

The Convergence of Security and Compliance

– An Integrated Approach to Risk Management

Larry Jewik, Executive Director, IT Compliance – Controls Integration
Ramy Houssaini, Director, Information Security - Strategy



Discussion Roadmap

Current Compliance
Landscape

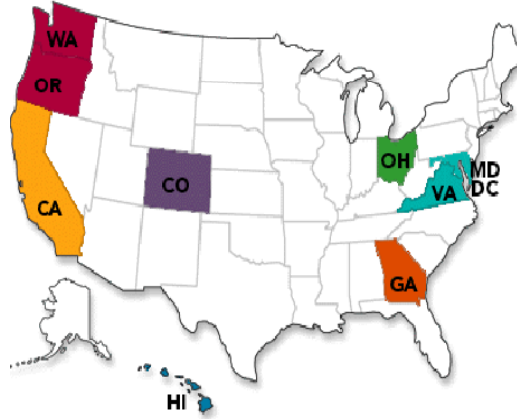
Integrated View of Risks
and review of Risk
Framework

Integration Case Study



About Kaiser Permanente

- One of nation's largest not for profit health plans
- 8.6 million members
- 179,000 employees and physicians
- 35 Hospitals, 454 Medical Office buildings
- 8 Regions, serving 9 states and the District of Columbia
- \$42.1 billion annual revenues
- 3 organizations
 - Kaiser Foundation Health Plan, Inc
 - Kaiser Foundation Hospitals and subsidiaries
 - The Permanente Medical Groups



(As of December 31, 2009)



3

Convergence of Compliance and Security

Compliance Overload



Brand Impact



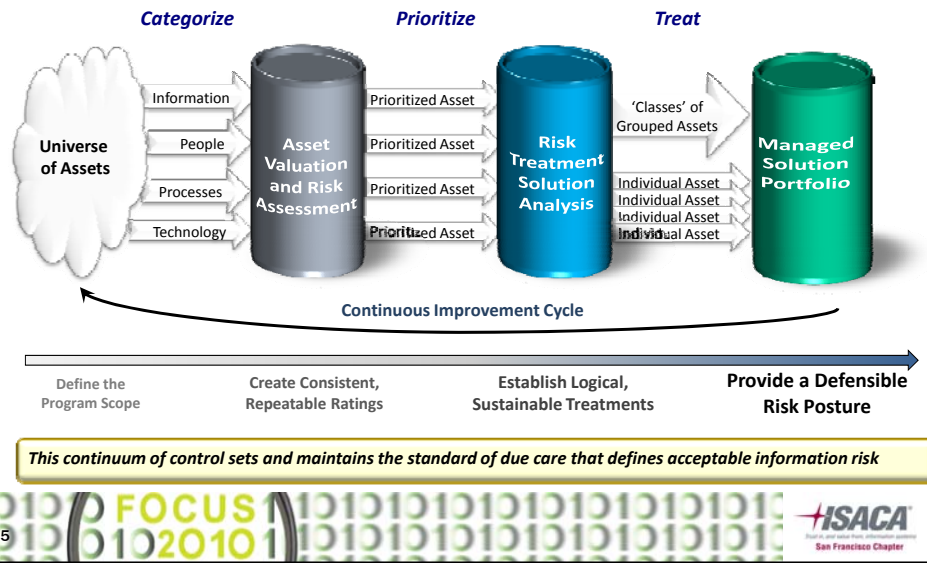
More Aggressive Enforcement



4

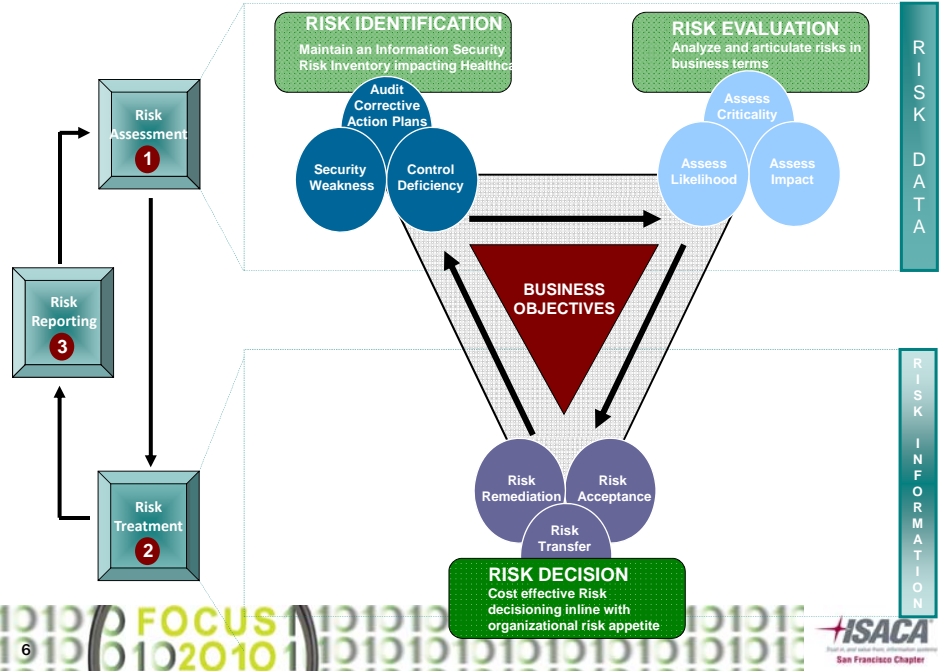
Risk Management Approach

Security Risk Management aims to establish a comprehensive lifecycle that ensures risk treatment solutions address all high value assets



5

Information Risk Management Framework



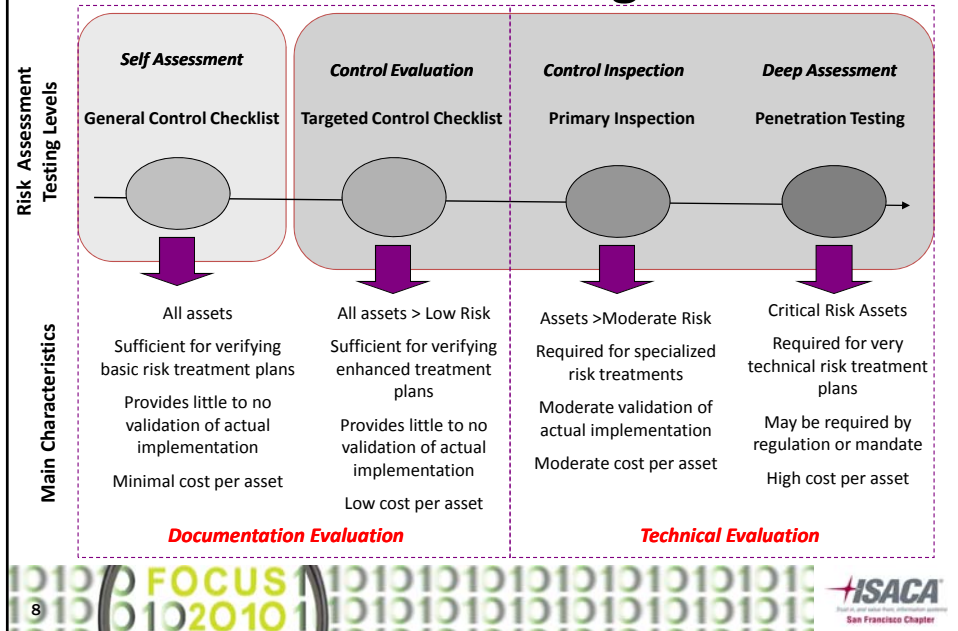
6

Risk Management Process

- Risk Identification
 - Security weakness reported in the environment tracked for detailed risk assessment activities to help define the risk profile
- Risk Assessment
 - A risk-based approach that recommends different protection methods depending on the asset’s value, the susceptibility to various threats, and the organization’s cost/benefit analysis of protection methods
- Risk Decision
 - Enforce Business Owner accountability to implement risk mitigation plans necessary for reducing inherent risks in their business areas to an acceptable and reasonable level



Risk Assessment Testing Continuum



Risk Decision & Agilience

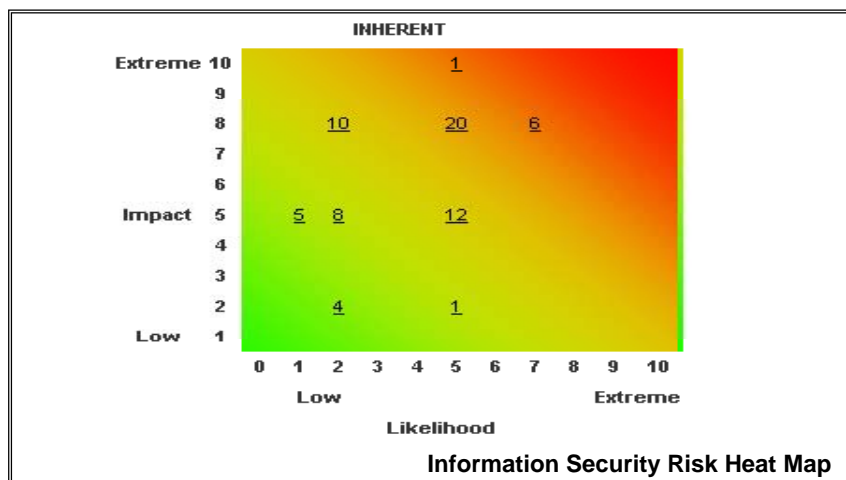
Governance Risk Compliance (GRC) Tool

- The Need for GRC
 - Fragmented Risk Information throughout the Enterprise resulting in limited management line of sight of Information Risk, duplication of assessment efforts and suboptimal resource utilization
- GRC Vision
 - Establish a risk decision platform based on an integrated and comprehensive view of risk information throughout the Enterprise
- Success Criteria
 - Accelerate the convergence of GRC processes
 - Substantially reduce the cost of Compliance Demonstrability by enforcing Continuous Compliance
 - Support a data driven approach to information security
 - Enable a risk based approach to decision making



Risk Identification

- Information Security Risk Inventory actively maintained in a GRC Platform



Risk Assessment

- KP Risk Matrix incorporated in Agilience Risk Assessment Module
- Active Directory and Messaging Risk Assessments being executed in Agilience

		Impact				Likelihood
		Low	Medium	High	Extreme	
Likelihood	Moderate	High	Critical	Critical	Extreme	
	Low	Moderate	High	Critical	High	
	Low	Moderate	High	High	Medium	
	Low	Low	Moderate	Moderate	Low	
		Low	Low	Low	Moderate	Negligible

KP Risk Matrix

Risk : R:2010:026
Please follow the instructions below to reduce risk.

Total Inherent Risk **56** Total Current Risk **56**

Risk Assessment Actions

Inherent Risk Determination (Based on All Opinions)
Risk scores are calculated automatically and may need to be reviewed and adjusted as per grounded realities.

Inherent Risk: **56** Likelihood: High Impact: High

Risk Assessment Rating

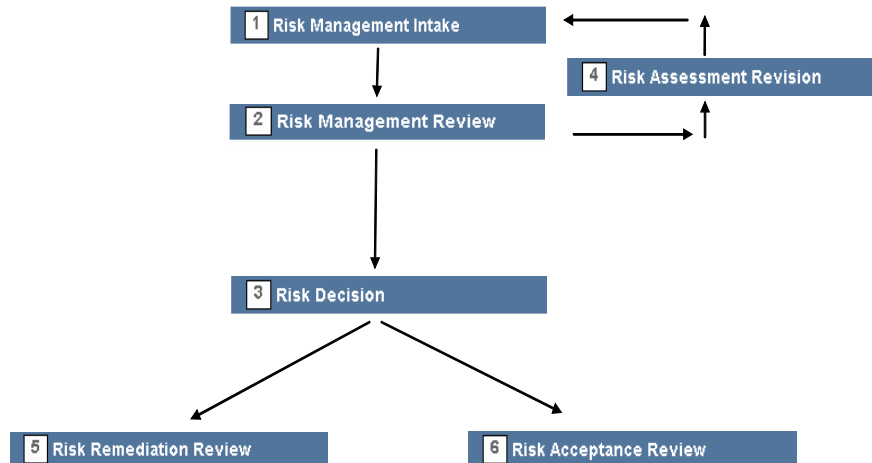


Risk Level Summary



Risk Decision

Workflow Template Name Risk Management Workflow



Integrating Security and Compliance

Scenario: An upgrade of a critical business process related system is taking place over an 18 months period. Compliance and Information Security teams have partnered to assess the system and ensure that it meets the desired set of controls.



13

Control Design: New Systems

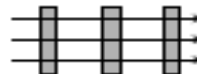
1. Identifying Risks



Challenges:

- The security risk vs. compliance risk debate

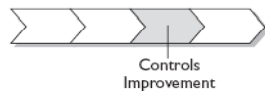
2. Risk Community Alignment



Challenges:

- Common and consistent evaluation criteria

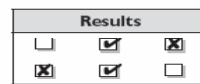
3. Design and Assessment



Challenges:

- Managing overlap and redundancy

4. Integrated Reporting



Challenges:

- Alignment of messaging



14

Risk Community Alignment

<p>National Compliance</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>	<p>Regional Compliance</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>	<p>Internal Audit</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>
<p>Technology Compliance</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>	<p>Project Stakeholders</p> <p>BUS. CONTACT: xxxxx IT CONTACT: xxxxx SCOPE: xxxxx</p>	<p>Legal</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>
<p>Information Security</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>	<p>SOX PMO</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>	<p>Other</p> <p>CONTACT: xxxxx SCOPE: xxxxx</p>



Design and Assessment

Challenges in Driving Organizational Self-Sufficiency

What the Requirement States



What the Requirement Means

SOX 12.14.03

Changes requests are appropriately authorized.

HIPAA §164.308 (a)(4)(ii)(B)

Access Authorization

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

- Authorization documented for the change?
- Approval to proceed documented?
- Segregation between requestor and approver?
- Approval by all stakeholders: Business + IT?
- Automated process for managing changes?
- Change history and artifact archival?

- Existing access to systems job function driven?
- Access to devices job function based?
- Managers approve access?
- Managers review access?
- Job changes drive access changes?
- Approvers are authorized?



Design and Assessment

Promoting Self-Assessment

Regulatory Requirements

SOX Requirements
(26 KP Controls, 90 sub-criteria)



HIPAA Requirements
(~200 Security/Privacy Requirements)



PCI-DSS Requirements
(~303 Requirements)



SAT Filtering Criteria

- Applicable Regulation
 - SOX
 - HIPAA
 - PCI
- Risk Category
 - Change Management
 - Access Control
 - Monitoring/Logging
- Layer
 - Application
 - Database
 - Network
 - Host
- User Role
 - Application
 - Infrastructure
 - Program
- TEAMS Phase
 - Definition
 - Development
 - Introduction
 - Deployment

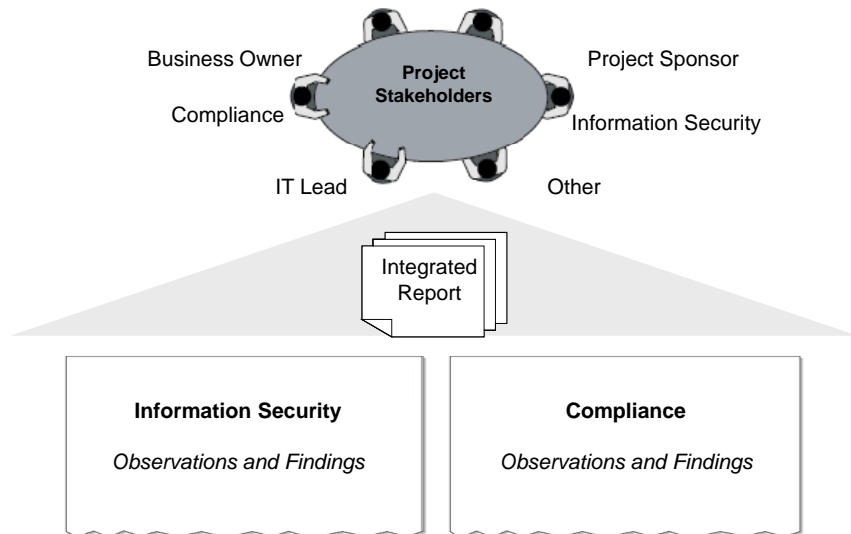
SAT Guidance

REGULATORY REQUIREMENT:
Activity of highly sensitive privileged user is reviewed for appropriateness
:
:
:

CONTROL GUIDANCE:
 Reviews capture all activity that could pose a risk to the environment.
 Activity reports are designed in a manner which provides a realistic ability to differentiate high risk activities from lower risk activities
 Activity reviews are performed with sufficient and consistent frequency
 Activity reviews are documented and evidenced.
:
:
:



Integrated Reporting



Outcome: An Enhanced View of the Risk

Successes:

- Pre-Implementation Engagement
- “Normalization” of Findings, Observations
- Strength in Numbers

Work in Progress:

- Overhead in Coordinating Efforts
- Differing Missions, Perspectives on Risk



19

Closing Thoughts

- Adopt a programmatic approach to integration: A common set of controls is always desirable but it is possible to develop an integrated view without it.
- Focus on Risks: ultimately, risk drives decision making. Stating control deficiencies in terms of risk is important.
- Do not neglect Communication: the assessment final results should never be a surprise to anyone.



20

The Convergence of Security and Compliance

An Integrated Approach to Risk Management

QUESTIONS?

Contact Information

Larry Jewik: larry.x.jewik@kp.org

Ramy Houssaini: ramy.x.houssaini@kp.org

