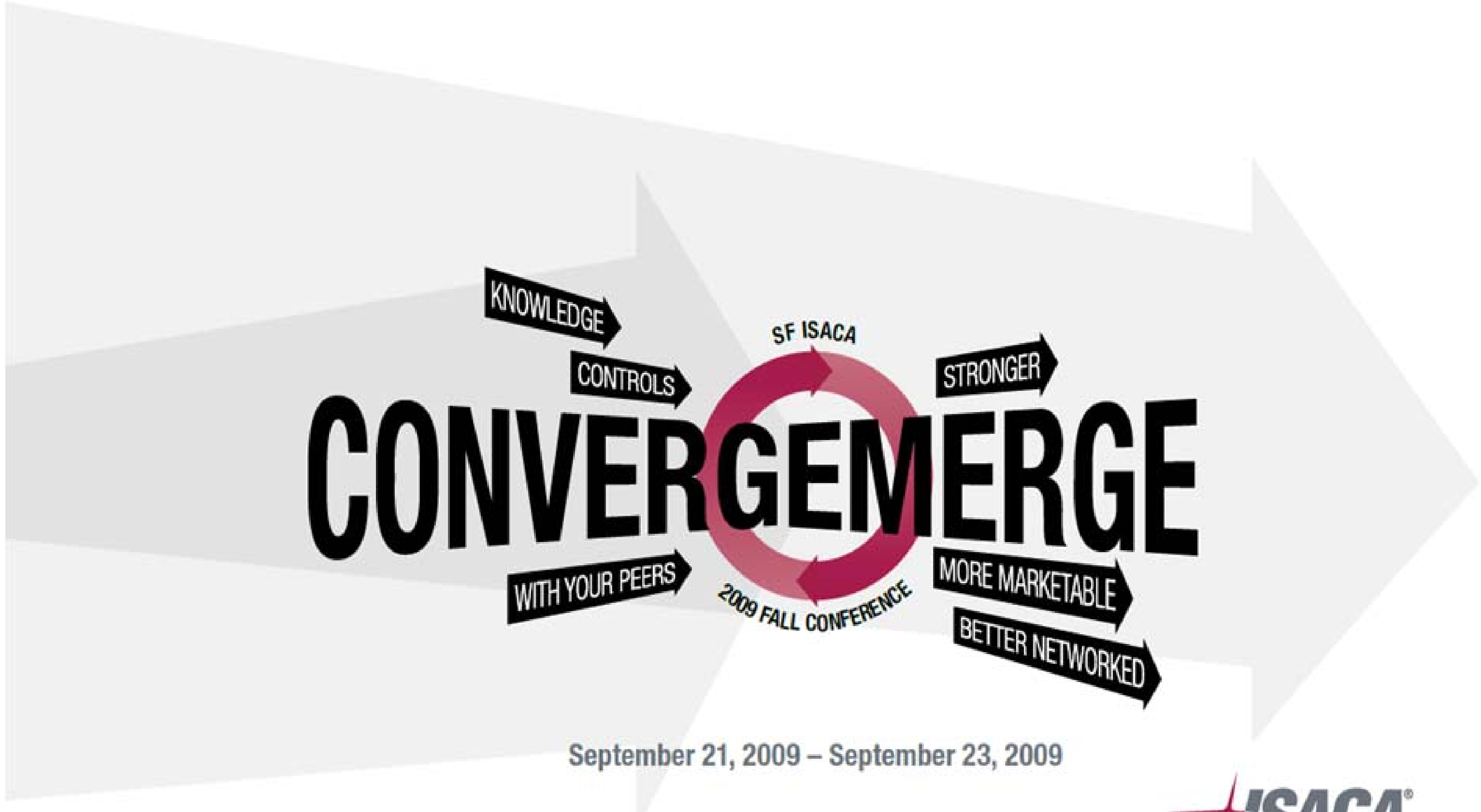
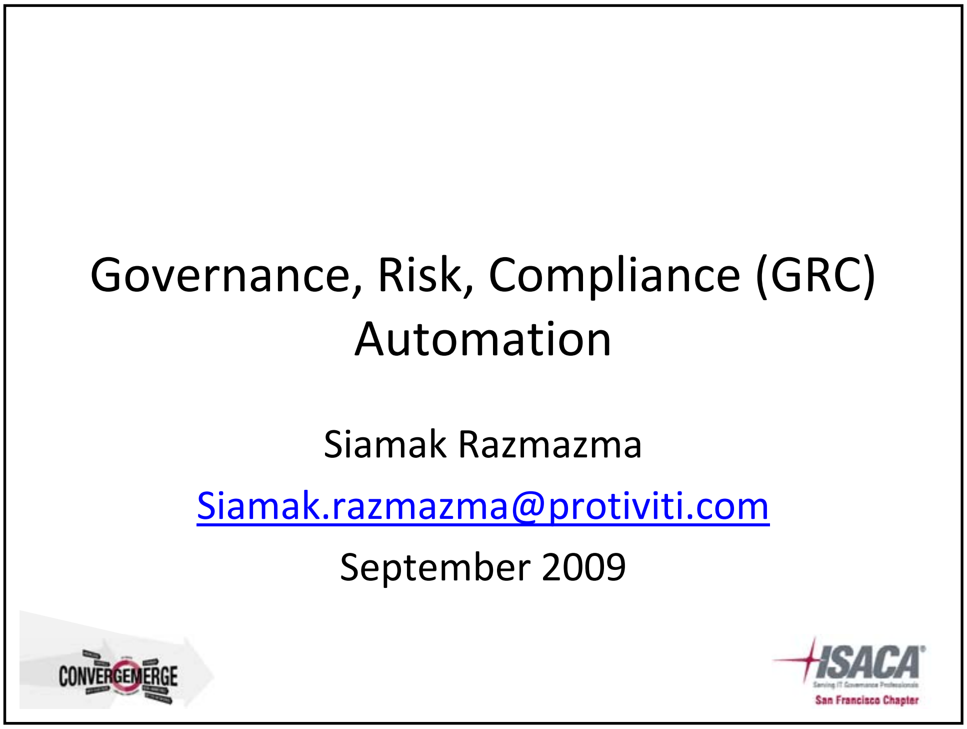
S24 - Governance, Risk, and Compliance (GRC) Automation

Siamak Razmazma



September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

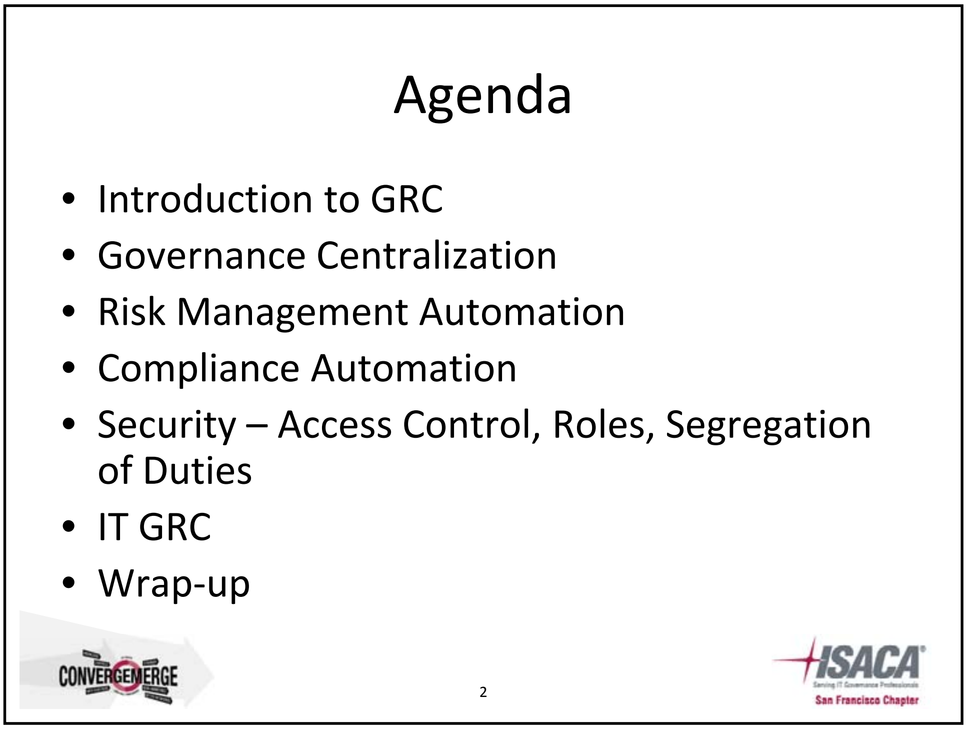


Governance, Risk, Compliance (GRC) Automation

Siamak Razmazma

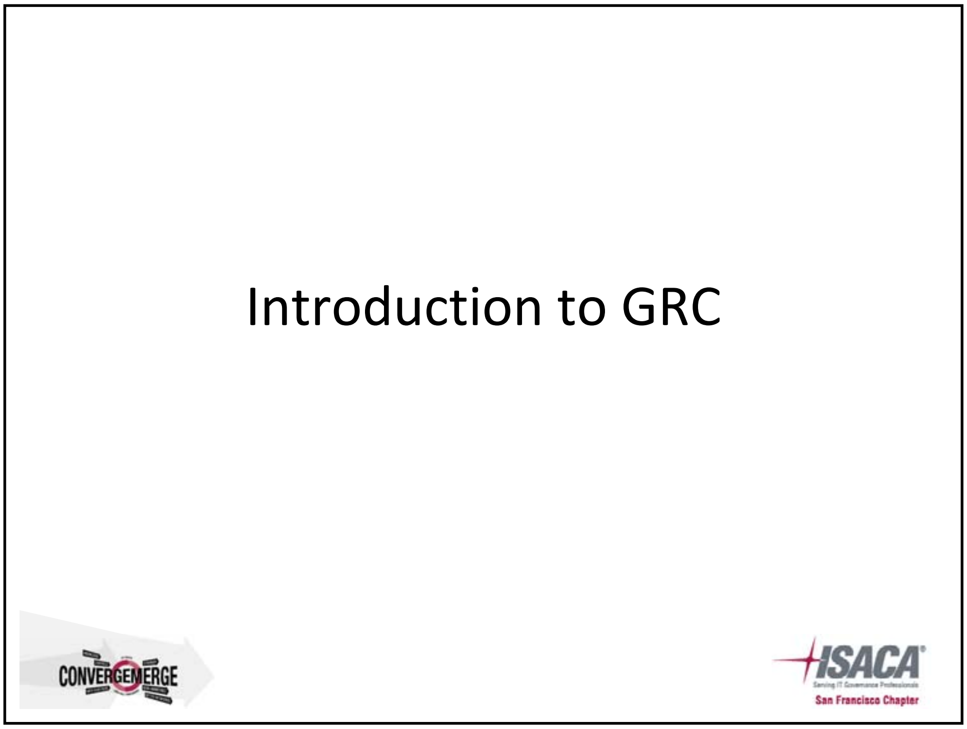
Siamak.razmazma@protiviti.com

September 2009

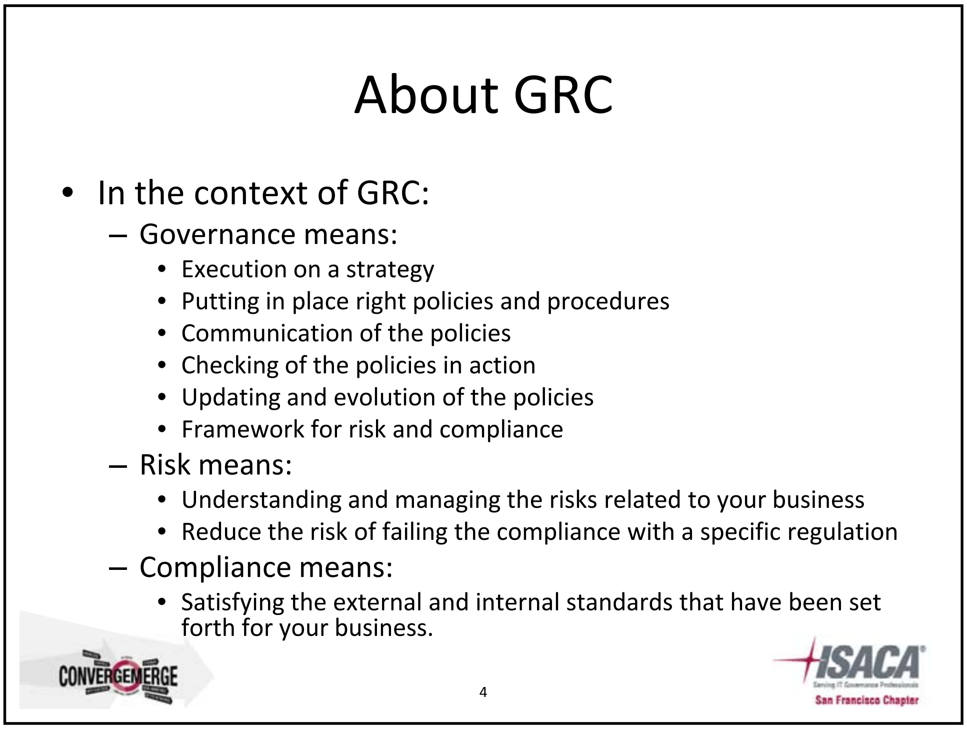


Agenda

- Introduction to GRC
- Governance Centralization
- Risk Management Automation
- Compliance Automation
- Security – Access Control, Roles, Segregation of Duties
- IT GRC
- Wrap-up

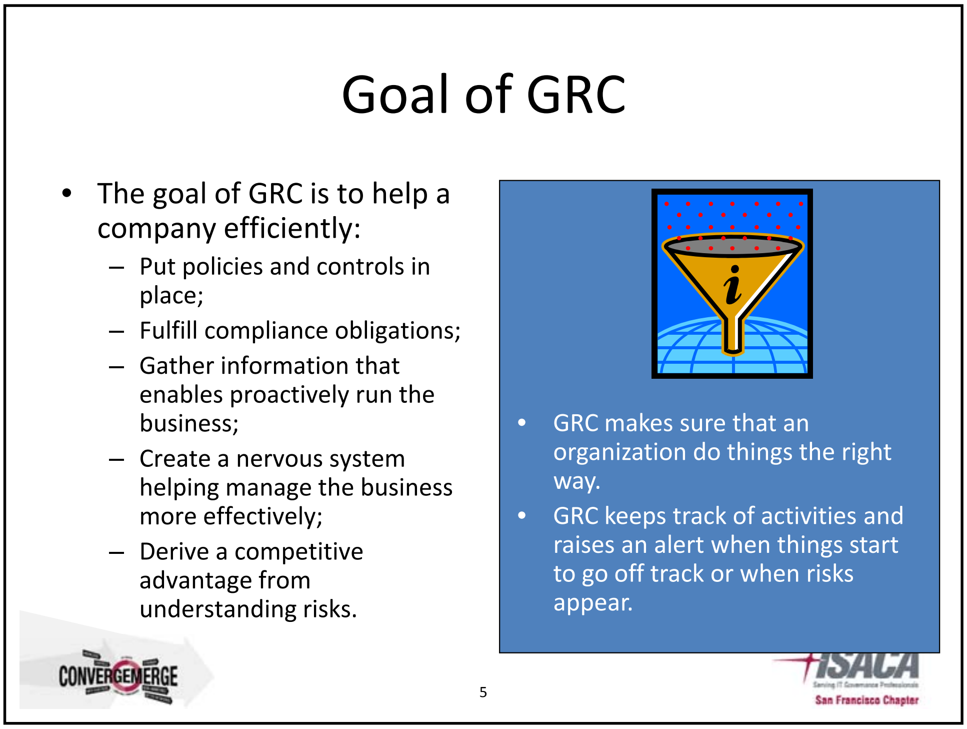


Introduction to GRC



About GRC

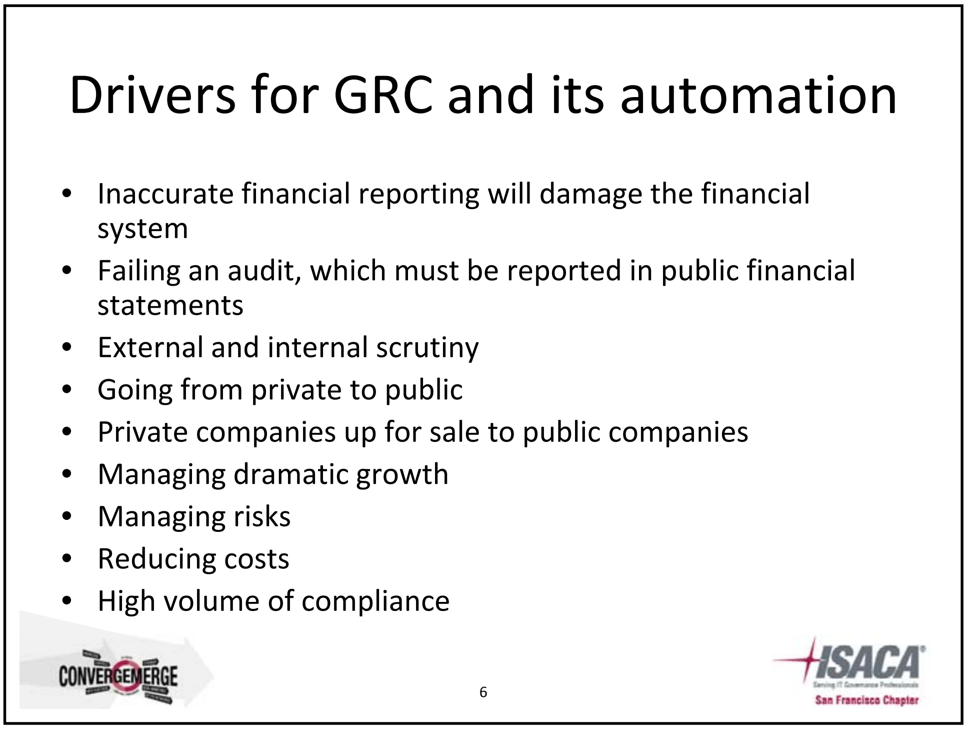
- In the context of GRC:
  - Governance means:
    - Execution on a strategy
    - Putting in place right policies and procedures
    - Communication of the policies
    - Checking of the policies in action
    - Updating and evolution of the policies
    - Framework for risk and compliance
  - Risk means:
    - Understanding and managing the risks related to your business
    - Reduce the risk of failing the compliance with a specific regulation
  - Compliance means:
    - Satisfying the external and internal standards that have been set forth for your business.



Goal of GRC

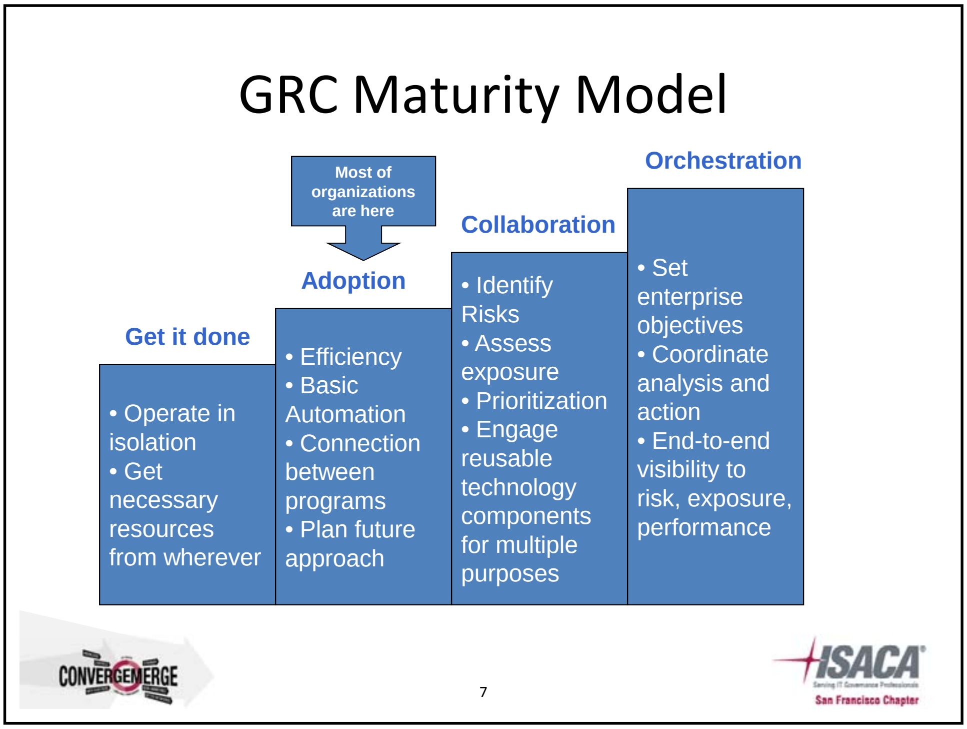
- The goal of GRC is to help a company efficiently:
  - Put policies and controls in place;
  - Fulfill compliance obligations;
  - Gather information that enables proactively run the business;
  - Create a nervous system helping manage the business more effectively;
  - Derive a competitive advantage from understanding risks.

- GRC makes sure that an organization do things the right way.
- GRC keeps track of activities and raises an alert when things start to go off track or when risks appear.



Drivers for GRC and its automation

- Inaccurate financial reporting will damage the financial system
- Failing an audit, which must be reported in public financial statements
- External and internal scrutiny
- Going from private to public
- Private companies up for sale to public companies
- Managing dramatic growth
- Managing risks
- Reducing costs
- High volume of compliance



GRC Maturity Model

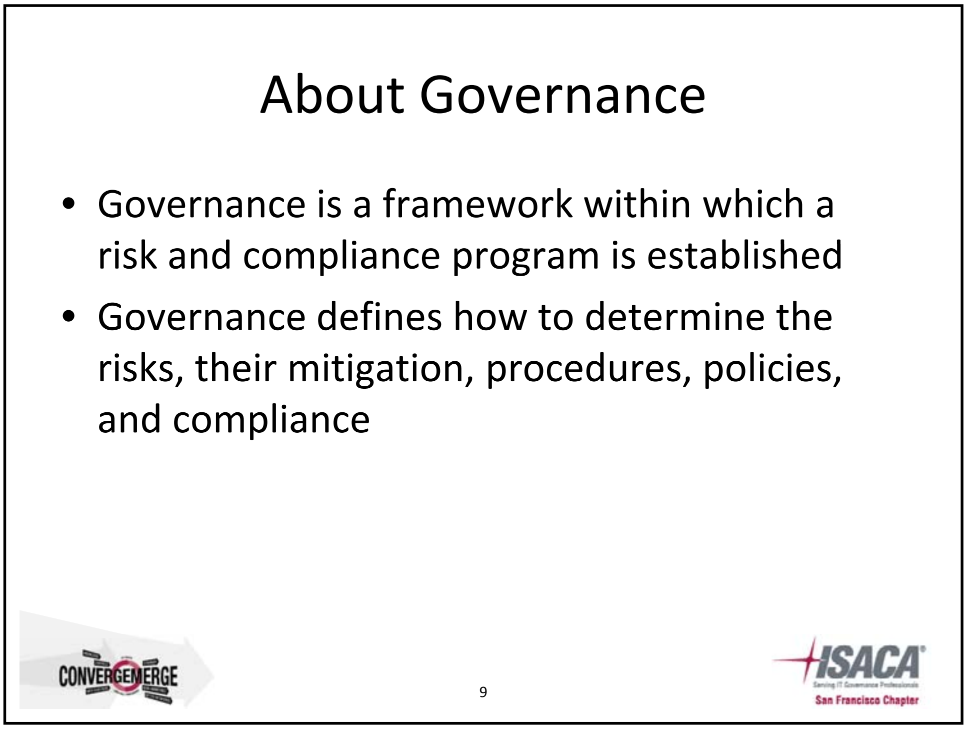
Get it done
- Operate in isolation
- Get necessary resources from wherever

Adoption
- Efficiency
- Basic Automation
- Connection between programs
- Plan future approach

Collaboration
- Identify Risks
- Assess exposure
- Prioritization
- Engage reusable technology components for multiple purposes

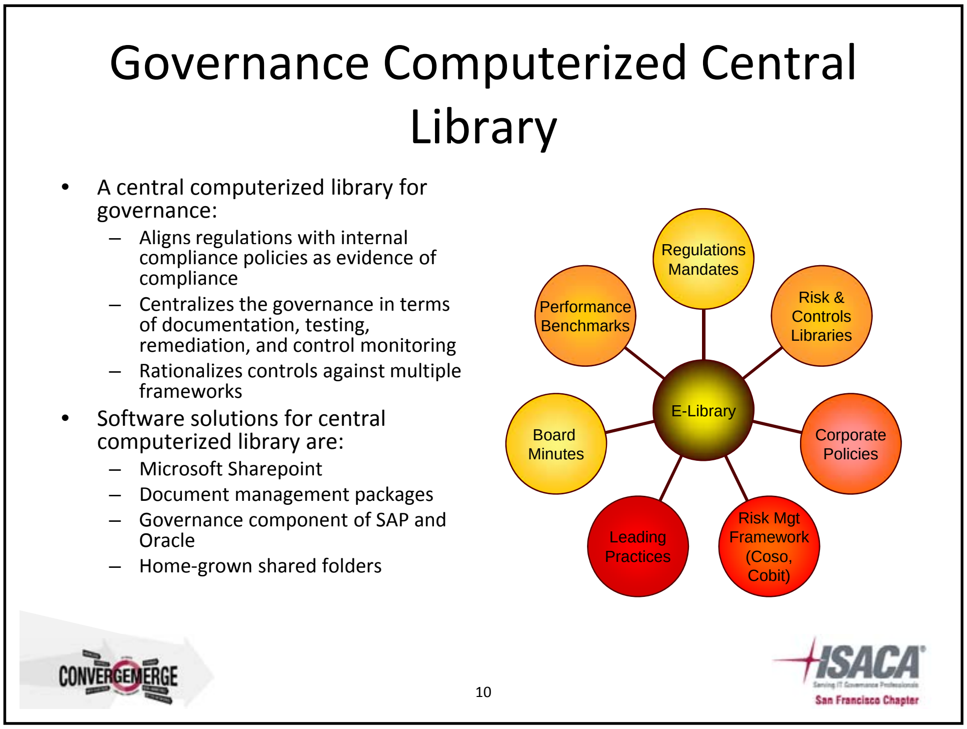
Orchestration
- Set enterprise objectives
- Coordinate analysis and action
- End-to-end visibility to risk, exposure, performance

Governance Centralization



About Governance

- Governance is a framework within which a risk and compliance program is established
- Governance defines how to determine the risks, their mitigation, procedures, policies, and compliance



Governance Computerized Central Library

- A central computerized library for governance:
  - Aligns regulations with internal compliance policies as evidence of compliance
  - Centralizes the governance in terms of documentation, testing, remediation, and control monitoring
  - Rationalizes controls against multiple frameworks
- Software solutions for central computerized library are:
  - Microsoft Sharepoint
  - Document management packages
  - Governance component of SAP and Oracle
  - Home-grown shared folders

E-Library

Regulations Mandates

Risk & Controls Libraries

Corporate Policies

Risk Mgt Framework (Coso, Cobit)

Leading Practices

Board Minutes

Performance Benchmarks

Challenges to implement Governance Computerized Central Library

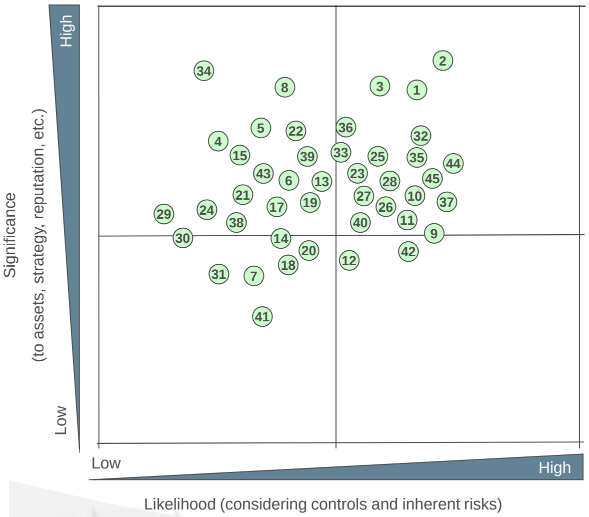
- Governance computerized central library may be perceived as:
  - A burden because of its costs
  - Constraints on the core functions of the organization
  - A change of current practices

Risk Management Automation

Risk Management Automation

- Automation of the process of monitoring risks is referred to as Risk Management Automation
- The leading practice for Risk Management Automation is to deploy an Enterprise Risk Management (ERM) software application
- The extent of automation of risk management depends on the level of integration between ERM and ERP (Enterprise Resource Planning)

Risk Map for Risk Management Automation



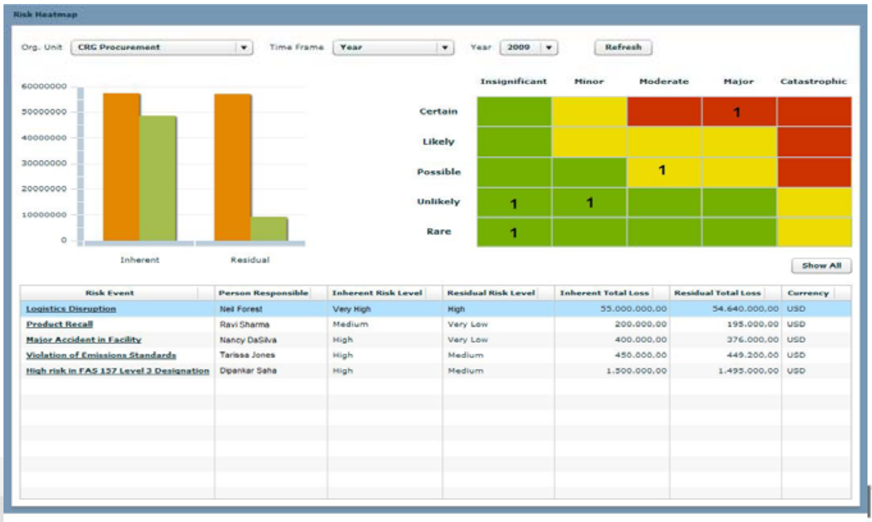
- 1 Competitor
- 2 Custom Wants
- 3 Technological Innovation
- 4 Sensitivity
- 5 Capital
- 6 Sovereign/Political
- 7 Regulatory
- 8 Customer Satisfaction
- 9 Human Resources
- 10 Knowledge Capital
- 11 Product Development
- 12 Efficiency
- 13 Capacity
- 14 Performance Gap
- 15 Cycle Time
- 16 Sourcing
- 17 Partnering
- 18 Compliance
- 19 Product/Service Failure
- 20 Environmental
- 21 Leadership
- 22 Authority
- 23 Change Readiness
- 24 Communications
- 25 IT Relevance
- 26 IT Integrity
- 27 IT Access
- 28 IT Infrastructure
- 29 Management Fraud
- 30 Third Party Fraud
- 31 Illegal Acts
- 32 Currency
- 33 Cash Flow
- 34 Concentration
- 35 Product/Service Pricing
- 36 Contract Commitment
- 37 Budgeting and Planning
- 38 Accounting Information
- 39 Financial Reporting
- 40 Taxation
- 41 Pension Fund
- 42 Investment Evaluation
- 43 Regulatory Reporting
- 44 Environmental Scan
- 45 Resource Allocation

Risk Management Automation Examples

Risk 1:

- Supply Chain Continuity
  - Indicator 1: Scrap Rate > 5%
  - Indicator 2: Supplier on time deliveries < 97%
  - Indicator 3: Contract Manufacturer planning accuracy <98%
  - Indicator 4: Critical Item A inventory level < 100
- Risk 2:
  - Human Resources
    - Indicator 1: Injuries > 3 in a given period
    - Indicator 2: Talent Exodus > 1 per functional area and period
- Risk 3:
  - Product Development
    - Indicator 1: Price > 2% of market (competition price)
    - Indicator 2: Customers Need Survey Gap < 95%

Example of Risk Management Dashboard



Org. Unit: CRG Procurement

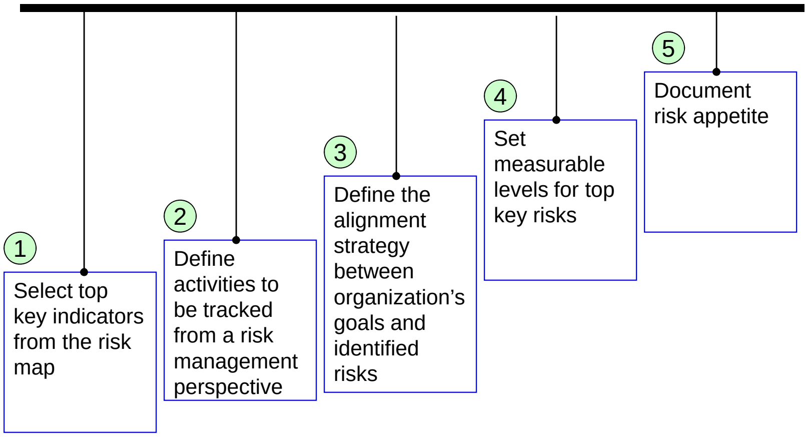
Time Frame: Year

Year: 2009

	Insignificant	Minor	Moderate	Major	Catastrophic
Certain	🟩	🟨	🟥	🟥 1	🟥
Likely	🟩	🟨	🟨	🟨	🟥
Possible	🟩	🟩	🟨 1	🟨	🟥
Unlikely	🟩 1	🟩 1	🟩	🟩	🟨
Rare	🟩 1	🟩	🟩	🟩	🟨

Risk Event	Person Responsible	Inherent Risk Level	Residual Risk Level	Inherent Total Loss	Residual Total Loss	Currency
Logistics Disruption	Neil Forest	Very High	High	55.000.000.00	54.640.000.00	USD
Product Recall	Ravi Sharma	Medium	Very Low	200.000.00	195.000.00	USD
Major Accident in Facility	Nancy DaSilva	High	Very Low	400.000.00	376.000.00	USD
Violation of Emissions Standards	Tarissa Jones	High	Medium	450.000.00	449.200.00	USD
High risk in FAS 157 Level 3 Designation	Dipankar Saha	High	Medium	1.500.000.00	1.495.000.00	USD

Main steps for Risk Management Automation



1 Select top key indicators from the risk map

2 Define activities to be tracked from a risk management perspective

3 Define the alignment strategy between organization's goals and identified risks

4 Set measurable levels for top key risks

5 Document risk appetite

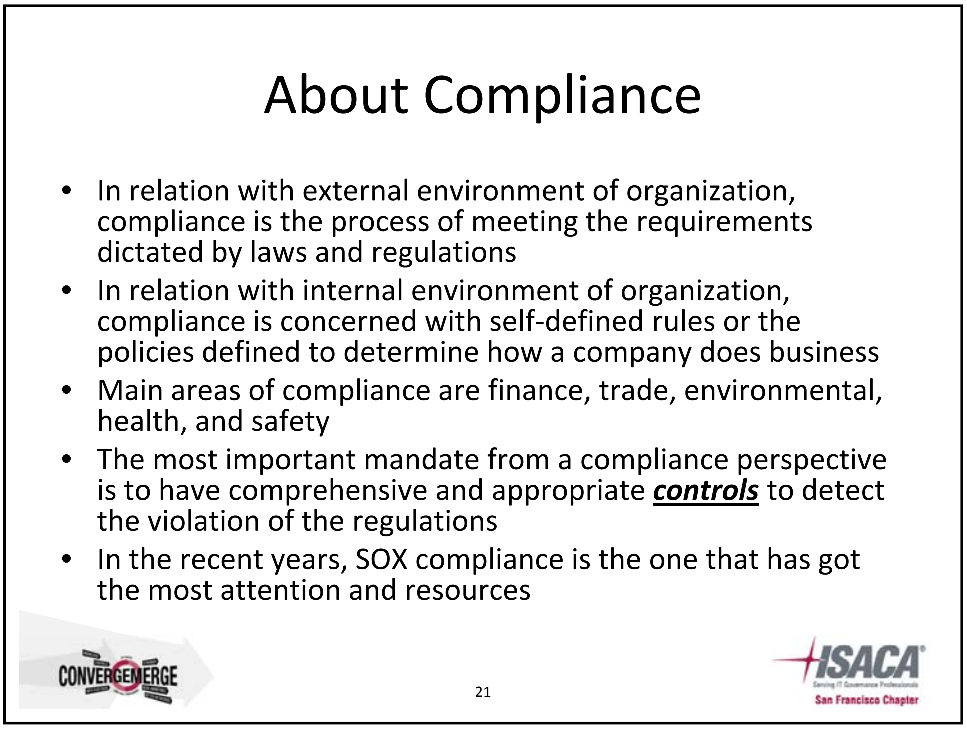
Benefits of Risk Management Automation

- Enablement and automation of enterprise risk management across lines of business.
- Leverage the vast data environments in your organization including ERP, e-mail systems, spreadsheets, and documents.
- Alignment of the risk management with corporate strategy.
- Good quality information to make better decisions taking into account key risk factors.

Challenges to Risk Management Automation

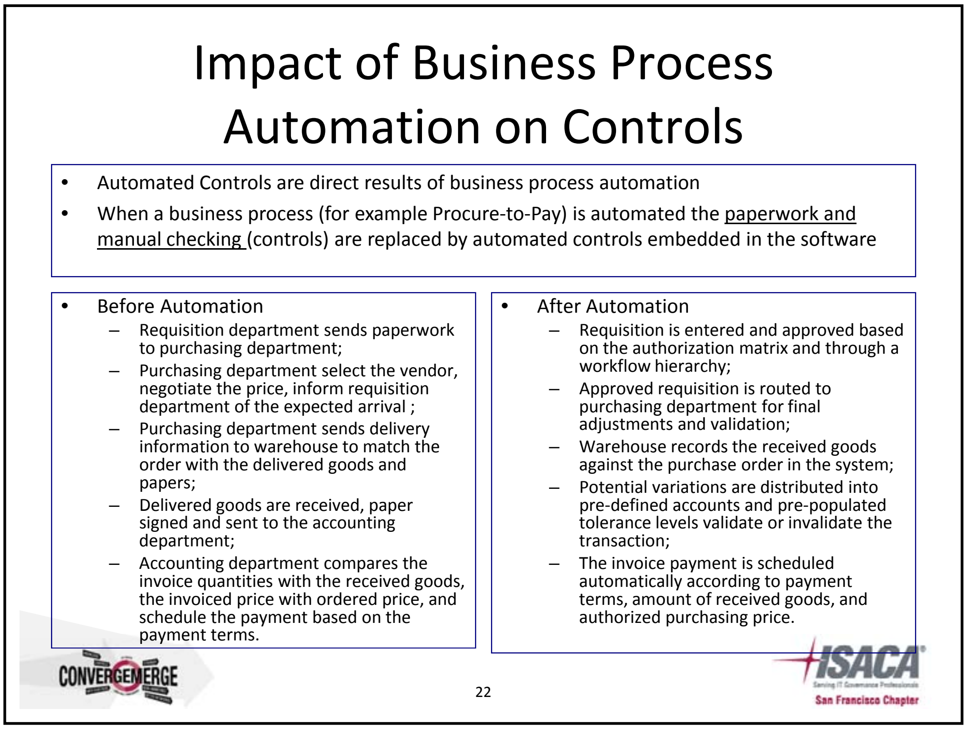
- Organization’s Culture
- Lack of proper Data and systems
- Risk management strategy and approach
- Role confusion (no risk manager)
- Disconnect between policies and processes
- Disconnect between governance and risks
- Consider risk management automation as an IT initiative or need

Compliance Automation



About Compliance

- In relation with external environment of organization, compliance is the process of meeting the requirements dictated by laws and regulations
- In relation with internal environment of organization, compliance is concerned with self-defined rules or the policies defined to determine how a company does business
- Main areas of compliance are finance, trade, environmental, health, and safety
- The most important mandate from a compliance perspective is to have comprehensive and appropriate ***controls*** to detect the violation of the regulations
- In the recent years, SOX compliance is the one that has got the most attention and resources



Impact of Business Process Automation on Controls

- Automated Controls are direct results of business process automation
- When a business process (for example Procure-to-Pay) is automated the paperwork and manual checking (controls) are replaced by automated controls embedded in the software

- Before Automation
  - Requisition department sends paperwork to purchasing department;
  - Purchasing department select the vendor, negotiate the price, inform requisition department of the expected arrival ;
  - Purchasing department sends delivery information to warehouse to match the order with the delivered goods and papers;
  - Delivered goods are received, paper signed and sent to the accounting department;
  - Accounting department compares the invoice quantities with the received goods, the invoiced price with ordered price, and schedule the payment based on the payment terms.

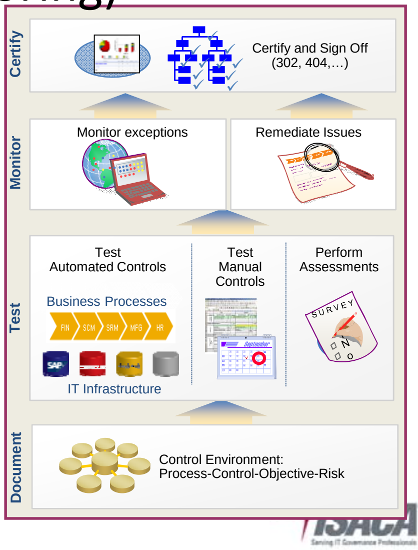
- After Automation
  - Requisition is entered and approved based on the authorization matrix and through a workflow hierarchy;
  - Approved requisition is routed to purchasing department for final adjustments and validation;
  - Warehouse records the received goods against the purchase order in the system;
  - Potential variations are distributed into pre-defined accounts and pre-populated tolerance levels validate or invalidate the transaction;
  - The invoice payment is scheduled automatically according to payment terms, amount of received goods, and authorized purchasing price.

Benefits of Automated Controls

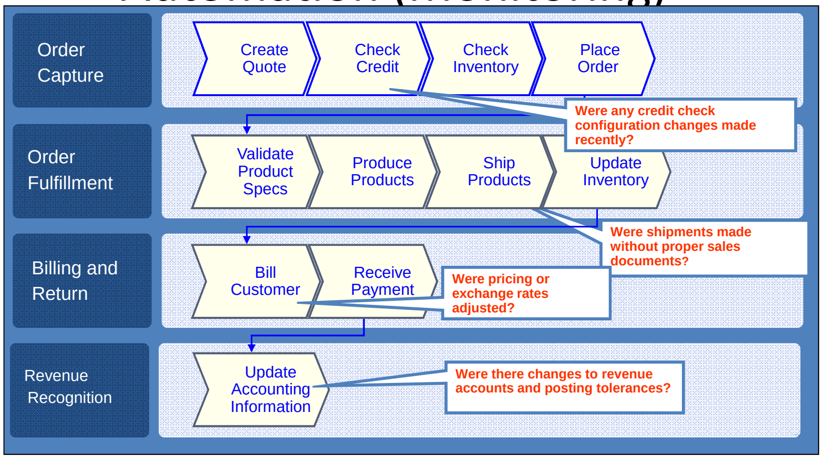
- Cheaper, with fewer errors
- Better protection
- Quicker to detect and fix
- Embedded into core systems
- Simultaneous control and monitoring
- Automatic evidence
- No sampling
- Ripple effect

Automation of Process Controls (Monitoring)

- Automation of process controls requires:
  - Single software solution for enterprise-wide control management;
  - Centralized management for both manual and automated controls;
  - Management by exception prioritizing remediation activities;
  - Visibility into what is happening in the control environment;
  - Management of financial, operational, and IT controls including one or across multiple enterprise systems;
  - Improvement of controls based on regular and frequent assessments.



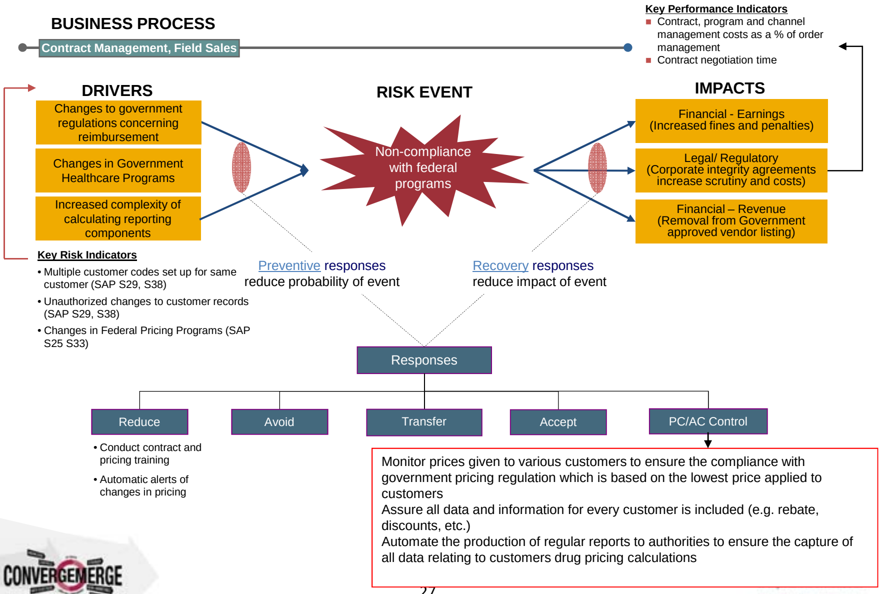
Examples of Process Controls Automation (Monitoring)


Order Capture
Create Quote
Check Credit
Check Inventory
Place Order
Were any credit check configuration changes made recently?
Order Fulfillment
Validate Product Specs
Produce Products
Ship Products
Update Inventory
Were shipments made without proper sales documents?
Billing and Return
Bill Customer
Receive Payment
Were pricing or exchange rates adjusted?
Revenue Recognition
Update Accounting Information
Were there changes to revenue accounts and posting tolerances?

Example of Pricing Compliance

- *Pricing is both competitive and extremely complex.*
- *An increasing number of lawsuits by Medicare focus on failure of companies to maintain their MFN (most favorite nation) clause to federal programs.*
- *This process is made increasingly difficult by both complexity of government programs (i.e. Medicaid Drugs Rebate Program, Medicare Part B and the Veteran’s Healthcare Act) and the ‘gross to net’ adjustments (rebates, discounts, etc) used with companies across the industry.*

Example of Pricing Compliance



Key Performance Indicators
- Contract, program and channel management costs as a % of order management
- Contract negotiation time

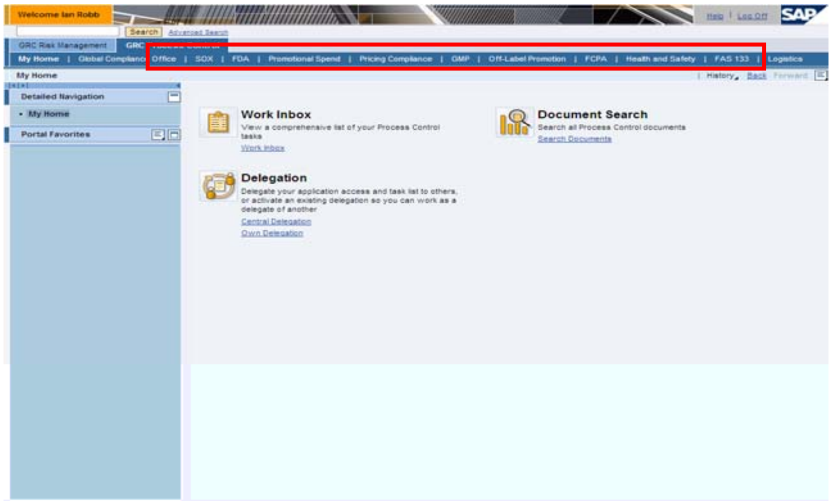
BUSINESS PROCESS
Contract Management, Field Sales
DRIVERS
Changes to government regulations concerning reimbursement
Changes in Government Healthcare Programs
Increased complexity of calculating reporting components
RISK EVENT
Non-compliance with federal programs
IMPACTS
Financial - Earnings (Increased fines and penalties)
Legal/ Regulatory (Corporate integrity agreements increase scrutiny and costs)
Financial – Revenue (Removal from Government approved vendor listing)
Preventive responses reduce probability of event
Recovery responses reduce impact of event
Responses
Reduce
Avoid
Transfer
Accept
PC/AC Control

Key Risk Indicators
- Multiple customer codes set up for same customer (SAP S29, S38)
- Unauthorized changes to customer records (SAP S29, S38)
- Changes in Federal Pricing Programs (SAP S25 S33)

- Conduct contract and pricing training
- Automatic alerts of changes in pricing

Monitor prices given to various customers to ensure the compliance with government pricing regulation which is based on the lowest price applied to customers
Assure all data and information for every customer is included (e.g. rebate, discounts, etc.)
Automate the production of regular reports to authorities to ensure the capture of all data relating to customers drug pricing calculations

Example of Process Control Automation (Monitoring)



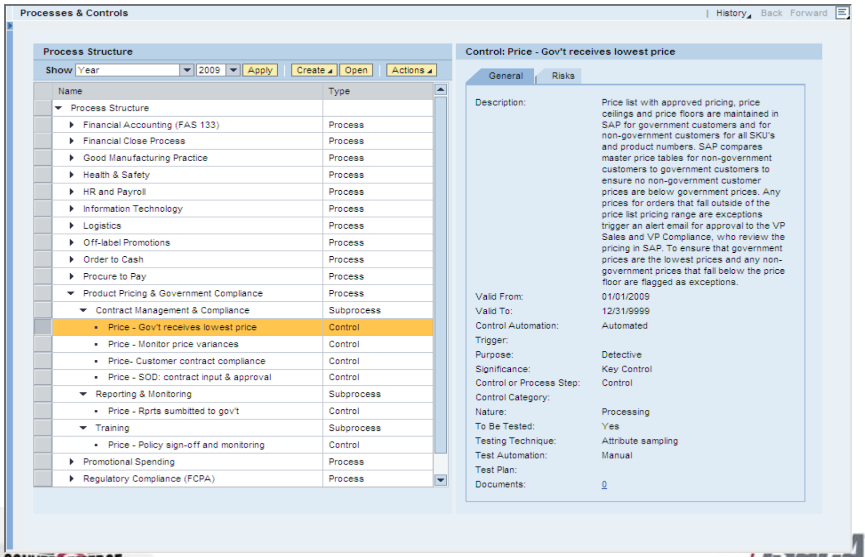
Welcome Ian Robb
Help | Log Off
SAP
Search
Advanced Search
GRC Risk Management
GRC Process Control
My Home | Global Compliance Office | SOX | FDA | Promotional Spend | Pricing Compliance | GMP | Off-Label Promotion | FCPA | Health and Safety | FAS 133 | Logistics
My Home
History
Back
Forward
Detailed Navigation
• My Home
Portal Favorites

Work Inbox
View a comprehensive list of your Process Control tasks
Work Inbox

Document Search
Search all Process Control documents
Search Documents

Delegation
Delegate your application access and task list to others, or activate an existing delegation so you can work as a delegate of another
Central Delegation
Own Delegation

Example of Process Control Automation (Monitoring)



Process Structure

Show Year 2009 Apply | Create Open | Actions

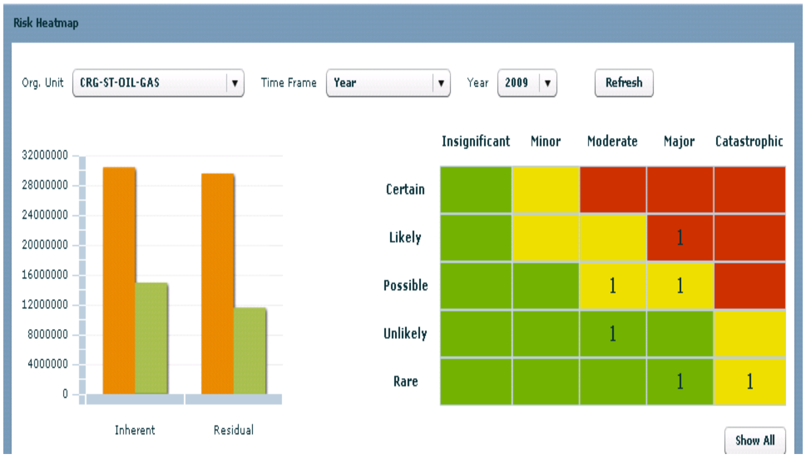
Name	Type
Process Structure	
Financial Accounting (FAS 133)	Process
Financial Close Process	Process
Good Manufacturing Practice	Process
Health & Safety	Process
HR and Payroll	Process
Information Technology	Process
Logistics	Process
Off-label Promotions	Process
Order to Cash	Process
Procure to Pay	Process
Product Pricing & Government Compliance	Process
Contract Management & Compliance	Subprocess
Price - Gov't receives lowest price	Control
Price - Monitor price variances	Control
Price- Customer contract compliance	Control
Price - SOD: contract input & approval	Control
Reporting & Monitoring	Subprocess
Price - Rprts sumbitted to gov't	Control
Training	Subprocess
Price - Policy sign-off and monitoring	Control
Promotional Spending	Process
Regulatory Compliance (FCPA)	Process

Control: Price - Gov't receives lowest price

General | Risks

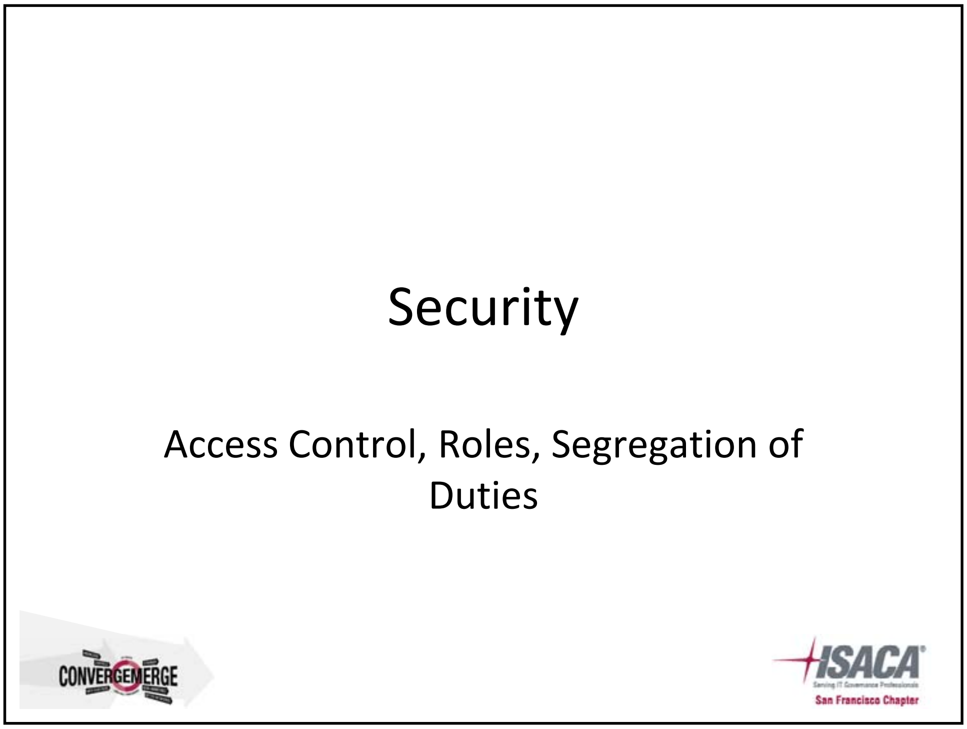
Description:	Price list with approved pricing, price ceilings and price floors are maintained in SAP for government customers and for non-government customers for all SKU's and product numbers. SAP compares master price tables for non-government customers to government customers to ensure no non-government customer prices are below government prices. Any prices for orders that fall outside of the price list pricing range are exceptions trigger an alert email for approval to the VP Sales and VP Compliance, who review the pricing in SAP. To ensure that government prices are the lowest prices and any non-government prices that fall below the price floor are flagged as exceptions.
Valid From:	01/01/2009
Valid To:	12/31/9999
Control Automation:	Automated
Trigger:	
Purpose:	Detective
Significance:	Key Control
Control or Process Step:	Control
Control Category:	
Nature:	Processing
To Be Tested:	Yes
Testing Technique:	Attribute sampling
Test Automation:	Manual
Test Plan:	
Documents:	0

Example of Process Control Automation (Monitoring)



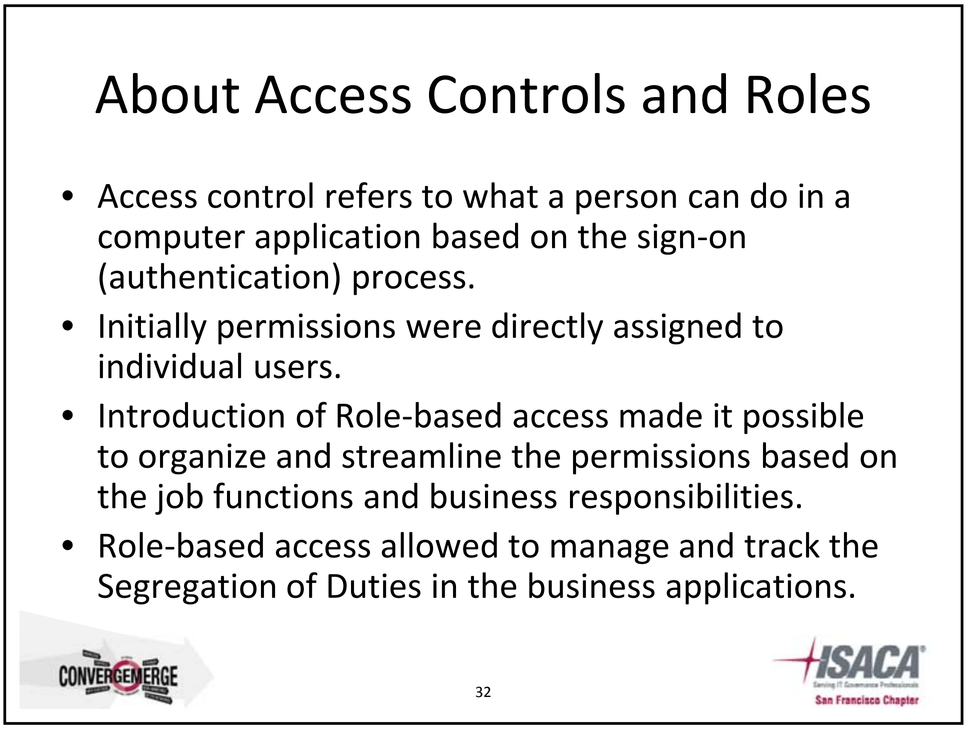
Org. Unit CRG-ST-OIL-GAS Time Frame Year Year 2009

	Insignificant	Minor	Moderate	Major	Catastrophic
Certain	🟩	🟨	🟥	🟥	🟥
Likely	🟩	🟨	🟨	🟥 1	🟥
Possible	🟩	🟩	🟨 1	🟨 1	🟥
Unlikely	🟩	🟩	🟩 1	🟩	🟨
Rare	🟩	🟩	🟩	🟩 1	🟨 1



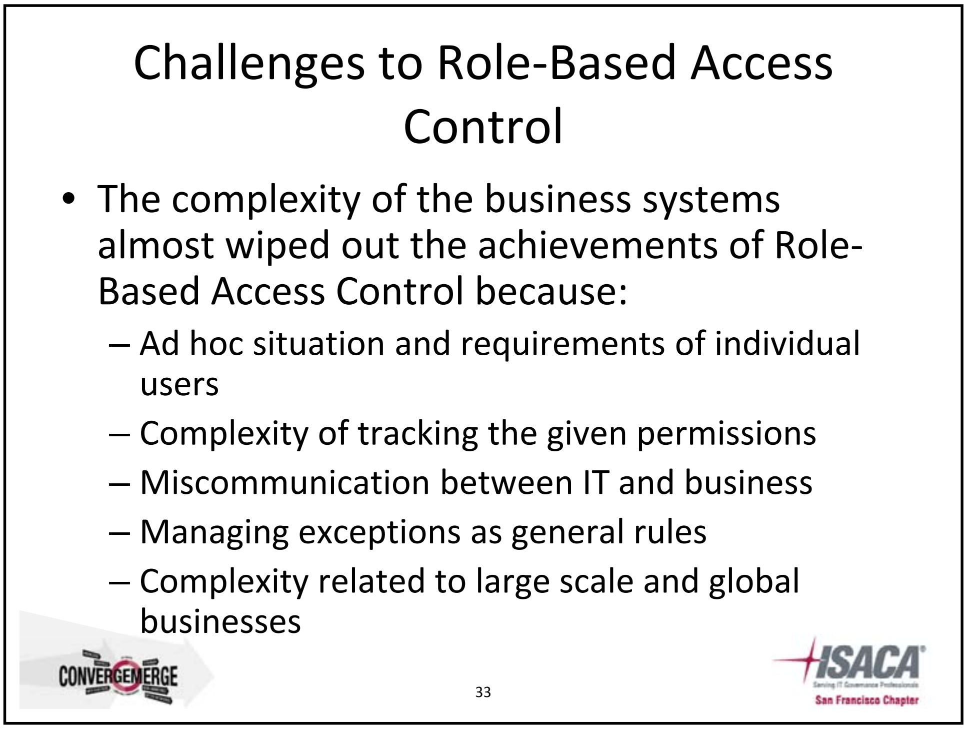
Security

Access Control, Roles, Segregation of Duties



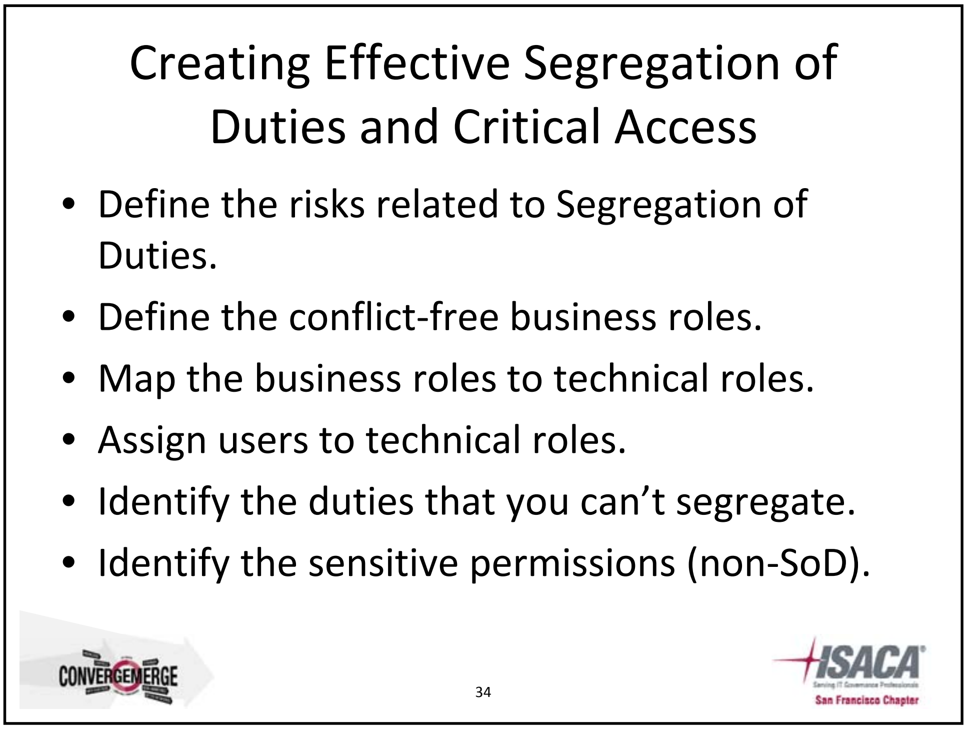
About Access Controls and Roles

- Access control refers to what a person can do in a computer application based on the sign-on (authentication) process.
- Initially permissions were directly assigned to individual users.
- Introduction of Role-based access made it possible to organize and streamline the permissions based on the job functions and business responsibilities.
- Role-based access allowed to manage and track the Segregation of Duties in the business applications.



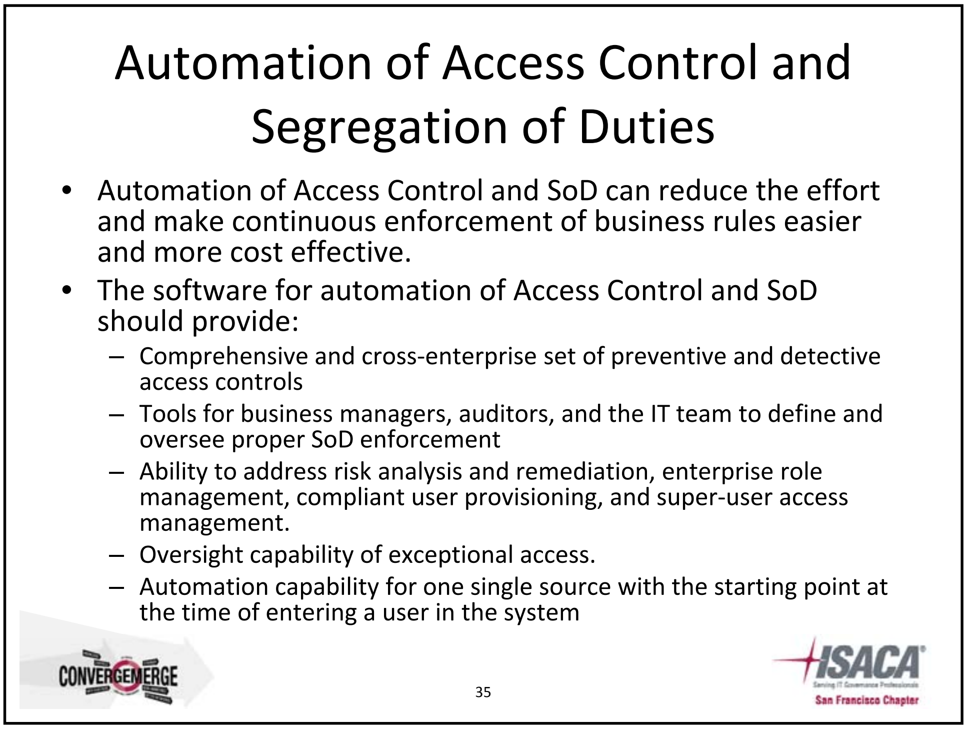
Challenges to Role-Based Access Control

- The complexity of the business systems almost wiped out the achievements of Role-Based Access Control because:
  - Ad hoc situation and requirements of individual users
  - Complexity of tracking the given permissions
  - Miscommunication between IT and business
  - Managing exceptions as general rules
  - Complexity related to large scale and global businesses



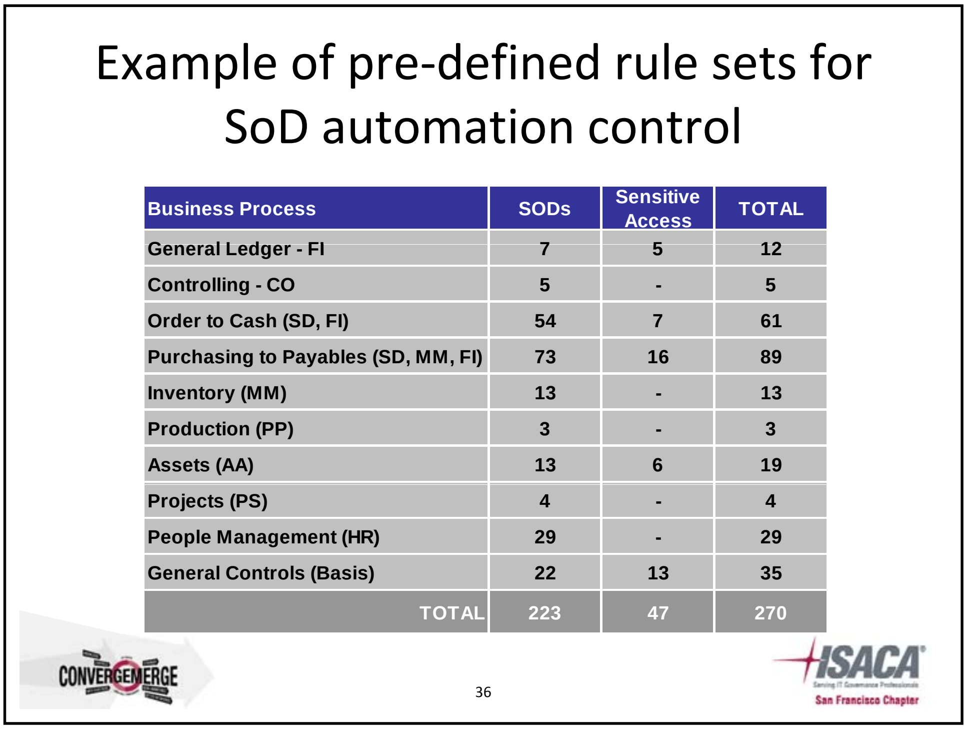
Creating Effective Segregation of Duties and Critical Access

- Define the risks related to Segregation of Duties.
- Define the conflict-free business roles.
- Map the business roles to technical roles.
- Assign users to technical roles.
- Identify the duties that you can’t segregate.
- Identify the sensitive permissions (non-SoD).



Automation of Access Control and Segregation of Duties

- Automation of Access Control and SoD can reduce the effort and make continuous enforcement of business rules easier and more cost effective.
- The software for automation of Access Control and SoD should provide:
  - Comprehensive and cross-enterprise set of preventive and detective access controls
  - Tools for business managers, auditors, and the IT team to define and oversee proper SoD enforcement
  - Ability to address risk analysis and remediation, enterprise role management, compliant user provisioning, and super-user access management.
  - Oversight capability of exceptional access.
  - Automation capability for one single source with the starting point at the time of entering a user in the system

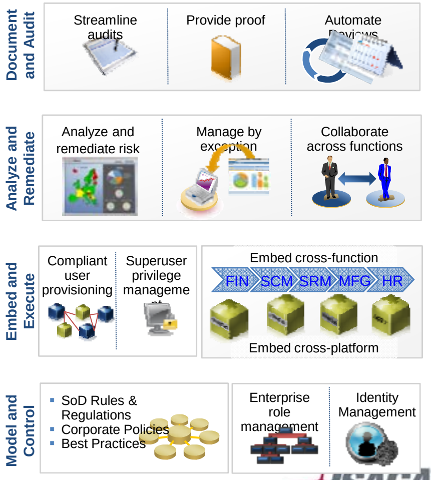


Example of pre-defined rule sets for SoD automation control

Business Process	SODs	Sensitive Access	TOTAL
General Ledger - FI	7	5	12
Controlling - CO	5	-	5
Order to Cash (SD, FI)	54	7	61
Purchasing to Payables (SD, MM, FI)	73	16	89
Inventory (MM)	13	-	13
Production (PP)	3	-	3
Assets (AA)	13	6	19
Projects (PS)	4	-	4
People Management (HR)	29	-	29
General Controls (Basis)	22	13	35
TOTAL	223	47	270

SoD and Access Control Automation Examples

- **Deposing cash & reconciling bank statements**
- **Approving time cards & distributing paychecks**
- **Preparing an order & distributing paychecks**
- **Preparing an order & changing a billing document**
- **Changing an order & creating a delivery**
- **Creating a journal entry & opening a closed accounting period**
- **Creating general ledger accounts & posting journal entries**
- **Maintaining accounts receivable master data & posting receipts**
- **Maintaining bank account information & posting payments**
- **Maintaining assets & creating a goods receipts**
- **Completing goods transfer & adjusting physical inventory counts**



Document and Audit

Streamline audits

Provide proof

Automate Reviews

Analyze and Remediate

Analyze and remediate risk

Manage by exception

Collaborate across functions

Embed and Execute

Compliant user provisioning

Superuser privilege management

Embed cross-function

FIN SCM SRM MFG HR

Embed cross-platform

Model and Control

- SoD Rules & Regulations
- Corporate Policies
- Best Practices

Enterprise role management

Identity Management

IT GRC

- IT GRC includes technical tools and related policies used to support compliance and risk management efforts:
  – Controls and policy mapping
  – Policy distribution and attestation
  – IT control self-assessment and measurement
  – GRC asset repository
  – Automated general computer control collection
  – Remediation and exception management
  – Basing compliance reporting
  – Advanced IT risk evaluation and compliance dashboarding