Chap 12

Governance, Risk, and Compliance

Dr. Yeffry Handoko Putra

Head Department of
Magister Information System
Universitas Komputer Indonesia


Governance, Risk,
and Compliance

Governance, Risk, and Compliance (GRC)

- GRC refers to taking an integrated, enterprise-wide approach to Governance, Risk Management, and Compliance:
  - **Governance** – The Board of Directors' and management's structures, policies, processes, and controls that focus on long-term value through the ethical, equitable, efficient, and effective operation of the business
  - **Risk Management** – An organization's systematic process to identify, assess, manage, and monitor upside and downside risks to the business
  - **Compliance** – An organization's process to demonstrate its employees and agents adherence to policies and procedures, laws, and regulations
- GRC is transformational and addresses the people, process, and technology enhancements required to achieve risk intelligence

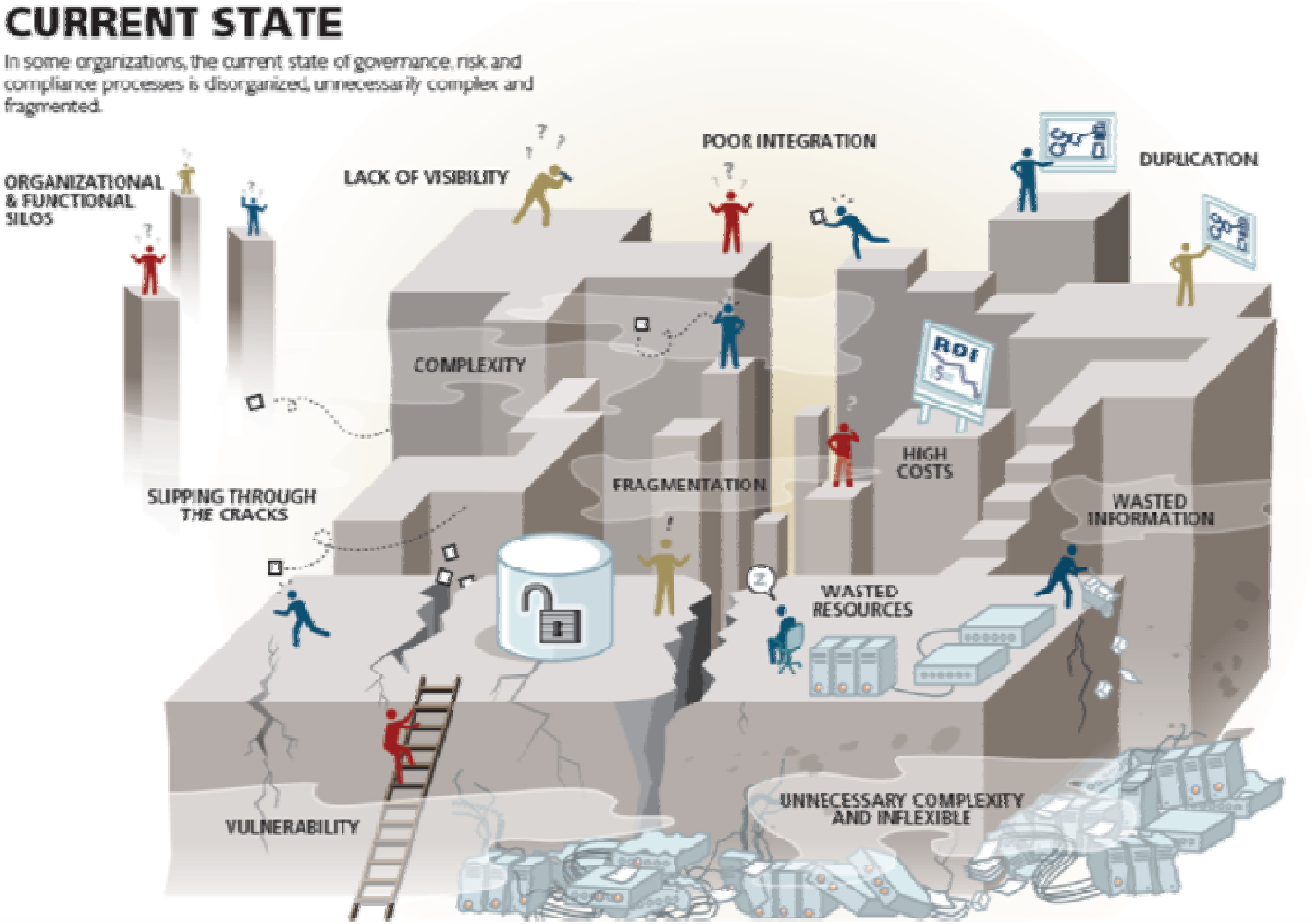
Current State

- The “universe” of risks, regulations, and compliance requirements continues to expand at an increasing rate

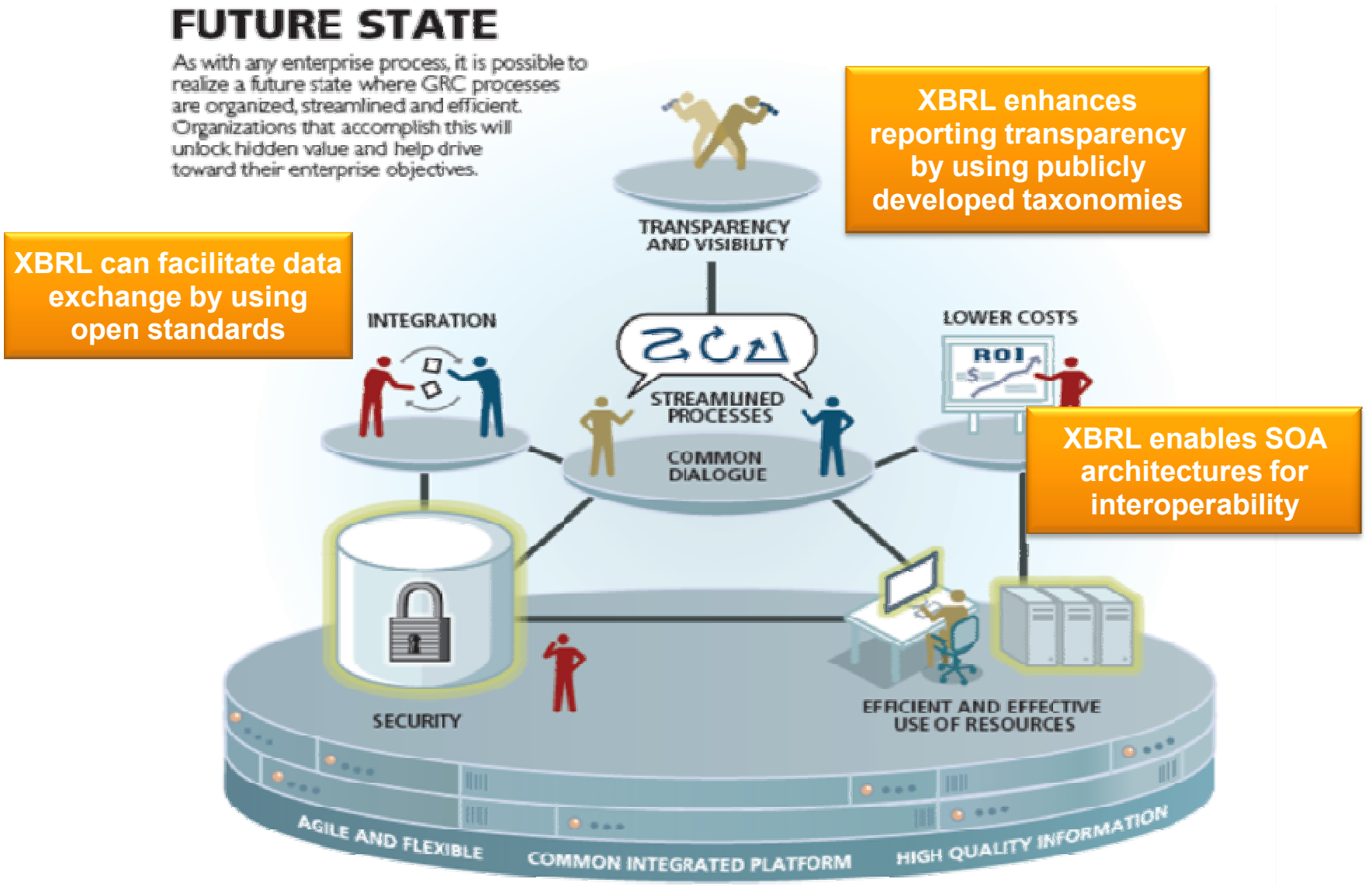
- Market, regulatory, and legal tolerance for failures continues to decrease

- Enterprise governance, risk management, and compliance activities are highly fragmented
  - Have evolved over time from the bottom up, often in reaction to “breakdowns” or new regulations
  - Highly expensive, but few have true handle on cost

Risk Ignorance



Risk Intelligence and Integrated GRC




Open Compliance
and Ethics Group
HOLY BIBLE
BOLD TEXT EDITION
OCEG
DRIVING PRINCIPLED PERFORMANCE

What is OCEG?

OCEG is the leading nonprofit that helps organizations drive principled performance™ with a global community of skilled practitioners focused on improving governance, risk management, and compliance processes.

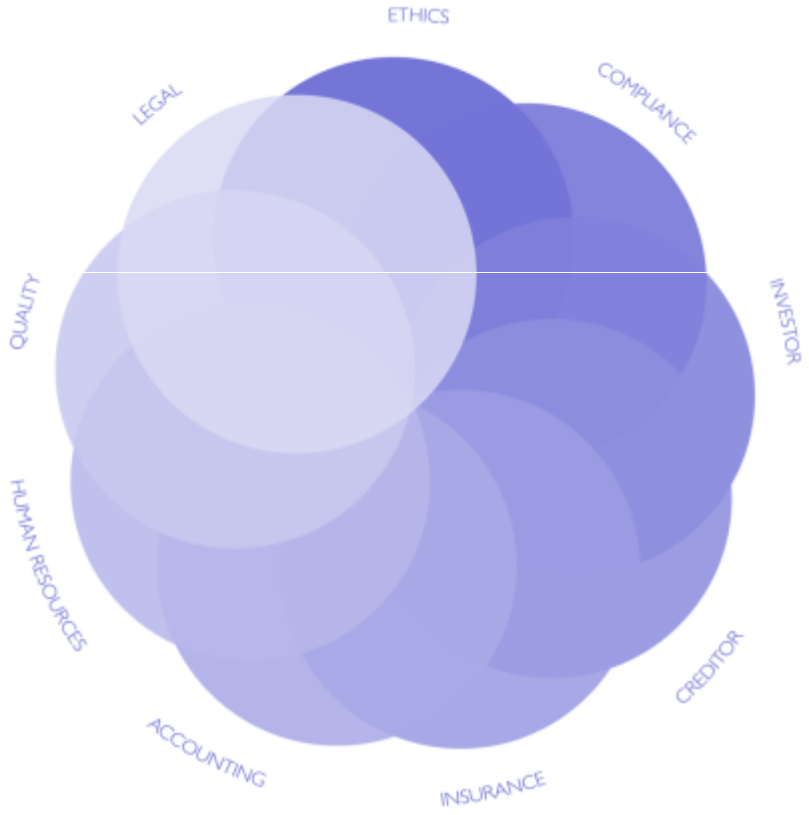
- **Guidelines and Standards – what should we do?**
  - Process standards (key concepts, components, and terminology)
  - Technical standards (key systems and integration points)
  - DEVELOPED by experts and PUBLICLY vetted to ensure quality
- **Evaluation Criteria and Metrics – how are we doing?**
  - Effectiveness and performance evaluation (suitable criteria)
  - Reporting and disclosure guidance
  - Tools and technologies to appropriately benchmark
- **Community of Practice – how/what is everyone else doing?**
  - Discover, create, and evolve guidelines
  - Use online tools and resources
  - Collaborate with peers in a NUMBER of professions

OCEG has over 15,000 members in 46 countries representing 66 GRC disciplines

Mission: The Integration of Disciplines

OCEG brings together disciplines and professions to collaborate and pursue a common mission: to refine and improve the practice of GRC

- Governance
- Risk Management
- Compliance/Legal Management
- Human Capital Management
- Change Management
- Ethics Management
- Internal Audit
- Security
- Quality Management
- Project Management
- Information Technology
- Financial and Resource Planning



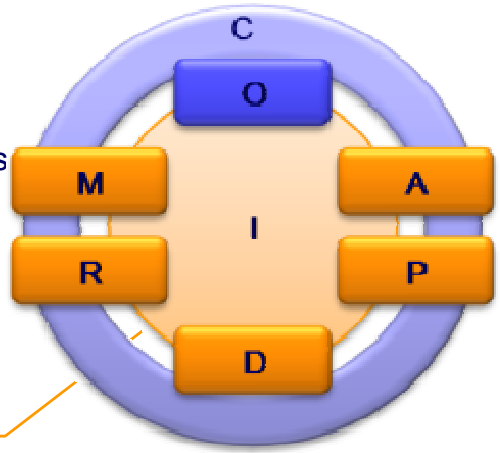
Elements of the OCEG GRC Capability Model

MONITOR AND MEASURE
M1 – Context Monitoring
M2 – Performance Monitoring and Evaluation
M3 – Systemic Improvement
M4 – Assurance

CONTEXT AND CULTURE
C1 – External Business Context
C2 – Internal Business Context
C3 – Culture
C4 – Values and Objectives

ORGANIZE AND OVERSEE
O1 – Outcomes and Commitment
O2 – Roles and Responsibilities
O3 – Approach and Accountability

RESPOND AND RESOLVE
R1 – Internal Review and Investigation
R2 – Third-Party Inquiries and Investigations
R3 – Crisis Response and Recovery
R4 – Remediation and Discipline



ASSESS AND ALIGN
A1 – Risk Identification
A2 – Risk Analysis
A3 – Risk Optimization

INFORM AND INTEGRATE
I1 – Information Management and Documentation
I2 – Internal and External Communication
I3 – Technology and Infrastructure

DETECT AND DISCERN
D1 – Hotline and Notification
D2 – Inquiry and Survey
D3 – Detective Controls

PREVENT AND PROMOTE
P1 – Codes of Conduct
P2 – Policies
P3 – Preventive Process Controls
P4 – Awareness and Education
P5 – Human Capital Incentives
P6 – Human Capital Controls
P7 – Stakeholder Relations and Requirements
P8 – Preventive Technology Controls
P9 – Preventive Physical Controls
P10 – Risk Financing/Insurance

OCEG Technology Council Overview

The Technology Council

- The OCEG Technology Council was formed to help address strategic, operational and technical issues that professionals face when applying Information Technology (IT) to governance, risk management, compliance (GRC) and ethics management.

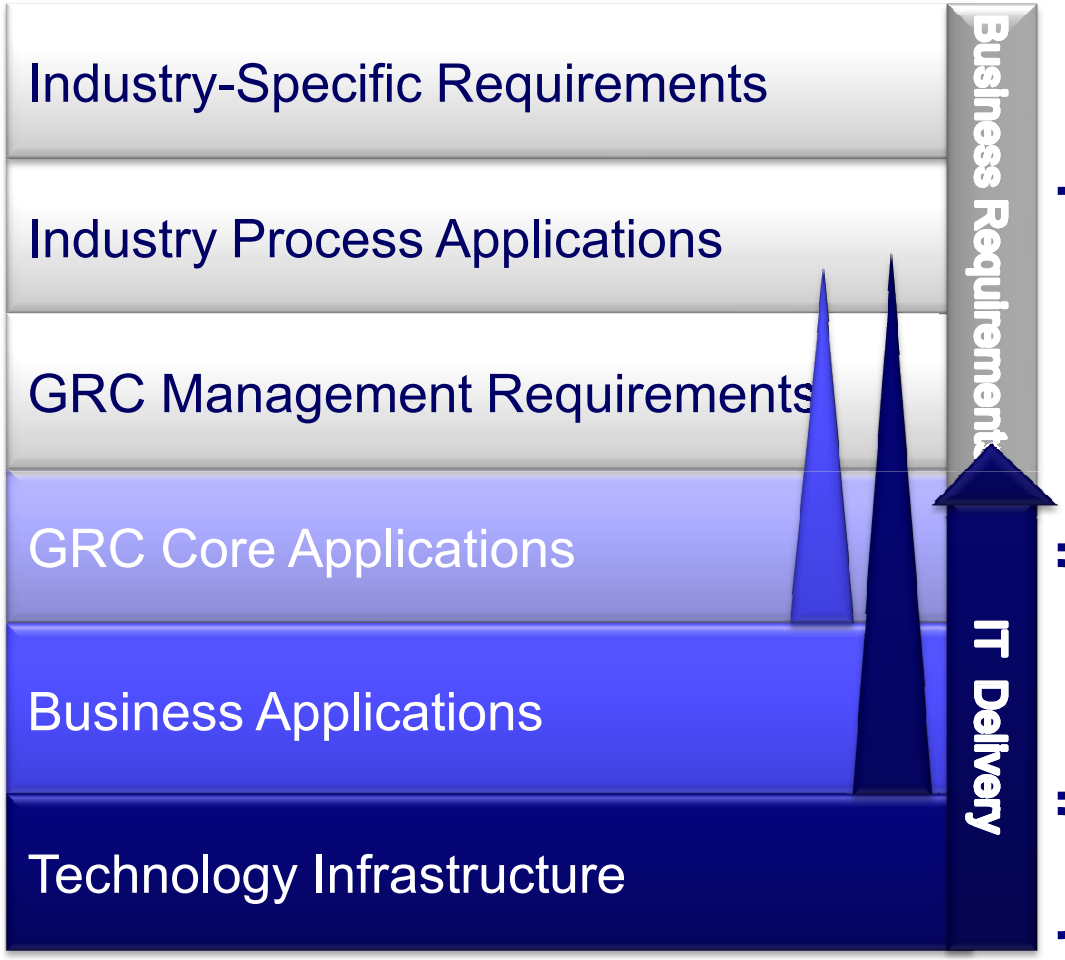
- Technology Council members meet monthly in specialized working groups focused on GRC technology architecture, standards, and implementation tools. These Work Groups include the GRC Blueprint™, GRC Roadmap™, and GRC-XML™ programs.

- The entire council convenes quarterly to review the progress of the individual working groups, discuss key issues facing GRC professionals, and to identify new GRC technology alignment programs for OCEG.

- The OCEG Technology Council engages 37 of the world's leading GRC software, services, and content providers and user organizations in the development of strategic and technical resources that help IT and business professionals improve the practice of GRC within their organizations.

OCEG Technology Council Members

The OCEG GRC Integrated Technology Model



Internal and External Content Specialists
(e.g., law firms, consultants, departmental staff, directors, managers)

Role and Context Applications
(e.g., compliance processes and reporting; risk, quality, audit, legal, and contract management)

Organizational Functionality
(e.g., ECM, BPM, BI, LMS, ERP)

IT infrastructure
(e.g., identity management, Databases, Information Security)

Member A Case:
GRC-XML (XBRL) Components (Case Management)

1. **Supporting interchange of help line data from content providers for this domain**
2. **Supporting interchange of current case management data**
3. **Supporting interchange of education status (i.e. courses taken by employees to mitigate risk)**

A. (1) and (2) are ways of communicating the result of an incident

B. (1) and (2) demand a unified solution so that a help line incident shares as much structure with a case management incident as possible

C. For (1) and (2) we are leveraging and extending taxonomy in the following domains:

I. Data Security
II. Risk classification
III. Performance-based controls
IV. Message Processing
V. Geographical Location
VI. User identity
VII. Data Privacy

D. Area (3) is necessary to communicate actions taken to prevent incidents

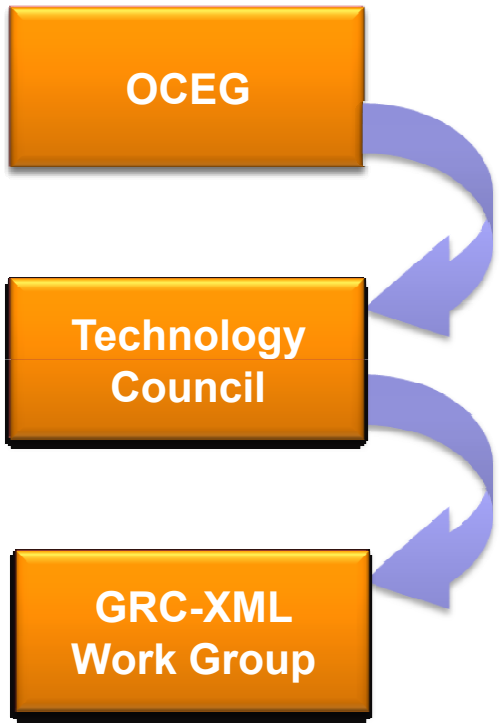
Member B Case:
GRC-XML (XBRL) Components (Controls)

1. **Identification of business control point(s)**
   A. Process, sub-process, control name, and ID
   B. Financial account(s) impacted
   C. Process owner details (name, address, business unit …)
2. **Risk assessment**
   A. ID, business risk(s) addressed by the control point, other mitigating controls
      I. Approval, version, effective date
      II. Related file attachments
3. **Control testing activities**
   A. Test plans (header-level)
      I. ID, objectives, budget, person responsible
      II. Approval, version, effective date
      III. Related file attachments
   B. Tests (detail)
      I. ID, objectives addressed, test type, selection method, source population details, test procedure
      II. Approval, version, effective date
      III. Related file attachments

Member B Case:
GRC-XML (XBRL) Components (Continued)

4. **Exceptions (related to one or many detail tests)**
   A. ID, description, owner, reviewed, resolution (plan) , resolution (actual), status
      I. Approval, version, effective date
      II. Related file attachments
5. **Control deficiencies (related to one or many detail tests, related to one or many control points)**
   A. ID, description, found by test(s), impacts control(s), severity, category
      I. Approval, version, effective date
      II. Related file attachments
6. **Control point assessment**
   A. ID, operating effectiveness (pass/conditional pass/fail), evidenced by control deficiencies, resolution (plan), resolution (actual)
      I. Approval, version, effective date
      II. Related file attachments
   B. Operational information which may impact the assessment (for example, whistle-blower reports) – According to Member A's taxonomy for incidents
   C. Vendor applications will manage specific test plans, as XBRL governs common criteria, standardized control language for incidents, defines related control values

OCEG GRC-XML (XBRL) Program Management Process



- **OCEG**
  - Owns the initiative
  - Is an official member of XBRL International
  - Provides “vision” and program governance
  - Promotes final schema adoption
- **Technology Council - Jurisdiction**
  - Encourages Member Contributions and Participation
  - Drives the production schedule
  - Provides the Work Group Members
  - Provides technology, technical skills, and methodology
- **Work Group – Steering Committee**
  - Executes the development methodology
  - Develops and reviews all deliverables
  - Builds schema consensus
  - Creates and delivers the Business Object Documents


Proof of Concept:
Internal Control and XBRL

Beyond Financial Reporting

- Exploring Taxonomy Development:
  - Global Ledger
    - Captures accounting system information (Journal Entries, Trial balance, Vendor/Employee/Customer data).
    - SRCD (Summary Reporting Contextual Document) provides mechanism for linking accounting system detail to reporting taxonomies.
  - Internal Control
    - Proof of concept using XBRL to document Internal Control structure and assessments. Initial work done by representatives of large accounting firms.
  - IFRS, FINREP, COREP, etc.
- Integration of Disparate Systems and Data
- XForms – A User Interface for XBRL
  - XForms is a standard from W3C, allows creation of sophisticated user interfaces for XBRL documents.

Proof of Concept Objectives

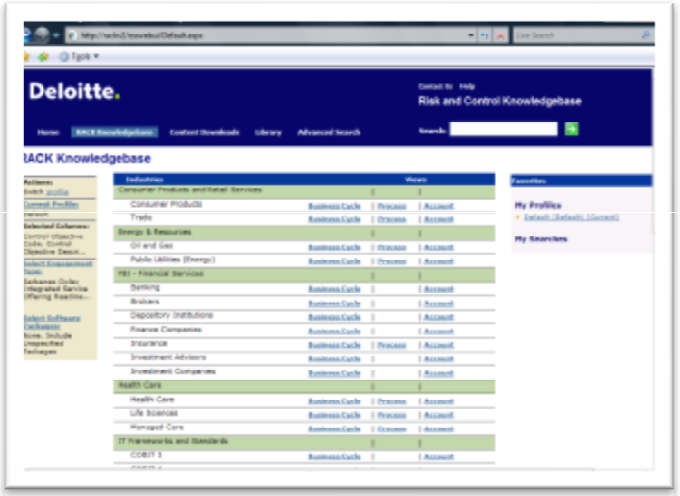
- Validated the ability create of a XBRL Internal Control taxonomy based of Deloitte's Risk and Control Knowledgebase (RACK)

- Validated ability to convert general ledger (GL) data from SAP and Oracle into XBRL GL instance documents

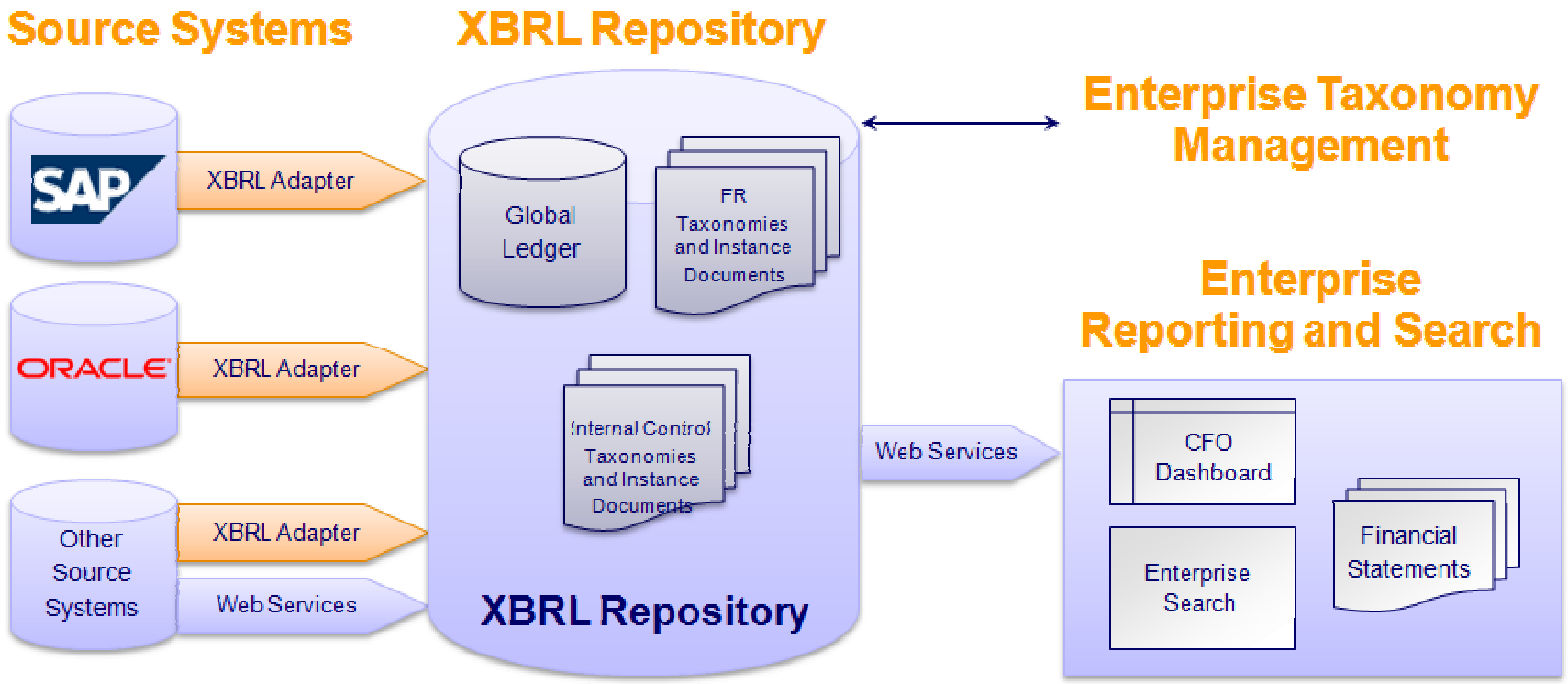
- Validated ability and value of combining XBRL GL, XBRL Internal Control, and XBRL FR instance documents for enhanced reporting:
  - Financial Statement → Internal Control and Assessment Detail
  - Financial Statement → GL Transaction Detail

Internal Control Taxonomy

- Explored opportunities and value of a taxonomy built for the purpose of reporting on Internal Controls:
  - XBRL Internal Control Taxonomy
    - Taxonomy comprised of processes, subprocesses, objectives, risks, and controls defined in a standard taxonomy
    - Utilizing dimensionality for entity uniqueness
    - Taxonomy populated with Deloitte RACK data – a proprietary set of internal control frameworks organized by Industry and Business Processes



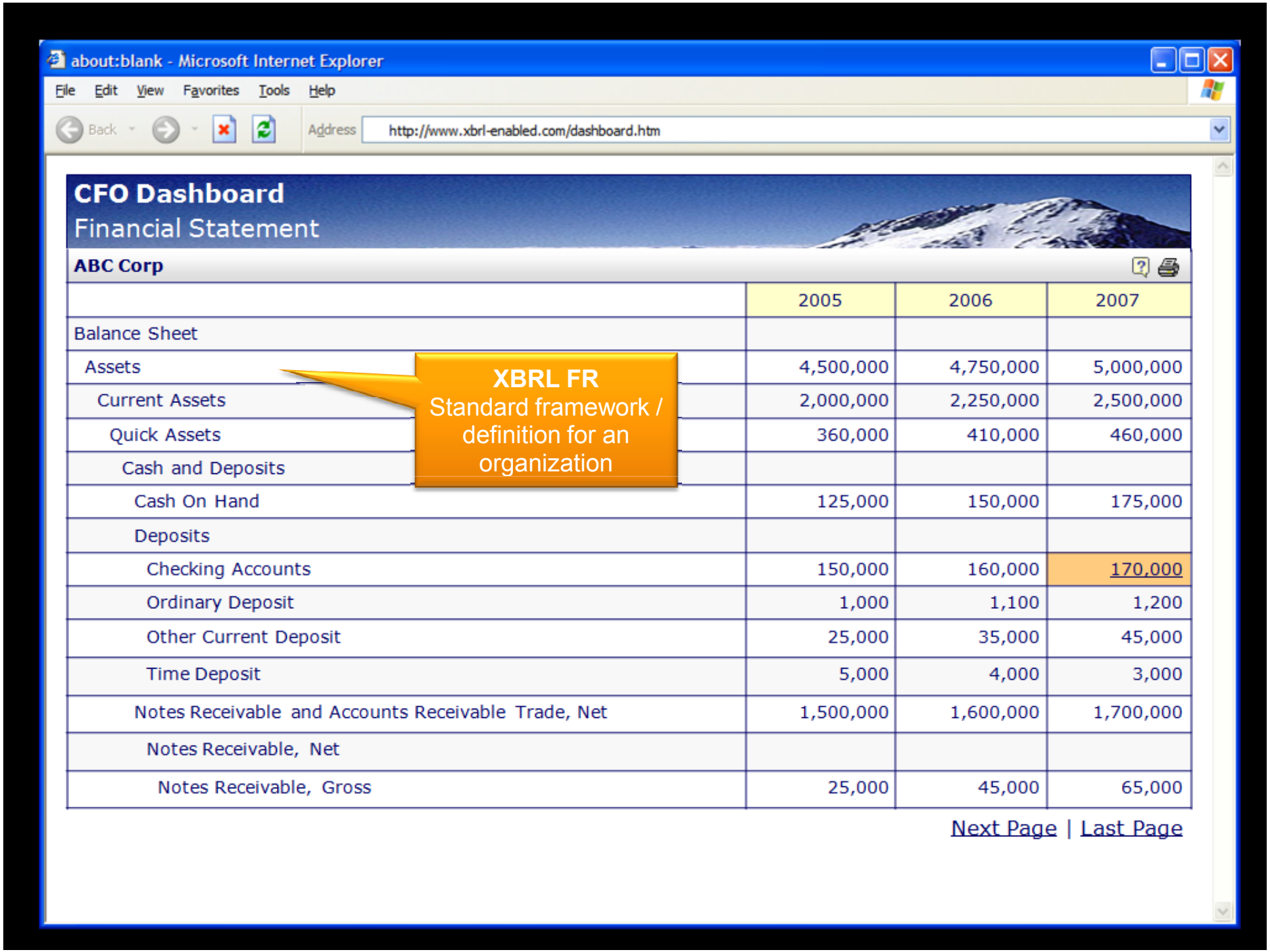
Integration Proof of Concept – Technical Overview



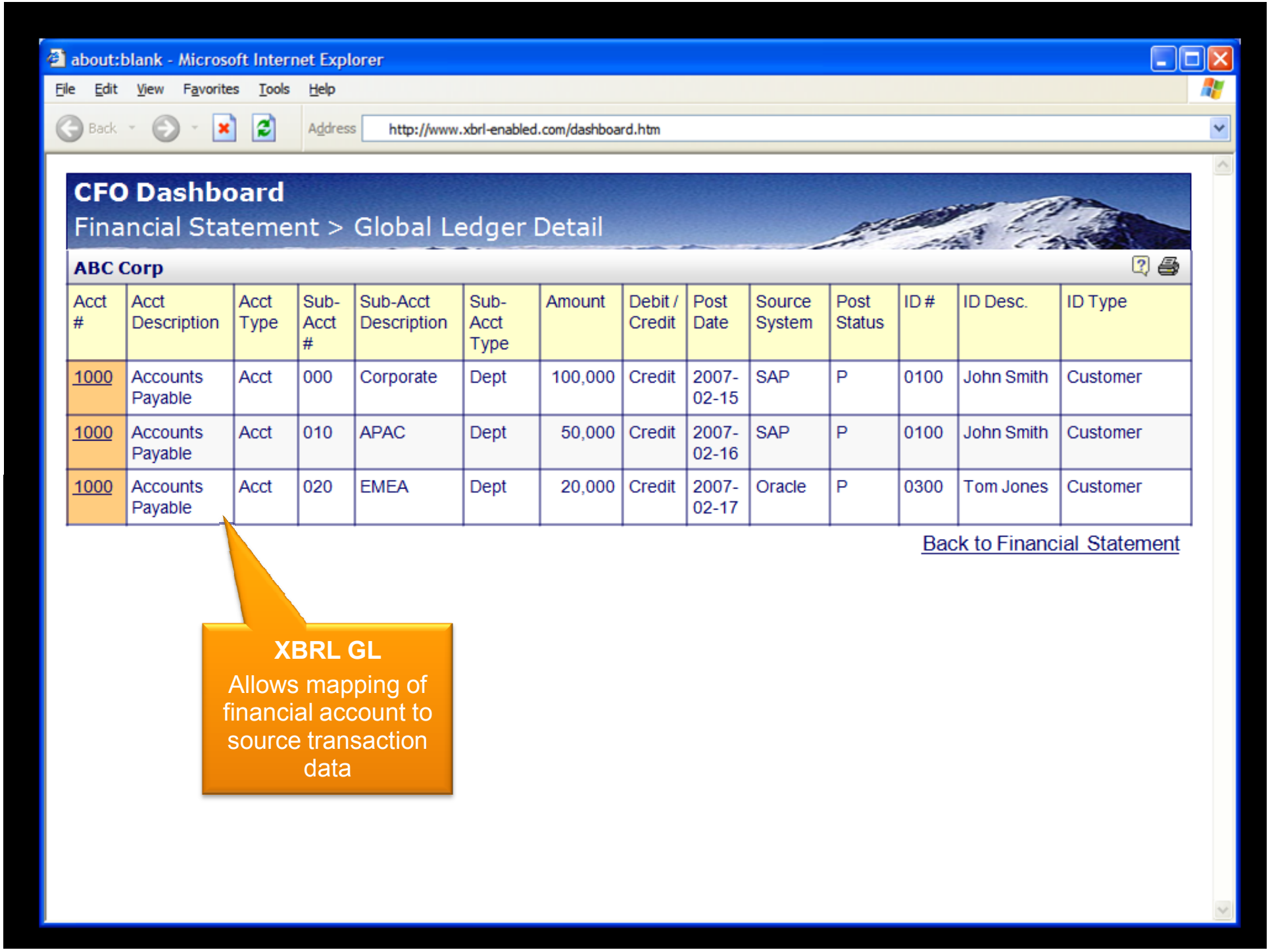
XBRL Adapters/Web Services
- Periodic pull of general ledger information from source systems and stored in summarized format
- Additional data can be extracted or queries executed if needed by GRC taxonomy for control monitoring purposes
- Other sources could include: Microsoft Excel or other Internal Control and Testing Data source systems

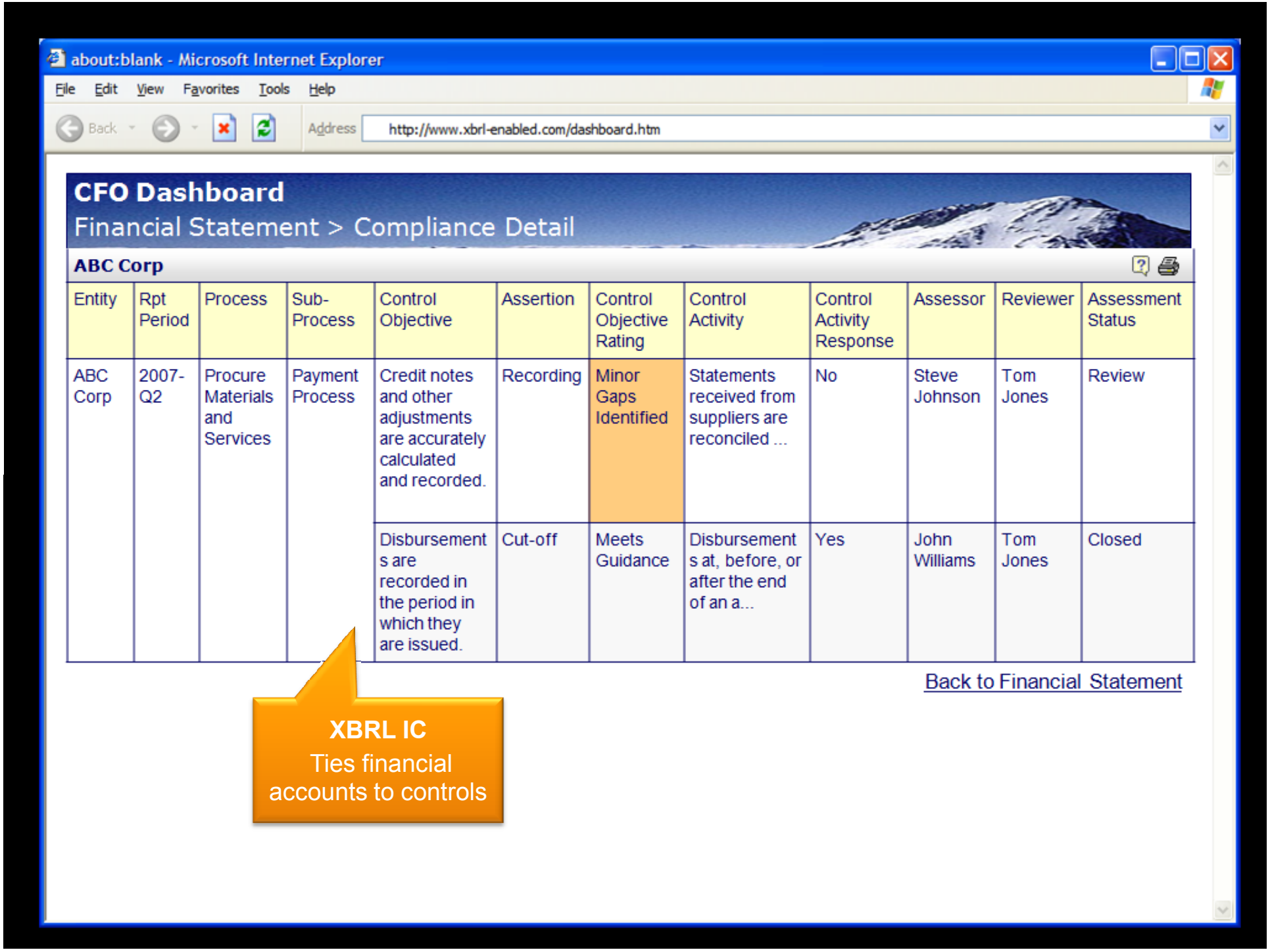
XBRL Repository
- Central repository for all enterprise XBRL taxonomies and instance documents
- Historical record of extracts allows for performance and trend reporting

CFO Dashboard
- Financial Performance and Compliance views



	2005	2006	2007
Balance Sheet			
Assets	4,500,000	4,750,000	5,000,000
Current Assets	2,000,000	2,250,000	2,500,000
Quick Assets	360,000	410,000	460,000
Cash and Deposits			
Cash On Hand	125,000	150,000	175,000
Deposits			
Checking Accounts	150,000	160,000	170,000
Ordinary Deposit	1,000	1,100	1,200
Other Current Deposit	25,000	35,000	45,000
Time Deposit	5,000	4,000	3,000
Notes Receivable and Accounts Receivable Trade, Net	1,500,000	1,600,000	1,700,000
Notes Receivable, Net			
Notes Receivable, Gross	25,000	45,000	65,000


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address
http://www.xbrl-enabled.com/dashboard.htm
CFO Dashboard
Financial Statement > Global Ledger Detail
ABC Corp
Acct # | Acct Description | Acct Type | Sub-Acct # | Sub-Acct Description | Sub-Acct Type | Amount | Debit / Credit | Post Date | Source System | Post Status | ID # | ID Desc. | ID Type
1000 | Accounts Payable | Acct | 000 | Corporate | Dept | 100,000 | Credit | 2007-02-15 | SAP | P | 0100 | John Smith | Customer
1000 | Accounts Payable | Acct | 010 | APAC | Dept | 50,000 | Credit | 2007-02-16 | SAP | P | 0100 | John Smith | Customer
1000 | Accounts Payable | Acct | 020 | EMEA | Dept | 20,000 | Credit | 2007-02-17 | Oracle | P | 0300 | Tom Jones | Customer
Back to Financial Statement
XBRL GL
Allows mapping of financial account to source transaction data


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address
http://www.xbrl-enabled.com/dashboard.htm
CFO Dashboard
Financial Statement > Compliance Detail
ABC Corp
Entity
Rpt Period
Process
Sub-Process
Control Objective
Assertion
Control Objective Rating
Control Activity
Control Activity Response
Assessor
Reviewer
Assessment Status
ABC Corp
2007-Q2
Procure Materials and Services
Payment Process
Credit notes and other adjustments are accurately calculated and recorded.
Recording
Minor Gaps Identified
Statements received from suppliers are reconciled ...
No
Steve Johnson
Tom Jones
Review
Disbursements are recorded in the period in which they are issued.
Cut-off
Meets Guidance
Disbursements at, before, or after the end of an a...
Yes
John Williams
Tom Jones
Closed
Back to Financial Statement
XBRL IC
Ties financial accounts to controls


Open Panel Discussions

GRC Goals and XBRL Benefits

GRC goals closely align with potential benefits provided by XBRL