# Strategies for Integrating the HIPAA Security Rule


## Kaiser Permanente:

**Charles Kreling, Executive Director**
**Sherrie Osborne, Director**
**Paulina Fraser, Director**


Professional Strategies – S21

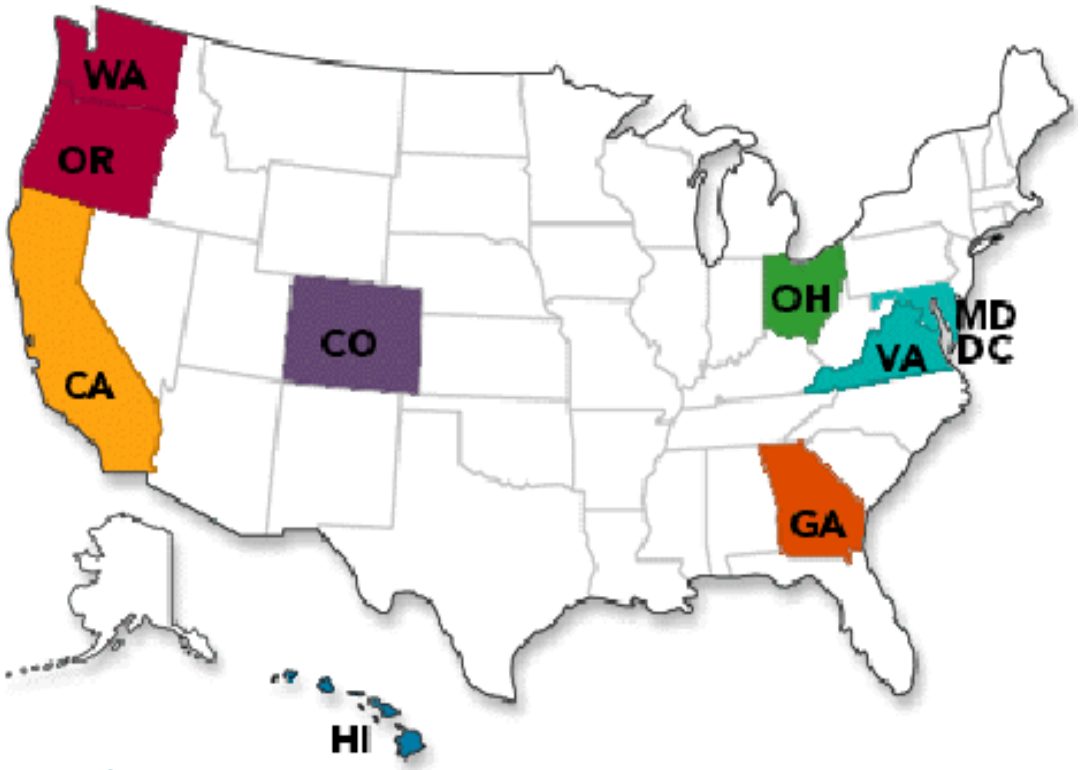
ISACA®
Trust in, and value from, information systems
San Francisco Chapter

# Agenda

1. About Kaiser Permanente
2. The Regulatory Compliance Challenge
3. Integrating Regulatory Compliance
4. Key Learnings

# About Kaiser Permanente

- Nation's largest nonprofit health plan
- Integrated health care delivery system
- 9.1 million members
- 17,000 physicians
- 175,000 employees
- Serving 9 states and the District of Columbia
- 37 hospitals
- 618 medical offices and other facilities
- $50.6 billion operating revenue (2012)






KAISER PERMANENTE®

# Integrated Regulatory & Information Security Services (IRISS)

***Mission****

- **Provide an integrated roadmap to simplify compliance with multiple security regulations in the Information Security area**

***Vision****

- **Integrated strategic solutions for SOX, HIPAA Security & PCI**
- **Integrated requirements, guidance, and how-to manuals**
- **Exceptional customer service to Kaiser Permanente information security clients**

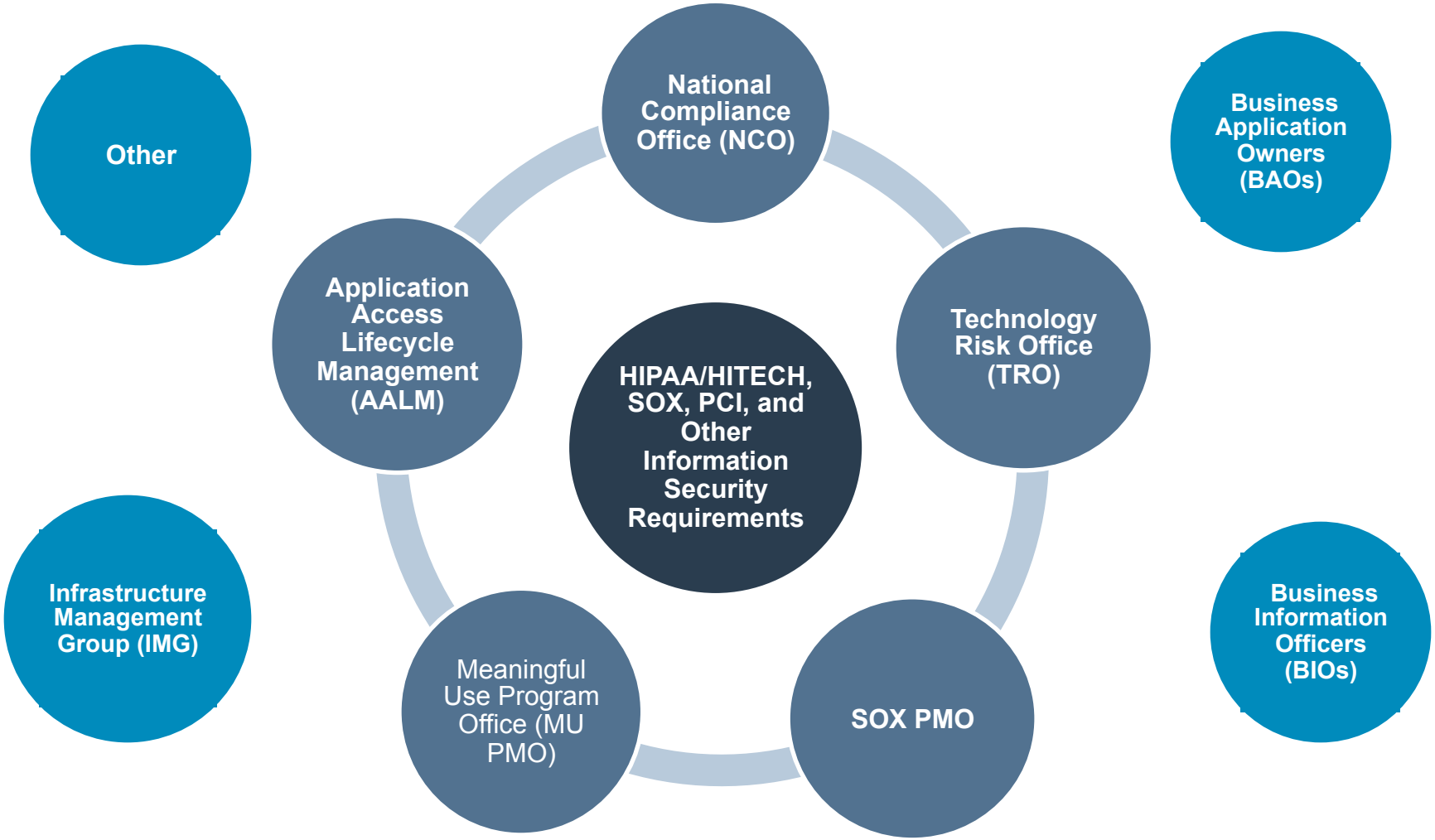
**Charles Kreling**
**Executive Director**
Integrated Regulatory & Information Security Services (IRISS)

**Sherrie Osborne**
**Director**
Integrated Regulatory & Information Security Services (IRISS)

**Paulina Fraser**
**Director**
Integrated Regulatory & Information Security Services (IRISS)

* IRISS was formed August 2013; mission & vision are draft.

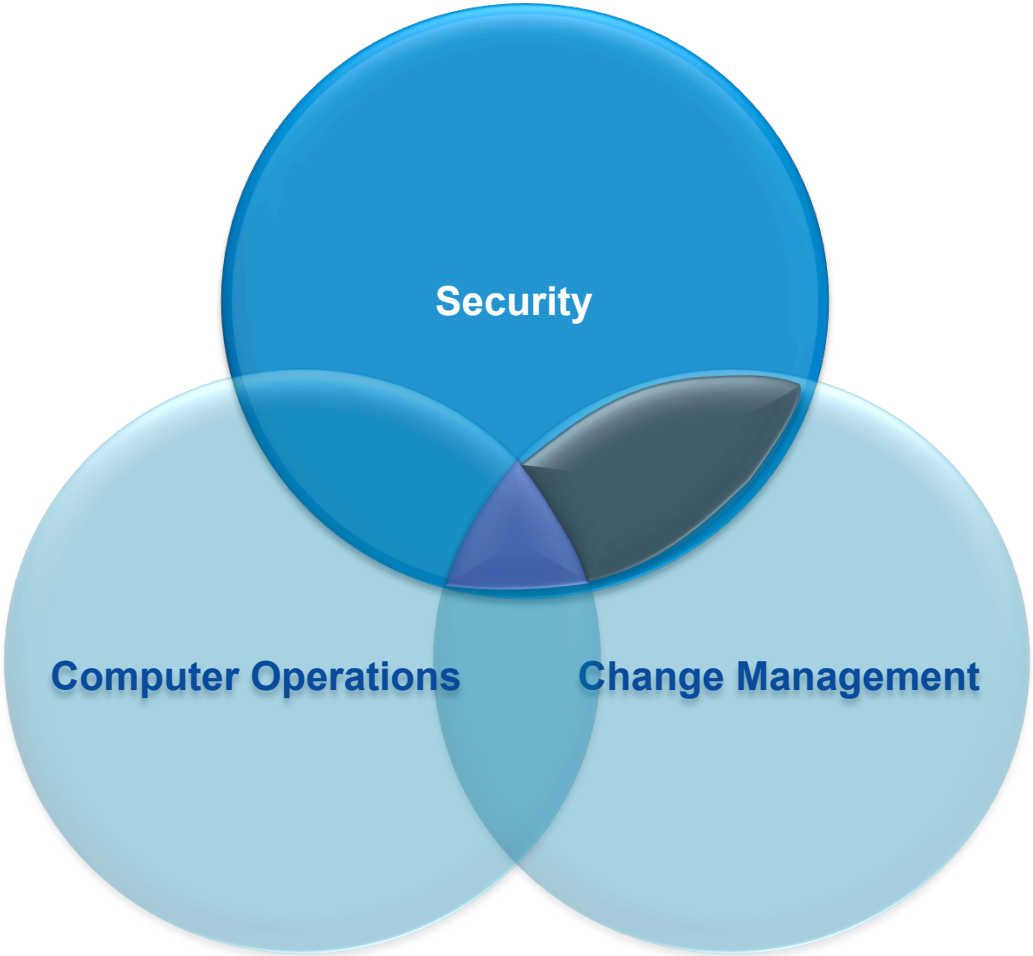
# The Regulatory Compliance Challenge
# SOX, HIPAA Security/HITECH, & PCI at Kaiser Permanente






KAISER PERMANENTE®

# Sarbanes-Oxley (SOX) at Kaiser Permanente






KAISER PERMANENTE®

# Sarbanes-Oxley (SOX) at Kaiser Permanente

**Security:**

Access Controls (Host & Database)
- 12.01.04 (Provision)
- 12.03.02, 12.30.01, 12.30.02 (De-provision)
- 12.02.02 (QAR)

Security Configurations (Host & Database)
- 12.04.03

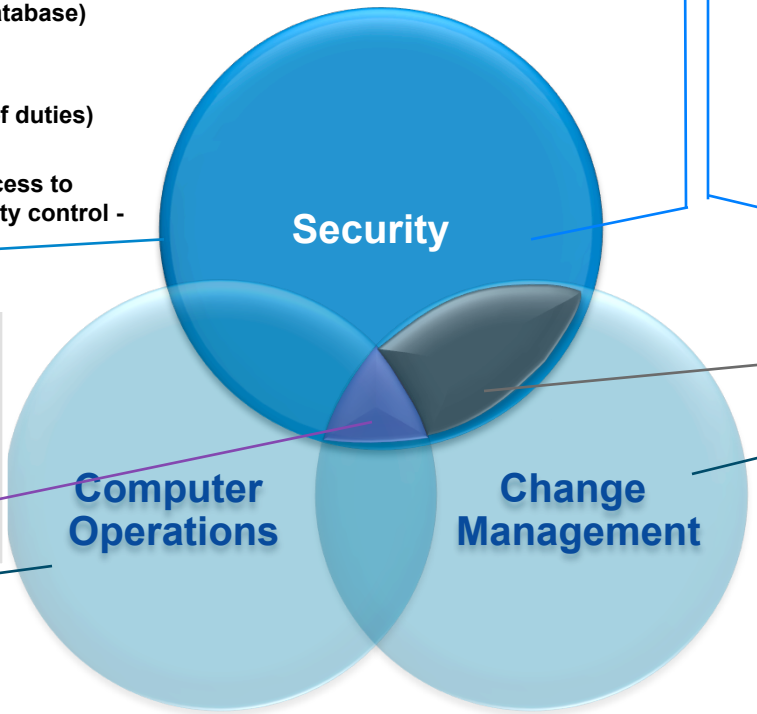
SOD (Segregation of Duties)
- 12.99.01 (Logical separation of duties)

Physical Security
- 12.08.02 (Review Physical Access to Production Hardware – security control - data center aspect)

(Application Access Lifecycle Management - Business Application Access Controls):
- 12.01.03 (Provision)
- 12.03.01 (De-provision)
- 12.02.01 (QAR)

**Intersection (Activity Monitoring):**

*Security & Change Management*
- 12.05.05 *(Application, Host & Database)*
- 12.05.03 *(Application)*




**Intersection (ALL):**

Population Management (Supporting function critical to success execution of controls)
- 12.06.01 (Network monitoring)
- 12.40.01 (Self Assessment monitoring)

**Change Management:**
- Change Management & Configuration Management
  - 12.14.03 (Changes authorized)
  - 12.16.01 (Version control)
  - 12.15.01 (Changes tested)
  - 12.16.02 (Changes approved prior to migration)
  - 12.18.02 (Review Logical Access to Production)

**Computer Operations:**
- Backup & Batch Jobs
  - 12.21.08 (Backup / Batch Approval)
  - 12.22.02 (Backup recoverable)
  - 12.21.09 (Backup / Batch Jobs Monitored)
- IT Incident Resolution
  - 12.23.02 (Problem & Incident)



KAISER PERMANENTE®

# HIPAA Security Rule/HITECH at Kaiser Permanente

**The HIPAA Security Rule aims to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). The HIPAA Security Rule comprises:**

1) Administrative Safeguards
2) Physical Safeguards
3) Technical Safeguards

} Some safeguards are **required** while others are **addressable**

## Meaningful Use Core Set Objective 14/15: Privacy and Security

**Objective**:

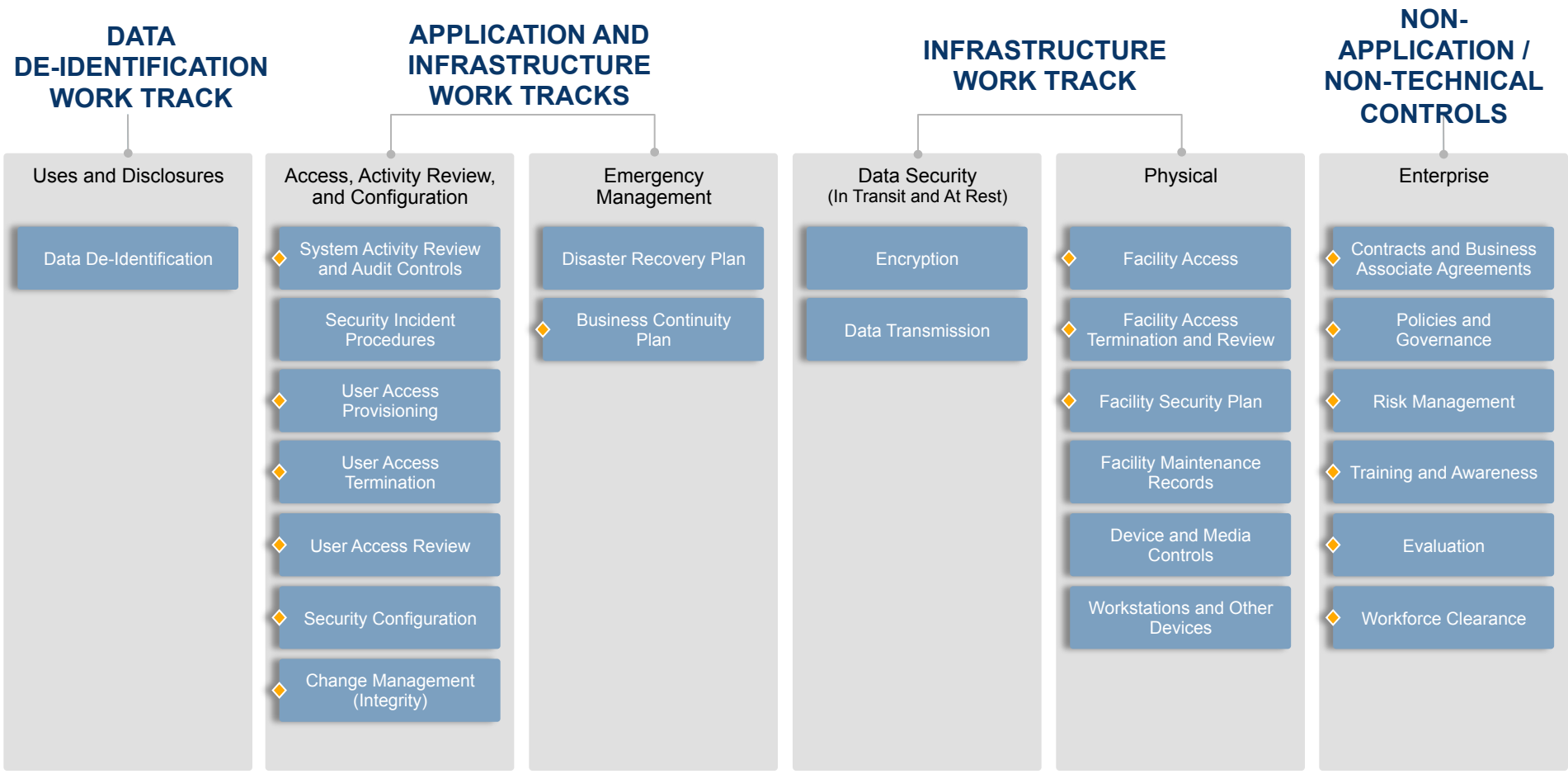
Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

**Measure:**

Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the Eligible Professionals (EP), Eligible Hospitals (EH), or Critical Access Hospitals (CAH) risk management process.

# HIPAA Security Rule/HITECH at Kaiser Permanente
# Risk and Control Matrix

The HIPAA Security Rule and Privacy Rule (data de-identification only) requirements (58 and 1 requirements, respectively) were organized into 24 control categories, aligned with SOX IT General Controls as applicable.




◆ Business is involvement is required in order to meet control objectives (e.g., application access controls, business continuity planning, etc.)



KAISER PERMANENTE®

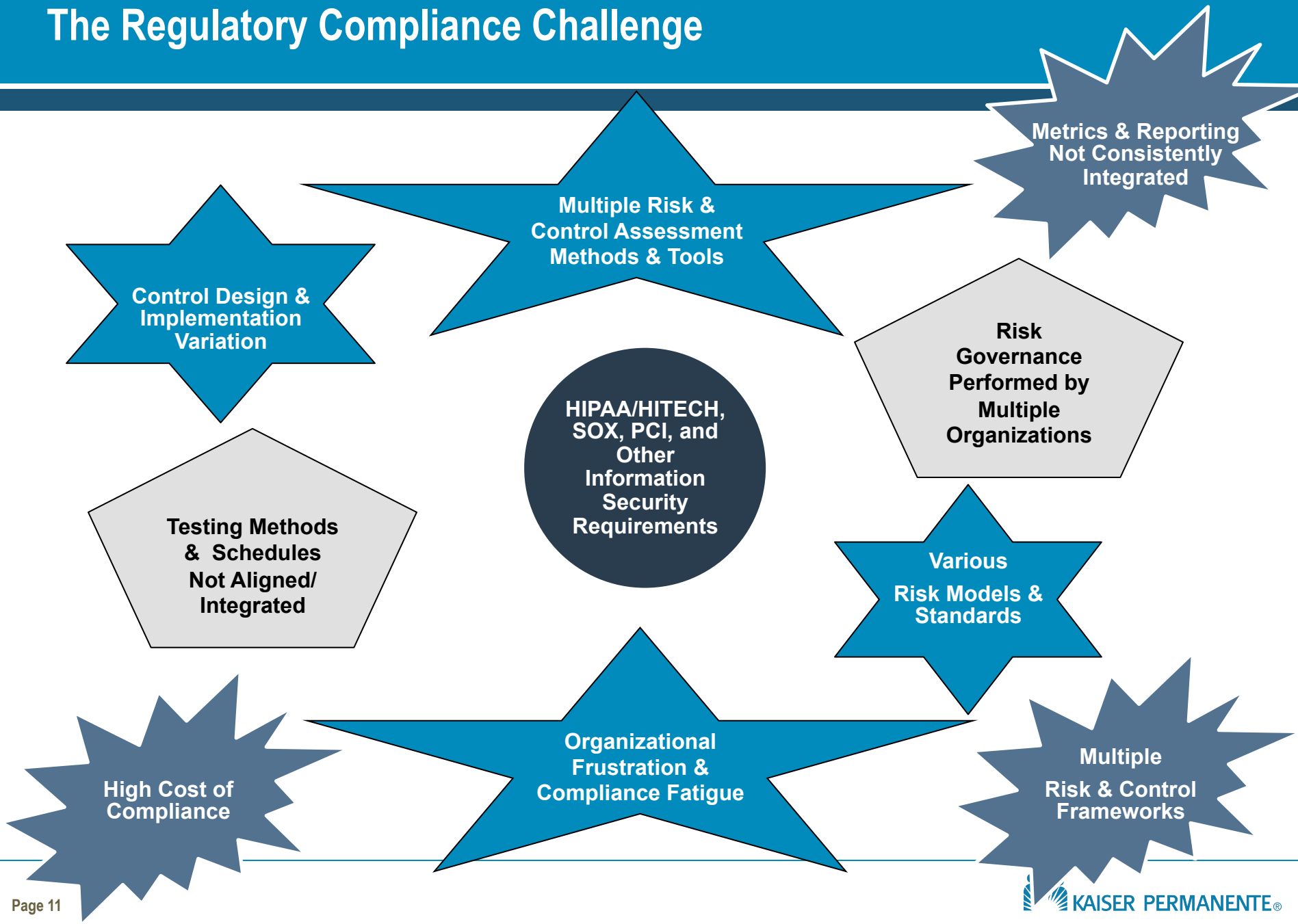
# PCI-DSS at Kaiser Permanente

**PCI-DSS Requirements**
*"The Dirty Dozen"*

| Objectives | Requirements |
|---|---|
| **Keep your network secure** | **1. Protect data with a firewall**<br>**2. Do not use default passwords** |
| **Protect cardholder data** | **3. Protect stored data**<br>**4. Encrypt data over public networks** |
| **Maintain a vulnerability management program** | **5. Perform regular anti-virus updates**<br>**6. Secure systems and applications** |
| **Control access to data and data systems** | **7. Restrict access to data**<br>**8. Assign unique IDs to each person**<br>**9. Restrict physical entry** |
| **Monitor and test** | **10. Monitor all data access**<br>**11. Test security systems and processes** |
| **Have an information security policy** | **12. Maintain an information security policy** |

Translates to more than 200 specific requirements.
PCI is a "100% Compliance" requirement → failing one requirement means overall non-compliance.

# The Regulatory Compliance Challenge





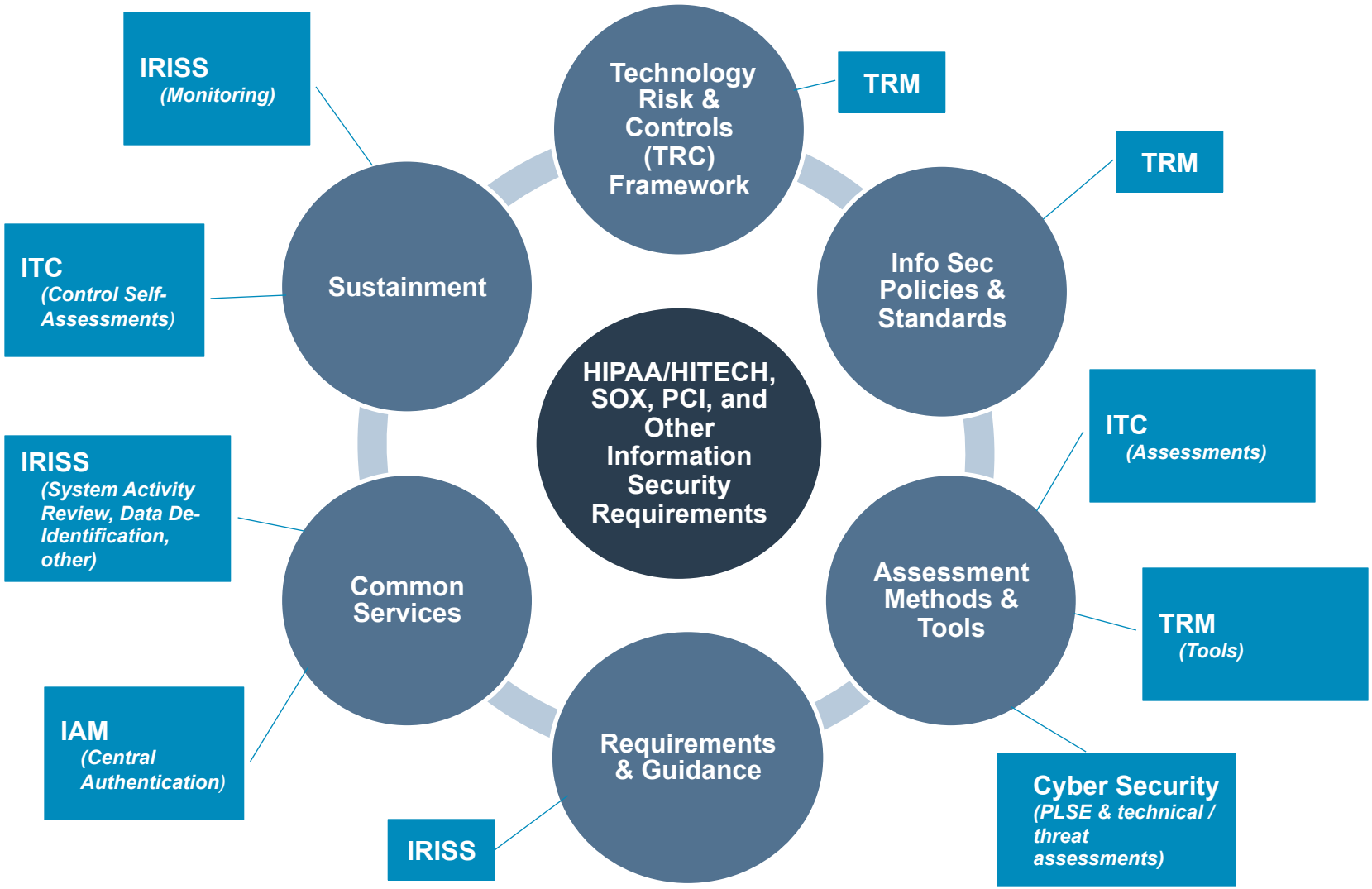

KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance




KAISER PERMANENTE®

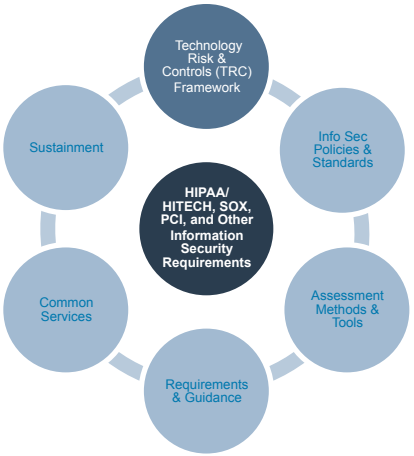
# Integrating Regulatory & Information Security Compliance






KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance
# Technology Risk & Controls (TRC) Framework




***Benefits***

- **Single framework encompassing all applicable regulations (including HIPAA, SOX, and PCI)**
- **Based on industry standards, but customized for Kaiser Permanente**
- **Basis for TRO risk assessment**

***Status***

- **Being rationalized for consistency**



KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance
# Technology Risk & Controls (TRC) Framework (example)

## Technology Risk and Controls Framework

- Enables aggregated, comprehensive management of multiple factors
- Captures key data such as:
  - Domain
  - Process description
  - Control objectives
  - Industry best practices
  - Integrates SOX, HIPAA Security & PCI


**KP TRC Framework - 4.17.2013 (DRAFT)**

| | | | | | | | KP Control Associations(PCI, HIPAA, SOX, IMG, etc.) | | | Industry Best Practice | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Domain | Process Areas | Process Description | Sub_Process | Control Objective | Control # | Control Description | Regulation / Control Source | KP - Control ID | KP - Control Description | ISO | COBIT | HITRUST |
| Service Support | Change Management | The initiation, risk analysis, approval, prioritization, and scheduling of changes to provide enhancements and modifications to technology assets. | Change Request | To ensure that changes are appropriately requested and reviewed and analyzed for development. | SS.CM.1 | Changes are appropriately requested and include change criticality, type, rating and business rational. | PCI | Requirement 6 | Develop and maintain secure systems and applications | 10.1.2 - Change Management | AI6.1 Change standards and procedures<br>AI6.2 Impact assessment, prioritization and | 09.b Change Management<br>10.k Change Control Procedures |
| | | | | | | | PCI | Requirement 6 | Develop and maintain secure systems and applications | | | |
| | | | | | SS.CM.2 | Change requests are reviewed for completeness and accuracy and have a risk and impact analysis performed. | PCI | Requirement 6 | Develop and maintain secure systems and applications | 10.1.2 - Change Management | AI6.2 Impact assessment, prioritization and authorization<br>AI1.2 Risk Analysis Report | 09.b Change Management |
| | | | Change Approval | To ensure that changes receive appropriate approval. | SS.CM.3 | Changes are approved by appropriate levels of management based on risk and impact levels. | PCI | Requirement 6 | Develop and maintain secure systems and applications | 10.1.2 - Change Management | AI6.2 Impact assessment, prioritization and authorization<br>AI7.2 Test plan<br>DS13.2 Job scheduling | 09.b Change Management<br>10.k Change Control Procedures |
| | | | | | | | SOX | 12.14.03 | Change requests are appropriately authorized. | | | |
| | | | | | | | IMG | N/A | N/A | | | |
| | | | Request Prioritization | To ensure that changes are prioritized to meet business needs in a timely manner. | SS.CM.4 | Changes are appropriately prioritized based on criticality and business needs. | | | | | AI6.1 Change standards and procedures<br>AI6.3 Emergency Changes | |
| | | | Emergency Change Scheduling | To ensure that emergency changes are migrated to production in an effective and timely manner. | SS.CM.5 | The change schedule is designed to allow emergency and critical changes to be made in between standard release dates in a effective manner. | | | | | AI7.3 Implementation plan<br>AI7.5 System and data conversion<br>AI6.1 Change standards and procedures<br>AI6.3 Emergency changes | |
| | | | Change Monitoring | To ensure that change requests are fulfilled in a timely manner. | SS.CM.6 | The status of change requests are tracked, monitored and reported to management. | IMG | N/A | N/A | | AI6.4 Change Status Tracking and Reporting | |
| | | | | | | | IMG | N/A | N/A | | | |



KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance
# Info Sec Policies & Standards

*Technology Risk Standard (TRS)*

- **Provides common language and integration for all regulatory terms**
- **Maps provisions to regulatory requirements, creating 100% traceability**
- **Aligns Assessment methods and tools with TRS requirements**

*Policies*

- **Ongoing refinement of policies to assure inclusivity and reduce redundancy**




KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance
# Info Sec Policies & Standards (example)

### 7.1. Technology Risk Management Lifecycle

Adopting the technology risk management lifecycle ensures that a consistent risk management methodology is applied across the technology environment. Functional areas that perform components of the technology risk management lifecycle must do so in alignment with the methodology defined within this standard and technology risk management processes. Figure 7.1-1 below illustrates the technology risk management lifecycle.

**Figure 7.1-1**


Table 7.1-1 below describes high-level functions of each process step in the risk management lifecycle.

**Table 7.1-1**

| Process | Process Description |
|---|---|
| **Request Intake** | Capture the initial data to help prioritize risk related activities and drive risk profiling. |
| **Risk Profiling** | Assess the technology asset value and criticality according to specific criteria and characteristics, then utilize that information to establish an asset profile to prioritize assets and support risk management activities. |


### 7.7.2. Risk Levels

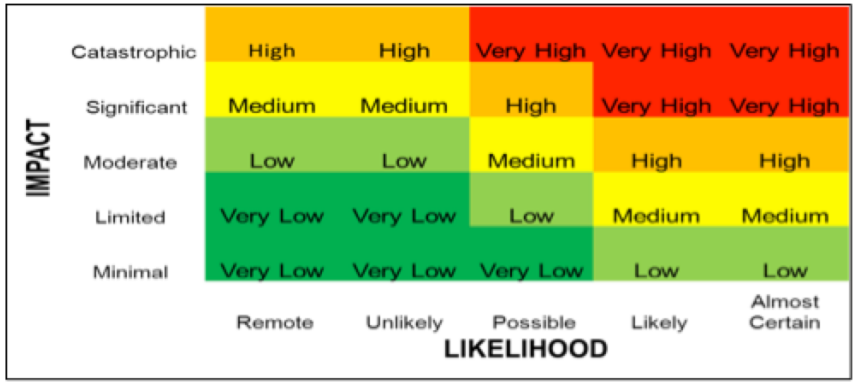
Use the impact and likelihood ratings described in the following sections to determine the overall risk rating for a given risk. IRM defined a five level risk-rating scale shown in Table 7.7.2-1 below.

**Table 7.7.2-1**

| Very High | High | Medium | Low | Very Low |
|---|---|---|---|---|

Use the matrix in Figure 7.7.2-1 below to combine impact and likelihood ratings to determine the overall risk rating.

**Figure 7.7.2-1**






KAISER PERMANENTE®

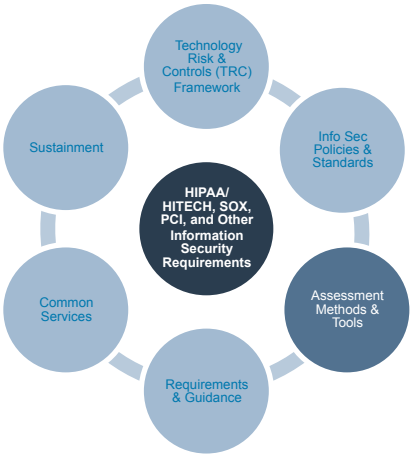
# Integrating Regulatory & Information Security Compliance Assessment Methods & Tools

*Benefits*

- **Provides common tools and methodologies based on TRC Framework**
- **Lessens compliance fatigue by developing a "test once, use many" methodology**
- **Standardizes and integrates HIPAA/HITECH, SOX, and PCI assessments based both on common and unique attributes**
- **Improves audit readiness**

*Status*

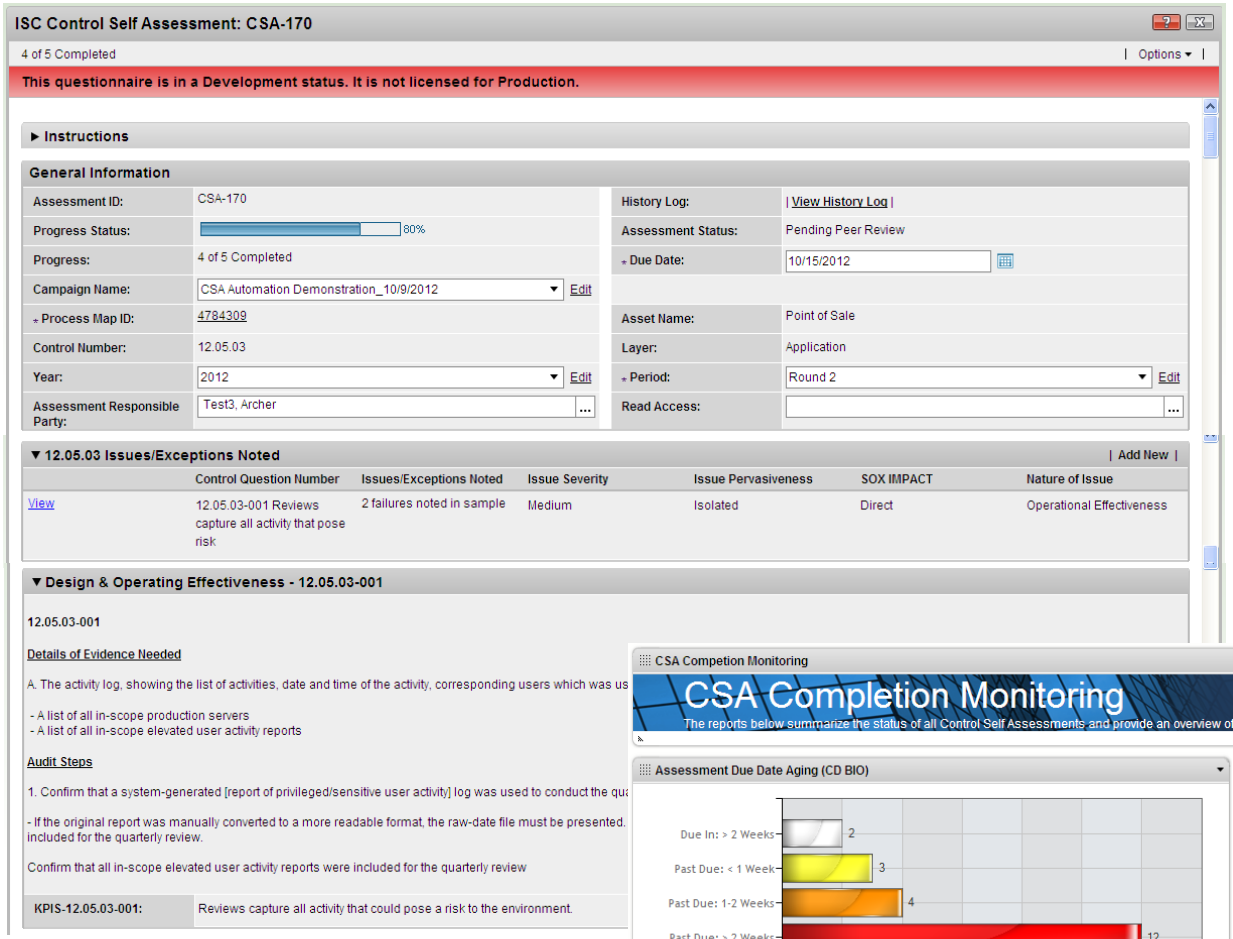
- **Integrated control assessment requirements in the process of being defined**

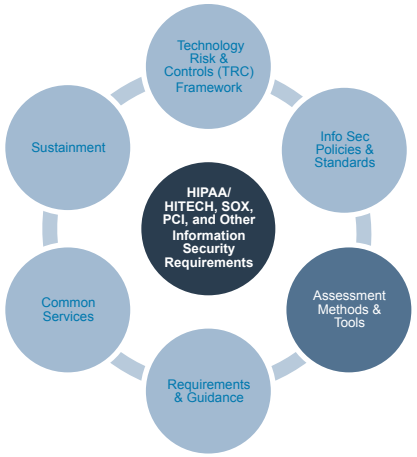


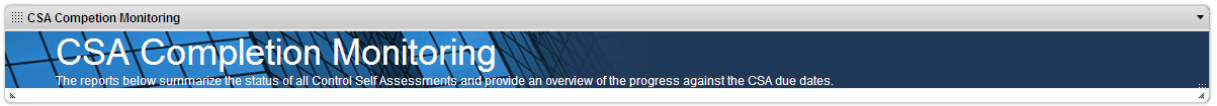



KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance Assessment Methods & Tools (example)

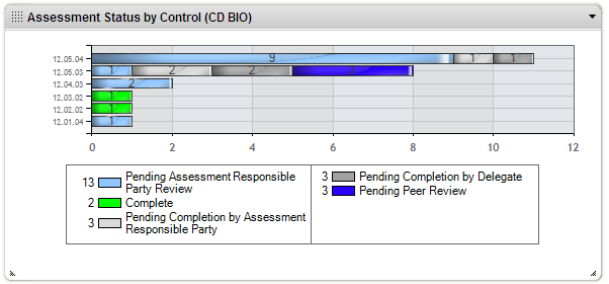











KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance Requirements and Guidance

## *Benefits*

- **Rationalizes all regulatory requirements into a single set of compliance instructions**
- **Customizable based on regulatory applicability**
- **Defines control attribute requirements for each regulatory framework**

## *Status*

- **Utilizes the 9 SOX Security Domain controls as its basis**




KAISER PERMANENTE®

# Integrating Regulatory and Information Security Compliance Requirements and Guidance (continued)

## Multiple inputs evaluated to create an integrated set of compliance manuals for HIPAA, SOX, and PCI

**Collaborate with Stakeholders**

Identify relevant HIPAA Standards/ Implementation Specifications

- 9 SOX Security Domain Controls
- HIPAA Security Rule
- Centers for Medicare and Medicaid Services (CMS) Guidance Docs

Align HIPAA-SOX-PCI requirements

- TRC Framework
- ITC Mapping
- Compliance Manuals, Narratives, other documents
- PCI DSS 2.0

Draft and Develop HIPAA-SOX-PCI Control Requirements

**Language** **Objective**

and Attributes

- Authoritative Sources (HITRUST, SIG, COBIT, ISO 27002, NIST 800-66)
- Compliance Manuals, Narratives, other documents

Enhance HIPAA-SOX-PCI Requirements and Attributes

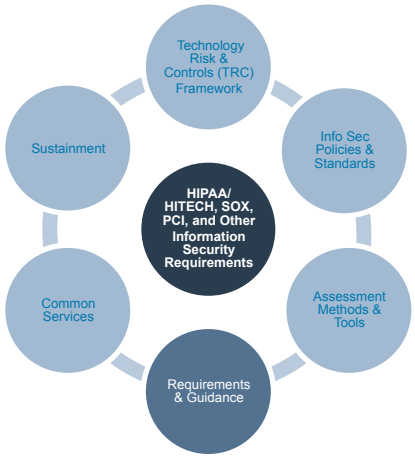
- Stakeholder feedback/comments on draft HIPAA-SOX-PCI requirements and guidance

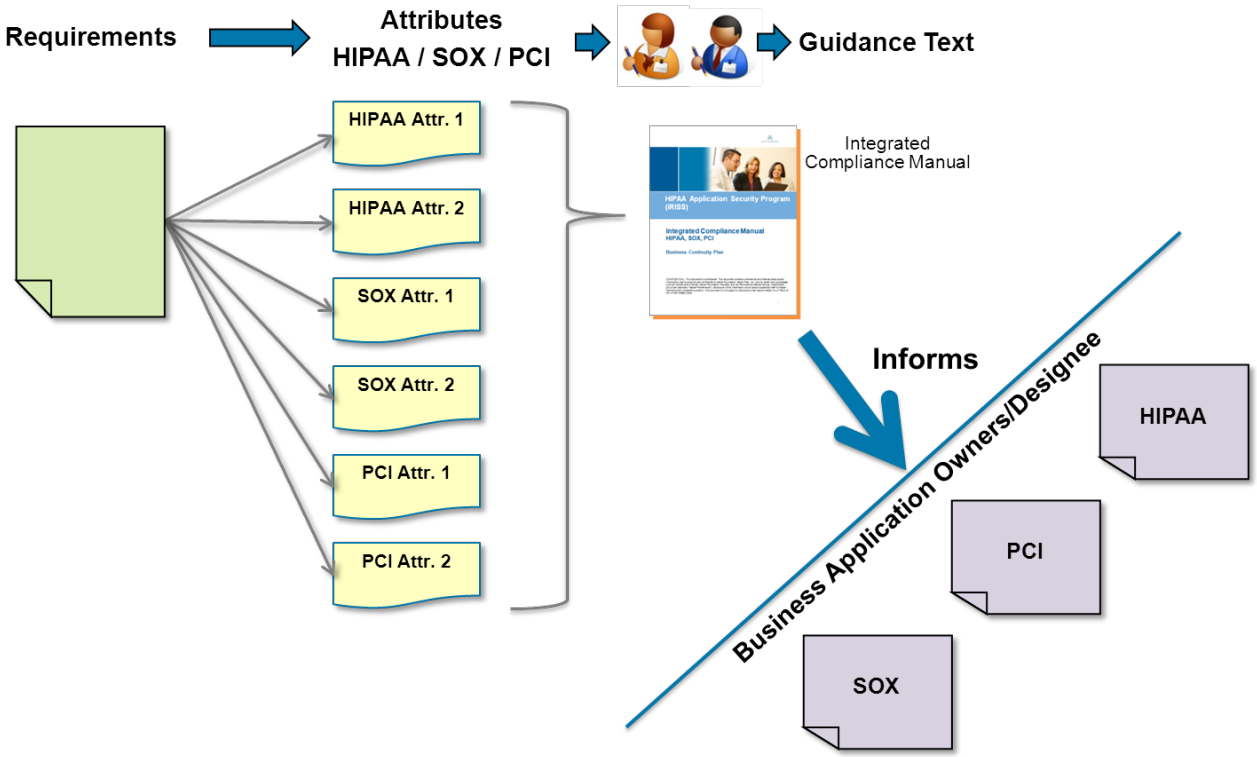
Deliver Integrated Compliance Manual

- Manuals, Narratives, other documents

# Integrating Regulatory and Information Security Compliance Requirements and Guidance (continued)

## Making compliance easier…





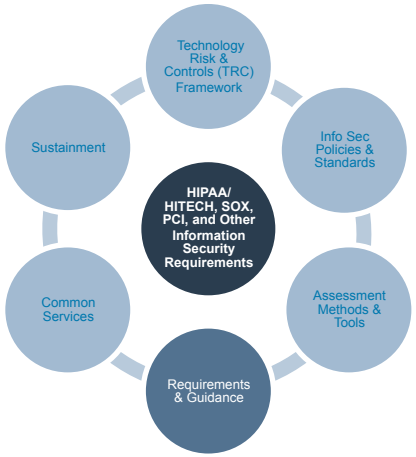

KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance Requirements and Guidance (example)

### 6.1.2 Integrated Objective and Requirements

The table below outlines the integrated objective and requirements. The corresponding requirement attributes and guidance can be found in Requirements and Attributes section. The integrated objective broadly covers all requirements.

| Integrated Objective | Integrated Requirements | HIPAA | SOX | PCI |
|---|---|---|---|---|
| Monitor sensitive system activity to detect inappropriate events related to financial and restricted health information. | ICM.SAR.01 – Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period. There should be a periodic review of audit logs. | ✓ | | ✓ |
| | ICM.SAR.02 – Elevated and privileged activities are logged and regularly reviewed by appropriate personnel. | ✓ | ✓ | |
| | ICM.SAR.03 – Periodic review of technical security configuration should be performed to check for compliance with security implementation standards. | ✓ | | |




| HIPAA, SOX and PCI Mapping | | | | | | | TRC Control Framework | | | Crosswalk to Authoritative Standards | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| KP Control ID | Reg # | Control Category | Implementation Specification Title | HIPAA Implementation Specification/Requirement | SOX Controls | PCI Reference | TRC Control # | TRC Control Objective | TRC Control Description | Reference Source Document | Control Reference Title | Reference Control ID and Language |
| HS.01 | 164.312(b) | System Activity Review and Audit Controls | Audit Controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic Protected Health Information | 12.05.03 (IT) Elevated Activity Monitoring<br><br>12.05.04 (Business) Elevated Activity Monitoring | 10.2 Implement automated audit trails for all system components to reconstruct the following events:<br>10.2.1 All individual accesses to cardholder data<br>10.2.2 All actions taken by any individual with root or administrative privileges<br>10.2.3 Access to all audit trails<br>10.2.4 Invalid logical access attempts<br>10.2.5 Use of identification and authentication mechanisms<br>10.2.6 Initialization of the audit logs<br>10.2.7 Creation and deletion of system-level objects<br><br>10.3 Record at least the following audit trail entries for all system components for each event:<br>10.3.1 User identification | SEC.OSM.10 | To ensure that management actively monitors activities for appropriateness and investigates suspicious activity as needed. | Security logging is enabled on appropriate systems, devices and processes and are monitored for suspicious and unauthorized activity. | HITRUST 2013 v5 | Information Systems Audit Controls | 06.i - Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes. |

| Proposed Integrated Security Requirements | | Proposed Requirements Attributes | | | |
|---|---|---|---|---|---|
| Requirement ID | KP Proposed Control Requirement | HIPAA Requirement Attributes | SOX Requirement Attributes | PCI Requirement Attributes | Common Attributes |
| 06.i.01 | Audit requirements and activities involving checks on operational systems shall be planned and agreed upon, to minimize the risk of disruptions to business processes. | Level 1<br>• An annual audit planning and scoping process exists and gives consideration to risk, involvement of technical and business staff, other ongoing projects, and business impacts.<br>• If a smaller quarterly process is utilized, the entire organization should be audited annually.<br><br>Level 2<br>• The organization develops, disseminates, and reviews and | None | None | N/A |

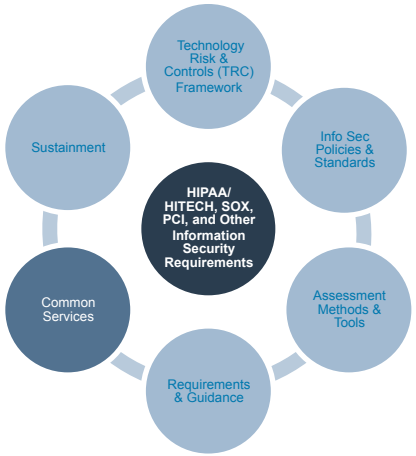


KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance Common Services

## *Benefits*

- **Utilizes standardized, centralized, and scalable solutions**
- **Provides consistent control execution across all regulatory frameworks**




## *Examples*

- **Identity and Access Management (IAM)**
- **Application Access Lifecycle Management (AALM)**
- **System Activity Review / Elevated Activity Monitoring**
- **Data De-Identification (DDI)**



KAISER PERMANENTE®

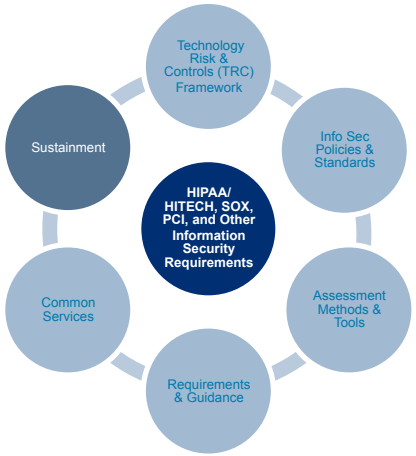
# Integrating Regulatory & Information Security Compliance Sustainment

*Benefits*

- **Provides ongoing reporting of the risk landscape**
- **Enhances controls effectiveness and maturity**

*Examples*

- **IRISS Monitoring services**
- **Controls Self-Assessments (CSAs)**






KAISER PERMANENTE®

# Integrating Regulatory & Information Security Compliance Approach to Compliance Sustainability

**Kaiser Permanente built a strategy that sustains compliance and includes compliance education, monitoring and enforcement.**

The fast changing regulatory environment requires that Kaiser Permanente take an aggressive and forward-thinking approach to regulatory compliance.

**Sarbanes-Oxley Act (SOX)**
**NAIC Model Audit Rule (MAR)**

**HIPAA Security Rule/**
**HITECH (MU P&S) and**
**HIPAA Privacy Rule (DDI only)**

**Payment Card Industry Data Security Standards (PCI-DSS)**

## Effects of Non-Compliance may include:

- **Damage to the Kaiser Permanente reputation and brand**
- **Loss of member trust through required breach notification**
- **Unable to attest to portions of HIPAA Security for Meaningful Use purposes**
- **Significant civil and/or criminal fines and penalties**
- **Increased scrutiny in the form of more enforcement audits**
- **Material financial misstatements**

# Integrating Regulatory & Information Security Compliance
## Approach to Compliance Sustainability
### Current State and Proposed Future State

**How do we accelerate compliance sustainability?**

**Current State**

- Fragmented sustainment processes
- Decentralized compliance monitoring and reporting
- Varied levels of compliance maturity
- Unclear accountabilities

**Leveraging SOX approach**

**Proposed Future State**

- Highly integrated compliance model
- Centralized compliance monitoring and reporting
- Standardized processes and tools
- Clearly defined accountabilities.

**Benefits of Compliance Integration**

- Accelerates and enhances compliance
- Increases visibility and transparency
- Drives standardization
- Leverages existing tools and processes
- Supports Technology Risk & Control (TRC) framework efforts

# Integrating Regulatory & Information Security Compliance
# Approach to Compliance Sustainability
## Control Maturity Levels (example)

| Business Maturity Level | Accountability | Documentation | Evidence | Process | Monitoring |
|---|---|---|---|---|---|
| | *-Accountable<br>-Knowledgeable<br>-Full authority<br>-Engaged/motivated* | *-Process documented<br>-Accurate & complete<br>-Updated periodically* | *-Evidence retained<br>-Centrally stored<br>-Complete population* | *-Consistent with narrative<br>-Follows internal & external best practices<br>-Standardized & automated* | *-Team self-monitors<br>-Issues resolved timely* |
| 0 – Does Not Exist | Does not exist | Does not exist | Does not exist | Does not exist | Does not exist |
| 1 – Incomplete | Exists but unsure & not clearly defined | Exists but inaccurate, incomplete or undefined | Exists but inadequate or incomplete | Exists but does not follow the narrative or incomplete | Ad-hoc monitoring in place, no resolution management process |
| 2 – Inconsistent | Accountable but no full authority to exercise responsibilities | Accurate & complete but informally managed | Complete & retained but informally managed | Complete but very manual, resource intensive & not standardized | Periodic monitoring in place, no resolution management process |
| 3 – Consistent & Streamlined | Accountable, knowledgeable, & full authority | Formally approved by management & centrally stored | Complete, retained, & centrally stored | Standardized, streamlined and manual or partially automated | Periodic monitoring & resolution management process in place |
| 4 – Optimized & Sustainable | Accountable, knowledgeable, fully authorized & engaged | Updated & approved regularly using a formal change management process | System-generated & managed using an integrated tool | End-to-end process is supported by integrated tools and automation | Automated, continuous monitoring & resolution management process in place |

| IT Criteria and Definition | Accountability | Documentation | Design and Operating Effectiveness | Self Assessment Process and Execution |
|---|---|---|---|---|
| | - Identified and confirmed<br>- Accountability understood<br>- Knowledgeable<br>- Full authority and empowerment<br>- Engaged | - Process documented<br>- Reflects control design<br>- Accurate & complete<br>- Reviewed and approved periodically<br>- Retained and readily available | Adequate control design (satisfies SOX PMO guidance)<br>- Control is evaluated either through self testing or management testing<br>- No design gaps and consistent, effective control operation (no open CAPs) | - Standard self assessment process<br>- Self assessment performed for each control/layer<br>- Testing sufficiently evidenced and documented<br>- Adequate disposition of test results (e.g. CAP decision) |
| Maturity Rating (0-4) | Overall control maturity considers all four criteria and is calculated based on weight of each criterion.<br>(Accountability 5%, Process and Controls Documentation 5%, Design and Operating Effectiveness 80%, and Self Assessment Process and Execution 10%) | | | |



KAISER PERMANENTE®

# Key Takeaways

- Collaborate, collaborate, collaborate!
- Clearly define ownership of critical functions and processes
- Clearly define roles/responsibilities
- Establish a RACI for organization and lower level RACIs for functions
- Understand the spirit of the regulation
- Plan and do the foundational work before diving into the detailed work
- Leverage and re-use what works
- Understand your population:
  - Asset inventory
  - What you do and don't know; work to reduce the unknowns
  - Your maturity model; which controls do/do not exist for in scope applications, infrastructure, and enterprise
- Find and fix early:
  - CSAs self-detect and correct; don't wait for tester to tell you what's wrong

# Questions