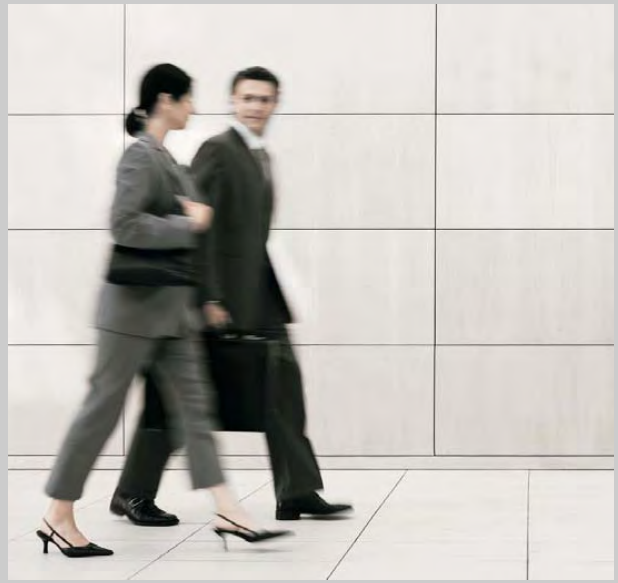
Compliance and Risk Management Best Practices for the Public Sector



Bradley Keith – PwC
Director, Washington Federal Practice

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

July 24th, 2008

Business Objects an SAP® company

PRICEWATERHOUSECOOPERS

THE BEST-RUN BUSINESSES RUN SAP™

SAP®

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

Introduction
PricewaterhouseCoopers, LLP

- 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

SOX 302/404 relevance to OMB Circular A123

302/404 Required Activity:

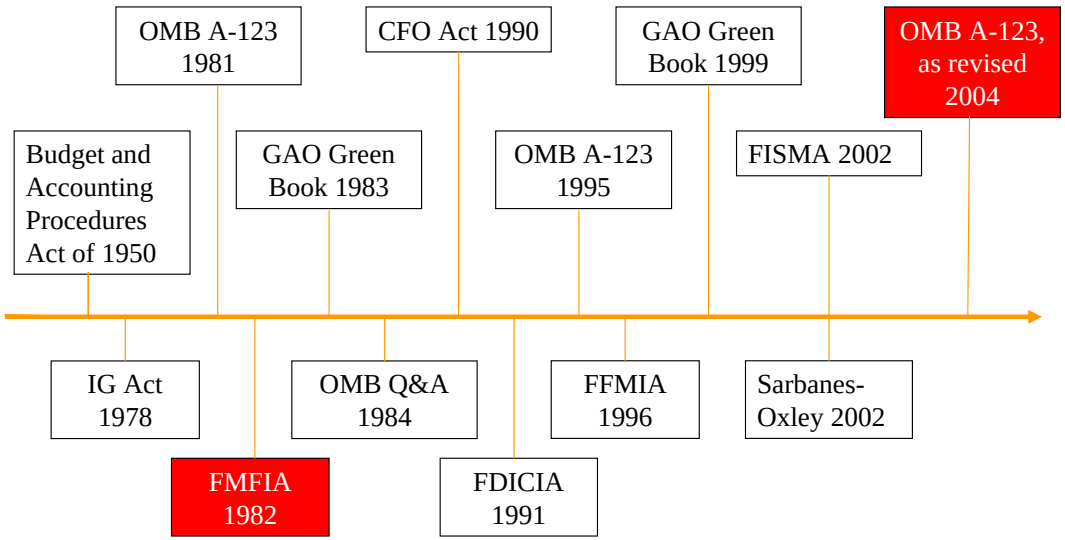
- Identify scope of disclosure controls and procedures and internal control over financial reporting
- Document business processes and controls over all major activities within an entity (beyond solely processes impacting financial reporting)
- Perform evaluation of control design and effectiveness
- 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 CircularA-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 it's associated compliance supplement, provide guidance on compliance requirements in several areas including:

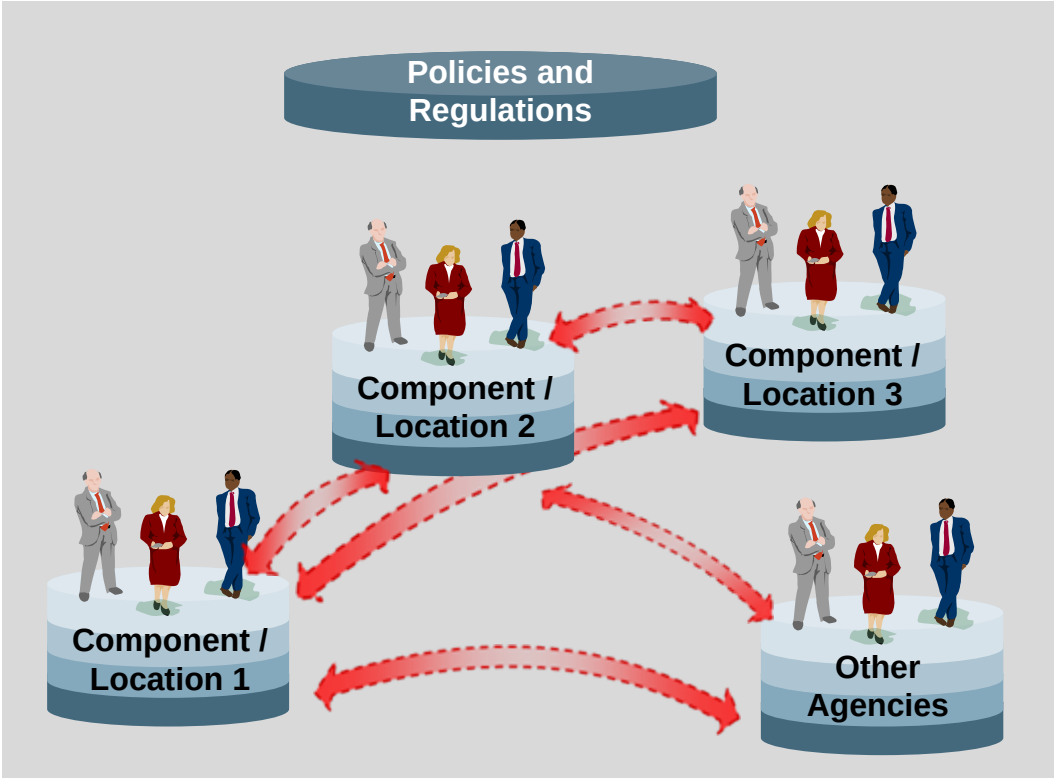
- Activities Allowed or Unallowed
- Allowable Costs / Cost Principals
- Cash Management
- Davis-Bacon Act
- Eligibility
- Matching, Level of Effort, Earmarking
- Period of Availability of Federal Funds
- Procurement and Suspension and Debarment
- Program Income
- Real Property Acquisition / Relocation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

Similar to the multitude of legal an 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

- FMFIA
- FFMIA
- A-123
- A-11
  A-34

CIO

- FISMA
- C&A

Procurement

- ADA
- IPIA

?

- JFMIP
- A-127
- A-130

Integrated Approach

- Fragmented
- Inefficient and Ineffective
- Manual
- Unsustainable

- Integrated
- Efficient and Effective
- Leverages Technology
- Sustainable

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

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

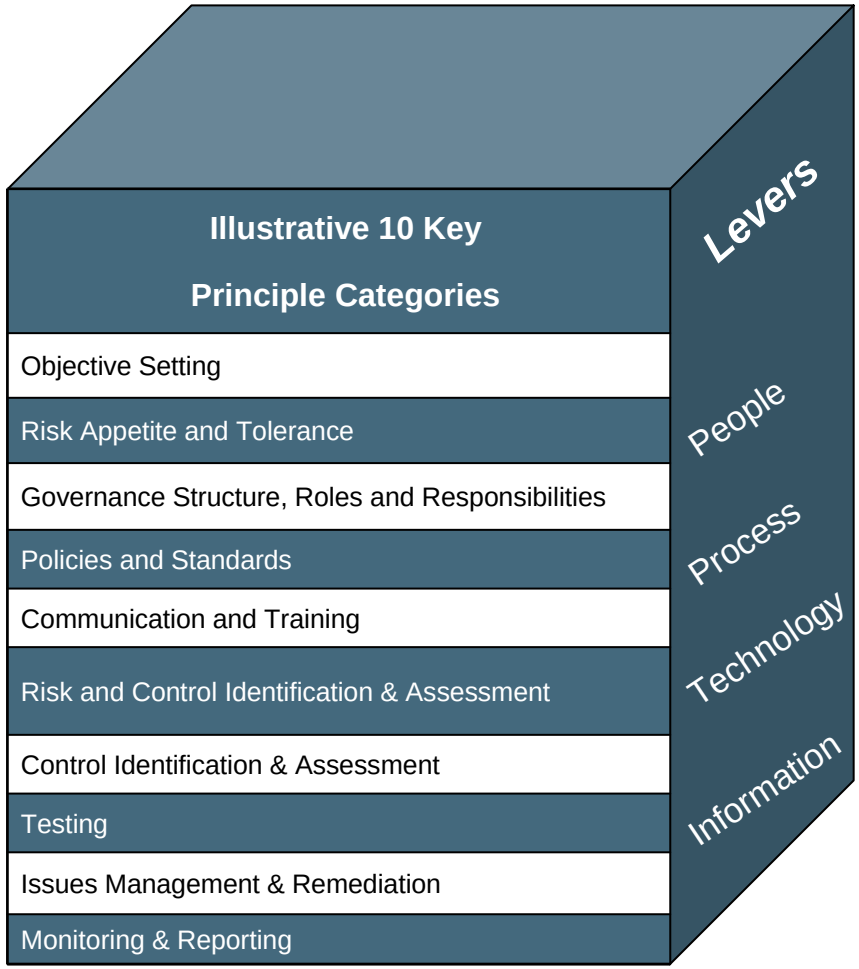
Integration Best Practices

- 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

Using a Principles-based Framework

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



Integration Best Practices Representative Mapping

A-123 Control Objectives and Financial Statement Assertions	Example Legal / Regulatory Requirements
Completeness & **A**ccuracy	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 reapportionment, or

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

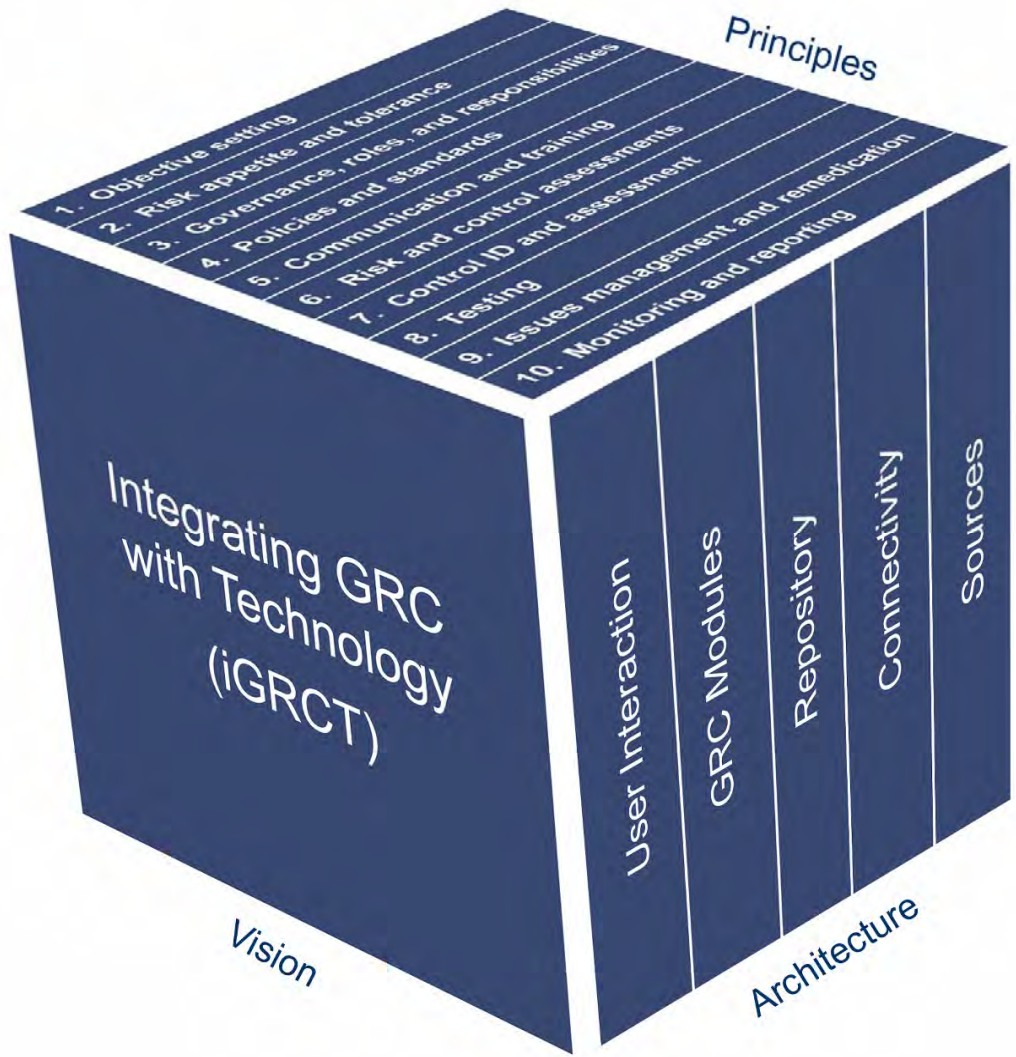
Cut-off

Prompt Payment Act

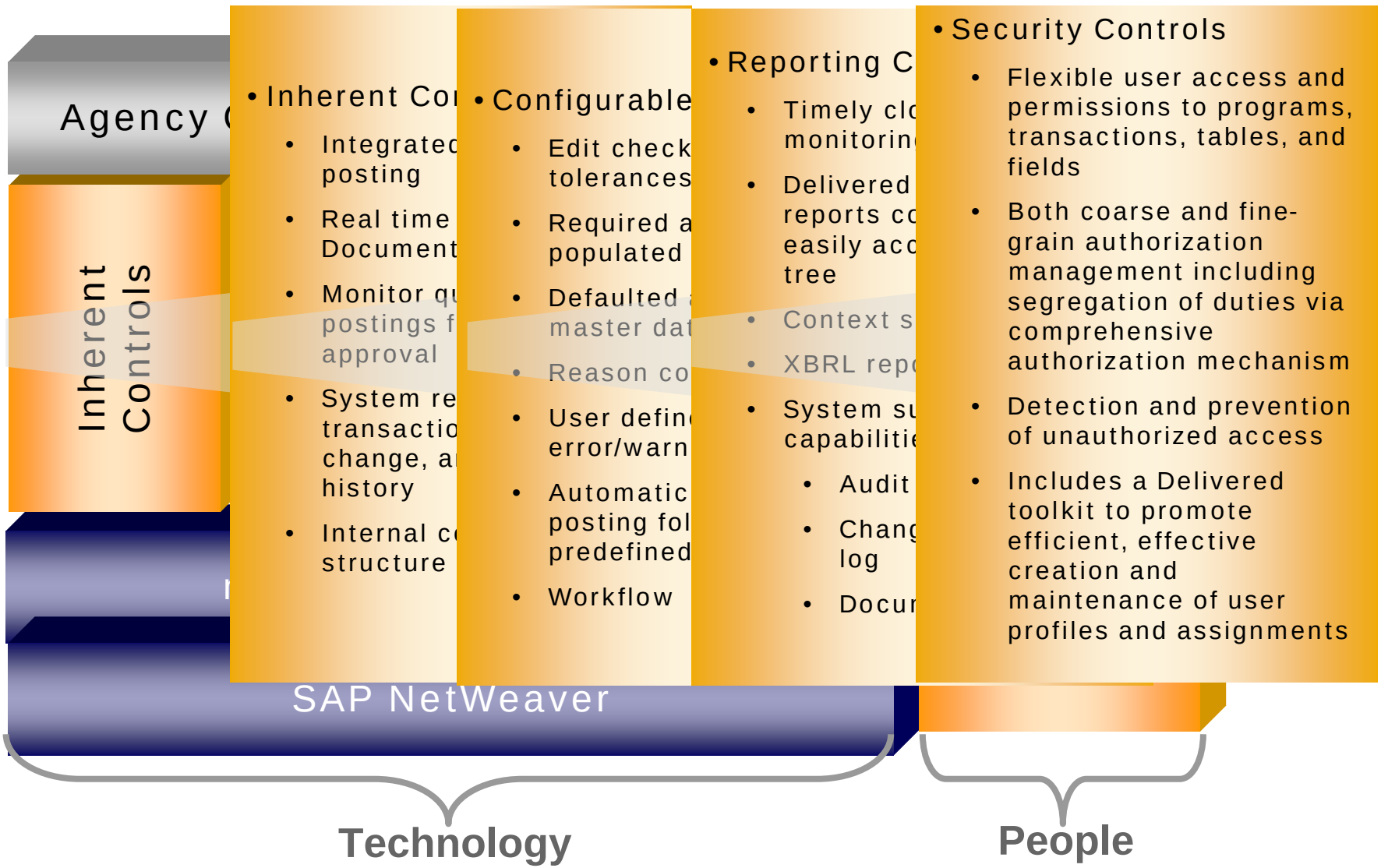
- Issuing Internal Procedures
- Internal Control Systems
- Financial Management Systems

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

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

Example 1
C&A / FISMA Integration

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 disbursed 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

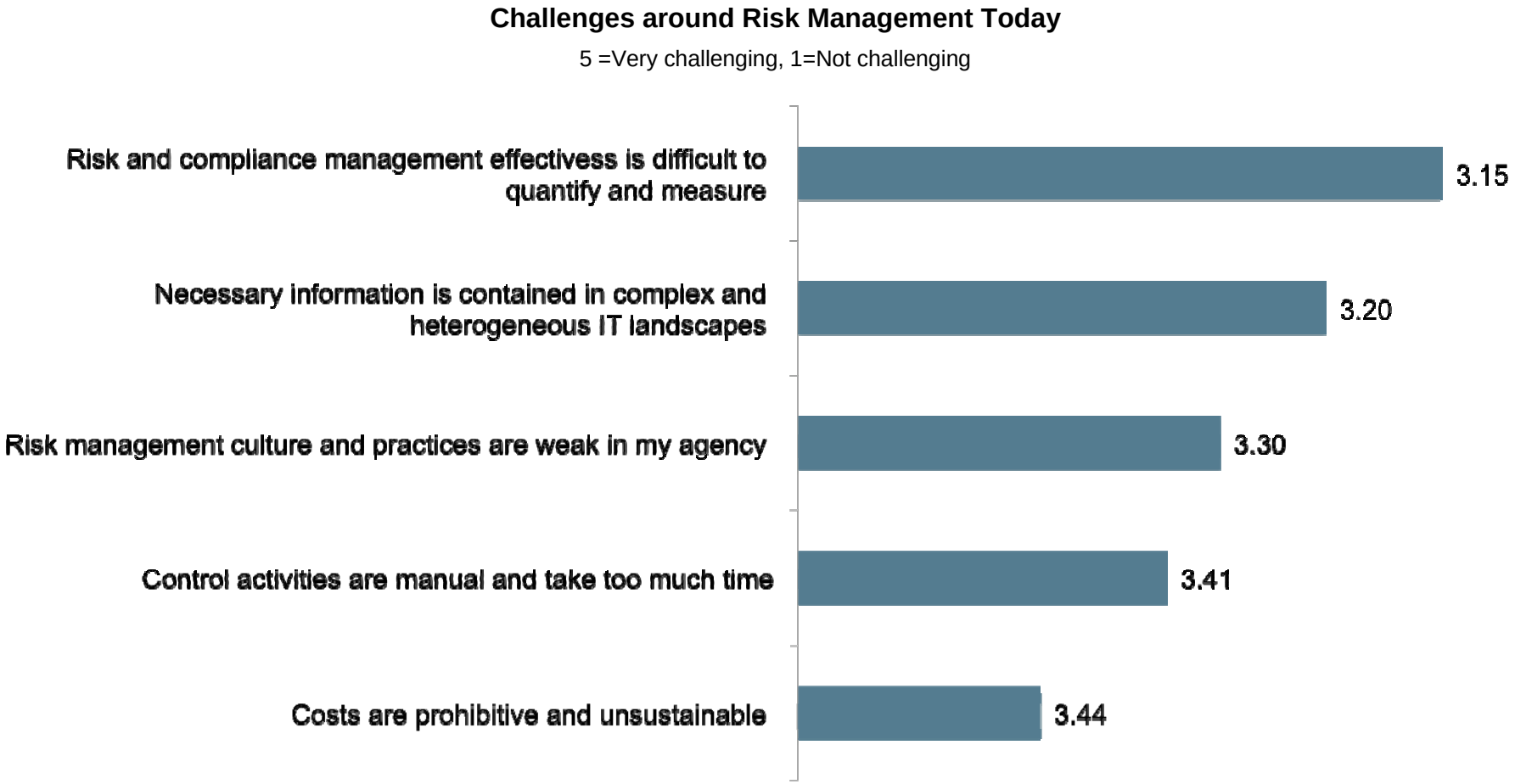
Business Objects
an SAP company

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

Research Background & Methodology

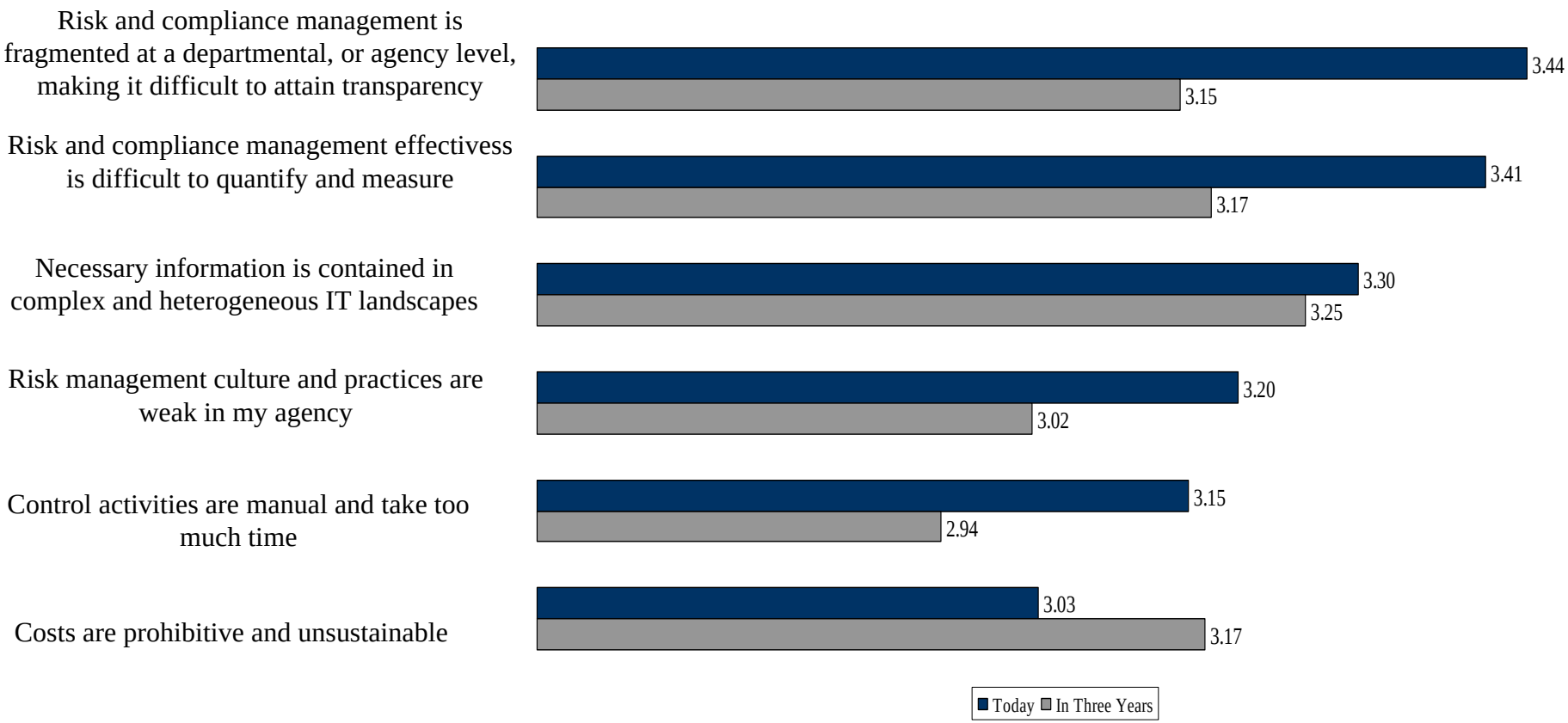
Difficulty Measuring Risk among Fragmented Efforts



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

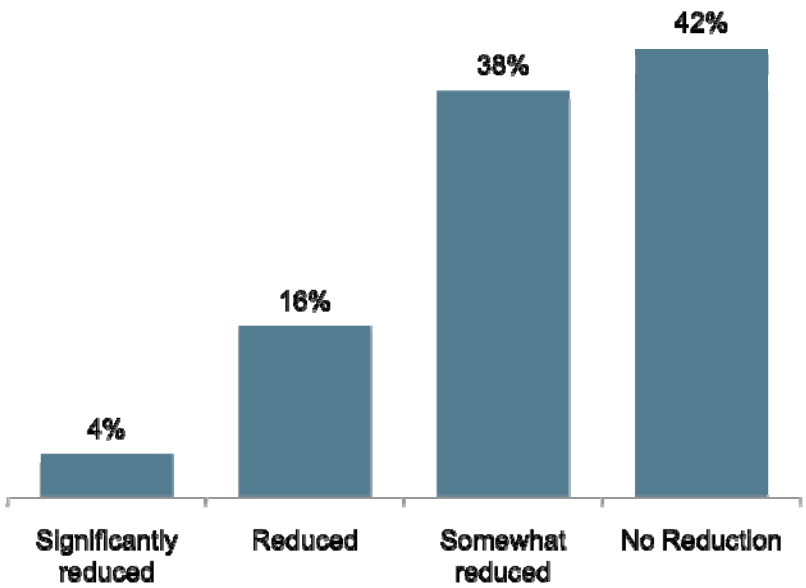
Effectiveness of Risk Management Initiatives

5 =Very effective, 1= Not effective

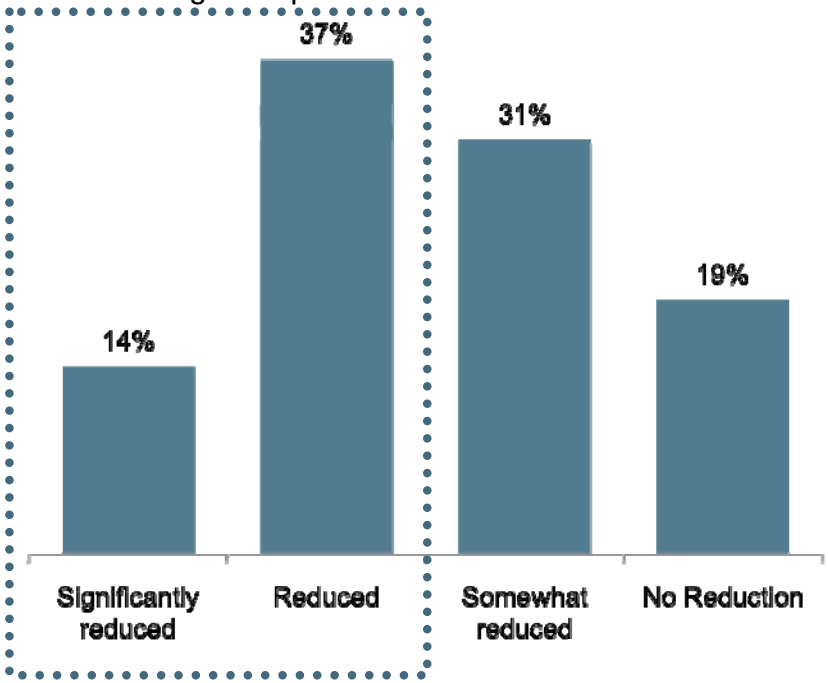
Risk Management Investments Reduce Deficiencies and Control Violations

Reduction of Deficiencies and Control Violations

Low Adopters of Best Practices



High Adopters of Best Practices



Contents

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

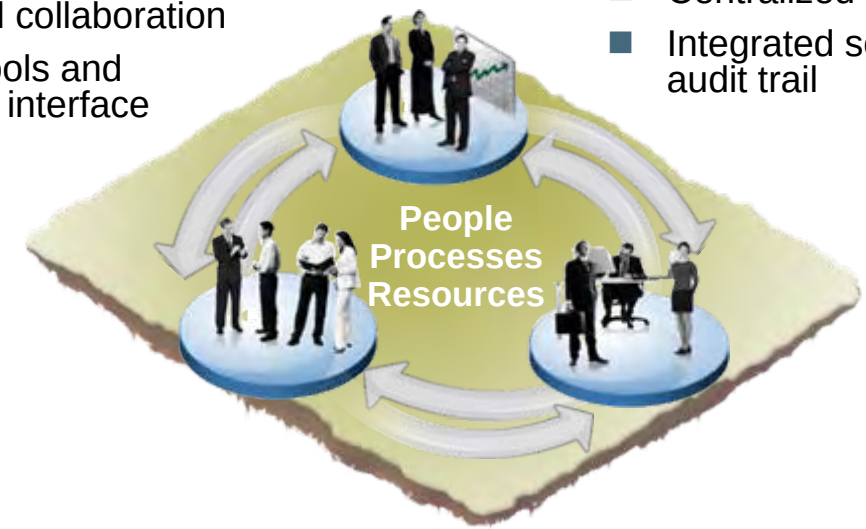
Alignment, Agility and Visibility

- 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

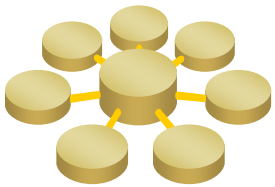
Free Up Resources, Time and Money for Innovation

- 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

SAP GRC Risk Management



Risk Repository

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

Access Control | Process Control | Global Trade | SONA/GRC xApp

SAP NetWeaver — **Business Process Platform** — CISCO SONA

Sources

ORACLE | PeopleSoft | SAP | Legacy

External Provider | KRIs / Content

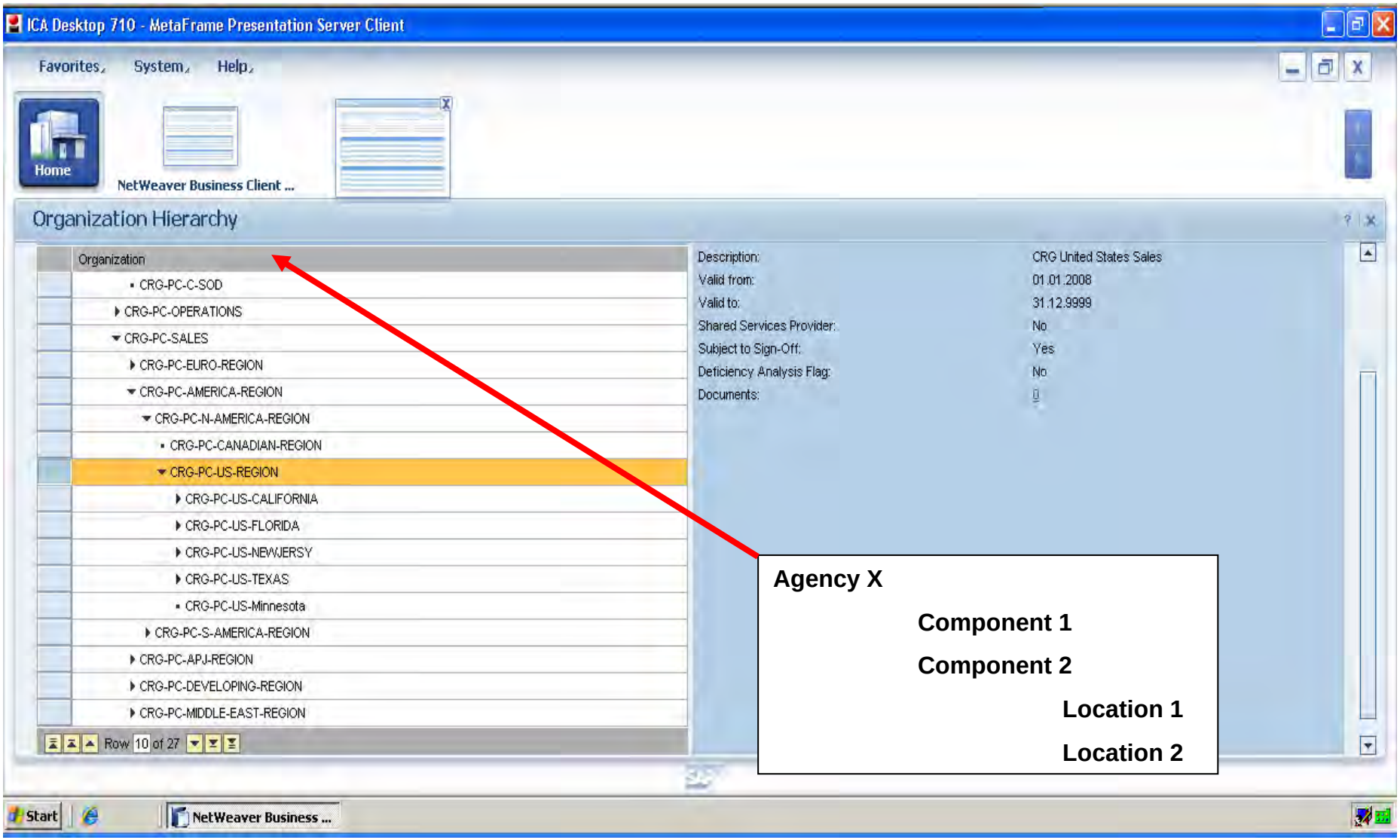
- **Delivers transparency to balanced global risk profile**
- **Standardizes on common GRC content and rules**
- **Automates and embeds GRC processes into business processes**
- **Integrates with existing IT assets and technology partners**
- **Enables easier collaboration with service and content partners**

SAP GRC Configuration Overview

Compliance Structure

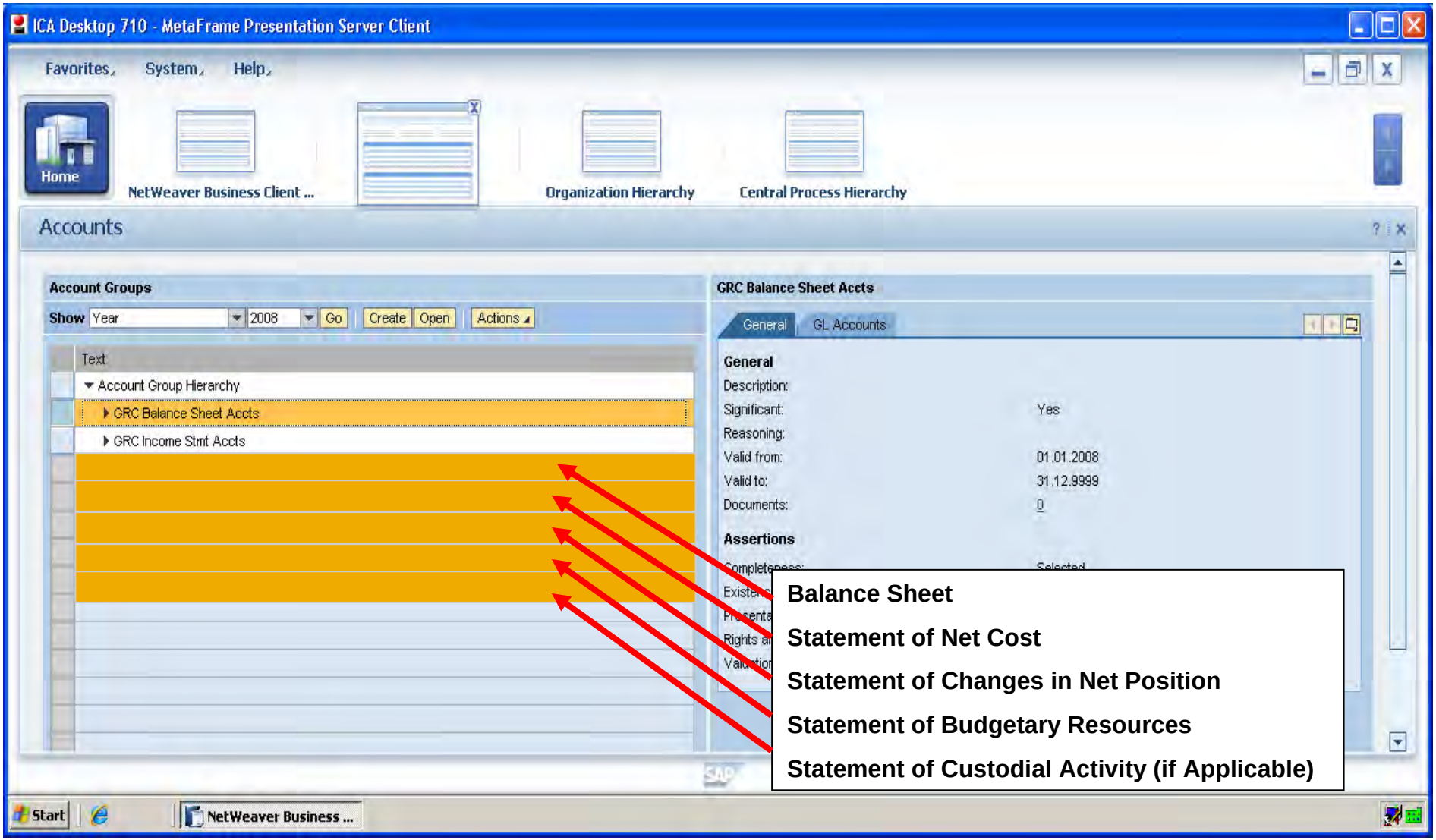
SAP GRC Configuration Overview

Organization Hierarchy



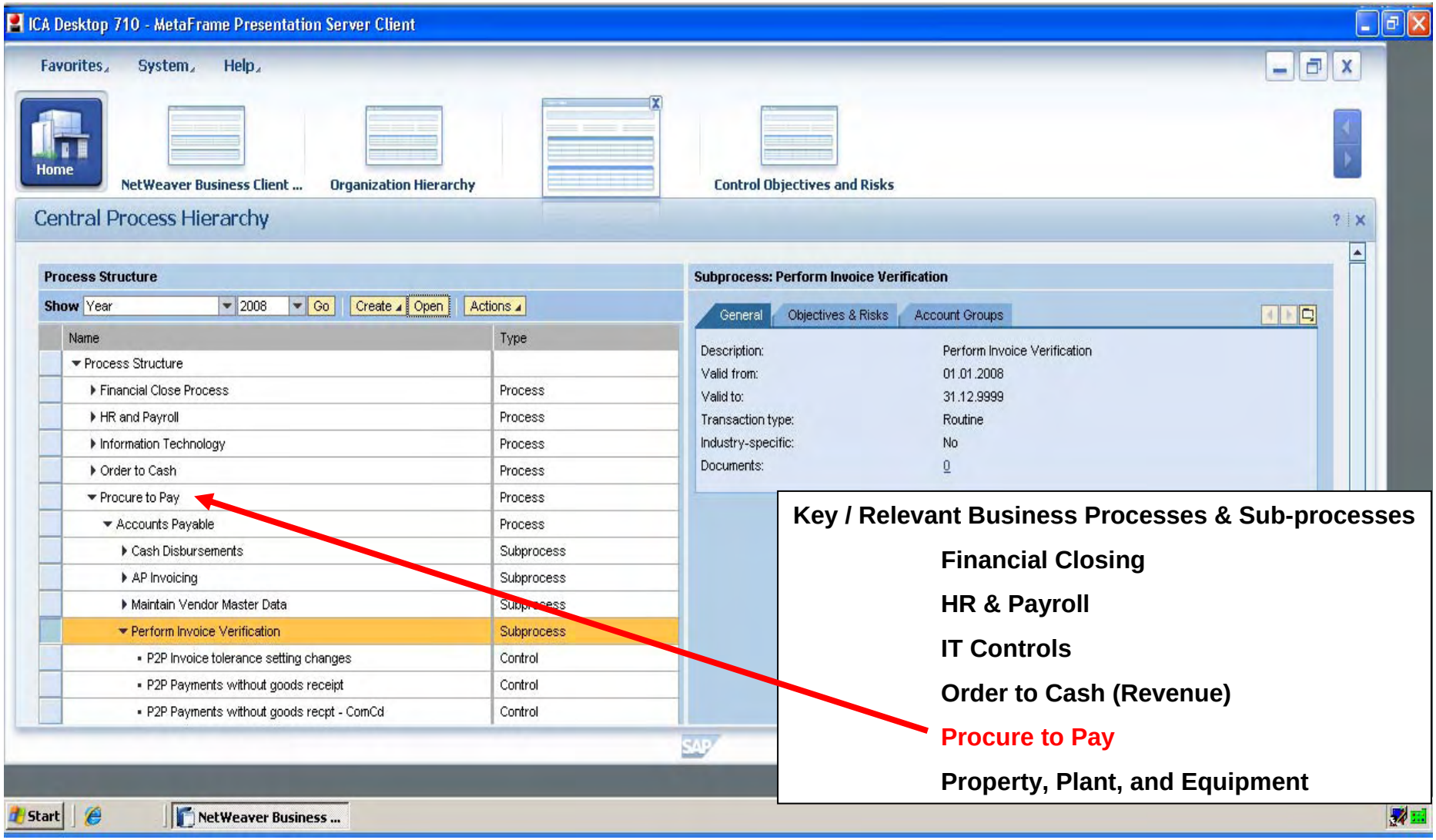
SAP GRC Configuration Overview

Account Group Hierarchy



SAP GRC Configuration Overview

Central Process Hierarchy/Catalog



Key / Relevant Business Processes & Sub-processes

Financial Closing

HR & Payroll

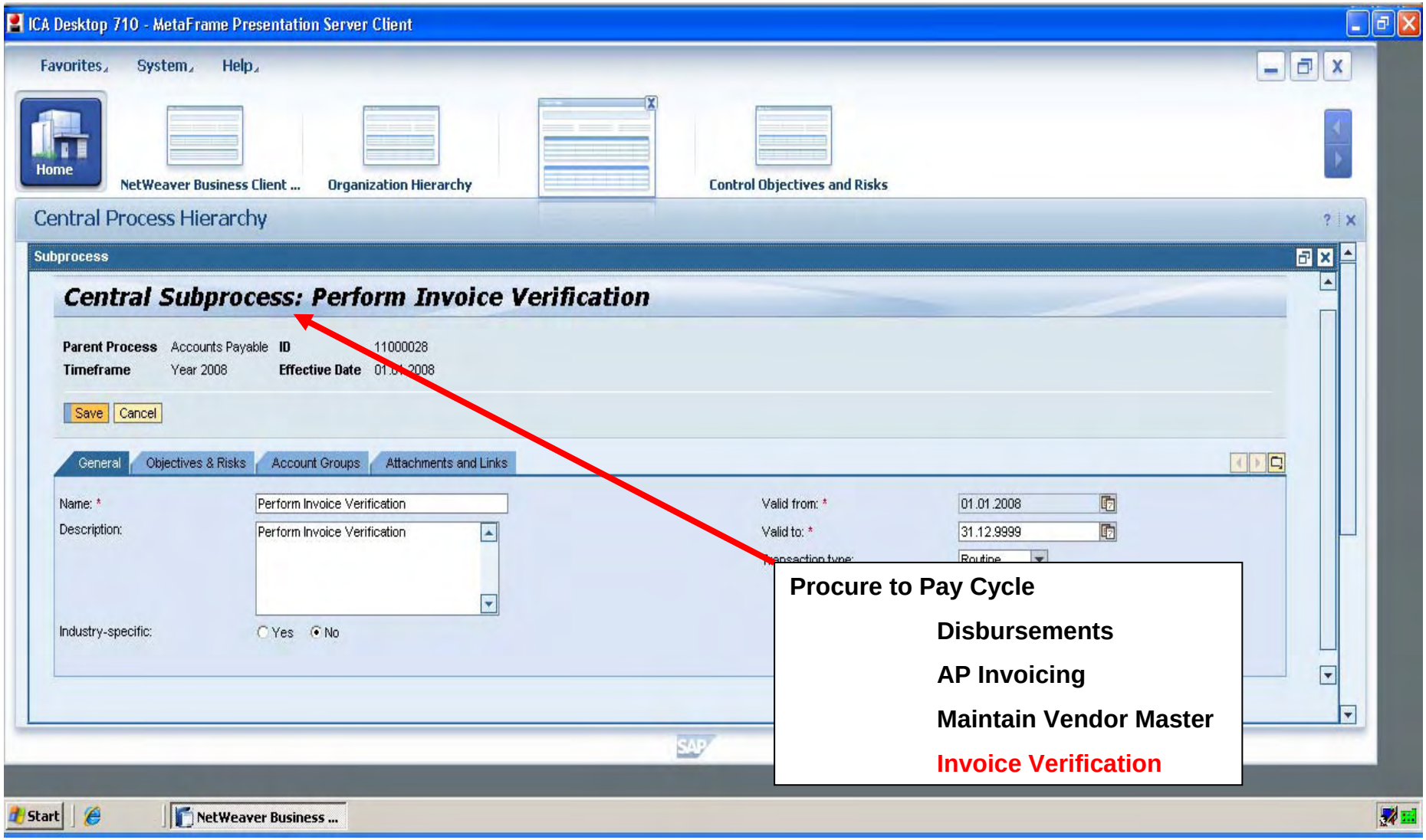
IT Controls

Order to Cash (Revenue)

Procure to Pay

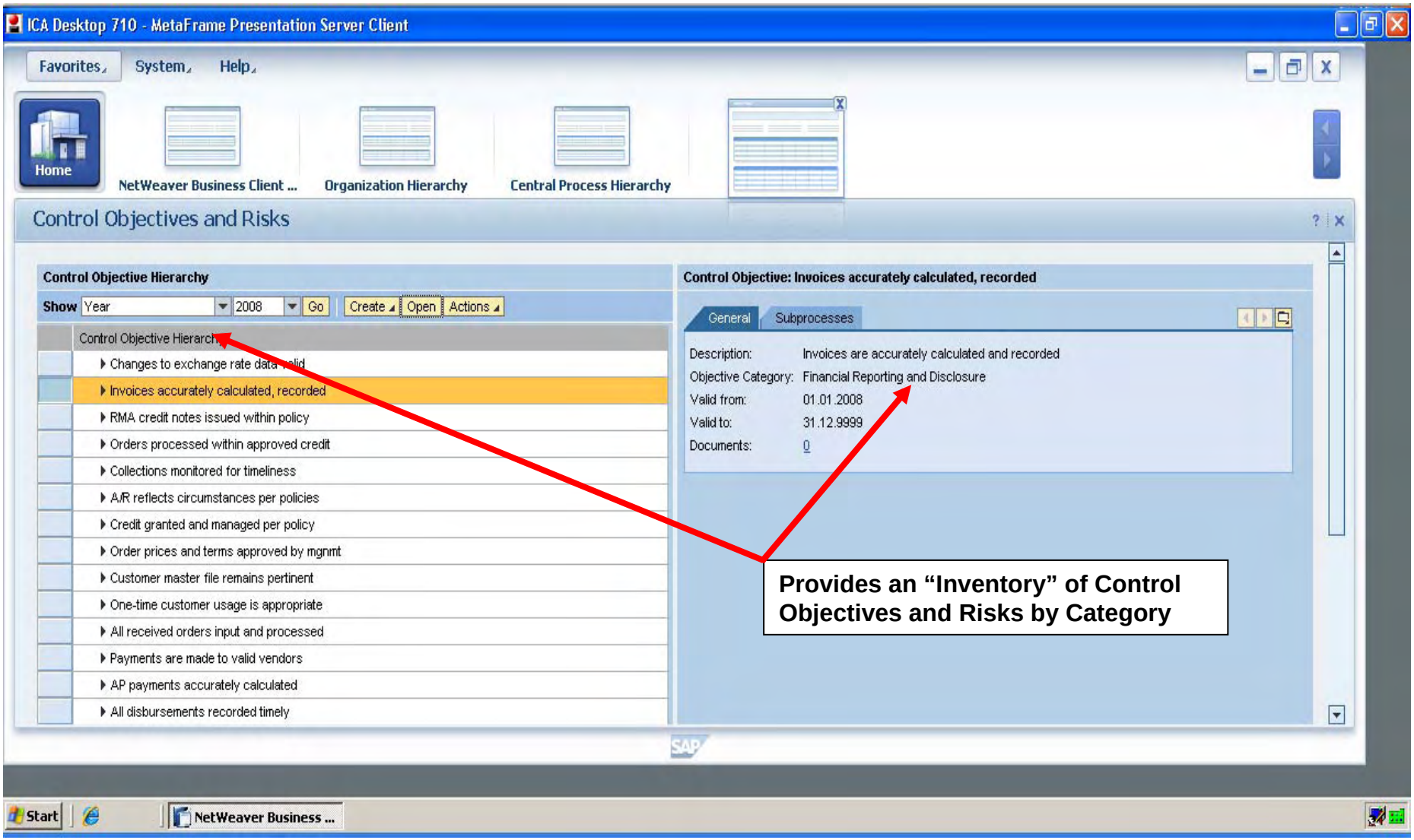
Property, Plant, and Equipment

SAP GRC Configuration Overview
Central Process Hierarchy/Catalog



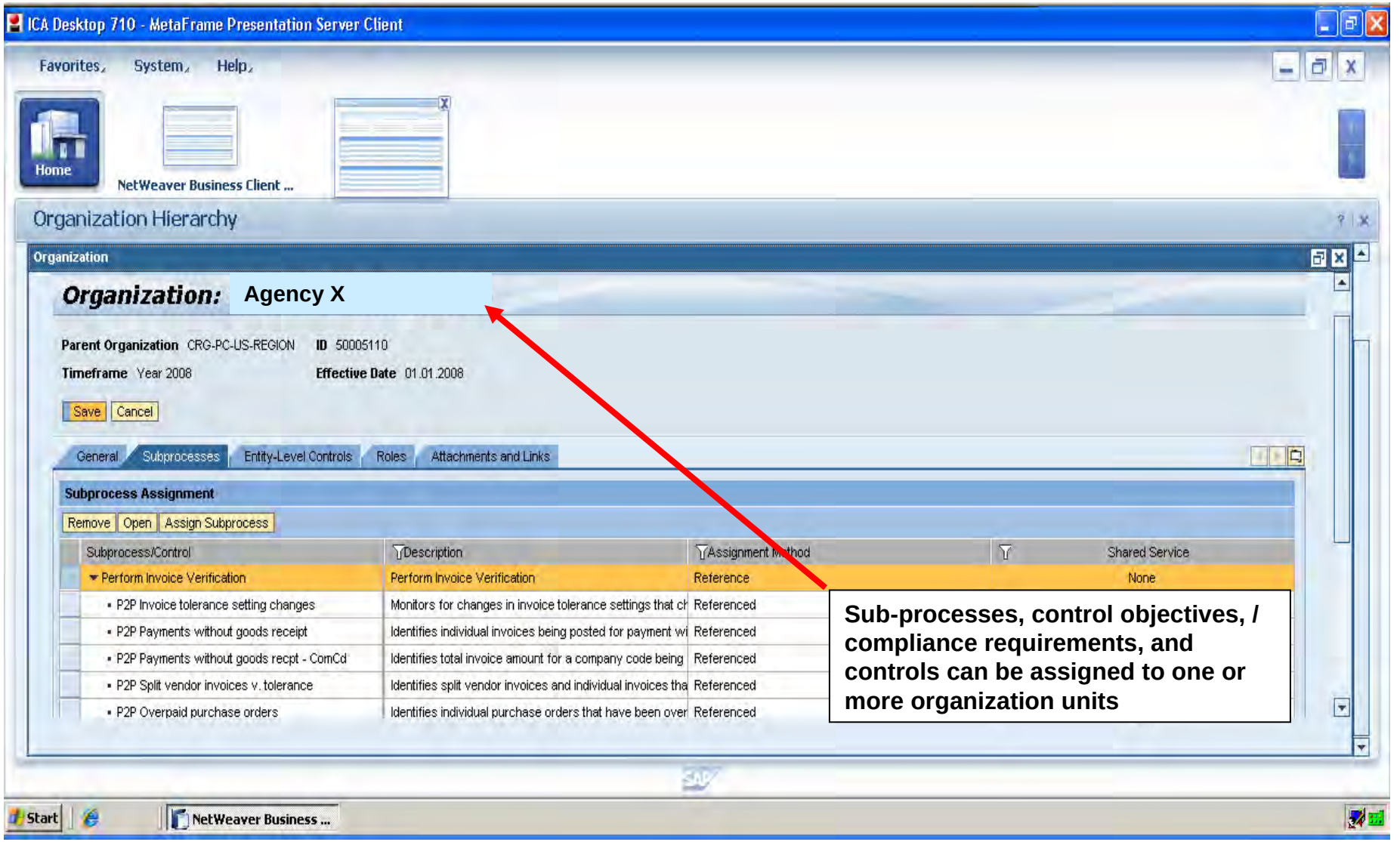
SAP GRC Configuration Overview

Control Objectives & Risks

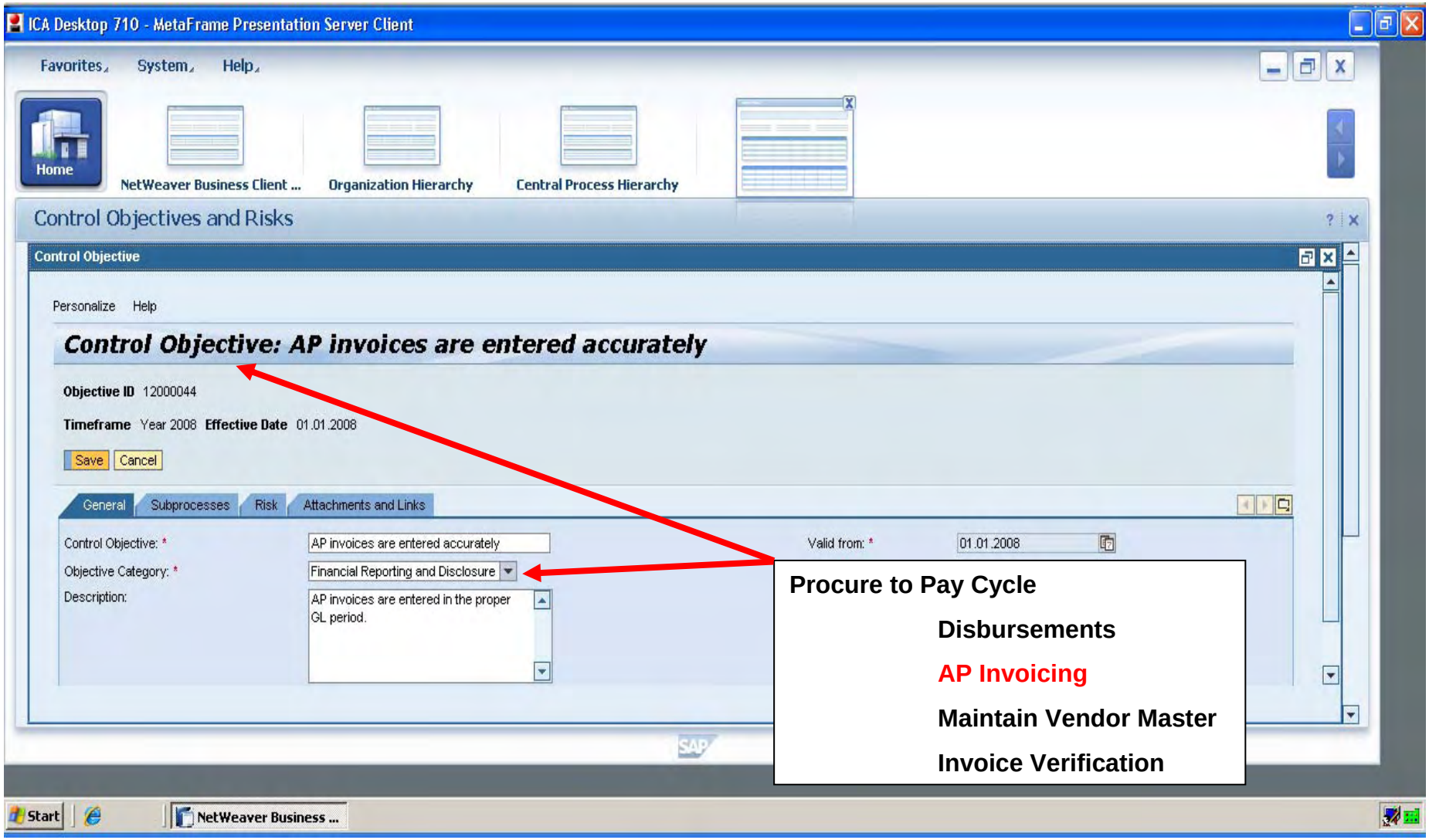


SAP GRC Configuration Overview

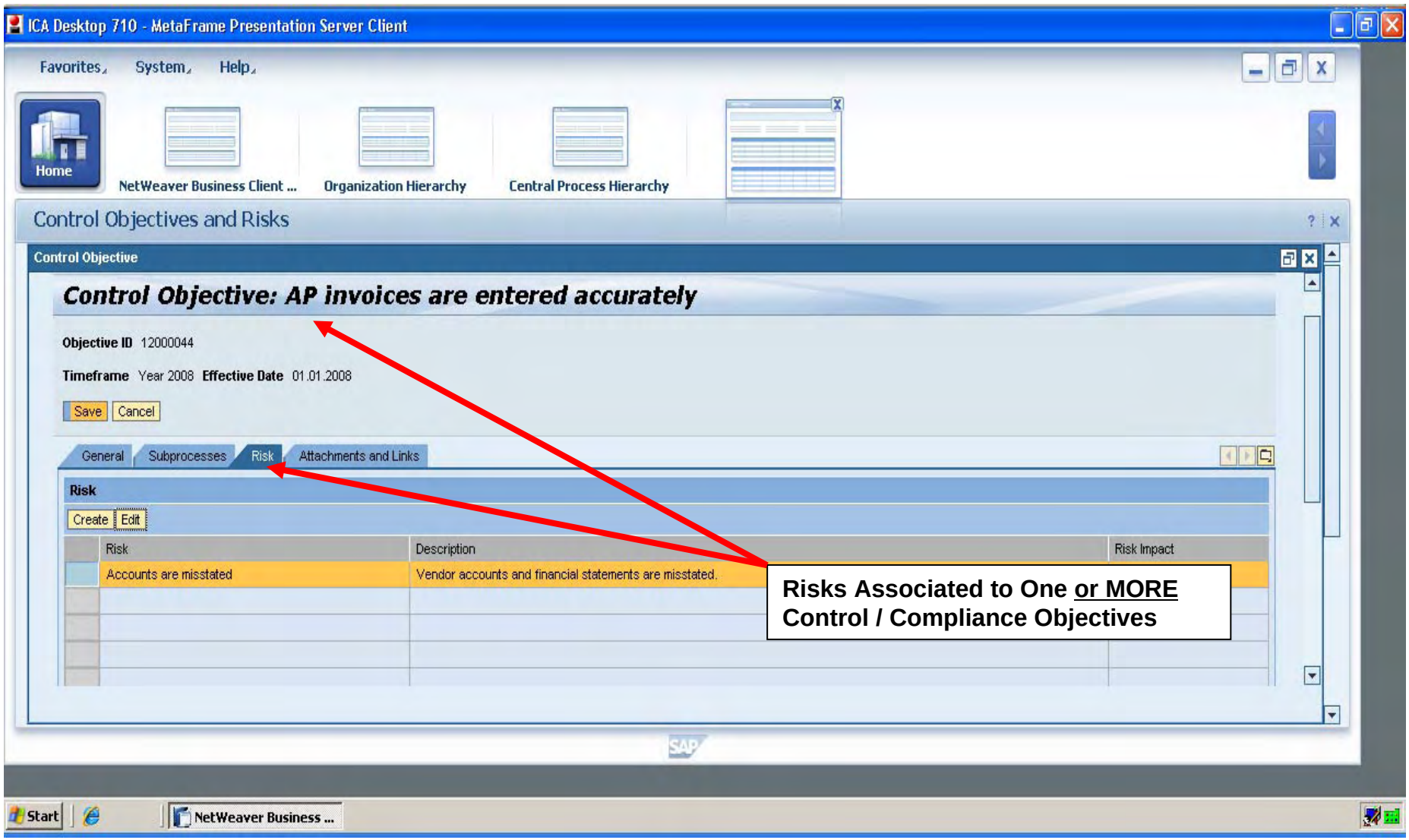
Assignment of Sub Process to Organization



SAP GRC Configuration Overview
Control Objectives and Compliance Requirements

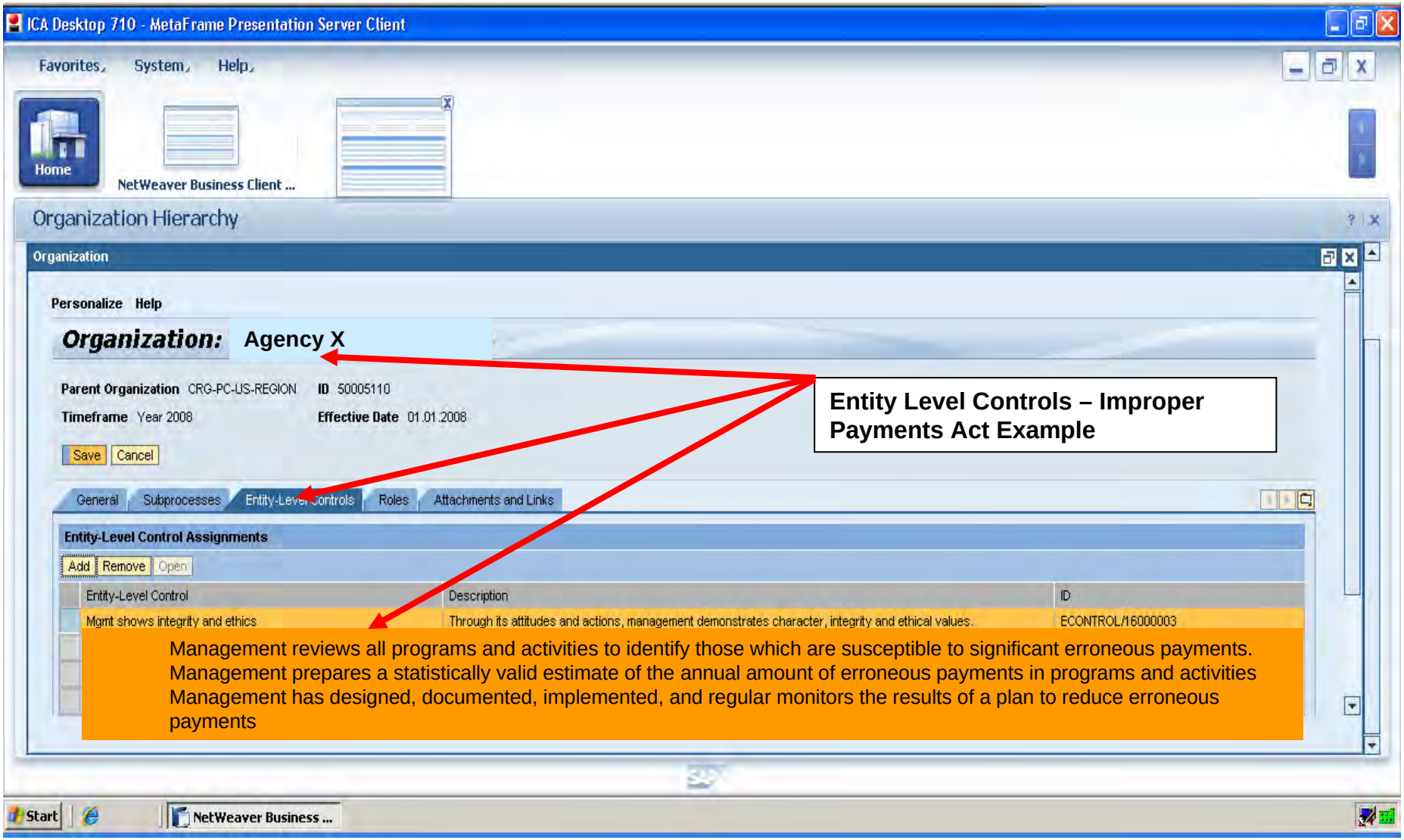


SAP GRC Configuration Overview
Risk Creation & Assignment



SAP GRC Configuration Overview

Addition of Entity Level Control



Entity Level Controls – Improper Payments Act Example

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

SAP GRC Delivers the Leading Compliance Solution for Public Sector

Business Objects
an SAP company

SAP

- 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

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