

Compliance and Risk Management Best Practices for the Public Sector



Bradley Keith – PwC
Director, Washington Federal Practice

SAP SPEAKER
Tom Todd – SAP
VP, Office of the CFO, Strategic Industries , SAP America

July 24th, 2008

Contents




Business Objects
an SAP® company



1. **Framing the Risk & Compliance Issue for Public Services**
2. Taking an Integrated Approach
3. Sample Business Cases
4. Government Studies/Findings
5. SAP GRC Solution
6. Q&A



- Authored the original COSO Internal Control Framework and the subsequent COSO Enterprise Risk Management – Integrated Framework.
- Performed hundreds of Sarbanes-Oxley readiness, assessment / audit, and remediation engagements over the last 5 years.
- Performed more than 50 Federal audits in the last five years and eight first-ever audits
- Supported over 28 components within 9 agencies during their A-123, Appendix A, implementations.
- Assisted the Government Accountability Office (GAO) in their update to the Federal Information Systems Control Audit Manual (FISCAM) methodology.
- Performed over 90 SAP GRC solution implementations in the US alone and several others world-wide

302/404 Required Activity:

- Identify scope of disclosure controls and procedures and internal control over financial reporting
- Document business processes and controls over all major activities within an entity (beyond solely processes impacting financial reporting)
- Perform evaluation of control design and effectiveness
- Identify and track resulting issues and remediation plans
- Document changes in processes and controls; surface any associated issues
- Cascade the accountability for control evaluation and roll up the results
- Prepare internal control report
- Support external auditor attestations



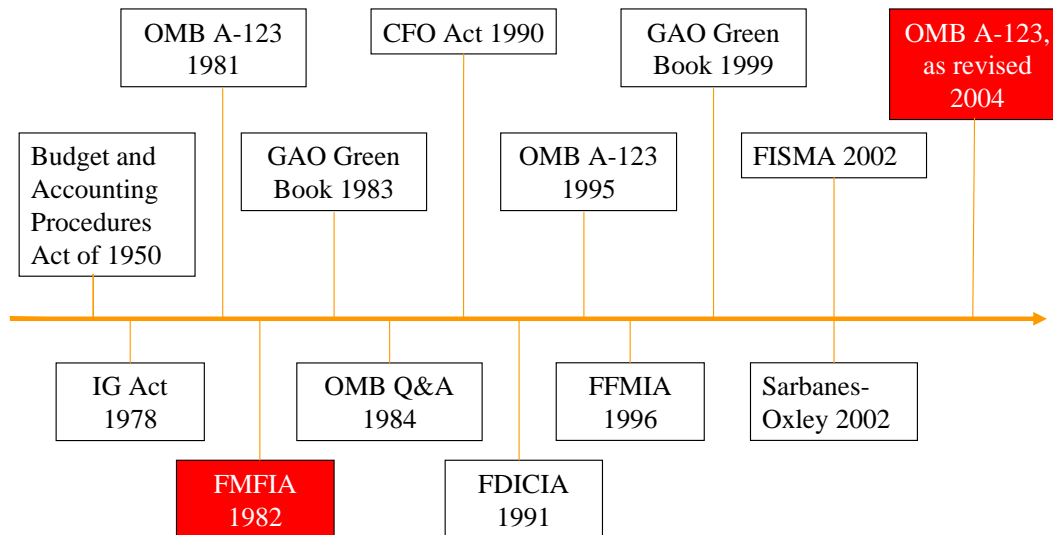
OMB A-123 Requirement

- Section II
 - Scope
- Section II
 - Document Internal Controls
- Section III
 - Assess/Test Internal Control
- Section IV
 - Identify Deficiencies
- Section V
 - Management's Assertions

Current Governance, Risk and Compliance Issues



While the Federal Managers' Financial Integrity Act (FMFIA) has been in place since 1992, OMB Circular A-123 (Appendix A), which defines management's responsibility for internal control, was revised in 2004 to provide further clarity on relevant internal control requirements.



The revisions to OMB Circular A-123 (Appendix A) and the level of effort required for compliance has gathered a significant level of attention across Federal agencies. However, there are number of additional (but related) internal control and security related laws and requirements, that are also challenging and important.

- JFMIP / FSIO System Requirements
- Improper Payments Act
- Anti-deficiency Act
- Prompt Payment Act
- OMB Circular A-127
- OMB Circular A-130
- OMB Circular A-11
- OMB Circular A-34

Current Governance, Risk and Compliance Issues (State / Local)



In addition to the many unique legal/regulatory compliance requirements enacted by State / Local authorities, there are also many common Federal requirements to which they must adhere. With respect to financial management, for those governments that receive federal funding, OMB Circular A-133 and its associated compliance supplement, provide guidance on compliance requirements in several areas including:

- Activities Allowed or Unallowed
- Allowable Costs / Cost Principals
- Cash Management
- Davis-Bacon Act
- Eligibility
- Matching, Level of Effort, Earmarking
- Period of Availability of Federal Funds
- Procurement and Suspension and Debarment
- Program Income
- Real Property Acquisition / Relocation Assistance
- Reporting
- Subrecipient Monitoring
- Special Tests and Provisions

Similar to the multitude of legal and regulatory compliance requirements facing Federal Government agencies, the compliance challenge faced by State and Local governments is most effectively and efficiently addressed through a proactive and integrated approach.

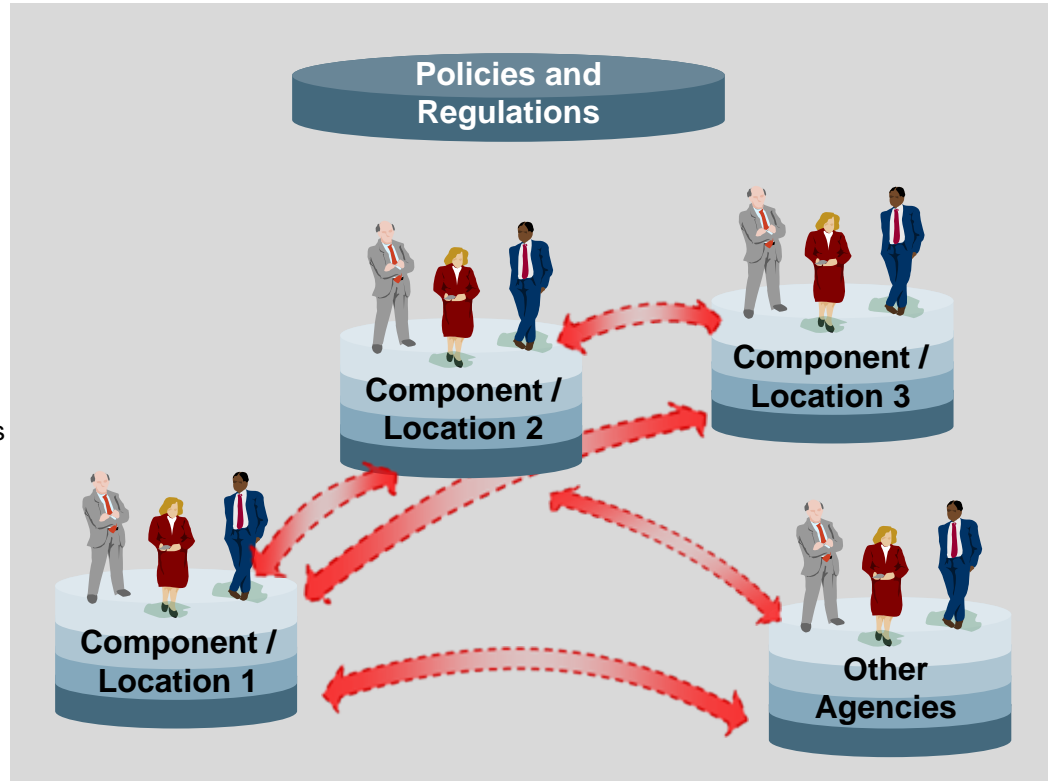
Current Governance, Risk and Compliance Issues



Pain: Compliance with multiple regulations

Implications

- Application of A-123 and related requirements
- Compliance with financial statement audit requirements
- Compliance with FISMA and other Federal level requirements
- Compliance with Agency level requirements.
- Providing clear evidence of internal controls to stakeholders (Executives, GAO, OIG Legislators, other interrelated Agencies).



Pain: Limited cross-agency visibility and access controls

Implications

- Poor controls, low compliance
- Limited governance
- Little accountability to stakeholders
- Lack of transparency



Pain: Gathering and continued maintenance of process controls documentation

Implications

- Manual documentation of processes
- Time and cost to maintain documentation
- Lack of reporting tools

Current Governance, Risk and Compliance Issues



CFO

CIO

Procurement

?

FMFIA

FISMA

ADA

JFMIP

FFMIA

C&A

IPIA

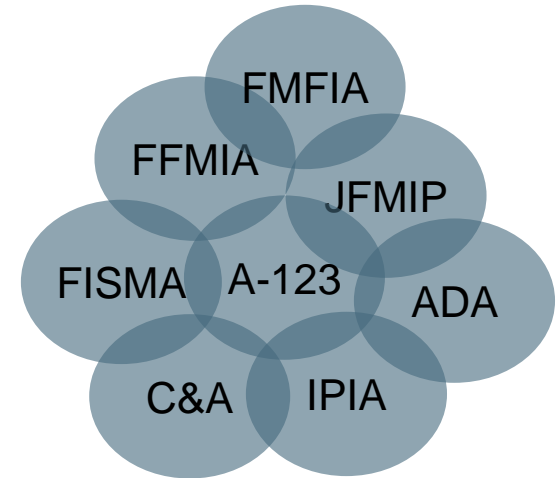
A-127

A-123

A-130

A-11
A-34

Integrated Approach



- Fragmented
- Inefficient and Ineffective
- Manual
- Unsustainable

- Integrated
- Efficient and Effective
- Leverages Technology
- Sustainable

Contents



Business Objects
an SAP® company

SAP

1. Framing the Risk & Compliance Issue for Public Services
- 2. Taking an Integrated Approach**
3. Sample Business Cases
4. Government Studies/Findings
5. SAP GRC Solution
6. Q&A

The Problem of “Fragmented and Duplicative” Controls



“...A common trend for both large and small organizations is the transition away from task-oriented compliance programs to process-oriented compliance programs.

Process-oriented programs require compliance to be tested and validated on an ongoing basis. In addition, fragmented and duplicative compliance activities are being scrapped for those that enable an understanding of compliance across the organization.

This is not to say, however, that local compliance activities in business units are obsolete but rather they should be part of an integrated, global program. This promotes consistency in expectations, documentation, assessments, and reporting...”

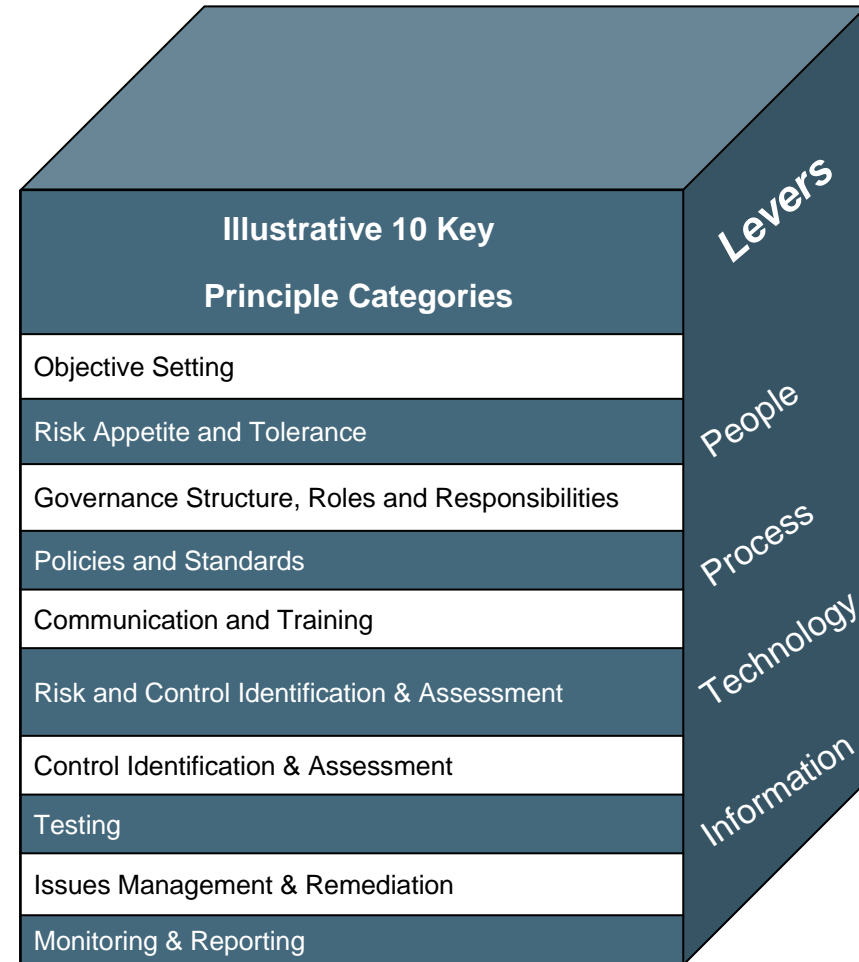
Remarks by (fmr) Governor Mark W. Olson, Board of Governors of the Federal Reserve System, and Chairman of PCAOB, April 10, 2006



- Risk-based Approach
- Common Objectives, Management, and Documentation
- Integration and Leverage of Existing Compliance Programs
- Leverage Technology to Support the Compliance Program and Business Processes
- Reduced Reliance on Manual Controls

For almost any organization, there is a set of common GRC activities that are executed across business units and control functions

- Based on the functions and activities in scope, identify relevant standards and regulatory requirements applicable across risk-related corporate governance functions
- Tailor accepted standards, as appropriate based on the scope and objectives of the analysis, into principles for evaluation
- Analyze target principles through four operating levers that are used to perform activities



A-123 Control Objectives and Financial Statement Assertions

Example Legal / Regulatory Requirements

Completeness
& Accuracy



Improper Payment Act
Step 4

Validity



Anti-Deficiency Act
665 Appropriation -Section (h)

Restricted Access

Presentation & Disclosure

Existence



Improper Payment Act
Steps 1-4

Rights & Obligations

Cut-off



Prompt Payment Act
1315a - c

Valuation

Integration Best Practices Representative Mapping



Completeness
& Accuracy



Existence

Improper Payments Act

- Review all programs and activities and identify those which are susceptible to significant erroneous payments.
- Statistically Valid Estimate of the annual amount of erroneous payments in programs and activities
- Implement a Plan to reduce erroneous payments

Validity



Anti-Deficiency Act

No officer or employee of the United States shall authorize or create any obligation or make any expenditure:

(A) in excess of an apportionment or reappportionment, or

(B) in excess of the amount permitted by regulations prescribed pursuant to subsection (g) of this section.

Cut-off



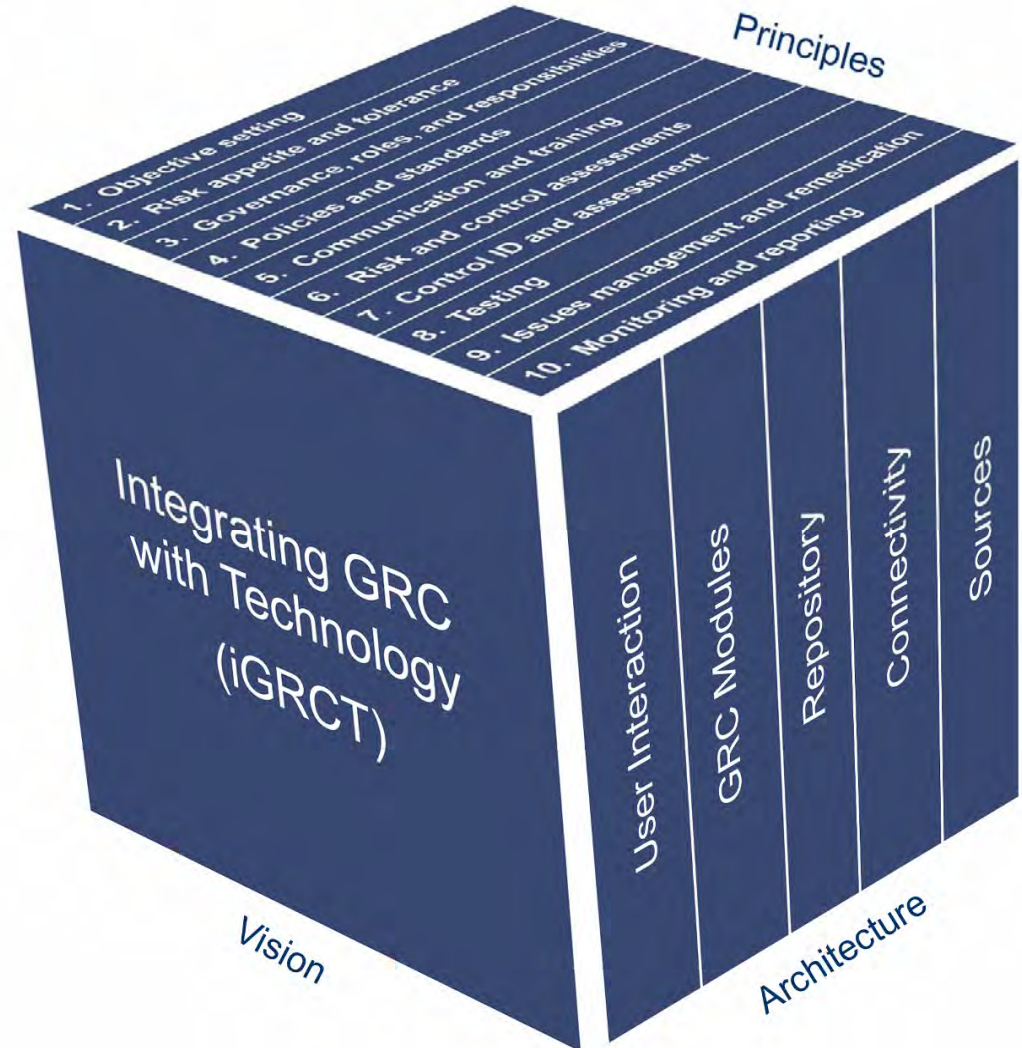
Prompt Payment Act

- Issuing Internal Procedures
- Internal Control Systems
- Financial Management Systems

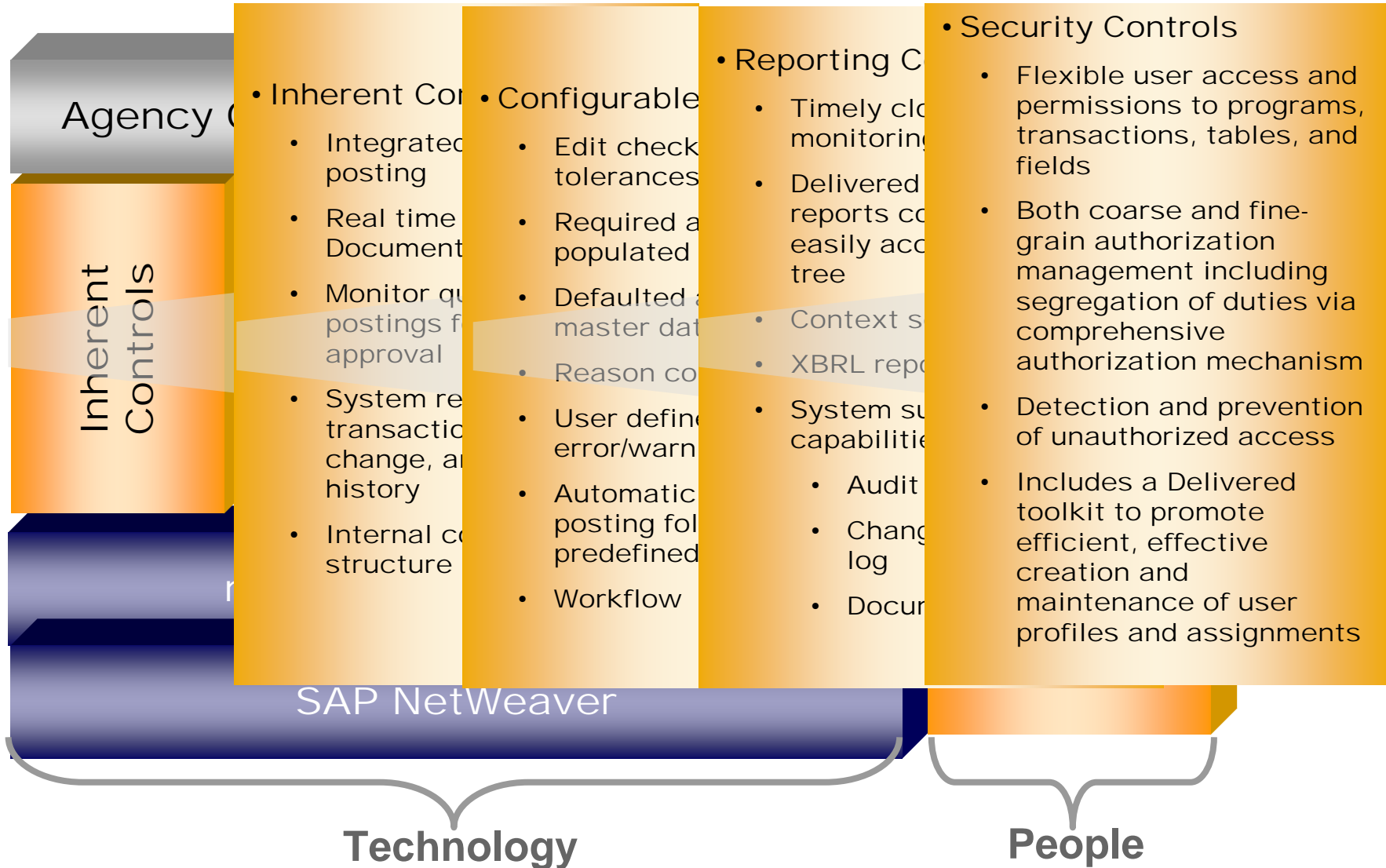
The iGRC Technology Vision



Using PwC's iGRC principles-based approach, the iGRC Technology lever provides a structured means - or architecture - to streamline and consolidate, standardize, and communicate governance, risk, and compliance information.



Regulations and Foundational Control Principles



Contents




Business Objects™
an SAP® company



1. Framing the Risk & Compliance Issue for Public Services
2. Taking an Integrated Approach
- 3. Sample Business Cases**
4. Government Studies/Findings
5. SAP GRC Solution
6. Q&A



Organization A

- Performed system certification and accreditation of new systems (NIST 800.26) and had a mature FISMA process (NIST 800.53) in place.
- Collectively, the NIST 800.26 and 800.53 requirements fully address 23% and partially address another 21% (approximately) of the information technology control objectives documented in the current GAO Federal Information System Control Audit Manual (FISCAM), which is typically followed for financial statement audits and the A-123 internal control assessments. This represents a combined 44% potential overlap in objectives and requirements.
- However, the manner in which the organization documented the results of their C&A and FISMA assessments only allowed them to “take credit” for less than 30% of the potential common requirements / objectives.

Plan your test procedures and documentation of results to satisfy the most stringent requirement(s) to allow maximum leverage.

Yes / No answers generally are not sufficient

Example 2

Organization & Integration



Organization B

- Composed of 9 Bureaus, 10 major offices, and several hundred geographically dispersed regional and field offices.
- Completed FFMIA assessment checklists and had a FISMA program in place
- Lack of a standard A-123 assessment process, documentation, and business practices across the organization
- PwC assisted the organization by:
 - Developing standard end-to-end business process and internal control documentation and establishing a centralized repository
 - Identifying best internal control practices to be shared / adopted across the organization
 - Identified 247 automated / programmed controls for which the organization could “take credit” against A-123 financial reporting control objectives. Of these 150 were designated a “KEY” by the organization.
 - Mapping of 28 key FISCAM controls to 54 FISMA (800.53) requirements for 8 financial and 22 non-financial systems resulting in a 20% reduction in overall effort

Implement a consistent, managed, risk based approach across the entire organization leveraging shared documentation, best practices, and technology assets

Contents



1. Framing the Risk & Compliance Issue for Public Services
2. Taking an Integrated Approach
3. Sample Business Cases
- 4. Government Studies/Findings**
5. SAP GRC Solution
6. Q&A



Research Background & Methodology

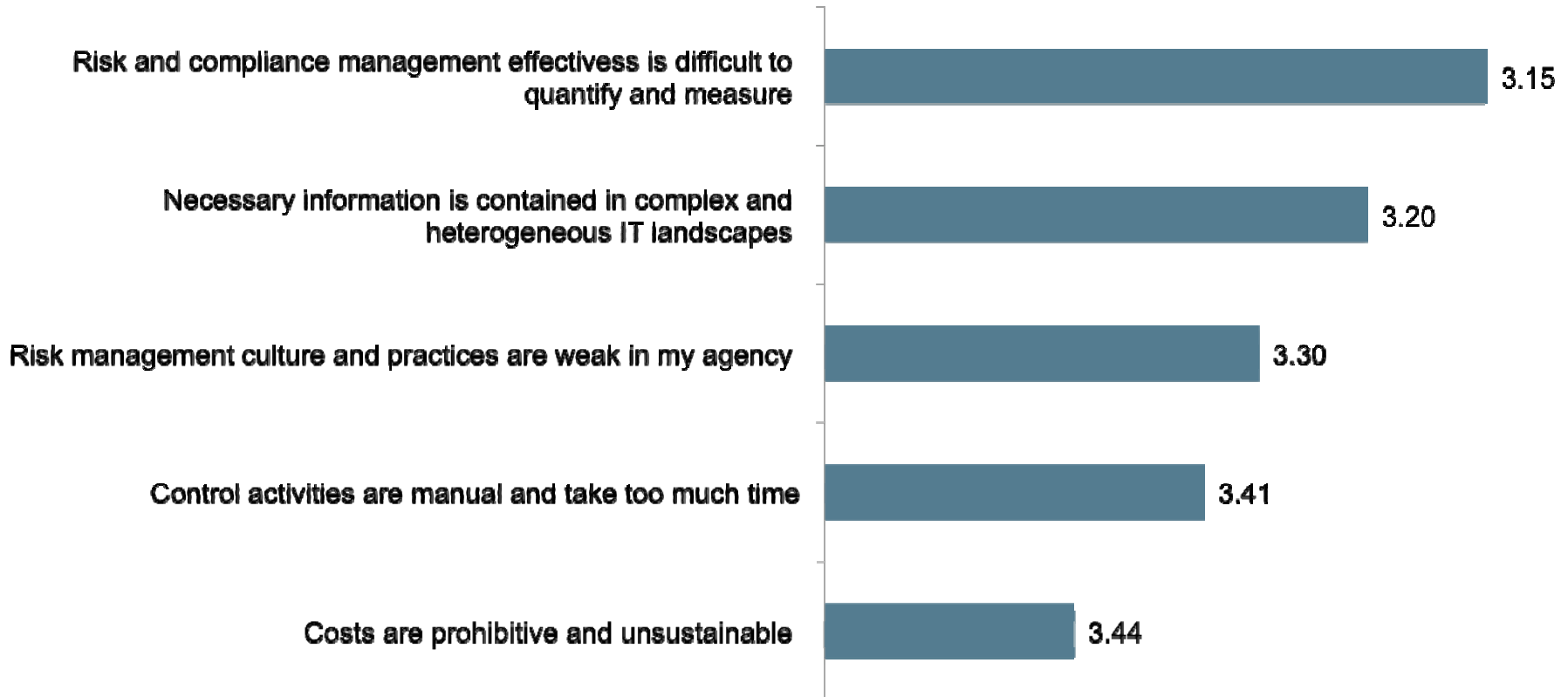


Difficulty Measuring Risk among Fragmented Efforts



Challenges around Risk Management Today

5 =Very challenging, 1=Not challenging

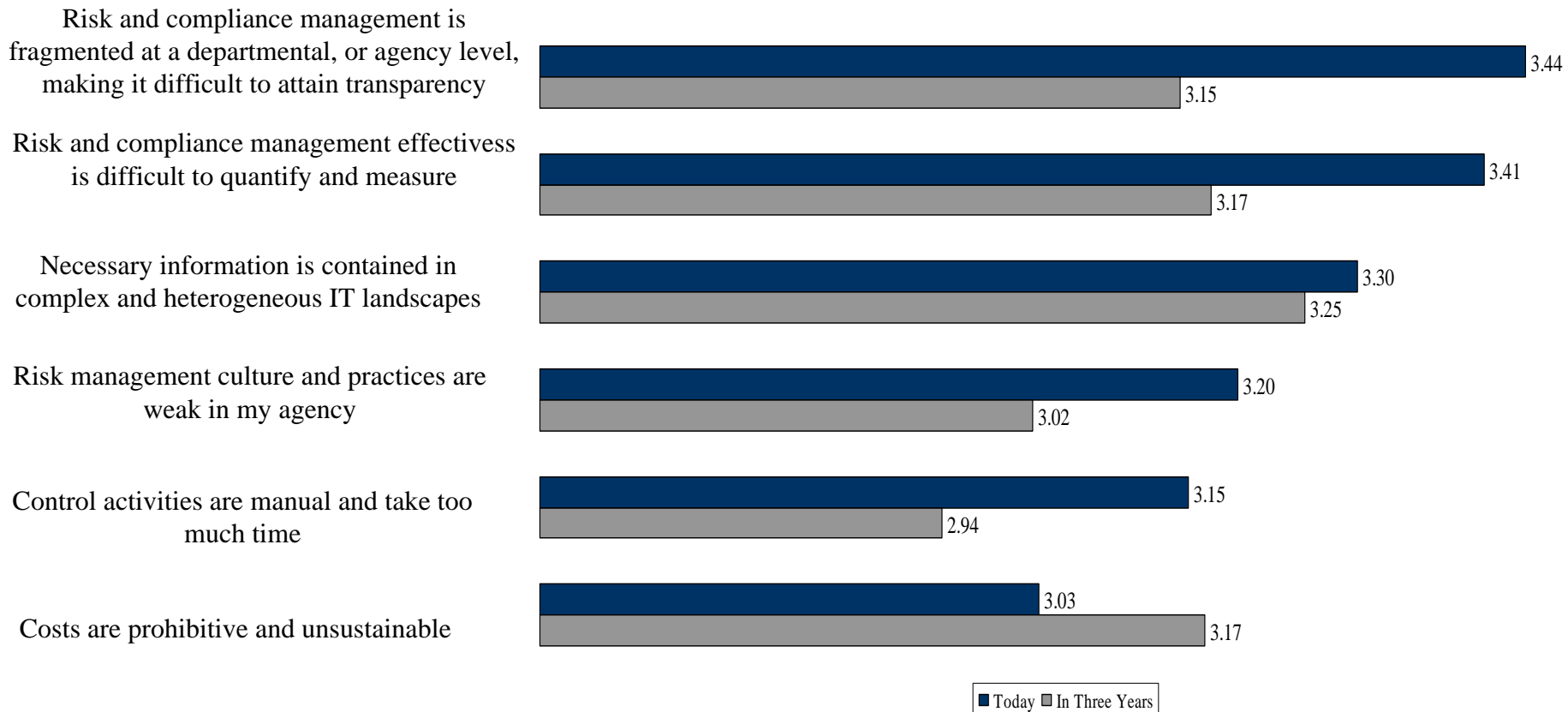


Dramatic Improvement on the Horizon, Cost as Exception



Challenges around Risk Management

5 = Very challenging, 1 = Not challenging

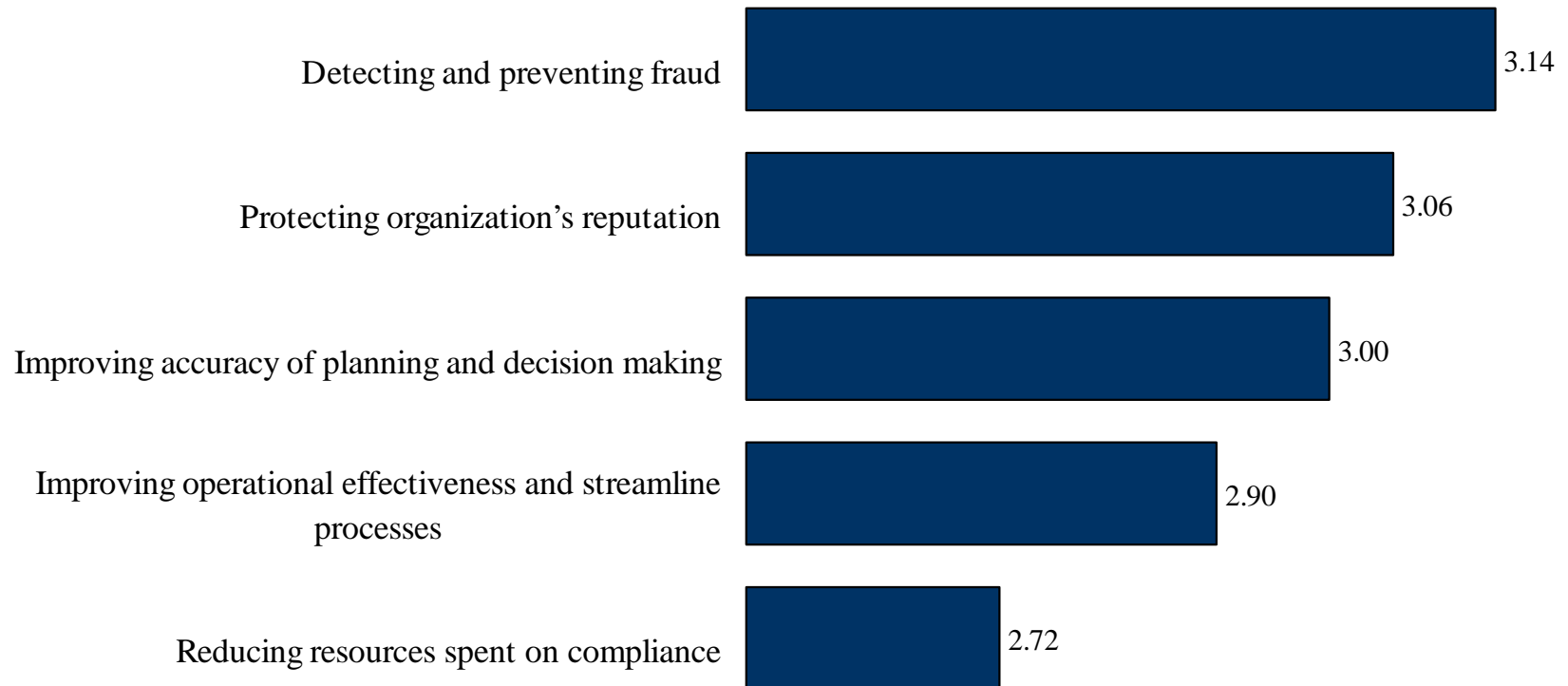


Greatest Tangible Benefits: Protecting Reputation, Detecting Fraud



Effectiveness of Risk Management Initiatives

5 = Very effective, 1 = Not effective

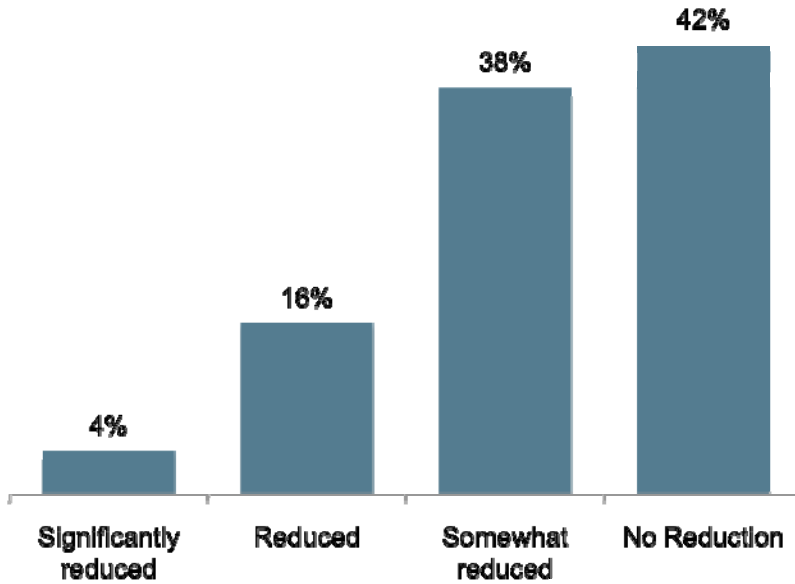


Risk Management Investments Reduce Deficiencies and Control Violations

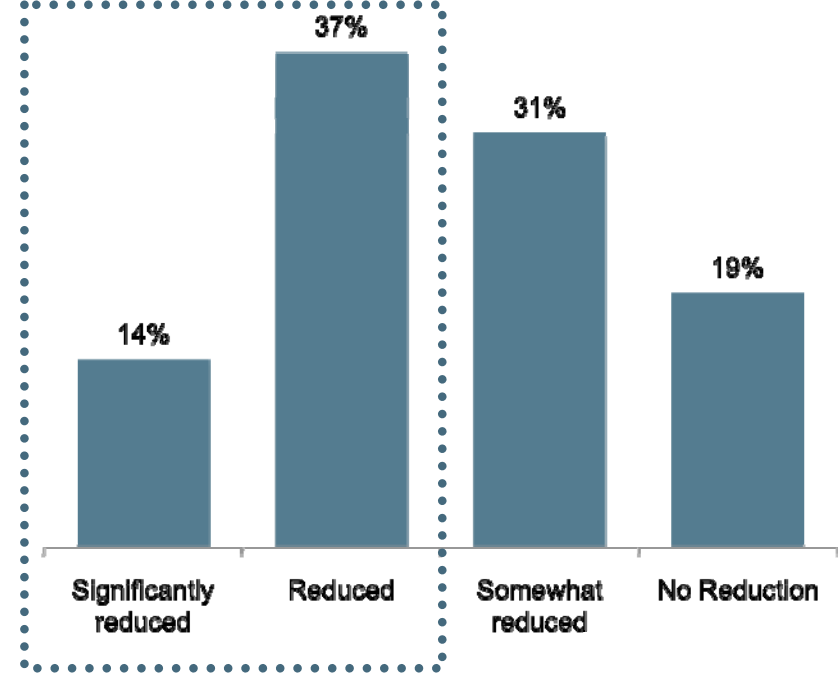


Reduction of Deficiencies and Control Violations

Low Adopters of Best Practices



High Adopters of Best Practices



Contents




Business Objects™
an SAP® company



1. Framing the Risk & Compliance Issue for Public Services
2. Taking an Integrated Approach
3. Sample Business Cases
4. Government Studies/Findings
- 5. SAP GRC Solution**
6. Q&A

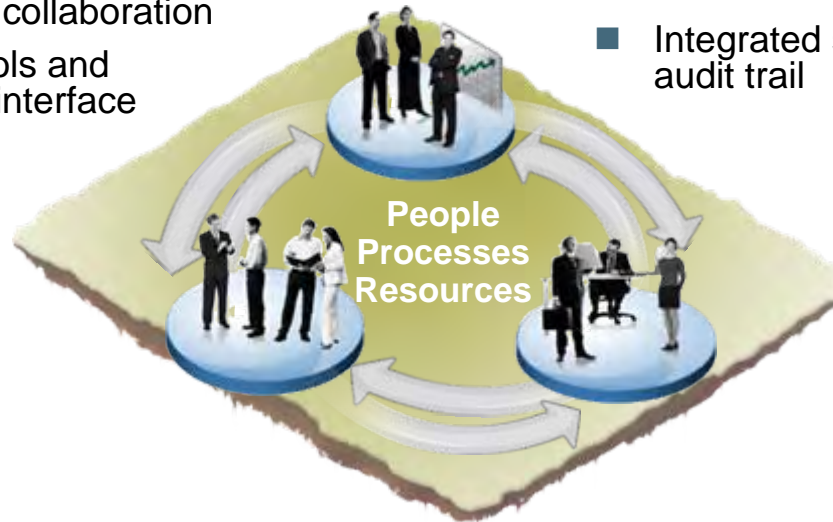
The Enterprise In Control of GRC



OPERATIONS

Alignment, Agility and Visibility

- Synchronize risks, initiatives, metrics with people, - establish accountability
- Intelligently manage resources and exceptions based on priorities
- Intelligent action panes plus strong visualization and collaboration
- Familiar office tools and intuitive web 2.0 interface



FINANCE

Risk Mitigation and Executive Confidence

- Preventative model and optimization of policies and procedures
- Automation to streamline financial and audit compliance process
- Centralized Control Management
- Integrated solution, real-time compliance, full audit trail

IT

Free Up Resources, Time and Money for Innovation

- Modern architecture leveraging ERP, GRC for effective service and ROI
- Accurate data repository for user confidence
- Data delivered in time and in context to every business user

SAP Solutions for GRC

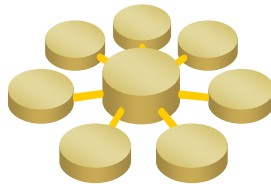
A unified solution for GRC management



Business Process



SAP GRC Risk Management



Risk Repository

- Risk Registry
- Links Risks and Controls
- Cisco SONA & Business Process Monitoring



- Delivers transparency to balanced global risk profile
- Standardizes on common GRC content and rules
- Automates and embeds GRC processes into business processes
- Integrates with existing IT assets and technology partners
- Enables easier collaboration with service and content partners



Business Process Platform



Sources



SAP GRC Configuration Overview

Compliance Structure



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

NetWeaver Business Client ... Organization Hierarchy

Compliance Structure

Welcome Ian Robb

- Organizations**
Maintain the company's organization structure for compliance, including assignment of subprocesses and offering or using shared services, plus assignment of entity-level controls to organizations
[Organizations](#)
- Central Process Hierarchy**
Maintain the central process hierarchy (processes, subprocesses and controls) with assignment of control objectives/risks, account groups/assertions, and test plans for manually tested controls
[Central Process Hierarchy](#)
- Accounts**
Maintain account groups with significance reasoning and relevant financial assertions
[Accounts](#)
- Entity-Level Controls**
Maintain and assign the company's entity-level control hierarchy to represent controls that are documented and evaluated at higher levels in the organization
[Entity-Level Controls](#)
- Control Objectives and Risks**
Maintain the catalog of control objectives and related risks, which will later be assigned to subprocesses and controls
[Control Objectives and Risks](#)

Start | NetWeaver Business ...

SAP GRC Configuration Overview

Organization Hierarchy



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ...

Organization Hierarchy

Organization	Description:	CRG United States Sales
CRG-PC-C-SOD	Valid from:	01.01.2008
CRG-PC-OPERATIONS	Valid to:	31.12.9999
CRG-PC-SALES	Shared Services Provider:	No
CRG-PC-EURO-REGION	Subject to Sign-Off:	Yes
CRG-PC-AMERICA-REGION	Deficiency Analysis Flag:	No
CRG-PC-N-AMERICA-REGION	Documents:	...
CRG-PC-CANADIAN-REGION		
CRG-PC-US-REGION		
CRG-PC-US-CALIFORNIA		
CRG-PC-US-FLORIDA		
CRG-PC-US-NEWJERSY		
CRG-PC-US-TEXAS		
CRG-PC-US-Minnesota		
CRG-PC-S-AMERICA-REGION		
CRG-PC-APJ-REGION		
CRG-PC-DEVELOPING-REGION		
CRG-PC-MIDDLE-EAST-REGION		

Row 10 of 27

Agency X

- Component 1**
- Component 2**
- Location 1**
- Location 2**

SAP GRC Configuration Overview

Account Group Hierarchy



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ... Organization Hierarchy Central Process Hierarchy

Accounts

Account Groups

Show Year: 2008 Go Create Open Actions

Text

- Account Group Hierarchy
 - GRC Balance Sheet Accts**
 - GRC Income Stmt Accts

GRC Balance Sheet Accts

General GL Accounts

General

Description:

Significant: Yes

Reasoning:

Valid from: 01.01.2008

Valid to: 31.12.9999

Documents: 0

Assertions

Completeness: Selected

Existence:

Presentation:

Rights and:

Valuation:

Balance Sheet

Statement of Net Cost

Statement of Changes in Net Position

Statement of Budgetary Resources

Statement of Custodial Activity (if Applicable)

Start NetWeaver Business ...

SAP GRC Configuration Overview

Central Process Hierarchy/Catalog



ICA Desktop 710 - MetaFrame Presentation Server Client

Home NetWeaver Business Client ... Organization Hierarchy Control Objectives and Risks

Central Process Hierarchy

Process Structure

Show Year 2008 Go Create Open Actions

Name	Type
▼ Process Structure	
▶ Financial Close Process	Process
▶ HR and Payroll	Process
▶ Information Technology	Process
▶ Order to Cash	Process
▼ Procure to Pay	Process
▼ Accounts Payable	Process
▶ Cash Disbursements	Subprocess
▶ AP Invoicing	Subprocess
▶ Maintain Vendor Master Data	Subprocess
▼ Perform Invoice Verification	Subprocess
▪ P2P Invoice tolerance setting changes	Control
▪ P2P Payments without goods receipt	Control
▪ P2P Payments without goods receipt - ComCd	Control

Subprocess: Perform Invoice Verification

General Objectives & Risks Account Groups

Description: Perform Invoice Verification
Valid from: 01.01.2008
Valid to: 31.12.9999
Transaction type: Routine
Industry-specific: No
Documents: 0

Key / Relevant Business Processes & Sub-processes

- Financial Closing
- HR & Payroll
- IT Controls
- Order to Cash (Revenue)
- Procure to Pay**
- Property, Plant, and Equipment

SAP GRC Configuration Overview

Central Process Hierarchy/Catalog



ICA Desktop 710 - MetaFrame Presentation Server Client

Home NetWeaver Business Client ... Organization Hierarchy Control Objectives and Risks

Central Process Hierarchy

Subprocess

Central Subprocess: Perform Invoice Verification

Parent Process: Accounts Payable ID: 11000028
Timeframe: Year 2008 Effective Date: 01.01.2008

Save Cancel

General Objectives & Risks Account Groups Attachments and Links

Name: * Perform Invoice Verification
Description: Perform Invoice Verification
Valid from: * 01.01.2008
Valid to: * 31.12.9999
Transaction type: Routine

Industry-specific: Yes No

Procure to Pay Cycle

- Disbursements
- AP Invoicing
- Maintain Vendor Master
- Invoice Verification**

Start NetWeaver Business ...

SAP GRC Configuration Overview

Control Objectives & Risks



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ... Organization Hierarchy Central Process Hierarchy

Control Objectives and Risks

Control Objective Hierarchy

Show Year 2008 Go Create Open Actions

- Control Objective Hierarchy
- ▶ Changes to exchange rate data valid
- ▶ Invoices accurately calculated, recorded
- ▶ RMA credit notes issued within policy
- ▶ Orders processed within approved credit
- ▶ Collections monitored for timeliness
- ▶ A/R reflects circumstances per policies
- ▶ Credit granted and managed per policy
- ▶ Order prices and terms approved by mgmnt
- ▶ Customer master file remains pertinent
- ▶ One-time customer usage is appropriate
- ▶ All received orders input and processed
- ▶ Payments are made to valid vendors
- ▶ AP payments accurately calculated
- ▶ All disbursements recorded timely

Control Objective: Invoices accurately calculated, recorded

General Subprocesses

Description: Invoices are accurately calculated and recorded
Objective Category: Financial Reporting and Disclosure
Valid from: 01.01.2008
Valid to: 31.12.9999
Documents: 0

Provides an "Inventory" of Control Objectives and Risks by Category

SAP GRC Configuration Overview

Assignment of Sub Process to Organization



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ...

Organization Hierarchy

Organization

Organization: Agency X

Parent Organization CRG-PC-US-REGION ID 50005110

Timeframe Year 2008 Effective Date 01.01.2008

Save Cancel

General Subprocesses Entity-Level Controls Roles Attachments and Links

Subprocess Assignment

Remove Open Assign Subprocess

Subprocess/Control	Description	Assignment Method	Shared Service
▼ Perform Invoice Verification	Perform Invoice Verification	Reference	None
• P2P Invoice tolerance setting changes	Monitors for changes in invoice tolerance settings that cl	Referenced	
• P2P Payments without goods receipt	Identifies individual invoices being posted for payment wi	Referenced	
• P2P Payments without goods receipt - ComCd	Identifies total invoice amount for a company code being	Referenced	
• P2P Split vendor invoices v. tolerance	Identifies split vendor invoices and individual invoices tha	Referenced	
• P2P Overpaid purchase orders	Identifies individual purchase orders that have been over	Referenced	

Sub-processes, control objectives, / compliance requirements, and controls can be assigned to one or more organization units

Start NetWeaver Business ...

SAP GRC Configuration Overview

Control Objectives and Compliance Requirements



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ... Organization Hierarchy Central Process Hierarchy

Control Objectives and Risks

Control Objective

Personalize Help

Control Objective: AP invoices are entered accurately

Objective ID 12000044

Timeframe Year 2008 Effective Date 01.01.2008

Save Cancel

General Subprocesses Risk Attachments and Links

Control Objective: * AP invoices are entered accurately Valid from: * 01.01.2008

Objective Category: * Financial Reporting and Disclosure

Description: AP invoices are entered in the proper GL period.

Procure to Pay Cycle

- Disbursements
- AP Invoicing**
- Maintain Vendor Master
- Invoice Verification

Start NetWeaver Business ...

SAP GRC Configuration Overview

Risk Creation & Assignment



ICA Desktop 710 - MetaFrame Presentation Server Client

Favorites, System, Help

Home NetWeaver Business Client ... Organization Hierarchy Central Process Hierarchy

Control Objectives and Risks

Control Objective

Control Objective: AP invoices are entered accurately

Objective ID 12000044
Timeframe Year 2008 Effective Date 01.01.2008

Save Cancel

General Subprocesses **Risk** Attachments and Links

Risk

Create Edit

Risk	Description	Risk Impact
Accounts are misstated	Vendor accounts and financial statements are misstated.	

Risks Associated to One or MORE Control / Compliance Objectives

Start NetWeaver Business ...

SAP GRC Configuration Overview

Addition of Entity Level Control



ICA Desktop 710 - MetaFrame Presentation Server Client

Organization Hierarchy

Organization

Personalize Help

Organization: Agency X

Parent Organization CRG-PC-US-REGION ID 50005110

Timeframe Year 2008 Effective Date 01.01.2008

Save Cancel

General Subprocesses **Entity-Level Controls** Roles Attachments and Links

Entity-Level Control Assignments

Add Remove Open

Entity-Level Control	Description	ID
Mgmt shows integrity and ethics	Through its attitudes and actions, management demonstrates character, integrity and ethical values.	ECONTROL/16000003

Management reviews all programs and activities to identify those which are susceptible to significant erroneous payments. Management prepares a statistically valid estimate of the annual amount of erroneous payments in programs and activities Management has designed, documented, implemented, and regular monitors the results of a plan to reduce erroneous payments

Entity Level Controls – Improper Payments Act Example

SAP GRC Delivers the Leading Compliance Solution for Public Sector



Product development started in 1996 – before Sarbanes-Oxley

Domain experts in enterprise controls and compliance

Compliance standard for large global enterprises

Proven world-wide in large enterprises and governmental organizations



Contents




Business Objects™
an SAP® company



1. Framing the Risk & Compliance Issue for Public Services
2. Taking an Integrated Approach
3. Sample Business Cases
4. Government Studies/Findings
5. SAP GRC Solution
- 6. Q&A**

Thank you!

Bradley Keith, Director – Washington Federal Practice, PricewaterhouseCoopers

(703) 918-3564

bradley.keith@us.pwc.com

Tom Todd, VP Office of the CFO, Strategic Industries – SAP America

(224) 622-2977

tom.todd@sap.com

pwc.com

This proposal is protected under the copyright laws of the United States and other countries as an unpublished work. This proposal contains information that is proprietary and confidential to PricewaterhouseCoopers LLP, and shall not be disclosed outside the recipient's company or duplicated, used or disclosed in whole or in part by the recipient for any purpose other than to evaluate this proposal. Any other use or disclosure in whole or in part of this information without the express written permission of PricewaterhouseCoopers LLP is prohibited.

© 2008 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity.