<Name>
<Date>

Managing Governance, Risk & Compliance

Agenda

➢ What is Governance, Risk & Compliance?

➢ Approaches to manage GRC: Benefits & Drawbacks

➢ Foundational elements to enable an integrated approach to GRC

➢ Managing Risk & Driving Performance with the IBM OpenPages GRC Platform

What is Governance, Risk & Compliance?

What is Governance, Risk & Compliance?

Governance – describes the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.

Risk management is the set of processes through which management identifies, analyzes, and, where necessary, responds appropriately to risks that might adversely affect realization of the organization's business objectives.

Compliance means conforming with stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, fund and initiate any corrective actions deemed necessary.

Examples: BASEL, ISO, COBIT, COSO, SOX, Solvency, Corporate Governance, Accounting Standards, etc

What is Governance, Risk & Compliance?

Enabling the process of making business decisions based on review of potential profit/loss against expected and/or unexpected risk
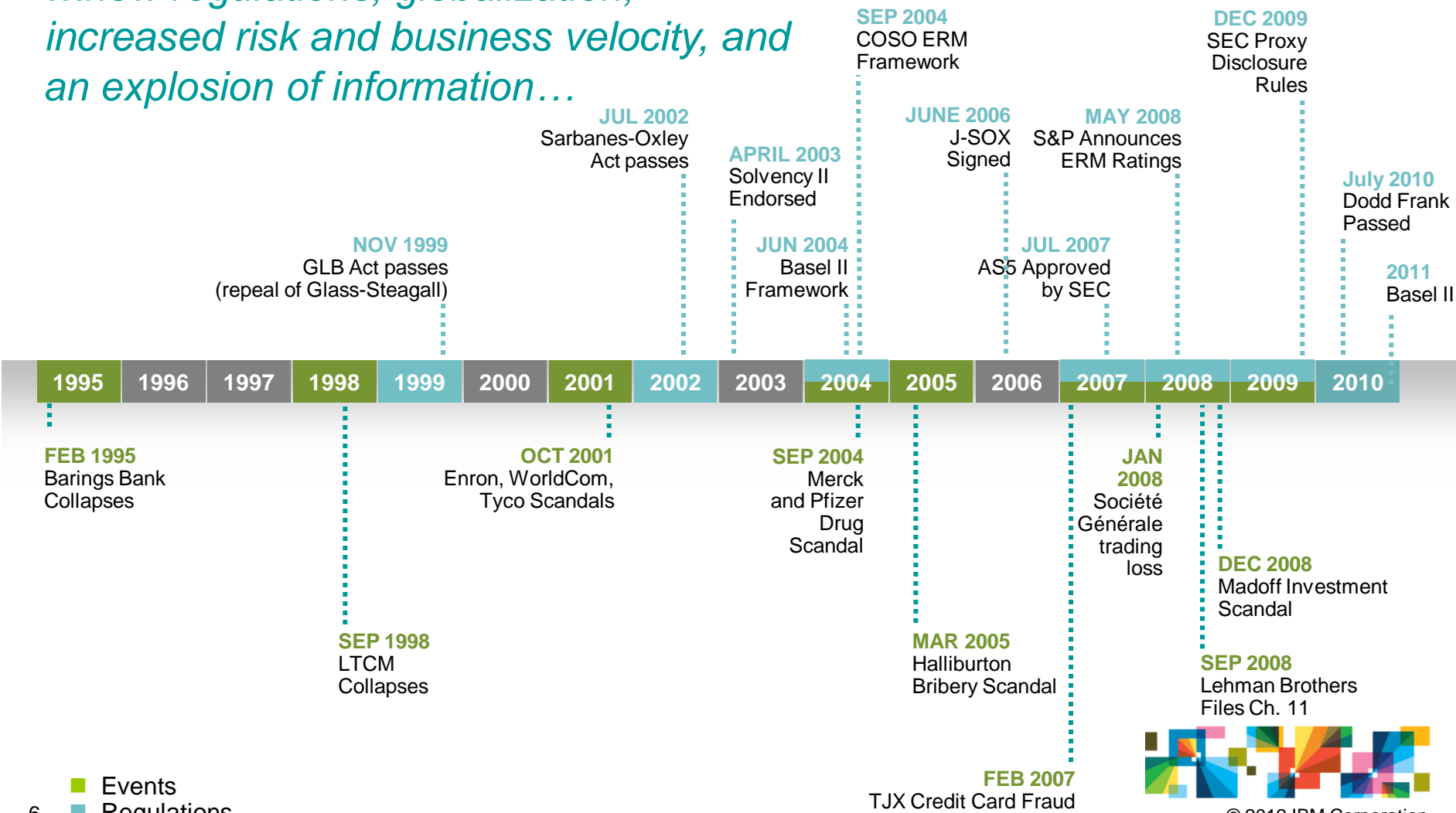
Risk Aware (Not Risk Averse)

Key Themes

- GRC has always existed; formalized structure being put in place.
- GRC should be pervasive throughout all business units and processes.
- Risk Appetite – Top down/bottom up? Qualitative/Quantitative?
- Cost Benefit Analysis of Controls
- Practical applicability of GRC framework is very specific to an industry and/or organization

Risk has never been a bigger challenge than in today's business environment

…new regulations, globalization, increased risk and business velocity, and an explosion of information…

SEP 2004
COSO ERM Framework

DEC 2009
SEC Proxy Disclosure Rules

JUL 2002
Sarbanes-Oxley Act passes

JUNE 2006
J-SOX Signed

MAY 2008
S&P Announces ERM Ratings

APRIL 2003
Solvency II Endorsed

July 2010
Dodd Frank Passed

JUN 2004
Basel II Framework

JUL 2007
AS5 Approved by SEC

NOV 1999
GLB Act passes (repeal of Glass-Steagall)

2011
Basel III

1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010

FEB 1995
Barings Bank Collapses

OCT 2001
Enron, WorldCom, Tyco Scandals

SEP 2004
Merck and Pfizer Drug Scandal

JAN 2008
Société Générale trading loss

DEC 2008
Madoff Investment Scandal

SEP 1998
LTCM Collapses

MAR 2005
Halliburton Bribery Scandal

SEP 2008
Lehman Brothers Files Ch. 11

FEB 2007
TJX Credit Card Fraud

■ Events
■ Regulations

6

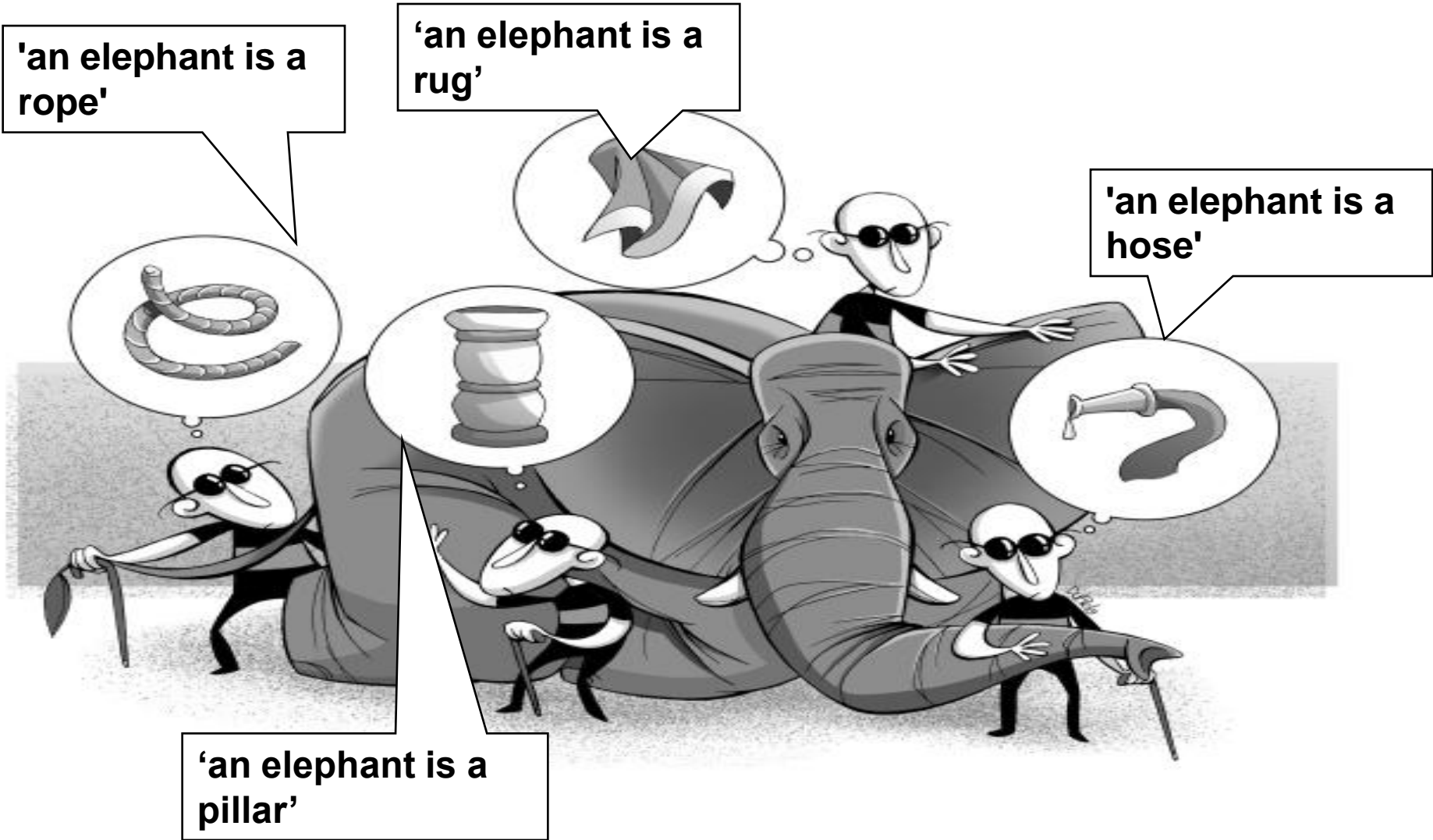Most companies cannot keep pace, and we can expect continued evolution

- New regulations doubling every six years
- Most process controls and risk management implemented manually
- Risk, Compliance, Audit are independent functions without any convergence
- Risk management focused on compliance not performance
- Compliance focused on regulations, no value add
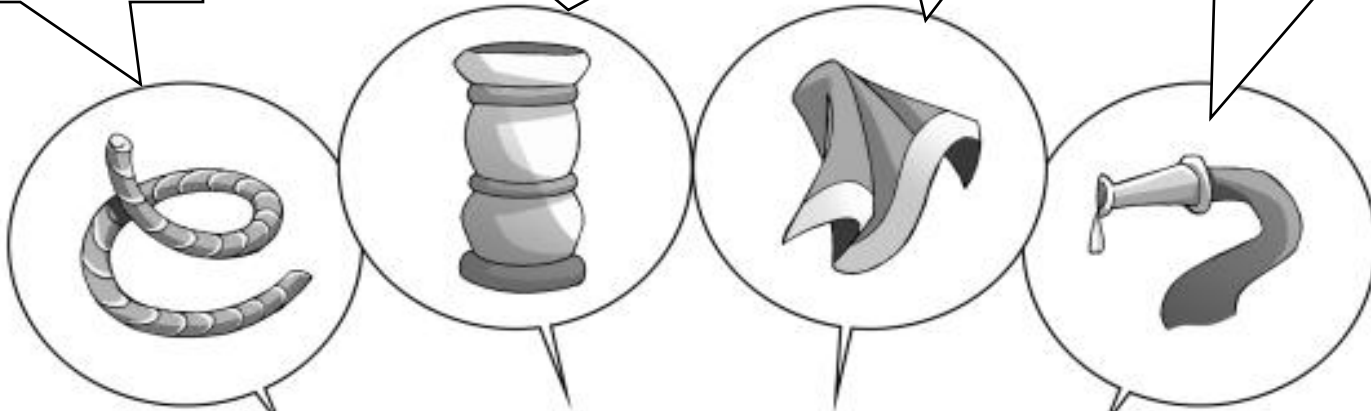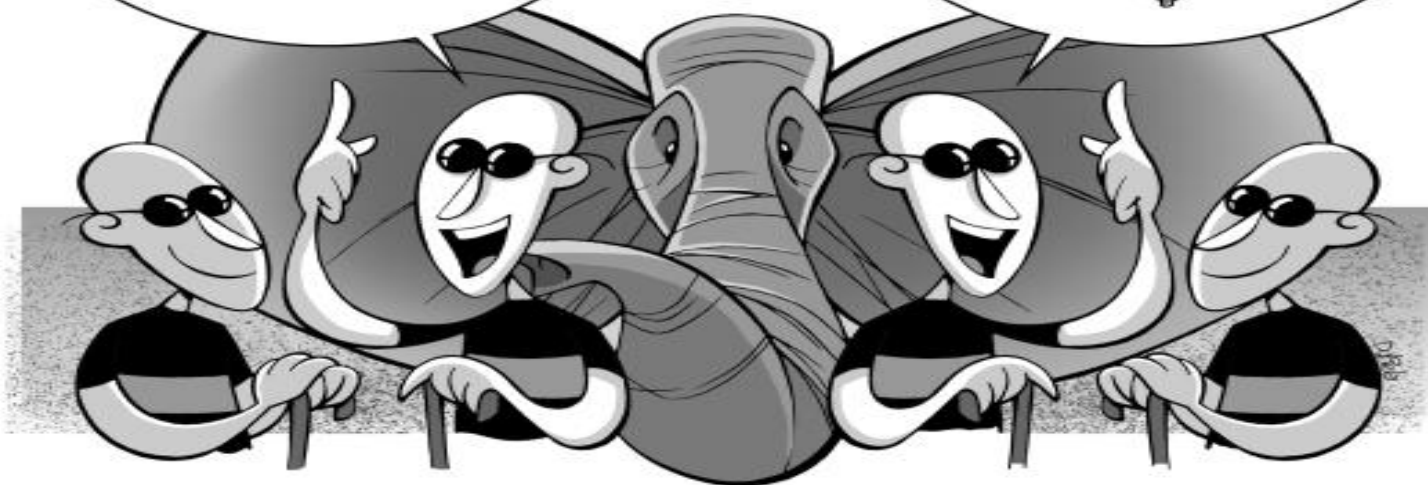
Approaches to manage GRC: Benefits & Drawbacks

The Siloed Approach

Best Practices	Regulations	Risk Management	Internal Policy

Sub-Sections   **Sub-Sections**   **Sub-Sections**   **Sub-Sections**

Redundant control framework

The Integrated Approach

Standardized Libraries

| Best Practices | Regulations | Risk Management | Internal Policy |

Common Requirements

Rationalized Control Framework
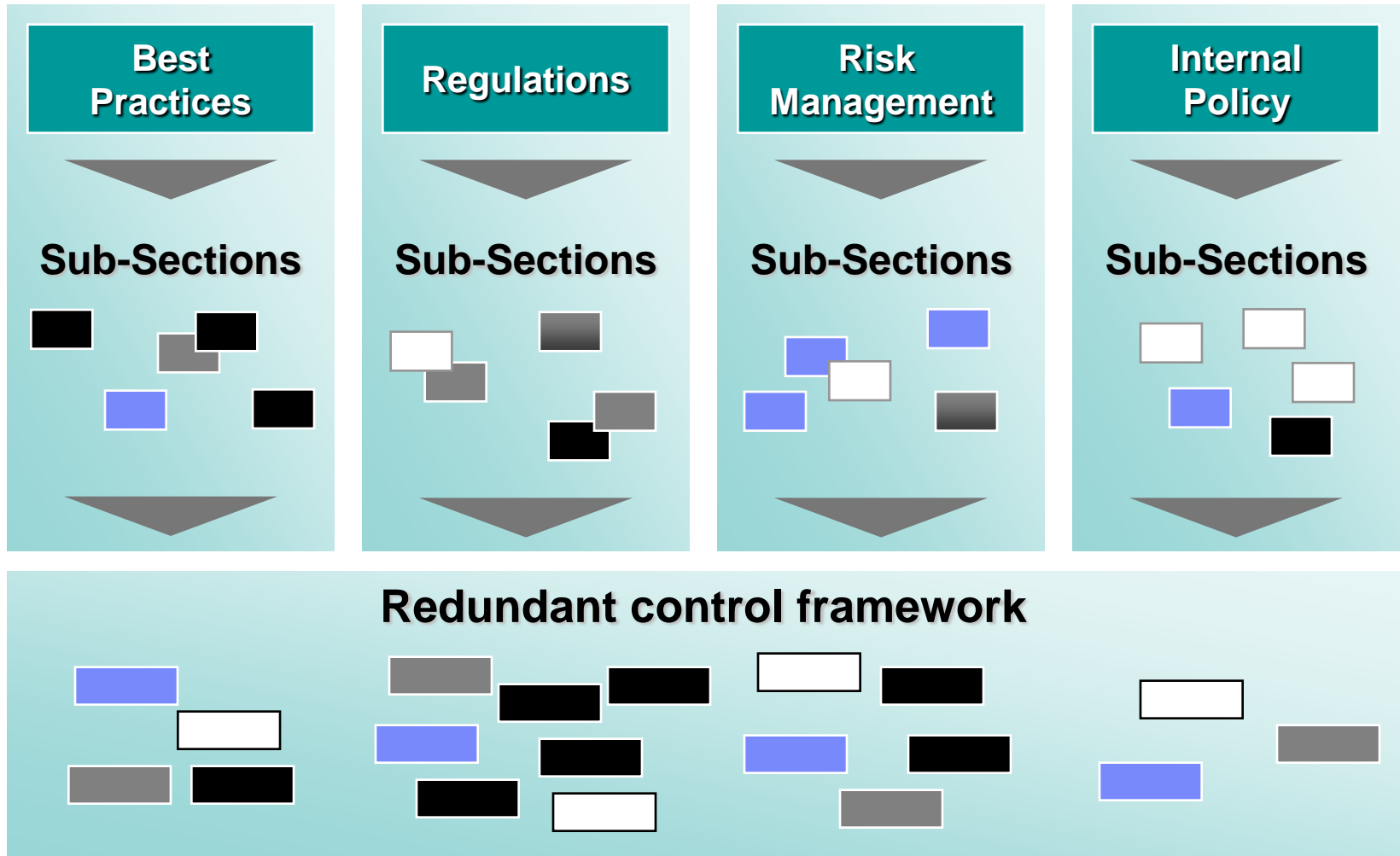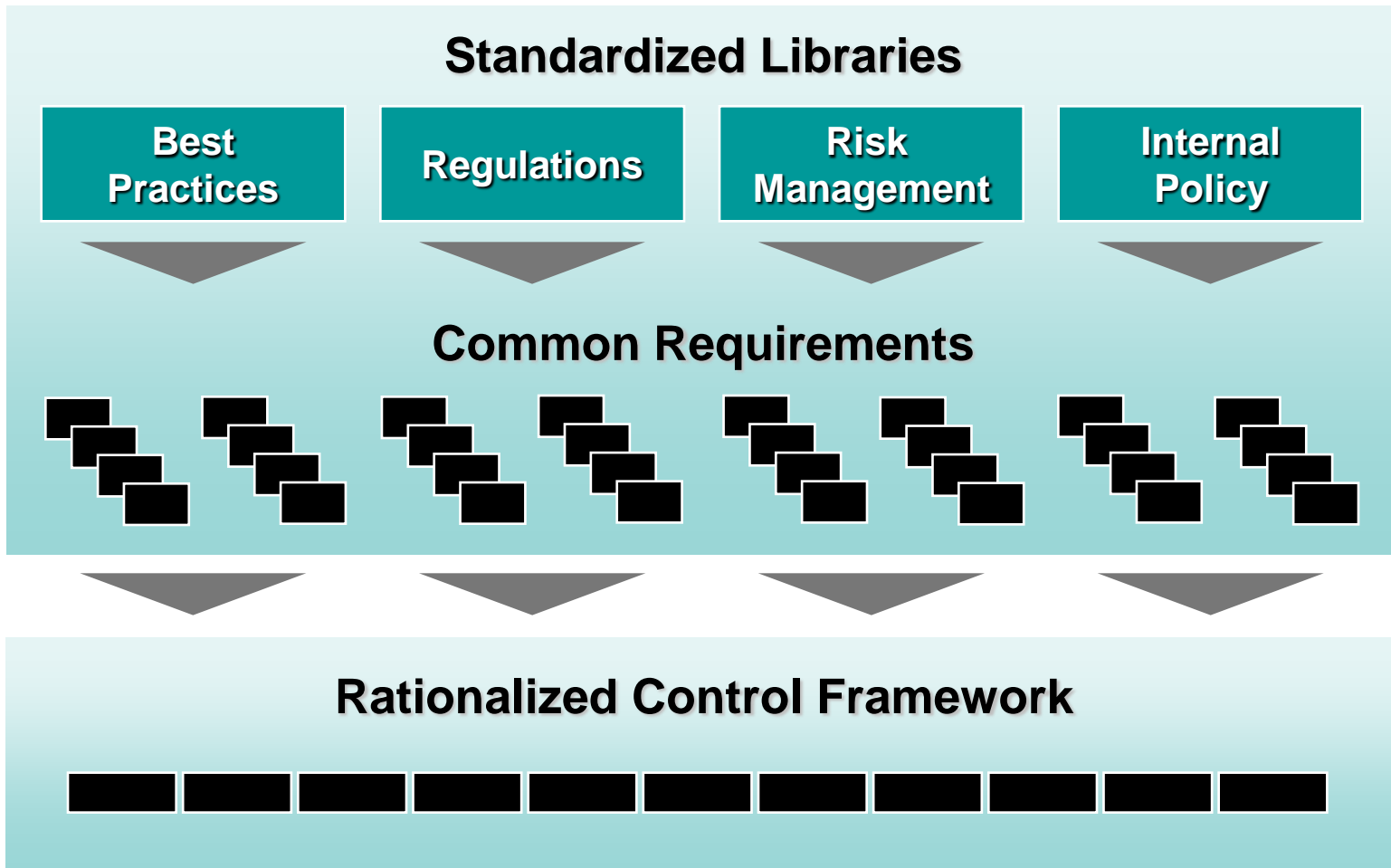
An integrated approach reduces redundancies in control testing, assessments and audits

GRC Function

Risk **Compliance** **Assurance**

Requirements

R1   R2   R3   R4

Controls

C1   C2   C3   C4

- Control testing
- Assessments
- Audits
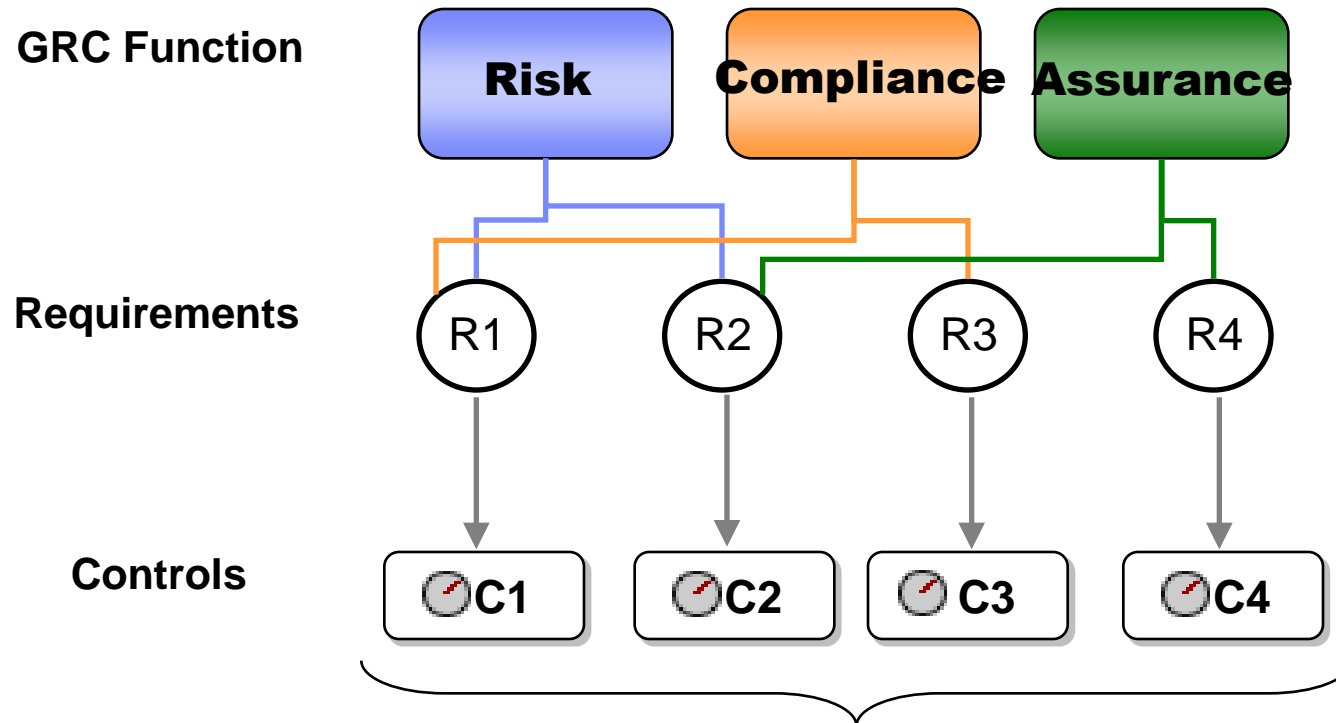
2010 OCEG GRC Maturity Survey
Those who have integrated GRC see…

Reduction in -

- gaps in risk and compliance processes
- redundant or duplicative activities
- impact on operations from siloed and uncoordinated risk assessments
- costs of GRC activities

Greater ability to -

- repeat processes in a consistent manner
- gather information quickly and efficiently
- present consolidated, meaningful information and analyses to the board and senior management

Foundational elements to enable an integrated approach to GRC

What are the foundational elements for a integrated approach to risk and compliance?

- Governance model
- Process mapping
- Common risk rating & taxonomy
- Centralized libraries
- Standard reporting requirements
- Technology solution to support the above
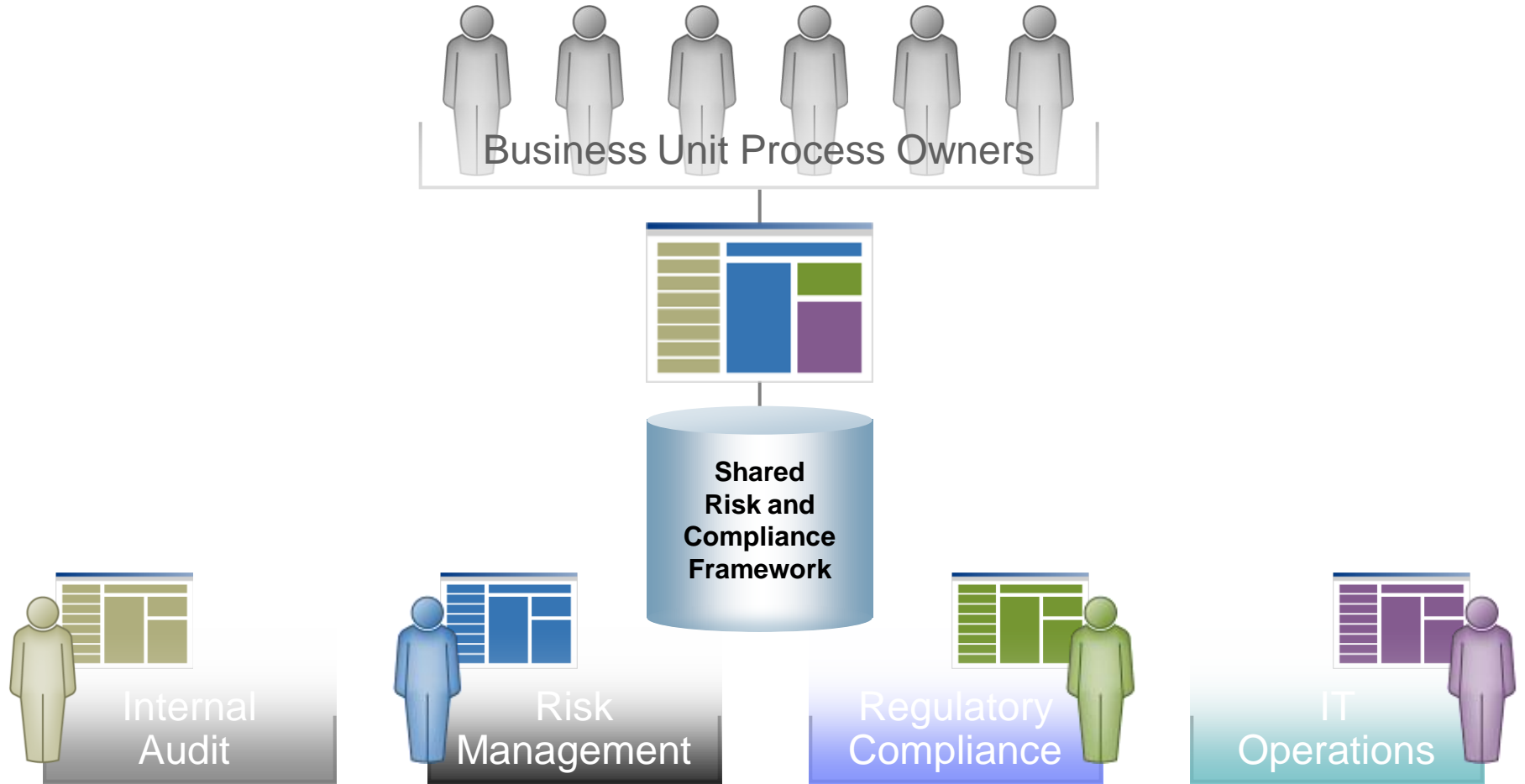
GRC Roles and Challenges

Roles

Board of Directors
CFO
CRO
COO
Chief of Audit
Chief Legal Officer
Chief Compliance Officer
Company Secretary
IT and Information Systems Auditors
BU Risk heads
BU Line Managers

Challenges

➢ **Objective setting** through policy management review and measurement

➢ **Accountability** through workflow, reporting and issues tracking, and roles and responsibilities

➢ **Oversight** through independent assessment, review and audit

➢ **Identifying risks and assessing their impact** within the context of corporate strategy and business objectives

➢ **Coordinating risk and compliance functions** across the enterprise

➢ **Aggregating and reporting risk and compliance information** for enterprise risk posture across multiple Roles

➢ **Making the best decisions** about aligning actions to Risk appetite and allocation of capital

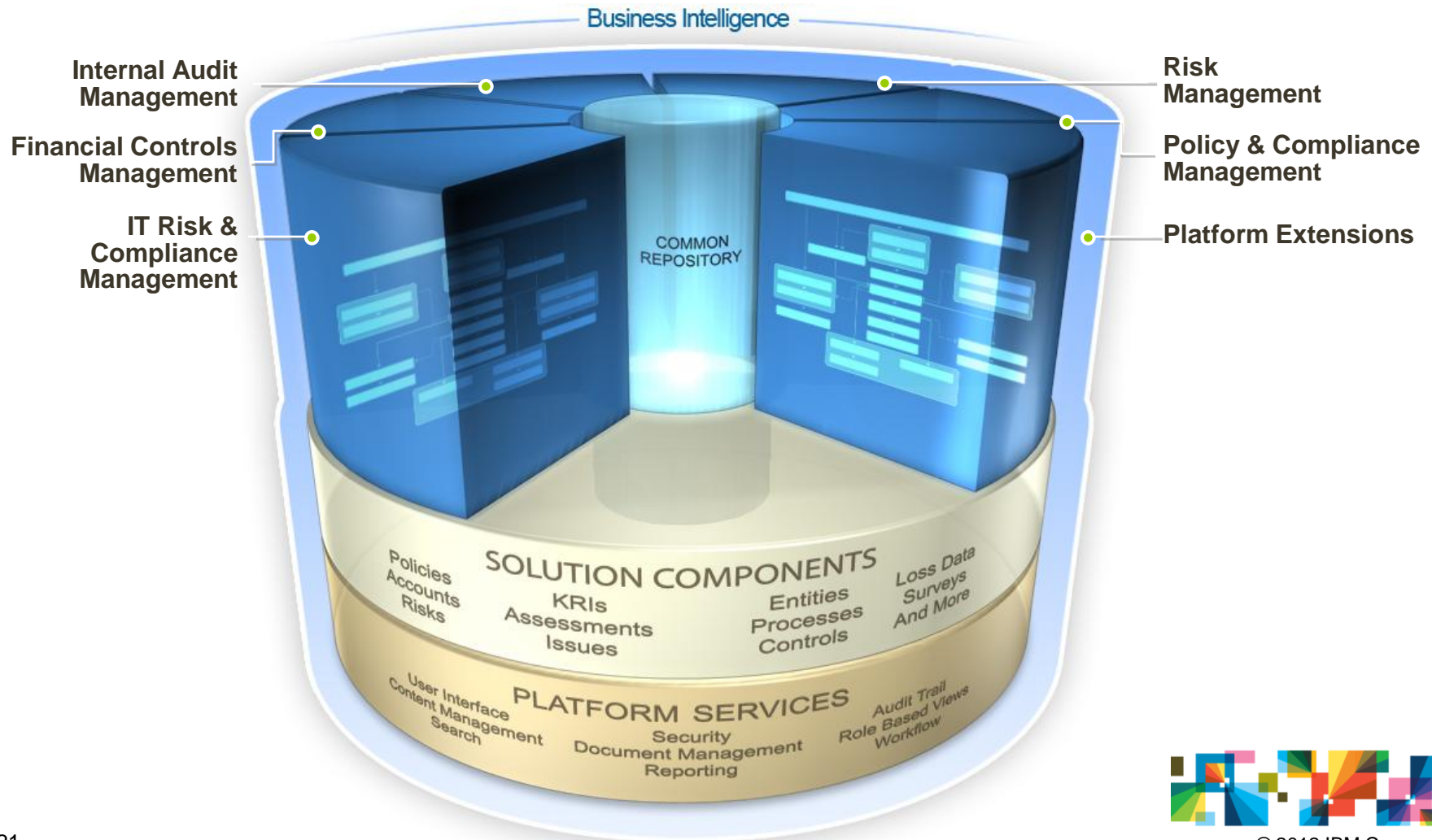# Huge Efficiencies and Business Process Improvement Through Convergence

Business Unit Process Owners

Shared Risk and Compliance Framework

Internal Audit

Risk Management

Regulatory Compliance

IT Operations

Managing Risk & Driving Performance with the IBM OpenPages GRC Platform

SmarterAnalytics

IBM ⚫

IBM OpenPages GRC Platform integrates key risk and compliance functions

Business Intelligence

Internal Audit Management

Financial Controls Management

IT Risk & Compliance Management

Risk Management

Policy & Compliance Management

Platform Extensions

COMMON REPOSITORY

SOLUTION COMPONENTS

Policies Accounts Risks

KRIs Assessments Issues

Entities Processes Controls

Loss Data Surveys And More

PLATFORM SERVICES

User Interface Content Management Search

Security Document Management Reporting

Audit Trail Role Based Views Workflow

Supporting the need of different GRC functions

ERM, Compliance users see localized views of the same risk

- Some fields are common to both views, some fields are specific to a single view
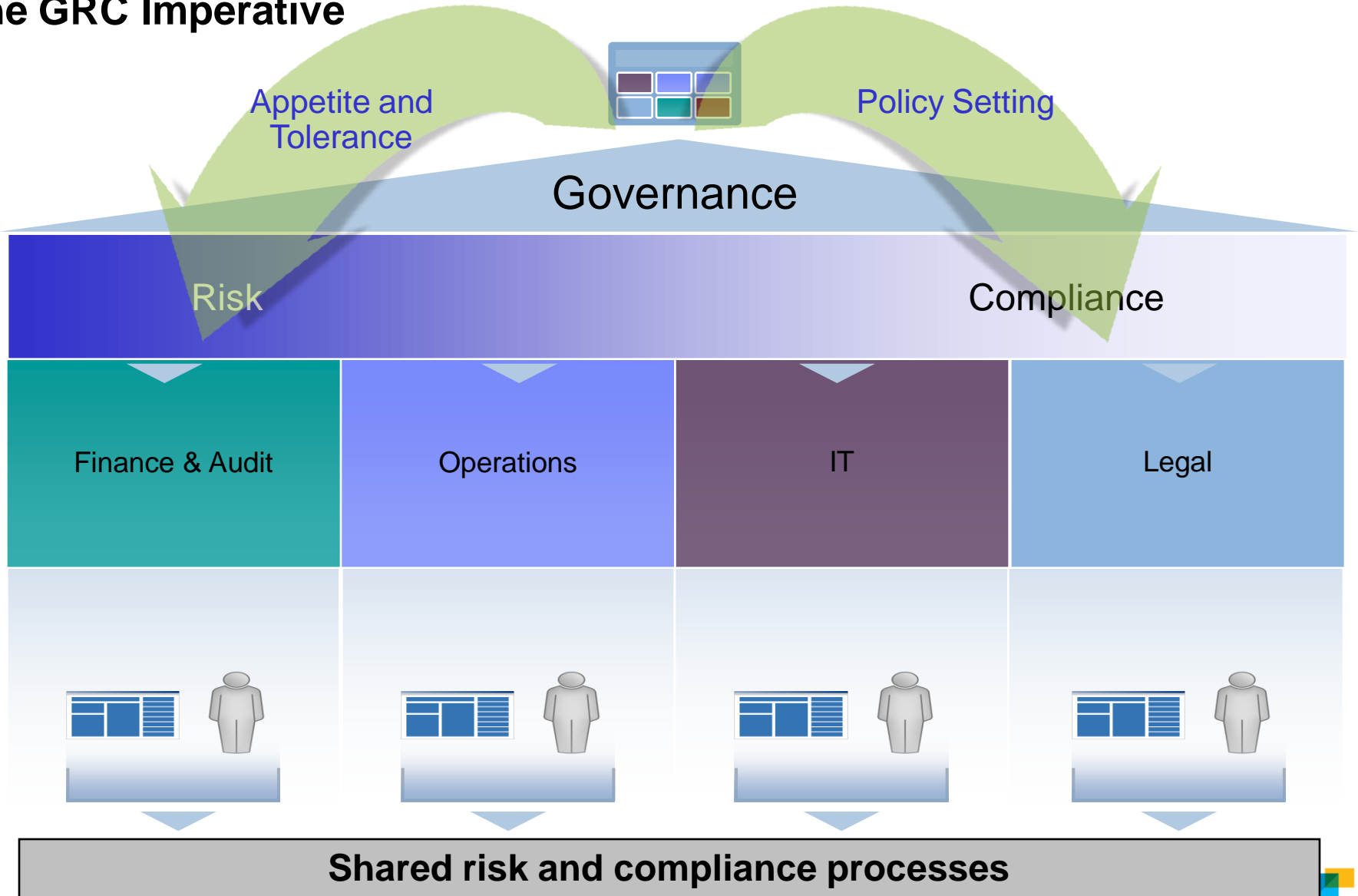- Everyone agrees on a base set of fields and a common risk taxonomy

ERM
view of Risk

Assessor: Sue Smith
Category: Int Fraud
Frequency: 10

Measurement
$5,000,000
$2,500,000
$1,000,000

Severity:

Business Entity

Process

Regulation / Policy

Sub-Process

Sub-Regulation / Procedure

⚠ **Risk**

Control

Compliance
view of Risk

Assertion: Existence
Category: Int Fraud
Likelihood: Medium

Measurement
High
Medium
Low

Impact:
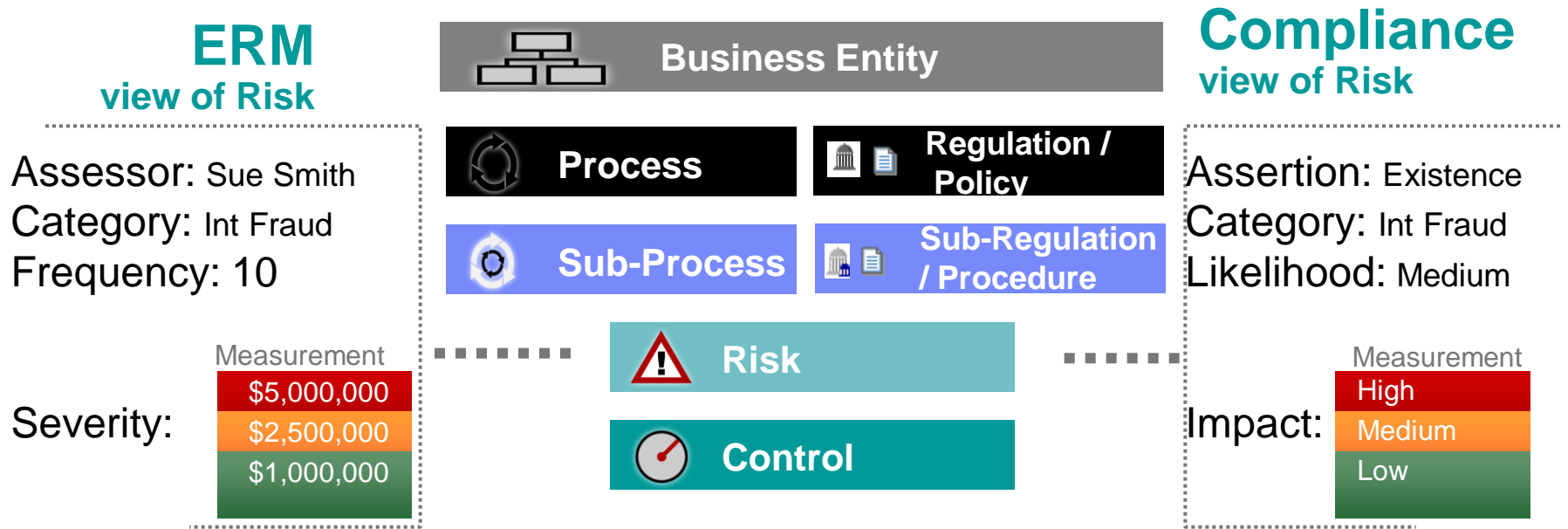
Further, you can reduce duplication across the spectrum of oversight activities

ACTIVITIES

FUNCTIONS	Assess-ment	Control Testing	Reporting	Issue Mgmt	Policy Mgmt
Risk	✓	✓	✓	✓	✓
Compliance	✓	✓	✓	✓	✓
IT	✓	✓	✓	✓	✓
Finance	✓	✓	✓	✓	✓
Audit	✓	✓	✓	✓	✓

The GRC Imperative

Appetite and Tolerance

Policy Setting

Governance

Risk

Compliance

| Finance & Audit | Operations | IT | Legal |

Shared risk and compliance processes

Risk and Compliance Intelligence: Moves GRC into business

From...
Risk and Compliance Office

CRO

Auditor

CCO

Legal

To...
Business Users and Managers

Business User

Executive

Business Analyst

Manager

# Representative Process A

Loss Events
Audit Findings
Issues
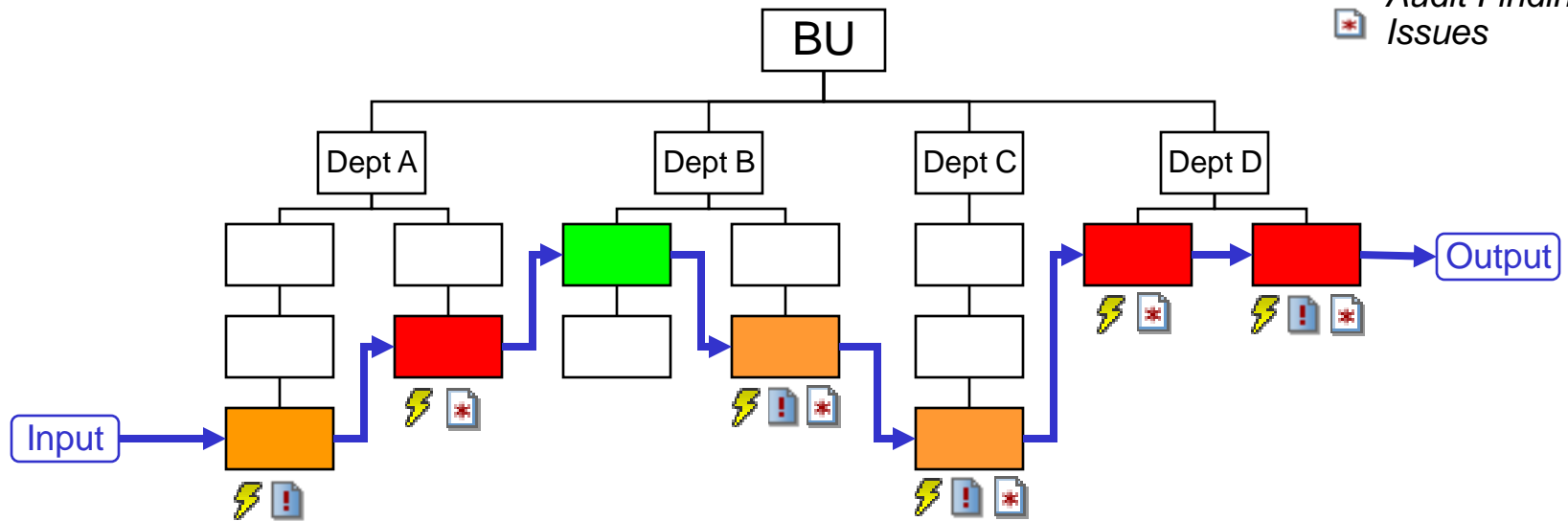

Representative Process B
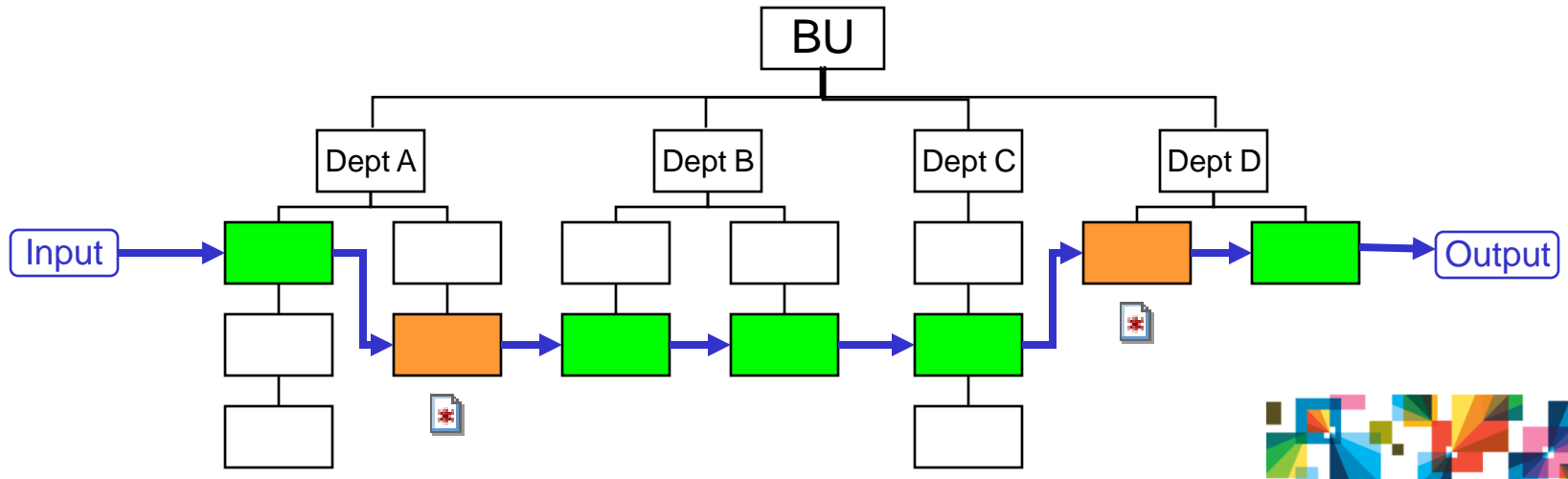
Using Smarter GRC framework to facilitate business decisions and drive process effectiveness

➢ Would you launch a new product with Process A?

➢ Would that product launch be more successful supported by Process B?

➢ All else equal, would you rather invest in a business supported by Process A or Process B?

➢ Which process might be a candidate for process redesign?
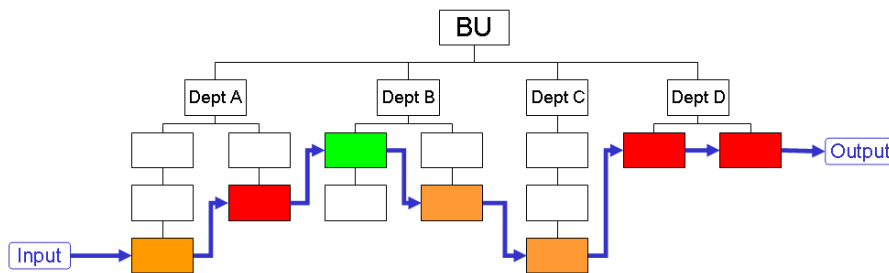
Process A
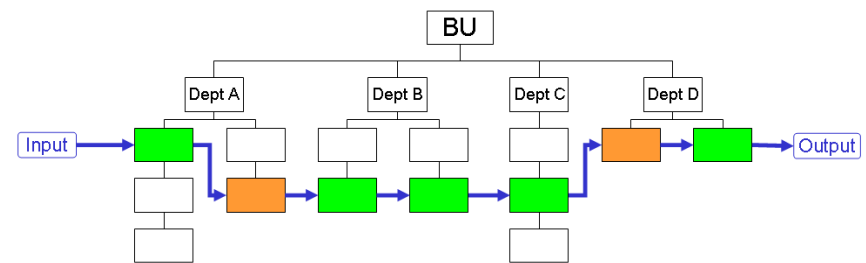
Process B

Better Business Outcomes with IBM OpenPages GRC

- **Lower costs, reduce redundancy and improve efficiencies** by rationalizing your GRC framework

- Deliver **consistent** and **accurate** information about the state of risk and compliance initiatives to assess exposure

- Improve **decision making** and **business performance** through increased insight and business intelligence

- **Competitive advantage** through better risk management

Business Analytics

IBM Smartphone Event Application

Question:

What function can IBM OpenPages Enterprise GRC Platform offer?

a) Risk Management

b) Policy & Compliance Management

c) Internal Audit Management

d) All of the above

Answer…..

Question:

What function can IBM OpenPages Enterprise GRC Platform offer?

a) Risk Management

b) Policy & Compliance Management

c) Internal Audit Management

d) All of the above

Answer is (d)