The San Francisco Chapter of ISACA proudly presents...
SF ISACA 2007 Fall Conference
IT Audit
Information Security
IT Governance
Risk Management
Compliance

Compliance in Multiple Regulatory Settings

a Holistic Approach

Vanessa Balogh

SPV AMERICA

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Key Problems

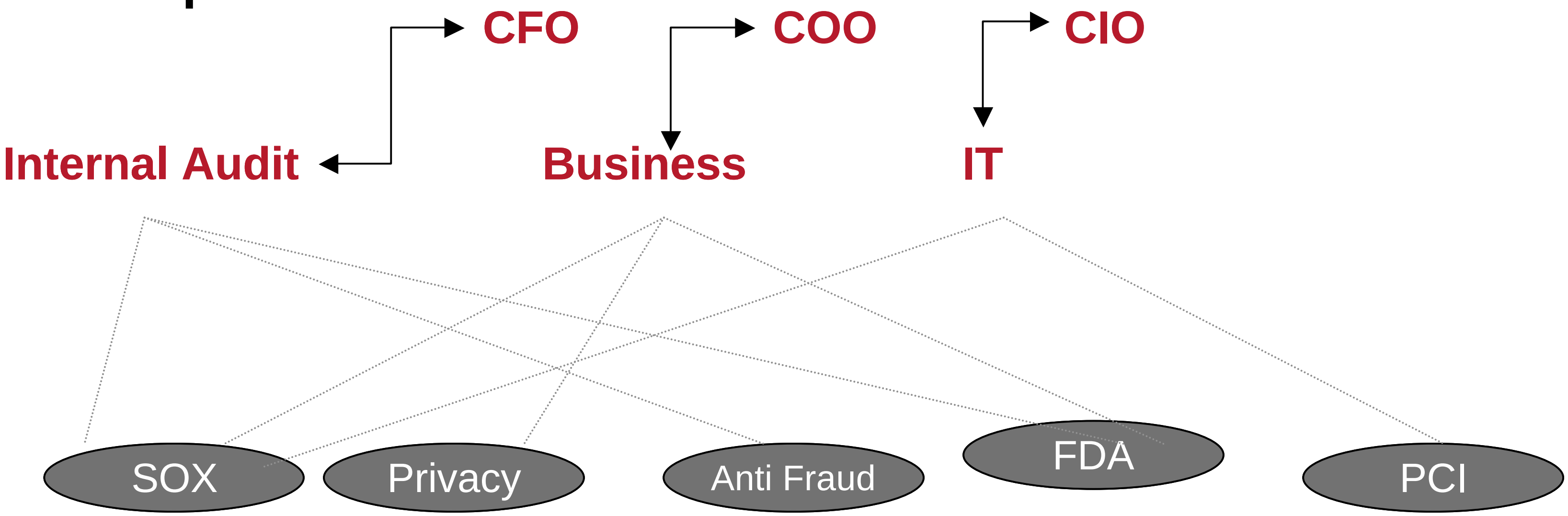
- Compliance with multiple regulations
  - FDA, SOX, HIPAA,GLBA,BASEL II, PCI, more
- Lack of transparency, ownership and accountability for risk management
- Multiple compliance efforts in multiple business areas
  - Policies, standards, procedures and documentation
- Reactive approach to technical and regulatory consequences of enterprise change

Complex Regulatory Settings

Industry	Regulations
Pharmaceutical	FDA, SOX*, HIPAA, SB1386
E-Commerce	PCI, SB1386, SOX
Public Utility	SOX, HIPAA, SB1386

Inefficiencies and Duplicate Effort

- No integrated risk assessment of business processes
- Every “function for itself” to get into compliance



SOX the ‘aftermath”

- Rules & Regulations forced to “quick and dirty” compliance solutions
- Inconsistent standards, processes and documentation
- Compliance effort still on shaky grounds

What companies face today?

- Deficiencies go unaddressed

- Strategic consequences arise if companies are unable to effectively, timely and efficiently adapt

Even the Regulator’s think it’s…..

- “…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 current Chairman of PCAOB, April 10, 2006

Goals of Process Oriented Compliance

- Risks and compliance are managed enterprise wide
- Holistic or integrated approach to compliance
- Enterprise Process Change Management (EPCM) is established

Path to Process Oriented Compliance

Establish the **GRC**

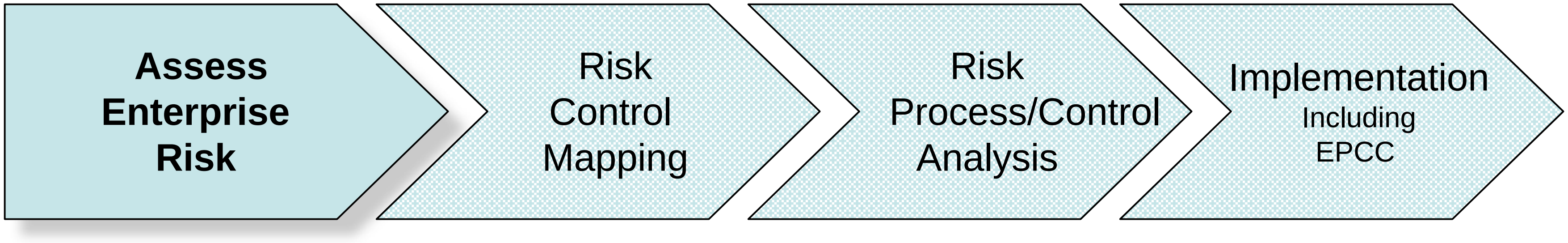
An enterprise wide Governance, Risk and Compliance function

Path to Process Oriented Compliance

GRC's MISSION:

- Ensure continuous alignment of risk management and compliance efforts
  - Corporate strategy, policies, goals and objectives
  - Control effort, tools and costs are aligned with magnitude of risk consequences
  - Controls do not overburden business operations
  - EPCM: Predefined plans for responding to enterprise level changes are implemented

Path to Process Oriented Compliance



Assess Enterprise Risk

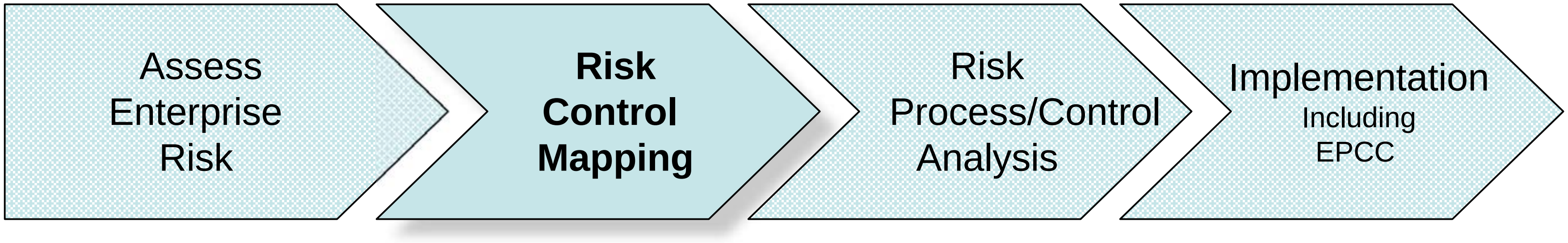
Risk Control Mapping

Risk Process/Control Analysis

Implementation
Including
EPCC

- Across value chain, globally
  - Identify and analyze risk
  - Categorize by process and regulations
  - Quantify
  - Prioritize
  - Validate with management and stakeholders

Path to Process Oriented Compliance



Assess Enterprise Risk

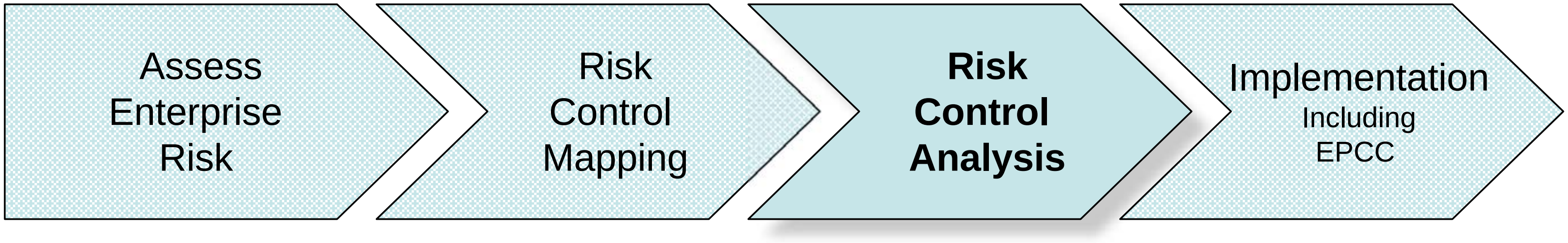
Risk Control Mapping

Risk Process/Control Analysis

Implementation
Including
EPCC

- Inventory existing controls
  - Interpret applicability for regulations
  - Flag redundant processes and controls
  - Identify gaps

Path to Process Oriented Compliance



Assess Enterprise Risk

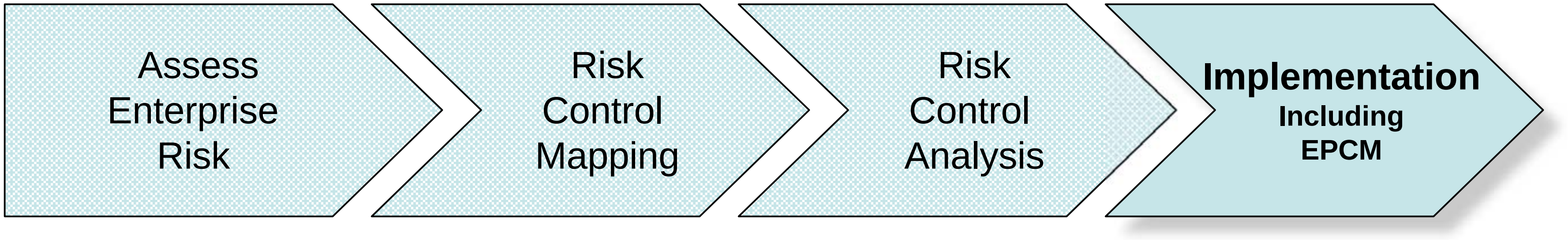
Risk Control Mapping

Risk Control Analysis

Implementation
Including
EPCC

- Assess control effectiveness
  - Review policies SOPs, historical testing, new testing
  - Rate effectiveness
  - Efficiencies, improvements and consolidation
  - Ensure cost of control does not exceed most probable consequences of risk occurrence
  - Document deficiencies and remediation plans

Path to Process Oriented Compliance



- Design, test and implement new Process Oriented Control environment
  - Update roles and responsibilities
  - Revise and update strategies, policies, standards, SOPs, control matrix, sampling and test plans
  - Close gaps and resolve deficiencies
  - Communication and training
  - Monitor and report

GRC Integration Objectives

- Enhance compliance effectiveness of the compliance program
- Reliable forecast and budget for GRC Expenditure
- Develop a baseline of integration opportunities and leverage the common activities (include risk-related corporate governance activities)
- Identify industry-specific standards and regulatory requirements

GRC Integration Objectives (*continued)*

- Analyze all business processes for risk, operational effectiveness and efficiency
  - Org Structure
  - Roles and responsibilities
  - Policies, standards, processes, procedures
  - Information (docs, records and data)
  - Systems/technology
- Recommend areas for in-depth analysis and study for potential
- Project portfolio of process improvements

GRC Integration Objectives (*continued*)

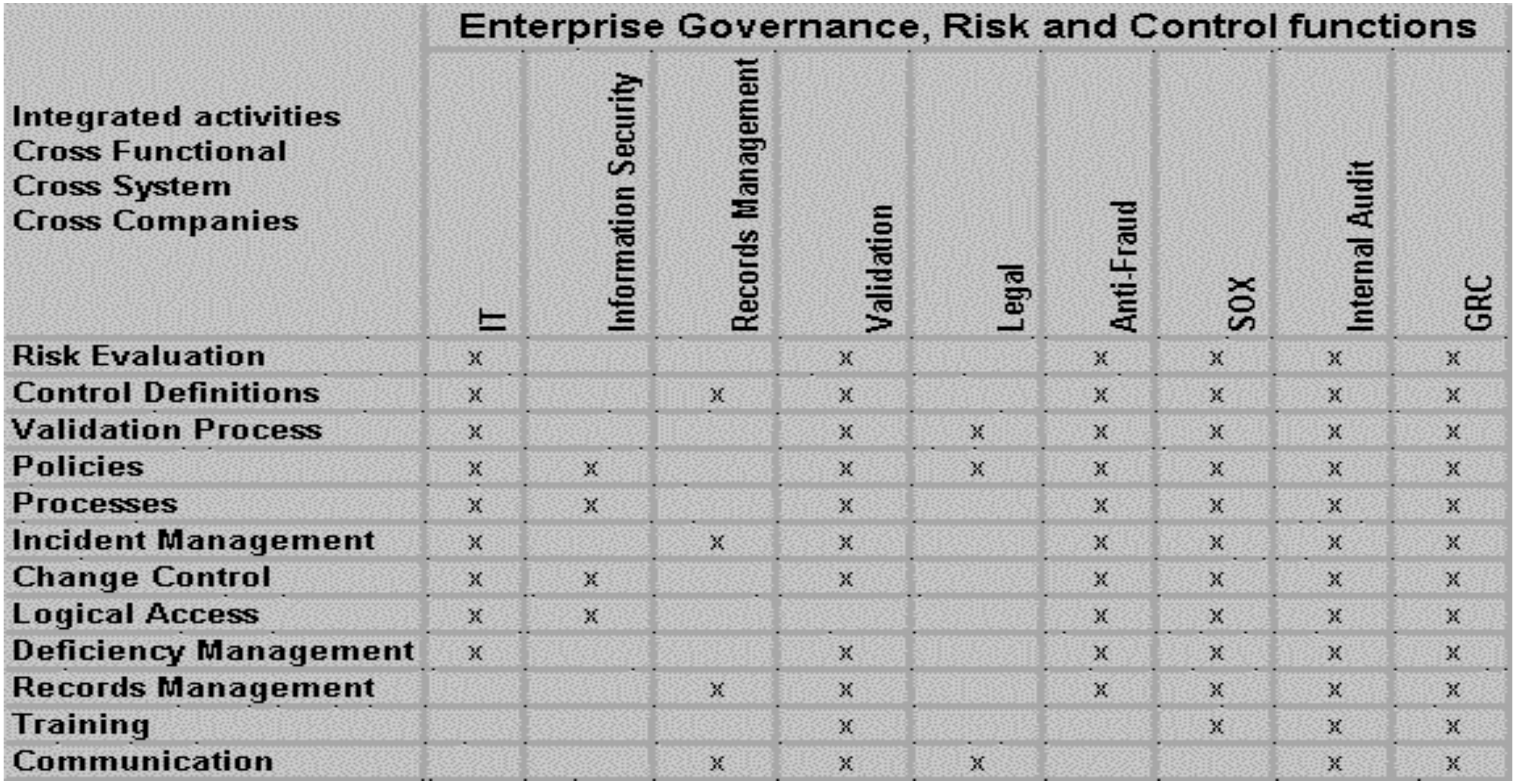
- Changes to the program are consistent with industry-accepted, risk-related corporate governance principles (e.g., CobIT, COSO), regulatory requirements, and management expectations
- Increase efficiency of compliance program
- Define measurable benefits of integration, monitor and report
- Continuous improvement

Use industry-accepted standards

- Based on the functions and activities in scope, identify relevant standards and regulatory requirements applicable across risk-related corporate governance functions
- Tailor industry-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 Matrix

- Integrate compliance functions



Integrated activities Cross Functional Cross System Cross Companies	Enterprise Governance, Risk and Control functions								
	IT	Information Security	Records Management	Validation	Legal	Anti-Fraud	SOX	Internal Audit	GRC
Risk Evaluation	x			x		x	x	x	x
Control Definitions	x		x	x		x	x	x	x
Validation Process	x			x	x	x	x	x	x
Policies	x	x		x	x	x	x	x	x
Processes	x	x		x		x	x	x	x
Incident Management	x		x	x		x	x	x	x
Change Control	x	x		x		x	x	x	x
Logical Access	x	x				x	x	x	x
Deficiency Management	x			x		x	x	x	x
Records Management			x	x		x	x	x	x
Training				x			x	x	x
Communication			x	x	x			x	x

Example GRC Process

Key Control

Logical Access

Roles & Responsibilities.

Roles	Responsibilities
Business Process Owners BPO's	• Identify risks and/or approve risks for monitoring • Approve remediation involving user access • Design controls for mitigating conflicts • Communicate access assignments or role changes • Perform proactive continuous compliance
Senior Officers	• Approve / Reject risks between business areas • Approve mitigating controls for selected risks
Security Teams and Technical Liaisons **GRC new "Governance and Risk" Team**	• Design and maintain roles according to Business decisions • Customize Virsa roles to enforce roles and responsibilities • Act as liaison between Profile Management and BPO's • Review and Approve Rule changes • Maintain controls over rules to ensure integrity

Roles & Responsibilities.

Roles	Responsibilities
Auditors & Regulators Business Units and IA	• Perform risk assessment on a regular basis • Provide specific requirements for audit purposes • Perform periodic testing of rules and mitigating controls • Act as liaison between external auditors
SOD Rule Keeper / Critical transaction DB **Enterprise Security Administration**	• Ownership of Access Management tools and security process • Design and maintain rules to identify risk conditions • Analysis and remediation of SOD conflicts at role level • Keep critical transaction, custom transactions and tables DB current • Responsible for Access Management tool configuration and administration

Global Access Management

- Policies and Processes across systems and Applications
  - Single sign on
  - Access request and deletion process
  - SODs
  - Sensitive access
  - Emergency access
- Access to Production and Non-Production system

Integrated and Global tools

- Integrated solutions for Governance, Risk and Compliance e.g. SAP's GRC suite
  - Integrate control design and documentation
  - Support manual and automated controls security, application and detective
  - Support various legal requirements SOX, FDA
- Global- cross system – cross application – cross country
  - Multinational Corporations

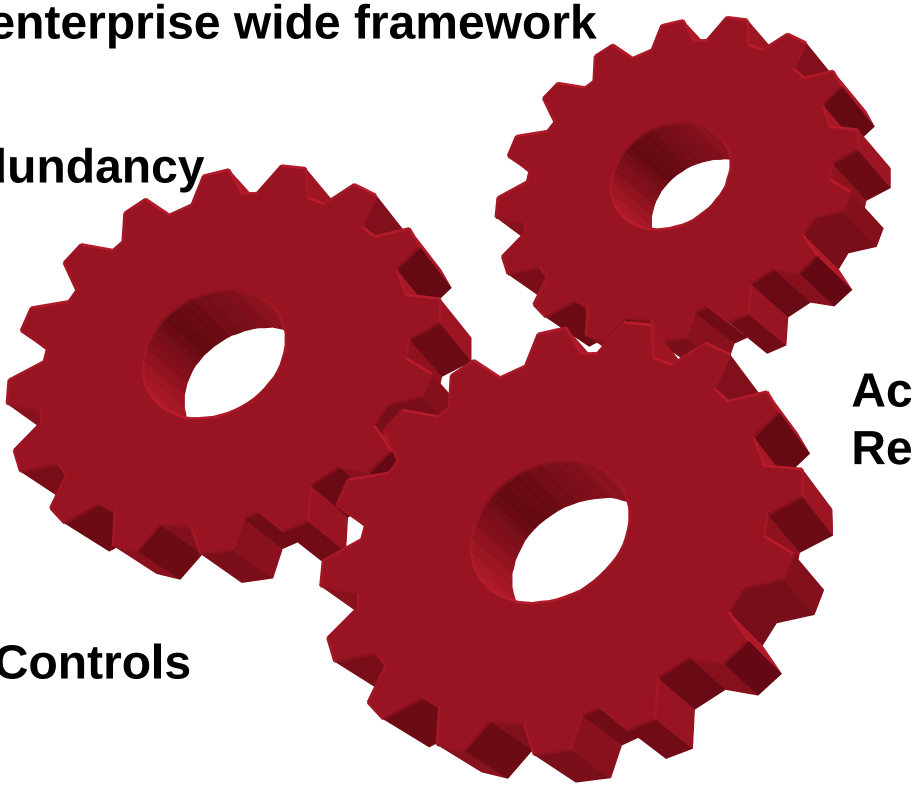
Integrating GRC Activities

- Through thoughtful analysis and action, institutions can integrate GRC activities and leverage common people, processes, technology, and information (i.e., operating “levers”) either enterprise-wide, or:
- Within a control function
- Across control functions
- Within a business unit
- Across business units
- For a single regulatory requirement
- Across multiple regulatory requirements

Integration

Holistic enterprise wide framework

Decrease Redundancy



Active vs.
Reactive Compliance

Centralized Controls

Defined Roles and Responsibilities

The Rules

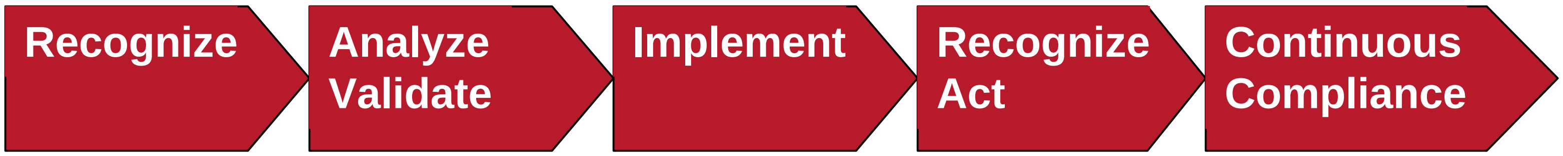
How can other’s success stories become your’s

- Successful Audit is based on solid Governance, Risk & Controls
- Solid Governance, Risk & Controls are based on:
  - organized structures
  - efficiency and
  - effectiveness

The Rules

Take the holistic approach and integrate

- Audit is performed the same way across systems and applications with the goal to detect weaknesses in the area of Governance Risk & Risk & Control
- Use one process:



Recognize

Analyze Validate

Implement

Recognize Act

Continuous Compliance

cross function, cross system, global

Summary

Need to comply with multiple regulations ?

- Look at all applications and systems commitments
- Reduce compliance costs, improve efficiency and effectiveness
  - One transactional system: SAP R/3
  - One reporting system: SAP BW
  - One customer relationship management system: SAP CRM

Summary

Integrated Compliance means

- Focus on common goals and mandates
- Aggregation of reporting cross system cross functional
- Enterprise wide accountability and responsibility
- Standardization
- Centralized controls

Summary

Effectiveness & Efficiency can be realized through Integrated Governance, Risk, and Compliance

- Clarified Roles and responsibilities
- Standardized Processes and Policies
- Well Defined Risk & Control Matrices
- Proactive vs. Reactive

Summary

Efficiency

- Maximized effort through
  - Merged Assessments - avoid duplicate Assessments
  - Transparent Risk Management – across functions
  - Technology and Platform consistency
    strategic applications / one platform cross country
- Centralize tasks reduce burden on business unit resources
  - Cross Functional effort – Enterprise wide budget
- Think long term
  - Scalable infrastructure with applications that support global business activities

Conclusion

Manage risk and compliance enterprise wide and integrated

Discussion

- ERP case studies
- Strategies
- Goals
- Success stories

Project Success/Failure Factors

- Analyze global requirements
- Centralize Controls
- Gather all regulations that need to be complied to
- Classify enterprise wide risks
- Be organized: Enterprise wide Data Owners – Approvers – Custom Objects

5Key Points to Take Home

- Risk and compliance efforts are migrating from compliance-based island solutions to strategic risk frameworks
- Generating value in managing risks requires understanding their sources, impacts, and, interrelationships while linking the risks to specific tasks
- Risk owners must be established to achieve effective risk management
- A comprehensive methodology that includes communication of strategy and goals must be defined to implement enterprise risk management
- The Implementation of an enterprise wide risk management framework based on a technology platform and a strategic ERP System (e.g. SAP) can help optimize business performance and is justifiable based on a rigorous cost benefit analysis

Q&A

How to contact me:

Vanessa Balogh
CEO / SPV America
vanessa.balogh@myspv.com

Vanessa Balogh
CEO/ SPV America
505 Montgomery St.
San Francisco, CA 1
www.spvus.com
Tel: +1.415.272.7552
vanessa.balogh@myspv.com

Resources

- Auditproof™ SAP Implementations – SPV America whitepaper
- Successful SAP implementations through Integrated Governance, Risk and Compliance Solutions / SPV America
- http://images.forbes.com/media/2006/11/02/right4.html
- **COSO framework www.coso.org**
- **www.sap.com/grc**