
Larry A. Jewik and Ramy Houssaini, Kaiser Permanente
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)

Convergence of Compliance and Security

Compliance Overload

Brand Impact

More Aggressive Enforcement

[Image with lock and checkmark]
Risk Management Approach

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

- **Categorize**
- **Prioritize**
- **Treat**

### Universe of Assets
- Information
- People
- Processes
- Technology

**Asset Valuation and Risk Assessment**
- Prioritized Asset
- Prioritized Asset
- Prioritized Asset

**Risk Treatment Solution Analysis**
- Individual Asset
- Individual Asset
- Individual Asset

**Managed Solution Portfolio**

**Continuous Improvement Cycle**

**Define the Program Scope**
**Create Consistent, Repeatable Ratings**
**Establish Logical, Sustainable Treatments**
**Provide a Defensible Risk Posture**

This continuum of control sets and maintains the standard of due care that defines acceptable information risk

---

Information Risk Management Framework

- **Risk Assessment**
  - Risk Identification
  - Risk Evaluation
  - Risk Decision

- **Risk Reporting**
- **Risk Treatment**

**BUSINESS OBJECTIVES**

**RISK IDENTIFICATION**
- Maintain an Information Security Risk Inventory impacting Health IT
- Audit Corrective Action Plans
- Security Weakness
- Control Deficiency

**RISK EVALUATION**
- Analyze and articulate risks in business terms
- Assess Criticality
- Assess Likelihood
- Assess Impact

**RISK DECISION**
- Cost effective risk decisioning inline with organizational risk appetite
- Risk Remediation
- Risk Acceptance
- Risk Transfer
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

<table>
<thead>
<tr>
<th>Risk Assessment Testing Levels</th>
<th>Documentation Evaluation</th>
<th>Technical Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Assessment</td>
<td>General Control Checklist</td>
<td></td>
</tr>
<tr>
<td>All assets</td>
<td>Sufficient for verifying basic risk treatment plans</td>
<td>Provides little to no validation of actual implementation</td>
</tr>
<tr>
<td>Control Evaluation</td>
<td>Targeted Control Checklist</td>
<td></td>
</tr>
<tr>
<td>All assets &gt; Low Risk</td>
<td>Sufficient for verifying enhanced treatment plans</td>
<td>Provides little to no validation of actual implementation</td>
</tr>
<tr>
<td>Control Inspection</td>
<td>Primary Inspection</td>
<td></td>
</tr>
<tr>
<td>Assets &gt; Moderate Risk</td>
<td>Required for specialized risk treatments</td>
<td>Moderate validation of actual implementation</td>
</tr>
<tr>
<td>Deep Assessment</td>
<td>Penetration Testing</td>
<td></td>
</tr>
<tr>
<td>Critical Risk Assets</td>
<td>Required for very technical risk treatment plans</td>
<td>May be required by regulation or mandate</td>
</tr>
</tbody>
</table>
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 Agiliance Risk Assessment Module
- Active Directory and Messaging Risk Assessments being executed in Agiliance

<table>
<thead>
<tr>
<th>Impact</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Critical</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Risk Assessment Rating

Risk Level Summary

Risk Decision

Workflow Template Name: Risk Management Workflow

1. Risk Management Intake
2. Risk Management Review
3. Risk Decision
4. Risk Assessment Revision
5. Risk Remediation Review
6. Risk Acceptance Review
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.

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
Risk Community Alignment

National Compliance
CONTACT: xxxxx
SCOPE: xxxxx

Regional Compliance
CONTACT: xxxxx
SCOPE: xxxxx

Internal Audit
CONTACT: xxxxx
SCOPE: xxxxx

Technology Compliance
CONTACT: xxxxx
SCOPE: xxxxx

Project Stakeholders
BUS. CONTACT: xxxxx
IT CONTACT: xxxxx
SCOPE: xxxxx

Legal
CONTACT: xxxxx
SCOPE: xxxxx

Information Security
CONTACT: xxxxx
SCOPE: xxxxx

SOX PMO
CONTACT: xxxxx
SCOPE: xxxxx

Other
CONTACT: xxxxx
SCOPE: xxxxx

Design and Assessment

Challenges in Driving Organizational Self-Sufficiency

What the Requirement States

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.

What the Requirement Means

- 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

SAT Filtering Criteria

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

HIPAA Requirements
(~200 Security/Privacy Requirements)

PCI-DSS Requirements
(~303 Requirements)

Applicable
Regulation
µ SOX
µ HIPAA
µ PCI

User Role
µ Application
µ Infrastructure
µ Program

Risk Category
µ Change Management
µ Access Control
µ Monitoring/Logging

TEAMS Phase
µ Definition
µ Development
µ Introduction
µ Deployment

Layer
µ Application
µ Database
µ Network
µ Host

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

Project Stakeholders

Business Owner
Compliance
Project Sponsor
Information Security
IT Lead
Other

Integrated Report

Information Security
Observations and Findings

Compliance
Observations and Findings
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

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.
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