



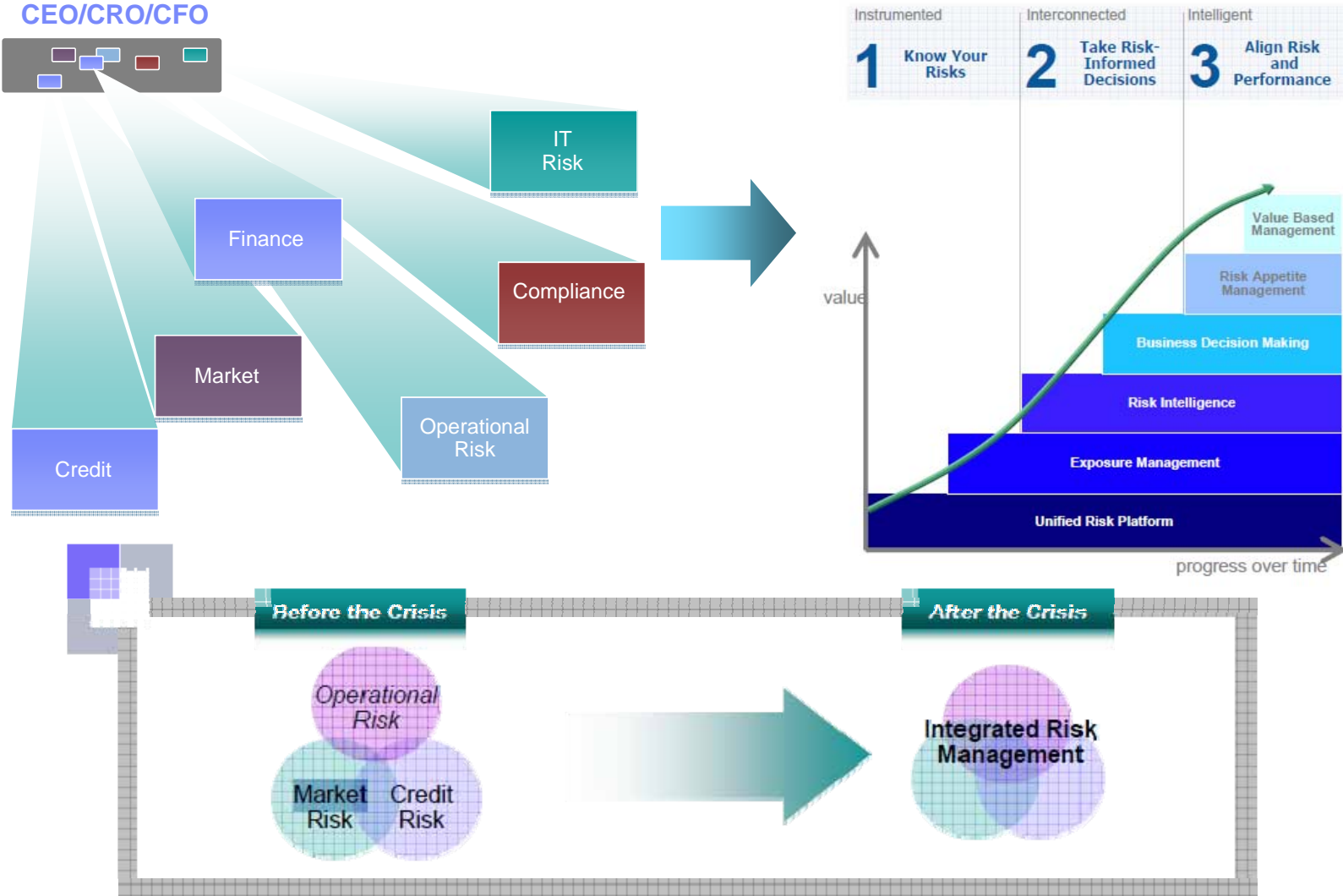
Implementing an IT GRC Program with IBM OpenPages ITG



IBM Risk Approach

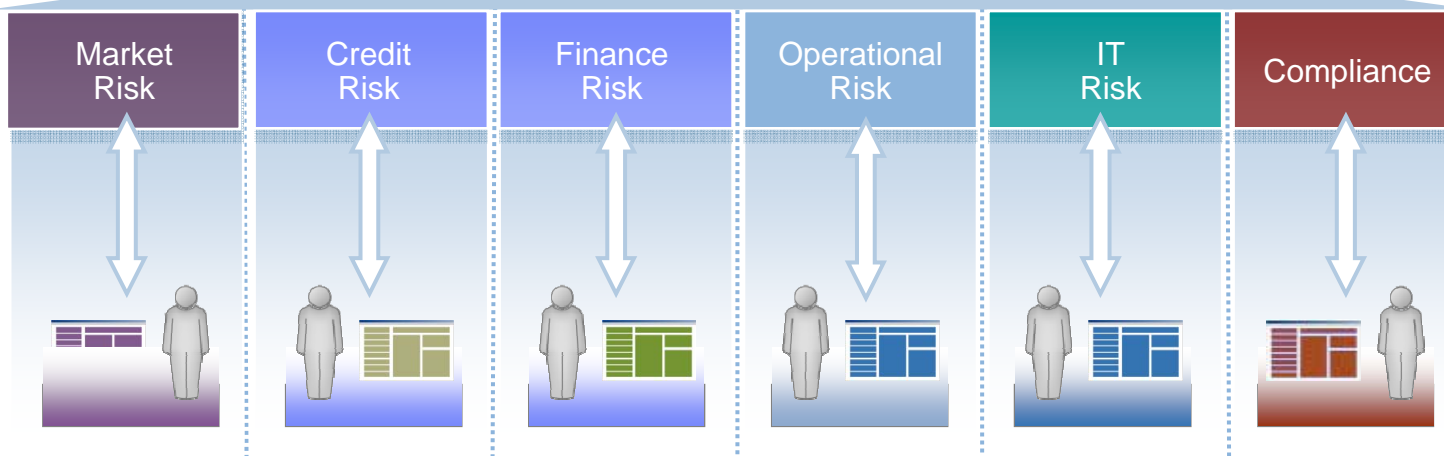


Fragmented risk approach increase cost and reduce governance ability

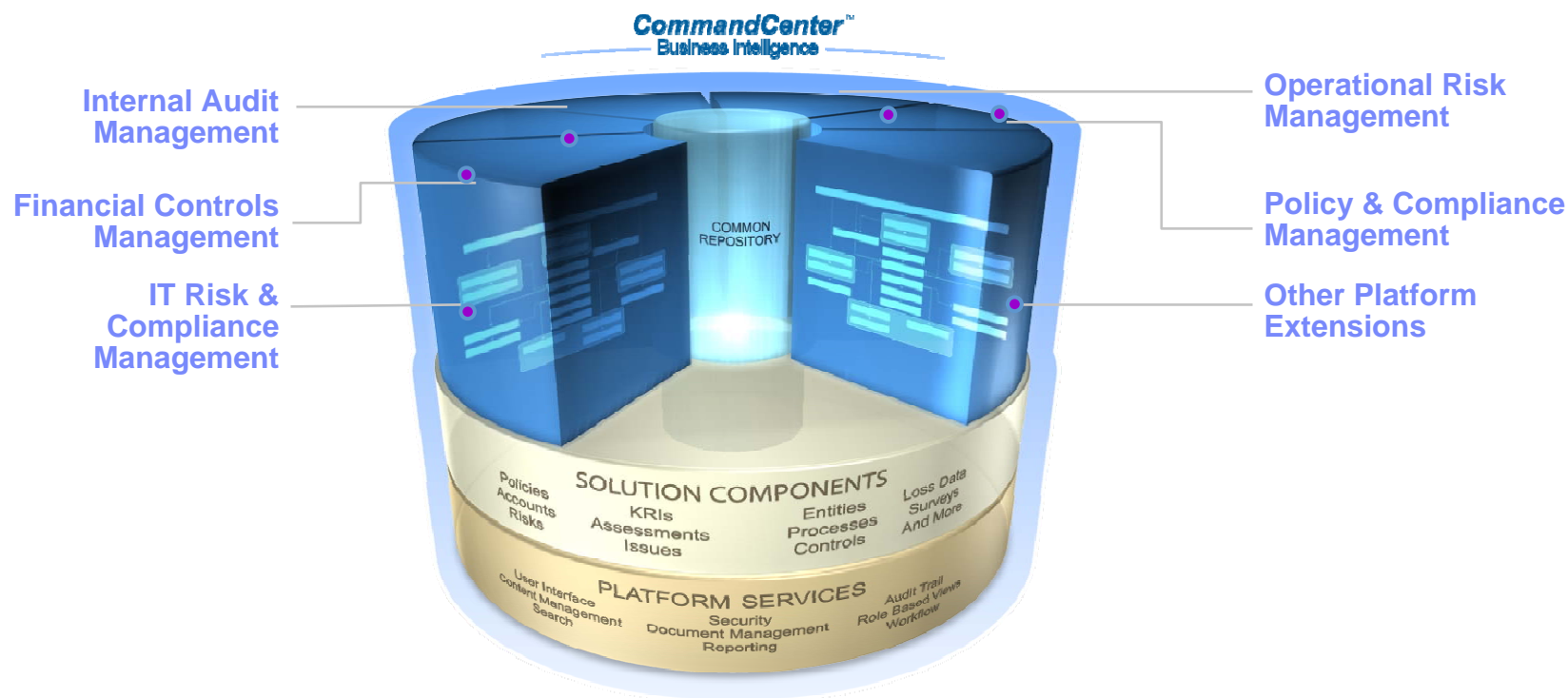
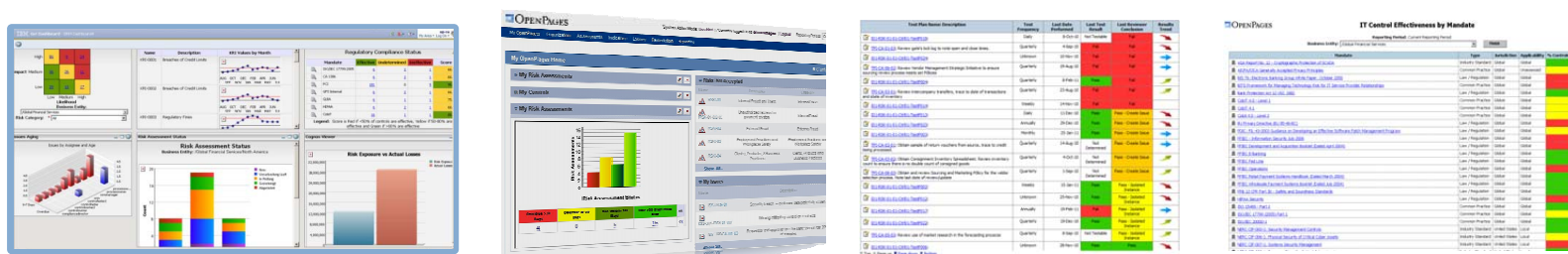


Integrated Risk Management Solves These Challenges

CEO/CRO/CFO



OpenPages Platform Provides an Integrated Approach to Risk Management



Proven by the World's Leading Companies

Financial Services



Insurance



Energy and Power



Health Services / Pharmaceuticals



Manufacturing



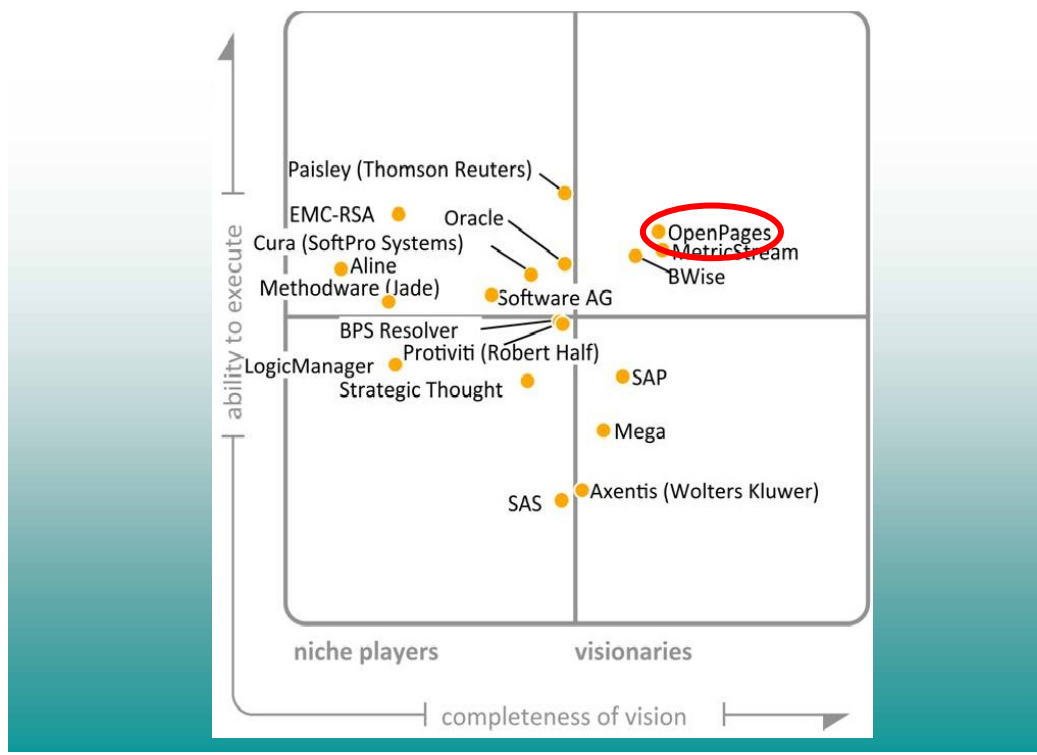
Retail/Consumer



Telecommunications



Recognized Enterprise GRC Platform Market Leader



Gartner

*Magic Quadrant for EGRC Platforms
October 2010*

FORRESTER

*The Forrester Wave: EGRC Platforms
July 2009*

IT Risk Governance Approach




Constraints and needs

External Drivers

- Federal and state regulations for data privacy and protection worldwide
- Industry-based standards (e.g. HIPAA, FFIEC, NERC, etc)
- Hackers, viruses and malware
- External auditors

Internal Drivers

- Minimize risk exposure and loss
- Ensure regulatory compliance
- Lower costs
- Preparing for internal audits
- Minimize duplicative control testing effort
- Integrate risk and policy management with enterprise reporting

-
- Reducing risk exposure
 - Ensuring regulatory compliance
 - Reducing control testing burden
 - Reporting on risk exposure against business objectives
 - Preparing for internal audit
-  CIO

Solutions

Policy Management

Track and manage internal policies

Map policies to regulatory compliance initiatives

IT Risk and Compliance

Identify, manage & monitor key IT risks in the business

Incident management and remediation

Technical controls integration

Other specific risk management initiatives

Vendor risk management

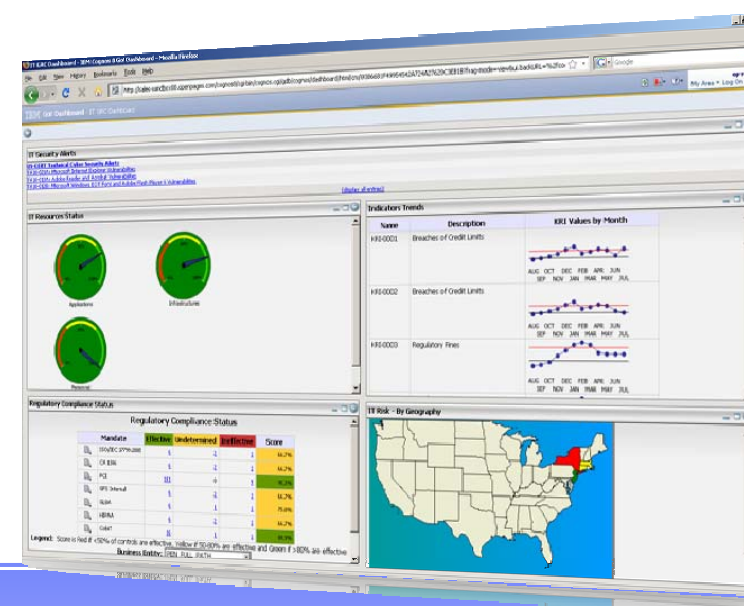
BCP and DR

Addressed by IBM OpenPages

OpenPages IT Governance Helps Companies Manage the Challenges Associated with IT GRC Programs

Key Features

- Integrated solution for managing IT Risk and compliance
 - Assess IT risk in context of business
 - Identify key risks, controls and/or gaps
- Support for the regulatory certification and audit process
- Track and manage IT incidents through their life cycle
- Manage common requirements across laws, regulations, standards and policies
- Integrated with UCF (Unified Compliance Framework), the industry's most comprehensive IT compliance database



Business Benefits

- Manage IT controls, risks and regulatory requirements according to the business services they support
- Deliver improved visibility, better decision support, and enhanced corporate performance
- Reduces the complexity of IT GRC programs

OpenPages ITG Supports the Key Use Cases

- IT Policy and Regulatory Compliance
- IT Risk Assessments and Management
- Control Monitoring and Assessment
- Integrated IT and Enterprise GRC

Use Case: IT Policy and Regulatory Compliance



Achieve and maintain compliance across multiple policies and regulations.

OpenPages ITG Capabilities

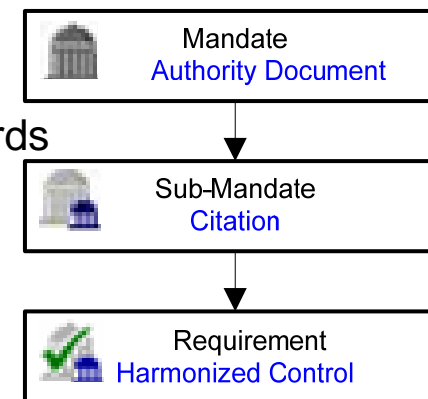
- Map IT policies and standards to authoritative sources such as ISO/IEC 2700x, COBIT®, PCI, FFIEC, HIPPA and NIST
- Assess and monitor compliance and manage exceptions
- Establish and implement best practice control frameworks for IT assets
- Executive and regulatory compliance dashboards

Business Benefits

- Provide confidence that compliance is achieved and corporate policies and procedures are enforced
- Quicker reaction time to changes in laws and regulations
- Minimize redundancies within control framework

IBM OpenPages ITG Includes UCF IT Regulatory Content

- 400+ Authority Documents in 23 Guidance Areas
 - Types: Laws, standards, best practices, etc.
 - Guidance Areas: Healthcare, energy, banking, payment card, records management, UK, Asia, US Fed, US States, IRS, etc.
- 27,000 Citations
 - Section identifiers plus Guidance
- 3800+ Harmonized Controls in 13 Impact Zones
- UCFmap enables easy browsing, filtering and loading UCF content



Leadership and High Level Objectives	Audits and Risk Management
Product Design and Development	Acquisition of Technology
Operational Management	Human Resources Management
Records Management	Technical Security
Physical Security	Systems Continuity
Monitoring and Reporting	Privacy
System Hardening through Configuration Management	

Piloter l'efficacité des contrôles



IT Control Effectiveness by Mandate

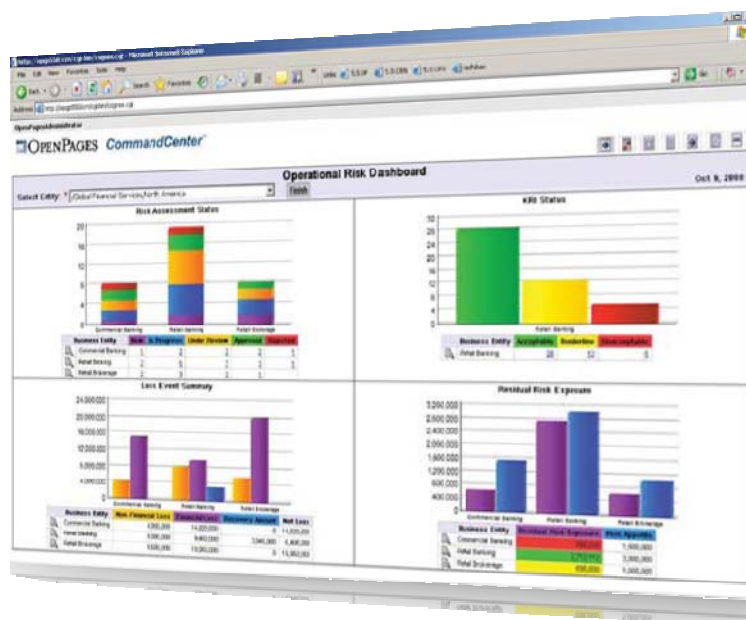
Reporting Period: Current Reporting Period

Business Entity:

Finish

Mandate	Type	Jurisdiction	Applicability	% Controls Effective
AGA Report No. 12 - Cryptographic Protection of SCADA	Industry Standard	Global	Global	100.0
AICPA/CICA Generally Accepted Privacy Principles	Common Practice	Global	Unassessed	83.3
BIS 76: Electronic Banking Group White Paper: October 2000	Law / Regulation	Global	Global	0.0
BITS Framework for Managing Technology Risk for IT Service Provider Relationships	Common Practice	Global	Global	25.0
Bank Protection Act 12 USC 1882	Law / Regulation	Global	Global	100.0
CobIT 4.0 - Level 1	Common Practice	Global	Global	83.8
CobIT 4.1	Common Practice	Global	Global	81.8
Cobit 4.0 - Level 2	Common Practice	Global	Global	83.3
EU Privacy Directive (EU 95-46-EC)	Law / Regulation	Global	Global	50.0
FDIC: FIL-43-2003 Guidance on Developing an Effective Software Patch Management Program	Law / Regulation	Global	Global	90.0
FFIEC - Information Security July 2006	Law / Regulation	Global	Global	72.2
FFIEC Development and Acquisition Booklet (Dated April 2004)	Law / Regulation	Global	Global	66.7
FFIEC E-Banking	Law / Regulation	Global	Global	100.0
FFIEC Fed Line	Law / Regulation	Global	Global	100.0
FFIEC Operations	Law / Regulation	Global	Global	80.0
FFIEC Retail Payment Systems Handbook (Dated March 2004)	Law / Regulation	Global	Global	100.0
FFIEC Wholesale Payment Systems Booklet (Dated July 2004)	Law / Regulation	Global	Global	100.0
FRB 12 CFR Part 30 - Safety and Soundness Standards	Law / Regulation	Global	Global	100.0
HIPAA Security	Law / Regulation	Global	Global	75.0
ISO 15489 - Part 2	Common Practice	Global	Global	100.0
ISO/IEC 17799 (2005) Part 1	Common Practice	Global	Global	83.9
ISO/IEC 20000-1	Common Practice	Global	Global	100.0
NERC CIP-003-1: Security Management Controls	Industry Standard	United States	Local	100.0
NERC CIP-006-1: Physical Security of Critical Cyber Assets	Industry Standard	United States	Local	85.7
NERC CIP-007-1: Systems Security Management	Industry Standard	United States	Local	75.0

Use Case: IT Risk Assessments and Management



Identify and manage IT risks that impact business performance.

OpenPages ITG Capabilities

- Risk control self-assessments, end-user surveys, key indicators, executive dashboards, automated workflow and issue remediation
- Map IT and technology risks into business processes and understand the interdependencies of risk across systems
- Top-down assessments and bottom up control monitoring

Business Benefits

- Identify key risks that can impact business performance
- Codify best practices and standardize control frameworks
- Increase visibility to risk exposure and reduce unexpected outcomes

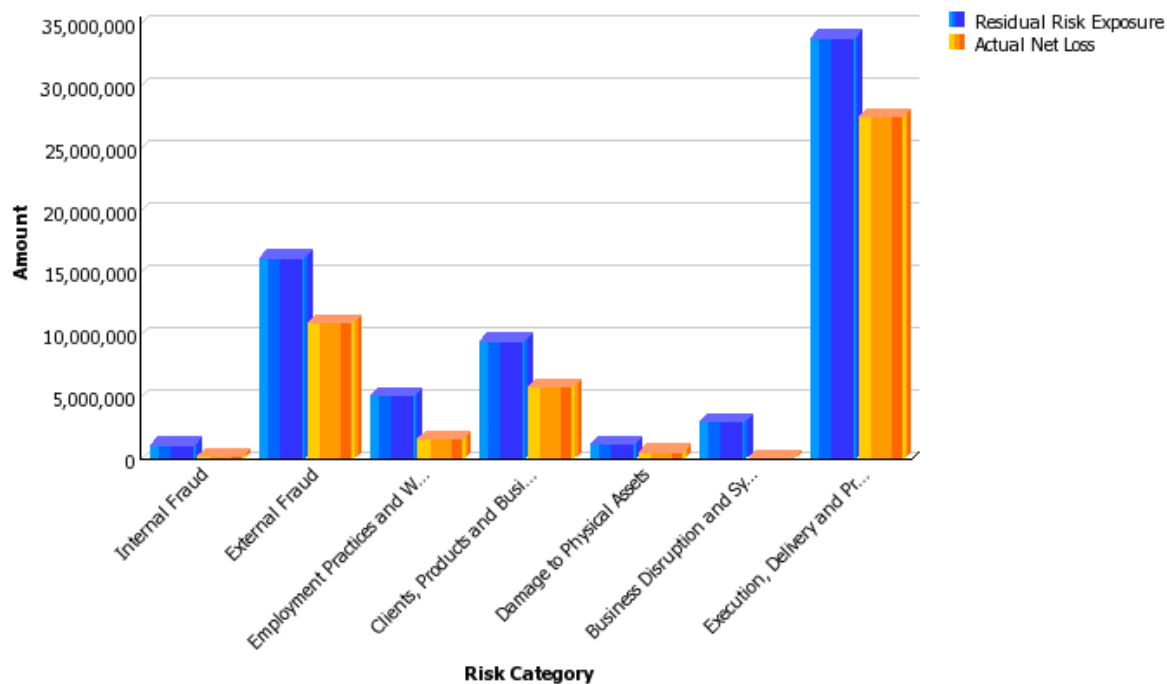
Rapprochement entre les pertes et les evaluation des risques



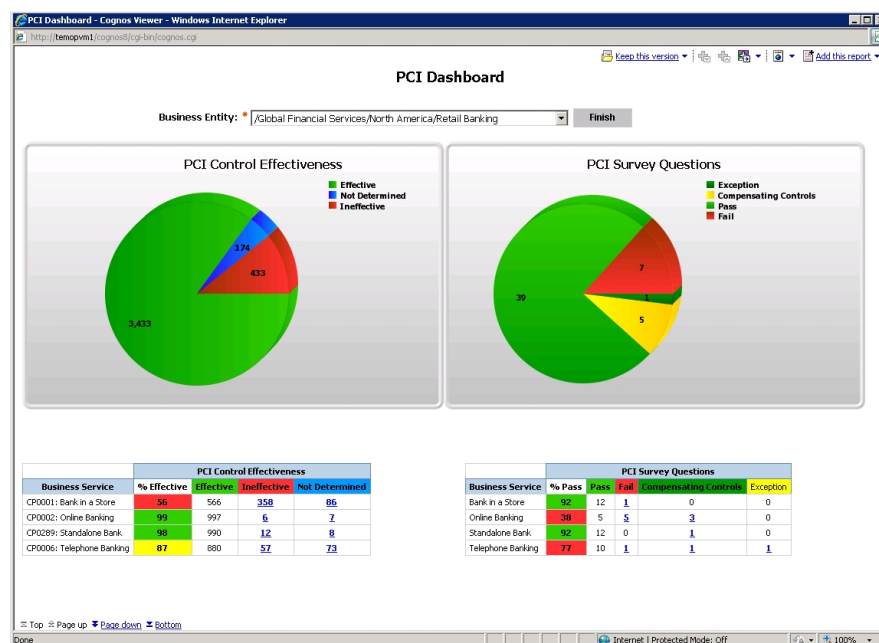
Risk vs Loss

Reporting Period: Current Reporting Period
Risk Appetite: \$100,000,000
Status: All
Domain: Operational
Occurrence Date Range: Jan 1, 2005 - Jan 1, 2006
Currency: USD

Business Entity: /Global Financial Services Finish



Use Case: Control Monitoring and Assessment



Provide business and regulatory context to IT system configurations, security and access control data.

OpenPages ITG Capabilities

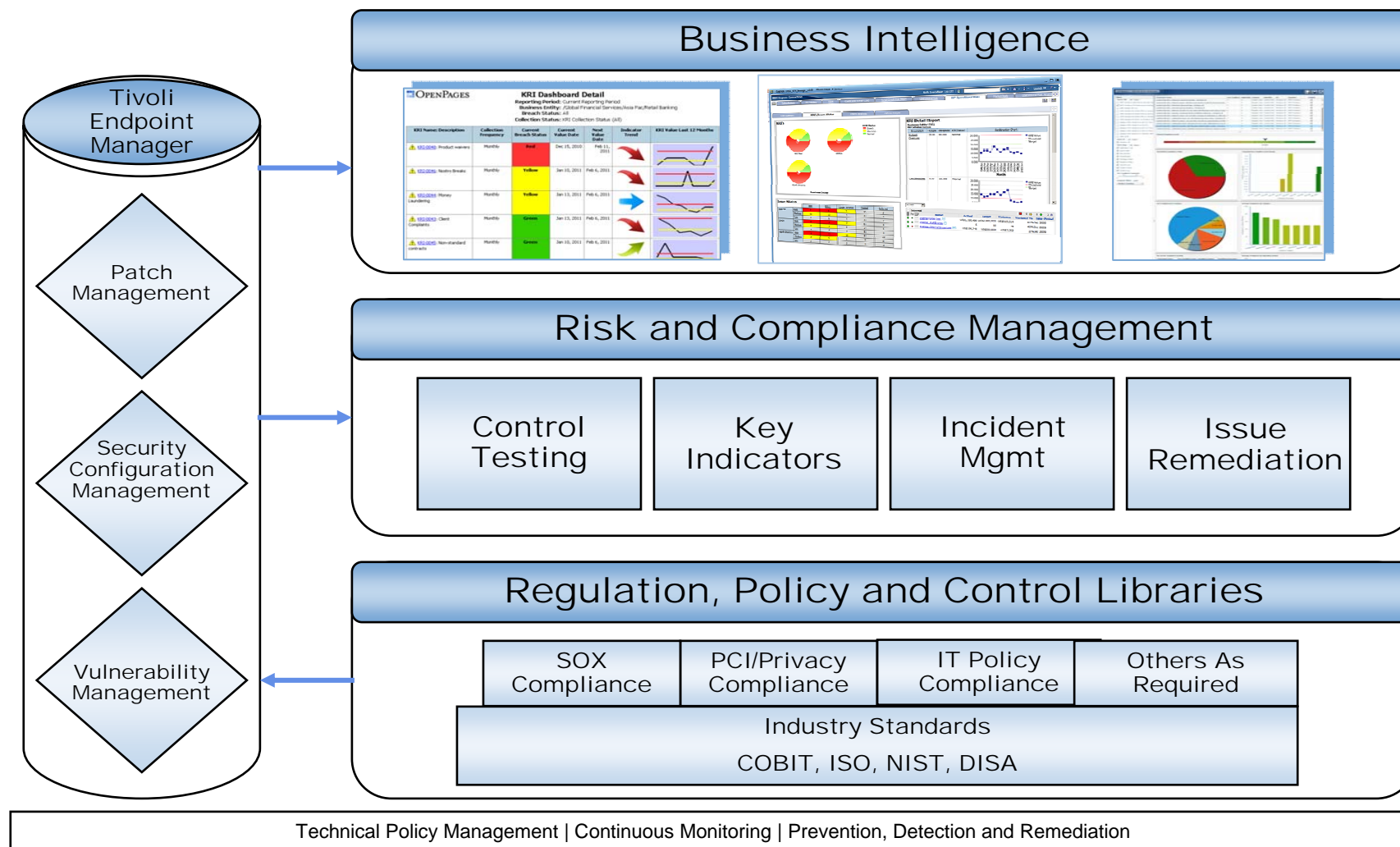
- Maps best practice control baselines to IT assets and the business services they support
- Collects data to assess the state of your IT operating environment
- When integrated with your preventative and detective IT control infrastructure, automates data collection and control monitoring
- Remediate control gaps

Business Benefits

- Provide risk and regulatory context for control data housed in multiple IT systems
- Consolidate data and report compliance initiatives across multiple mandates
- Effectively assess business impact of control failures, threats, vulnerabilities and incidents
- Optimize control infrastructure based on business impact

Drive effective monitoring using rich asset, security compliance and configuration management data

Example: Integration with Tivoli Endpoint manager



Pilotage automatique par alertes



KRI Dashboard Detail

Reporting Period: Current Reporting Period

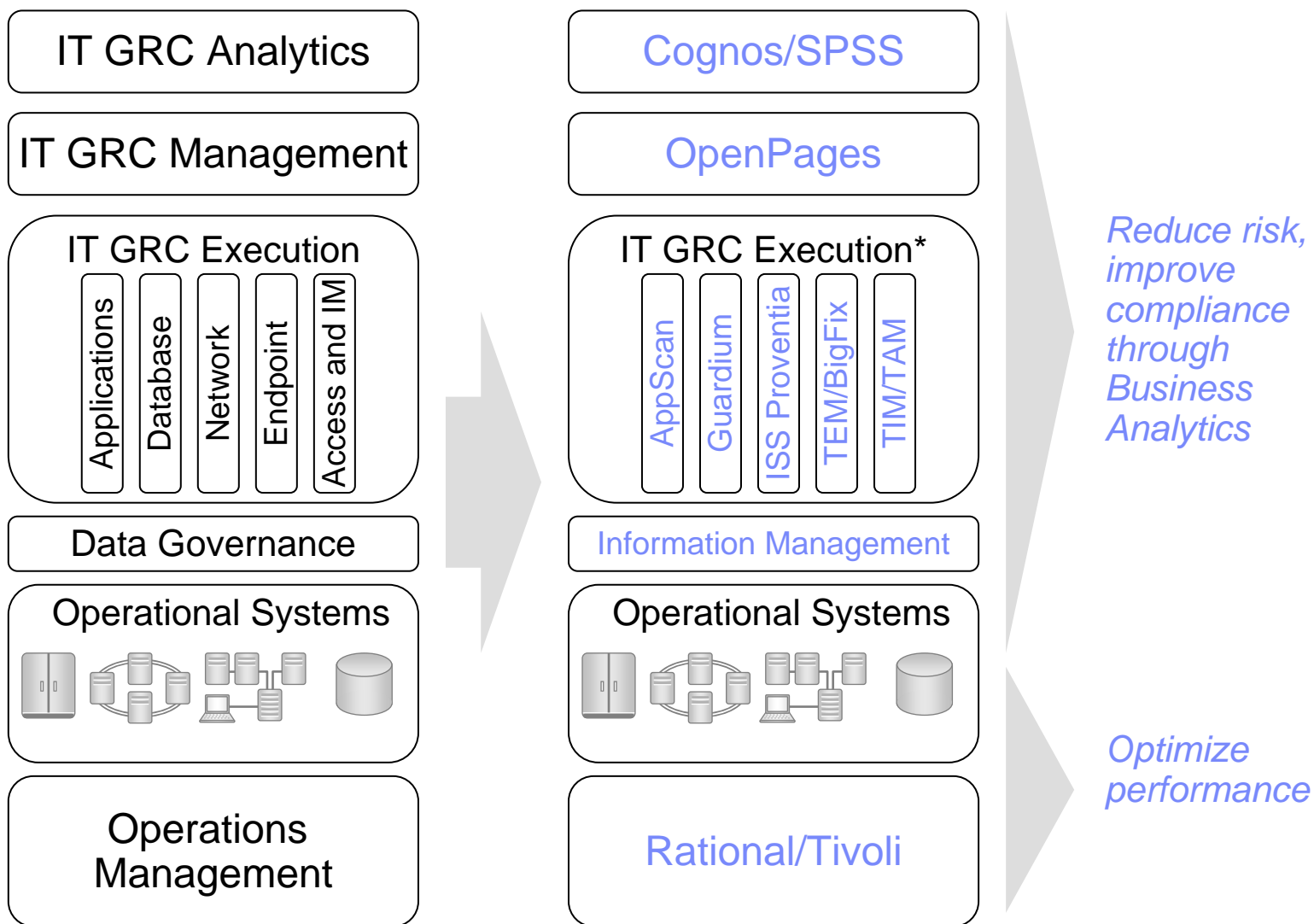
Business Entity: /Global Financial Services/Asia Pac/Retail Banking

Breach Status: All

Collection Status: KRI Collection Status (All)

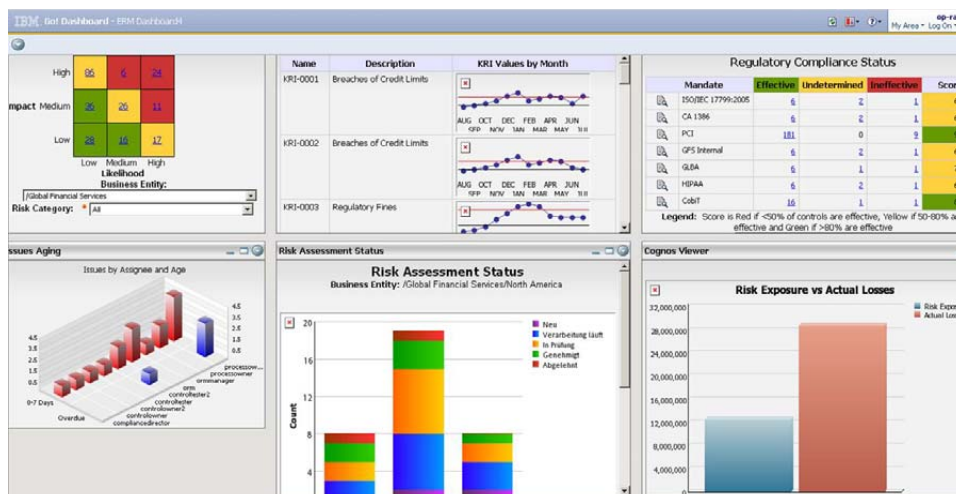
KRI Name: Description	Collection Frequency	Current Breach Status	Current Value Date	Next Value Date	Indicator Trend	KRI Value Last 12 Months
KRI-0048 : Product waivers	Monthly	Red	Dec 15, 2010	Feb 11, 2011		
KRI-0046 : Nostro Breaks	Monthly	Yellow	Jan 10, 2011	Feb 6, 2011		
KRI-0044 : Money Laundering	Monthly	Yellow	Jan 13, 2011	Feb 6, 2011		
KRI-0043 : Client Complaints	Monthly	Green	Jan 13, 2011	Feb 6, 2011		
KRI-0045 : Non-standard contracts	Monthly	Green	Jan 10, 2011	Feb 6, 2011		
KRI-0047 : Payment Frauds	Monthly	Green	Sep 15, 2010	Feb 11, 2011		
KRI-0049 : Suspense Account Balances	Monthly	Green	Jan 3, 2011	Feb 11, 2011		
KRI-0050 : Unauthorized transactions	Monthly	Green	Jan 10, 2011	Feb 16, 2011		

IBM's IT GRC Approach Closes the Loop Between Oversight and Operations



*representative solutions

Use Case: Integrated IT and Enterprise GRC for Enterprise-wide View of Risk



Integrate risk management and compliance processes to leverage GRC information and make better business decisions.

OpenPages ITG Capabilities

- Eliminates siloed risk management
- Harmonizes common IT controls across multiple regulations, including SOX, PCI, data privacy requirements and industry regulations
- Leverages a centralized repository and provides integrated, cross-module reporting, dashboards, workflow, and security

Business Benefits

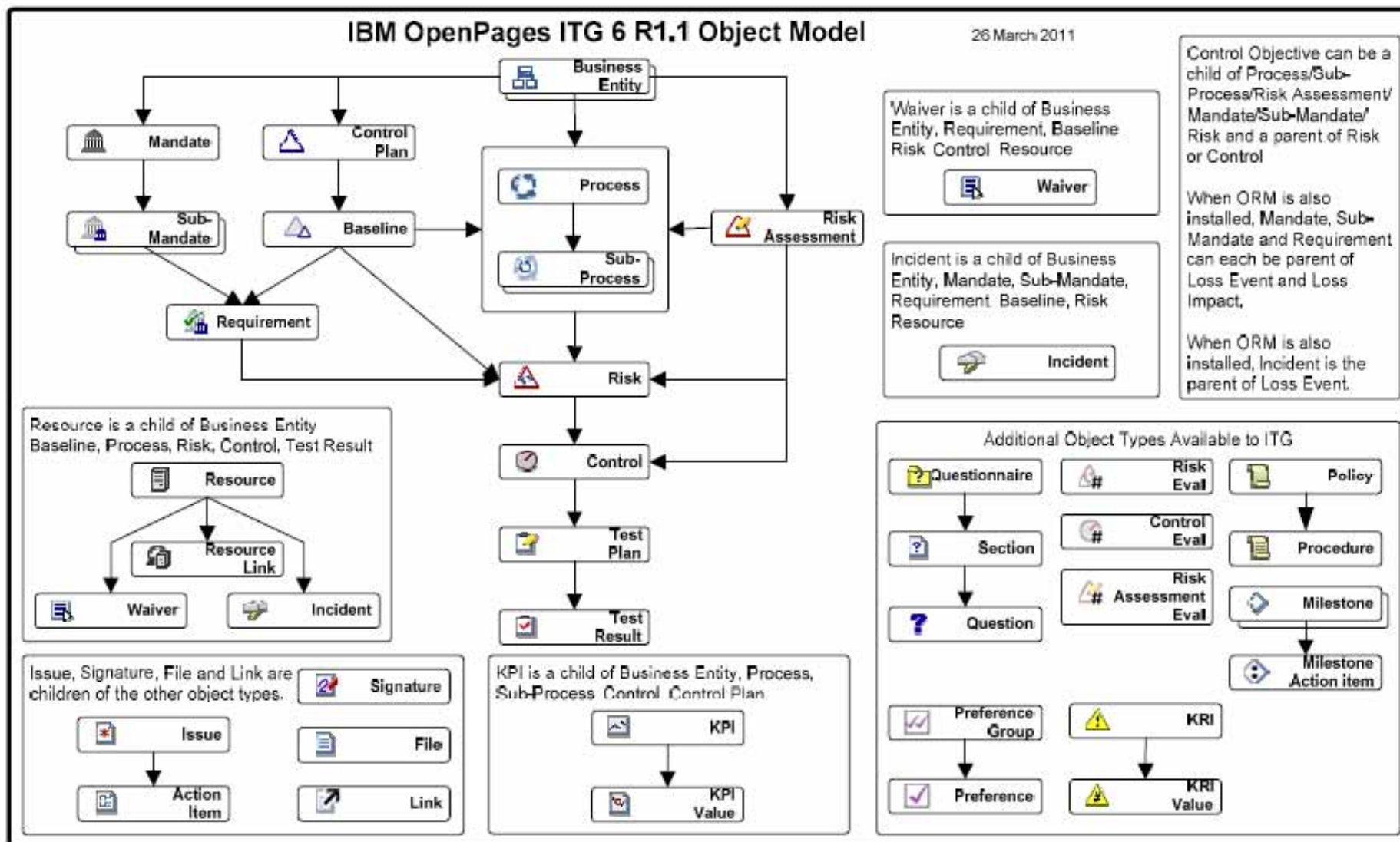
- Deliver improved visibility, better decision support, and enhanced corporate performance
- Heat maps and executive dashboards provide enterprise-wide view of risk exposure
- Provide confidence that compliance is achieved, risks are mitigated and corporate policies and procedures are enforced

Benefits Summary

- Manage IT controls, risks and regulatory requirements according to the business services they support
- Codify best practices and standardize control frameworks
- Increase visibility to risk exposure and reduce unexpected outcomes
- Minimize redundancies within control framework
- Provide confidence that compliance is achieved, risks are mitigated and corporate policies and procedures are enforced

MERCI

OpenPages Data Model



IBM OpenPages ITG 6 R1.1 Reference Library and IT Operating Environment View

8 April 2011

