24th XBRL International Conference

“Transparency: with Available, Reliable, Comparable and Re-usable Data”

March 20-22, 2012
Abu Dhabi, UAE

ORSA Track

Enabling Governance, Risk and Compliance Information Sharing with XBRL Technology

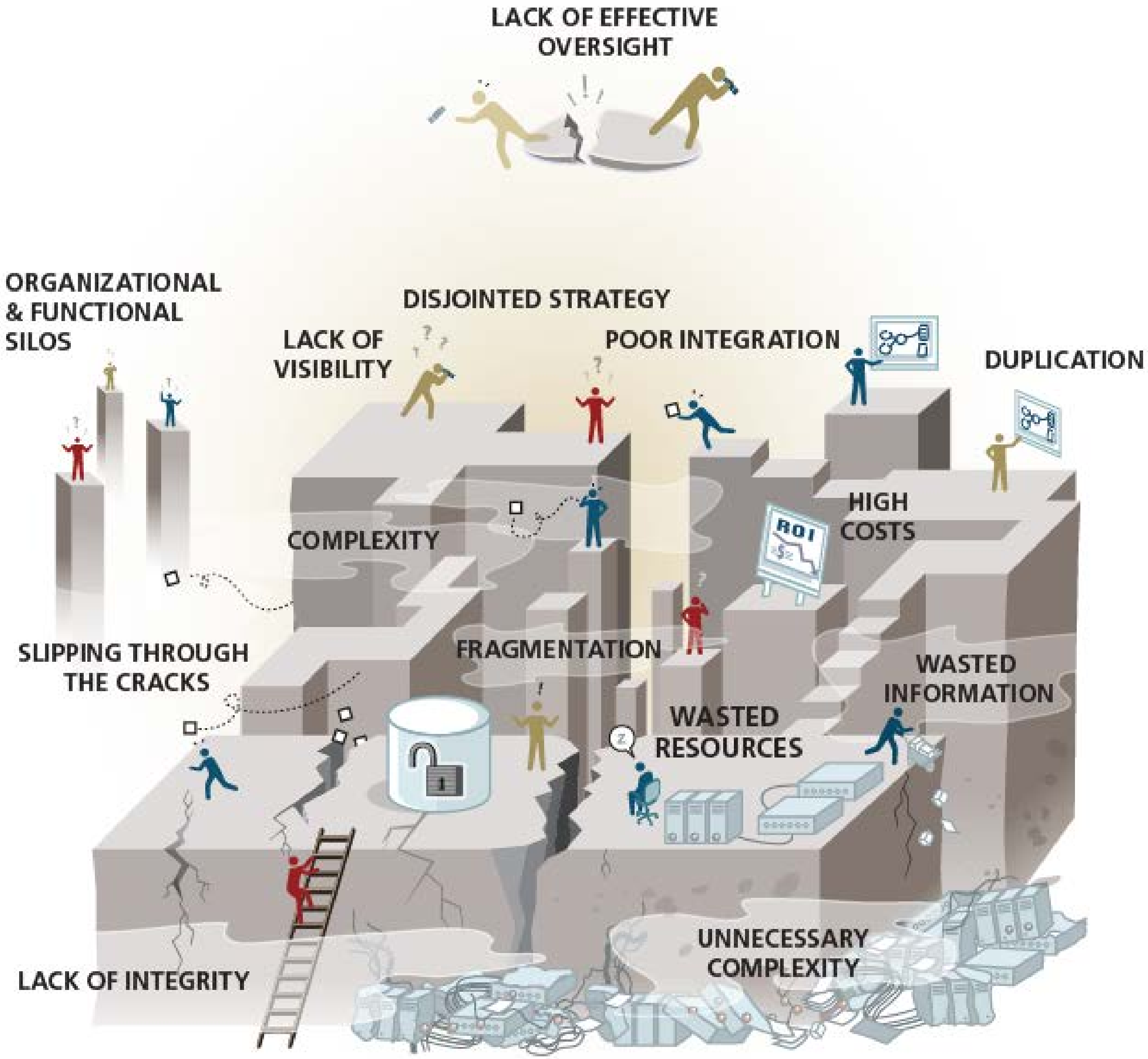
Said Tabet and John Dill

Thursday, 22 March 2012

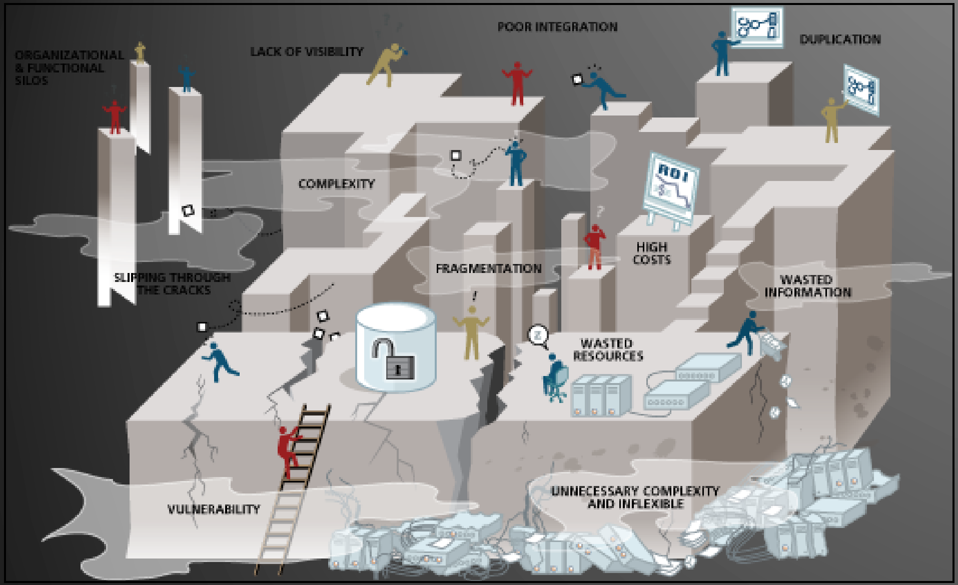
AGENDA

- Brief Overview
- What is GRC?
- Business Case
- GRC-XML Working Group
- GRC and XBRL
- GRC-XML Taxonomy and Information Model

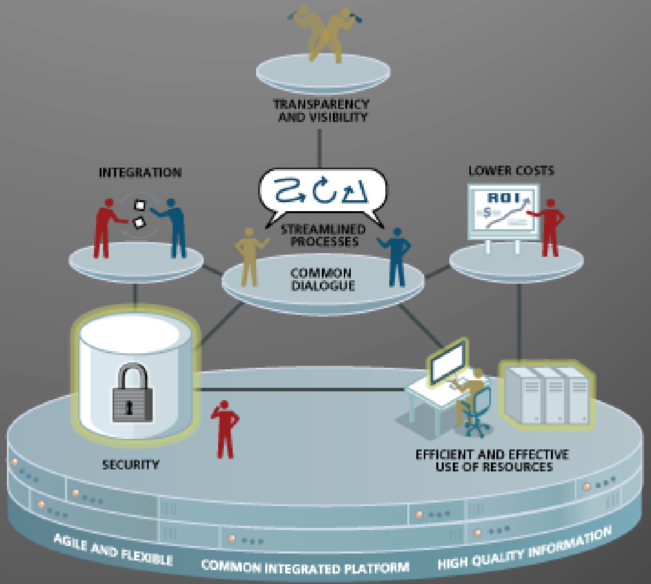
GRC: The Problem



A Transformational Opportunity For All Stakeholders



SOURCE: OCEG Illustrated Series



SOURCE: OCEG Illustrated Series

Current State

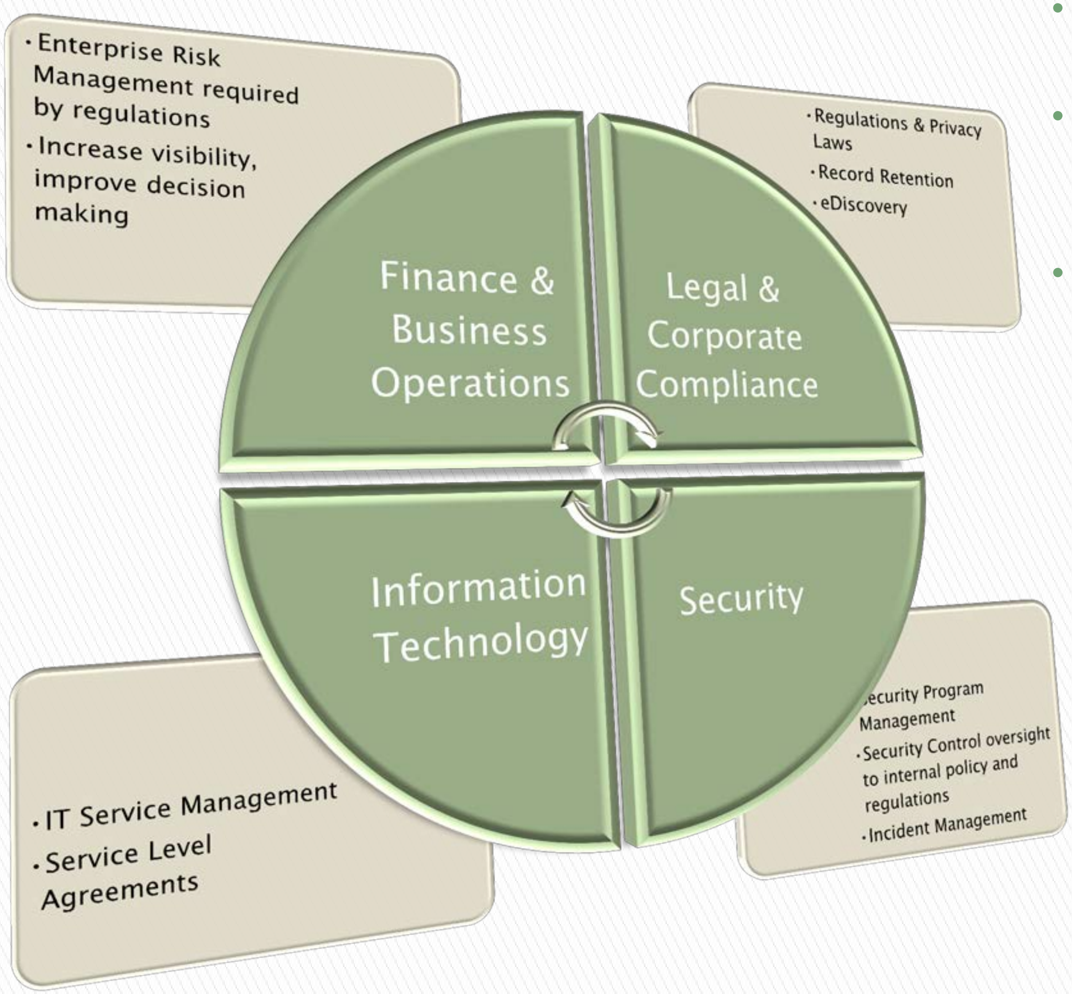
- Fragmented silos
- Mostly reactionary
- Individual projects
- Separate from mainstream processes and decision-making
- Spreadsheets, spreadsheets, spreadsheets
- Limited and fragmented use of technology

Future State

- Integrated management & performance
- Proactive planning & execution
- Integrated capability
- Embedded within mainstream processes and decision-making
- Coordinated transactions & shared data
- Architected solutions

Governance, Risk and Compliance

GRC Program Oversight



- Enterprise Risk Management required by regulations
- Increase visibility, improve decision making

Finance & Business Operations

- Regulations & Privacy Laws
- Record Retention
- eDiscovery

Legal & Corporate Compliance

Information Technology

- IT Service Management
- Service Level Agreements

Security

- ecurity Program Management
- Security Control oversight to internal policy and regulations
- Incident Management

- Requirements are not new, but have expanded
- Automation and standardization is a trend and opportunity
- Historically required of Managed Service Providers (MSP):
  - IT Service Level Agreements with metrics
    - IT Service Management
    - Business Continuity
  - Compliance certification against a framework such as ISO27001/2

Overview

- A common language of risk and control is a prerequisite for effective management of audit, risk, and compliance processes
- Most organizations currently struggle with a common language of risk and control between their internal GRC silos
- There is no standard risk and control language for multiple information systems to communicate or pass information

Overview (Cont'd)

- Standard risk and control models exist and are utilized by many organizations (COSO, COBIT, ITIL, …), yet there is no common language for systems to communicate on these taxonomies

- XBRL is a functional technology for enabling systems to communicate business and financial reporting information

- XBRL can be effectively leveraged to enable information systems to communicate Risk, Control and Test of Control information

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

GRC-XML Mission

As a working group, we focus on

- Creating the next version of the GRC-XML Taxonomy Framework
- Providing guidance and support to enable tooling and prototyping in order to demonstrate how standard libraries can be integrated and translated to GRC-XML, where possible.

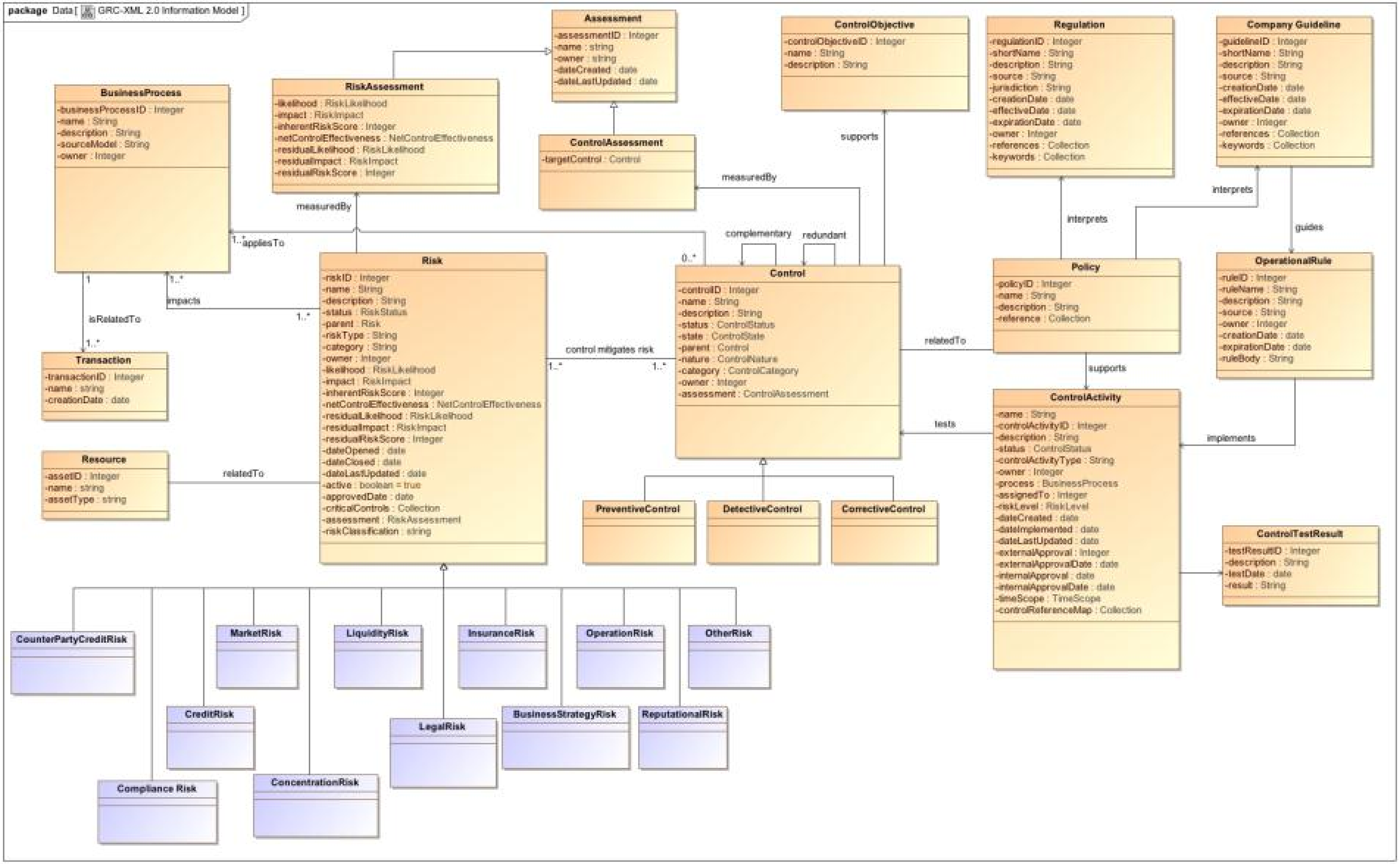
We expect vendors and other organizations to create their own mappings between GRC-XML and their proprietary formats

© 2011

Scope and Taxonomy Requirements

- Enhance the current version of GRC-XML
- Define the GRC-XML requirement for Cloud environments (Security needs, Service level agreements, data governance, etc.)
- Refine and formalize vocabulary and update it as needed
- Ability to support conversion and versioning between the many standards and libraries that are available (ITIL, COSO, COBIT, NIST, UCF, Basel2/3, and proprietary libraries)
- Support the tagging and the traceability from the data layer all the way to the business level (goals, processes, objectives, policies, etc.)
- Use XBRL GL as the standard format for evidence and input, and XBRL FR for summarized reporting

GRC-XML Information Model



package Data [GRC-XML 2.0 Information Model]

Assessment
-assessmentID : Integer
-name : string
-owner : string
-dateCreated : date
-dateLastUpdated : date

RiskAssessment
-likelihood : RiskLikelihood
-impact : RiskImpact
-inherentRiskScore : Integer
-netControlEffectiveness : NetControlEffectiveness
-residualLikelihood : RiskLikelihood
-residualImpact : RiskImpact
-residualRiskScore : Integer

ControlAssessment
-targetControl : Control

BusinessProcess
-businessProcessID : Integer
-name : String
-description : String
-sourceModel : String
-owner : Integer

Transaction
-transactionID : Integer
-name : string
-creationDate : date

Resource
-assetID : Integer
-name : string
-assetType : string

Risk
-riskID : Integer
-name : String
-description : String
-status : RiskStatus
-parent : Risk
-riskType : String
-category : String
-owner : Integer
-likelihood : RiskLikelihood
-impact : RiskImpact
-inherentRiskScore : Integer
-netControlEffectiveness : NetControlEffectiveness
-residualLikelihood : RiskLikelihood
-residualImpact : RiskImpact
-residualRiskScore : Integer
-dateOpened : date
-dateClosed : date
-dateLastUpdated : date
-active : boolean = true
-approvedDate : date
-criticalControls : Collection
-assessment : RiskAssessment
-riskClassification : string

ControlObjective
-controlObjectiveID : Integer
-name : String
-description : String

Regulation
-regulationID : Integer
-shortName : String
-description : String
-source : String
-jurisdiction : String
-creationDate : date
-effectiveDate : date
-expirationDate : date
-owner : Integer
-references : Collection
-keywords : Collection

Company Guideline
-guidelineID : Integer
-shortName : String
-description : String
-source : String
-creationDate : date
-effectiveDate : date
-expirationDate : date
-owner : Integer
-references : Collection
-keywords : Collection

Control
-controlID : Integer
-name : String
-description : String
-status : ControlStatus
-state : ControlState
-parent : Control
-nature : ControlNature
-category : ControlCategory
-owner : Integer
-assessment : ControlAssessment

Policy
-policyID : Integer
-name : String
-description : String
-reference : Collection

OperationalRule
-ruleID : Integer
-ruleName : String
-description : String
-source : String
-owner : Integer
-creationDate : date
-expirationDate : date
-ruleBody : String

ControlActivity
-name : String
-controlActivityID : Integer
-description : String
-status : ControlStatus
-controlActivityType : String
-owner : Integer
-process : BusinessProcess
-assignedTo : Integer
-riskLevel : RiskLevel
-dateCreated : date
-dateImplemented : date
-dateLastUpdated : date
-externalApproval : Integer
-externalApprovalDate : date
-internalApproval : date
-internalApprovalDate : date
-timeScope : TimeScope
-controlReferenceMap : Collection

ControlTestResult
-testResultID : Integer
-description : String
-testDate : date
-result : String

PreventiveControl

DetectiveControl

CorrectiveControl

CounterPartyCreditRisk

MarketRisk

LiquidityRisk

InsuranceRisk

OperationRisk

OtherRisk

CreditRisk

LegalRisk

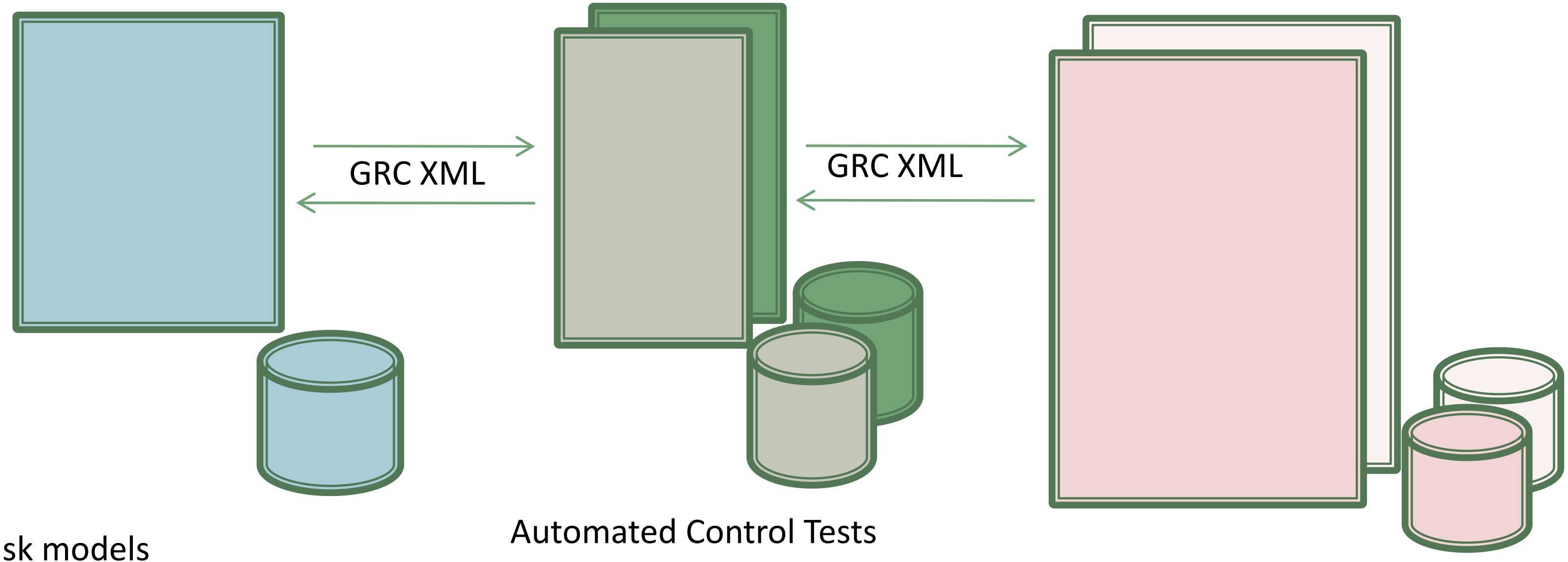
BusinessStrategyRisk

ReputationalRisk

Compliance Risk

ConcentrationRisk

Sample Deployment



Risk & Controls
Repository

GRC XML

Controls
Testing & Monitoring

GRC XML

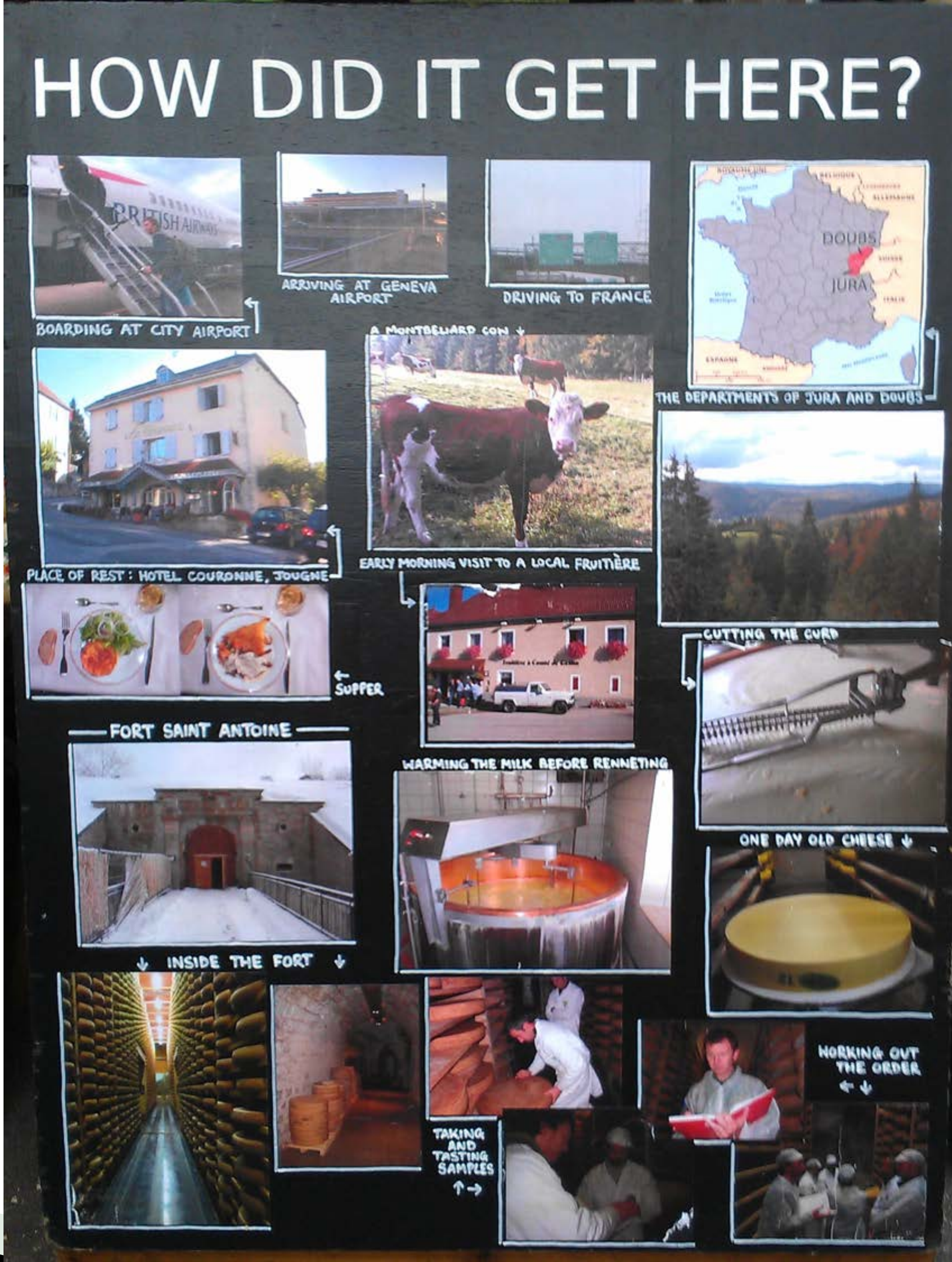
GRC
Applications & Systems

Risk models
Controls documentation
  Organization / Process
  Test Procedures
  Test Results

Automated Control Tests
  Transactions
  Configurations
  User access
Manual Control Tests
  Surveys
  Sampling

Enterprise GRC,
Operational GRC,
IT GRC, etc.

Enabling transparency and traceability



Summary

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

To Get Involved

- Join our working group
- Collaborate with us:
  - Use Cases in your specific sector(s)
  - Reviews of published specification
  - Implement and support the standard

- Contact us:
  Said Tabet: stabet@oceg.org
- John Dill: jdill@bma.bm

Discussion

© 2011