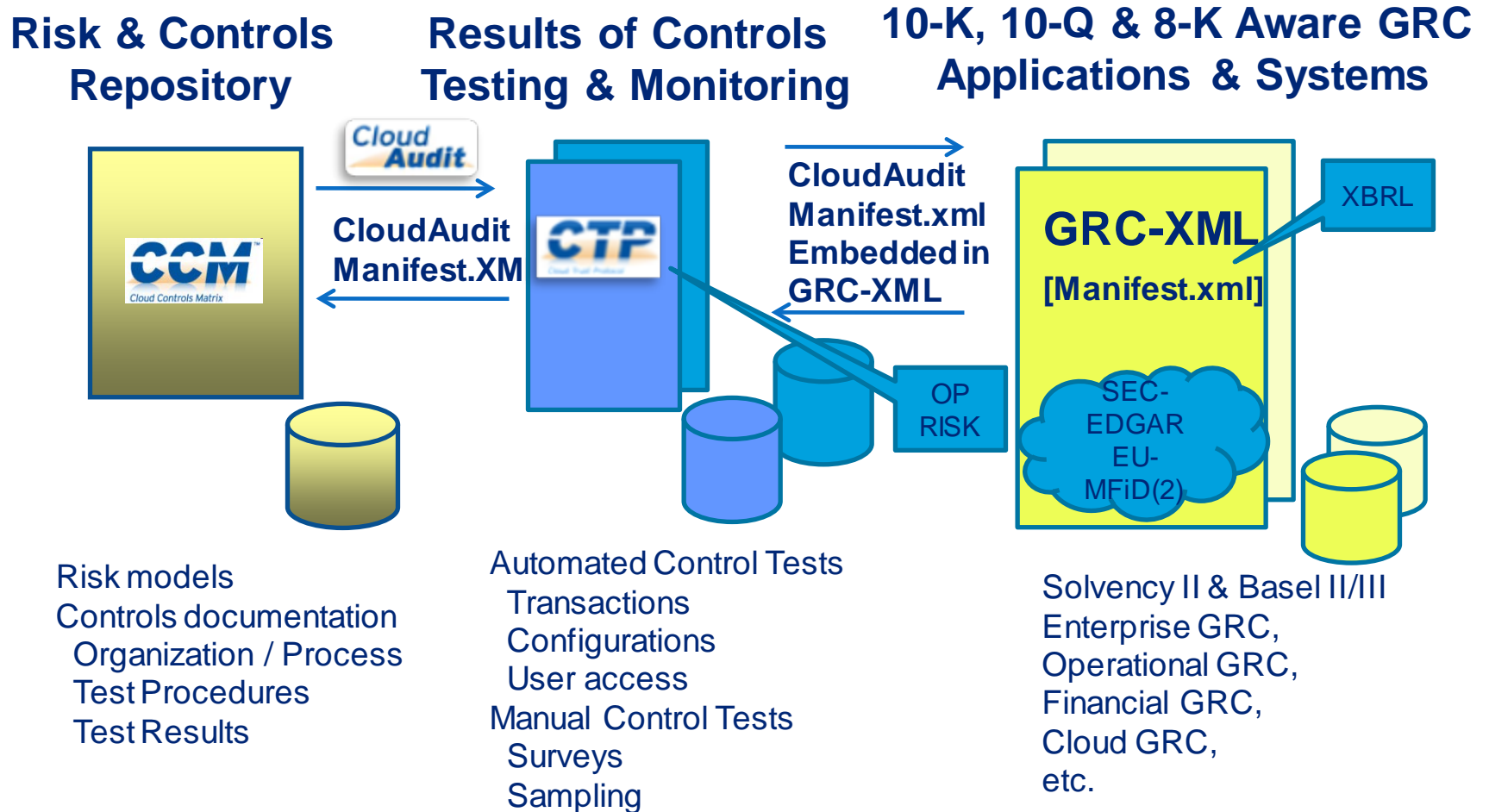
GRC-XML Information Model



Sample architecture



Proposed Cloud Service providers Scenarios



Additional opportunities for GRC-XML

- The Solvency II GRC Extension Taxonomy under development addresses the problem of ORSA inconsistencies
- GRC-XML can also be leveraged similarly for Basel3
- Alignment with revision of ISO 31000 Framework (Family of risk management standards in ISO)

Key take aways

- Integration of different GRC areas: security risk, IT risk, financial risk, operational risk, and others – many areas, one language
- Reduction of redundancies and duplications
- Visibility across silos
- Standardization, simplification
- Reduced information friction to facilitate (more) monitoring and audit of controls
- Consistency of Regulatory Supervision
- Facilitate Efficient Regulatory Oversight



Questions & discussion

