# An Integrated Approach to Technology Risk Management and Compliance

Kerry Bryan, Sr. Manager Policy & Guidance
Michael Makstman, Sr. Director
Sherrie Osborne, Director, HIPAA Security Program Technology

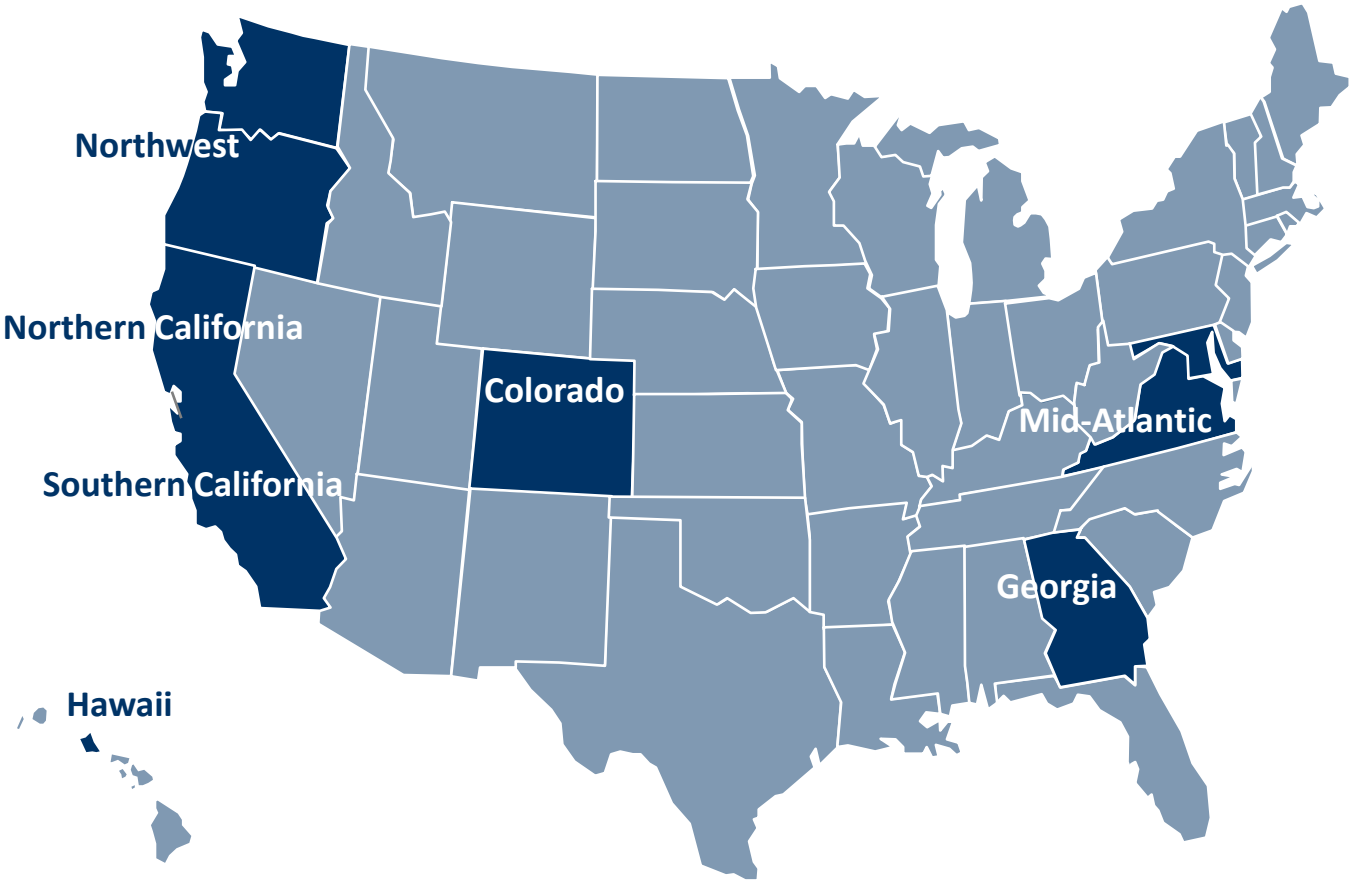
Technology Risk Management, Kaiser Permanente

Governance, Risk & Compliance – G22

# An Integrated Approach to Technology Risk Management (TRM) and Compliance

- Kaiser Permanente
- Foundations of Technology Risk Office
- Key Business Drivers
- What Could Go Wrong
- The Regulatory Compliance Challenge
- Integrating TRM and Compliance @ Kaiser Permanente
- Value Proposition
- Lessons Learned
- Q&A

# Kaiser Permanente




**integrated**

- 9.3 million members
- 17,000+ physicians
- 49,000+ nurses
- 192,000+ employees
- 8 states + District of Columbia
- 38 hospitals
- 600+ medical offices
- $53 billion operating revenue

**Nation's largest not-for-profit health plan**

Scope includes ambulatory, inpatient, ACS, behavioral health, SNF, home health, hospice, pharmacy, imaging, laboratory, optical, dental, and insurance

# Foundations of Technology Risk Office (TRO)

Organization Coordinating the IT Security Compliance Efforts (HIPAA, SOX, PCI)

- TRO
  - Cyber Security.
  - IT Compliance.
  - Technology Risk Management (TRM).
  - Other functions.

- TRM Focus
  - Technology risk and control framework.
  - Technology risk management standard.
  - Policies, standards, and guidance.
  - Technology control and risk assessment methods.
  - Technology risk portfolio management.

# Key Business Drivers

What is Driving Technology Risk Management and Compliance?

- External
  - Regulatory requirements (specifically HIPAA Security, SOX, and PCI).
  - Electronic health record, bio med and mobile devices, and all things attached to the network (e.g., communications) providing new attack vectors.
  - Threat landscape has become more sophisticated.
  - Criminals have figured out how to monetize health care.
- Internal
  - Protection of member/patient and other sensitive data is a top priority.
  - An information security or data breach compromising the ability to provide member/patient care.
  - Business model complexity
  - Information security controls not standard across the company, nor yet mature.

# What Could Go Wrong?

Consequences of an Information Security or Data Breach

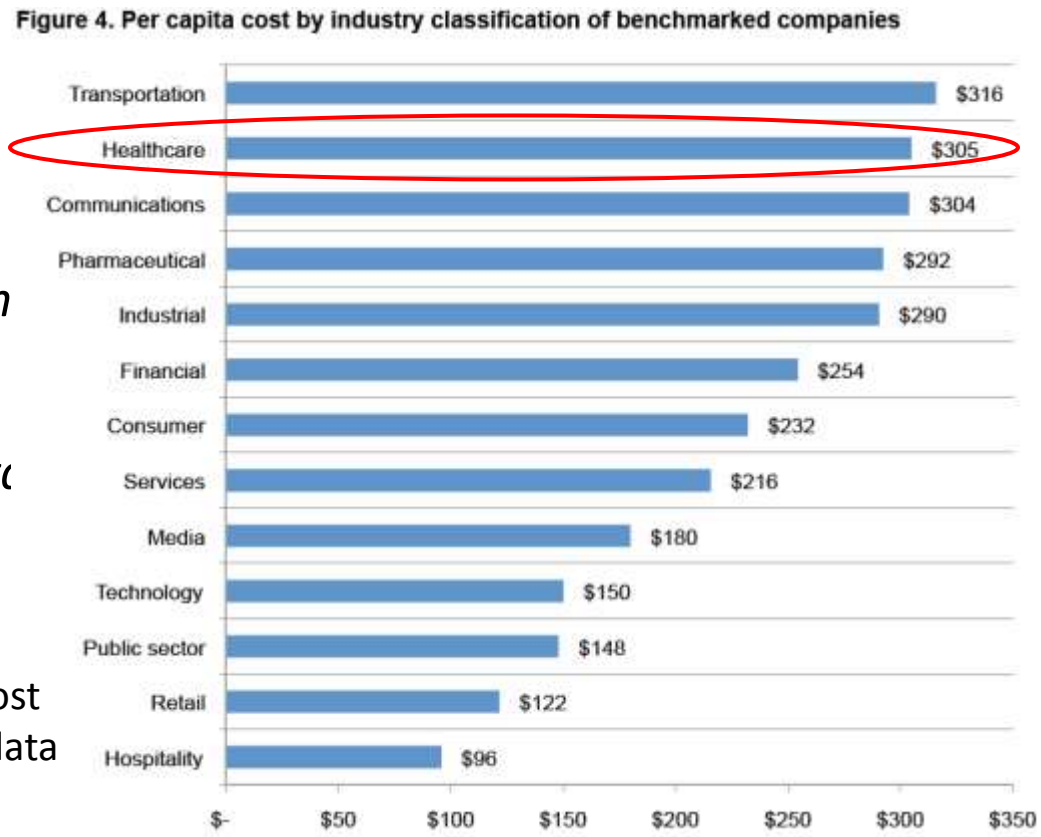
- Member/patient care delivery and services compromised.
- Damage to member/patient confidence.
- Medicare / Medicaid fraud.
- Damage to reputation.
- Fines/penalties.
- Increased regulatory scrutiny.

# Data Breach Cost Per Record

## Cost of an Information Security or Data Breach

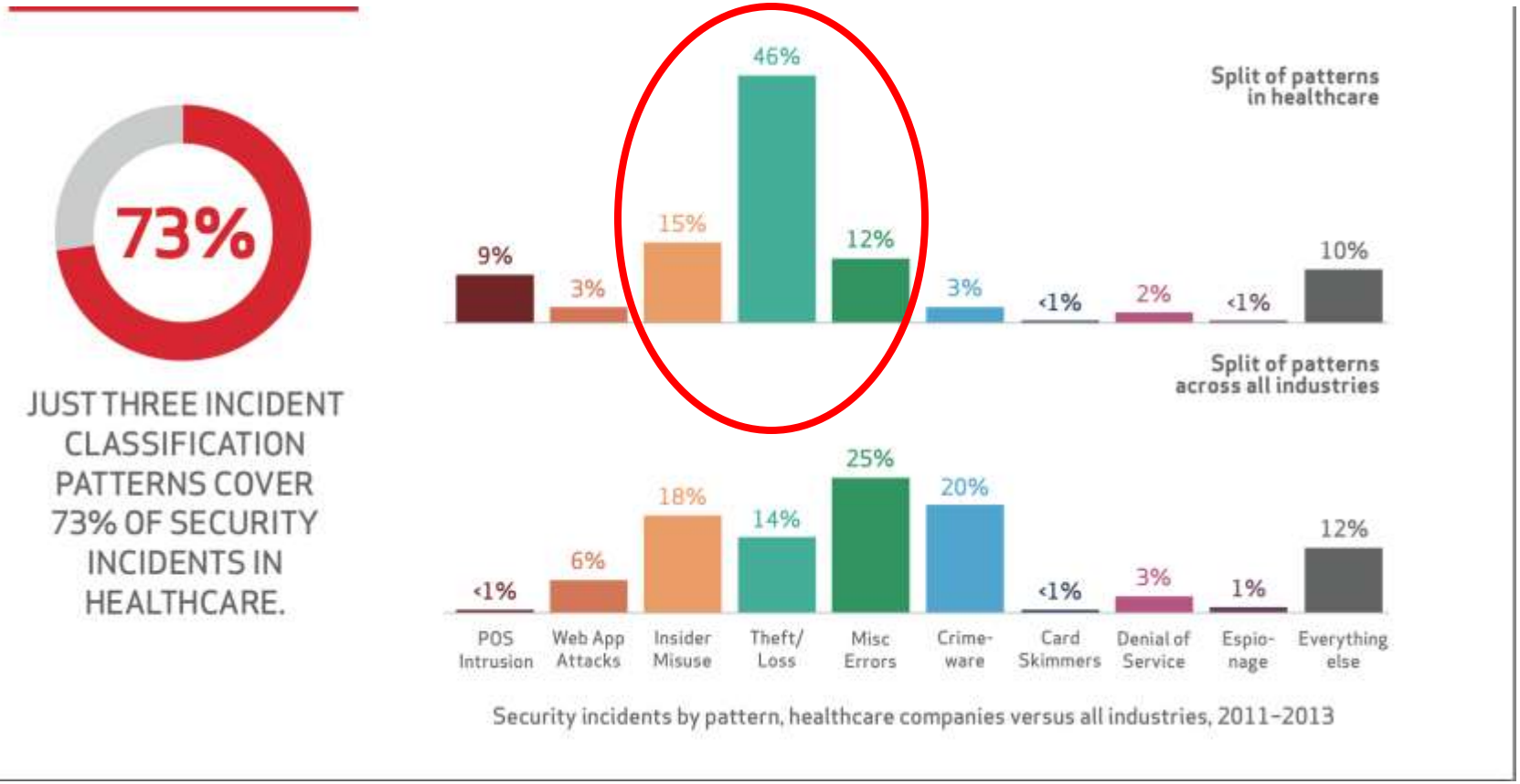
- *"Certain industries have higher data breach costs. Figure 4 reports the per capita* costs for the 2012 study by industry classification. …….. Specifically, heavily regulated industries such as healthcare, communications, pharmaceuticals and financial services tend to have a per capita data breach cost substantially above the overall mean of $188. ……."*

* **Per capita cost** is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records.



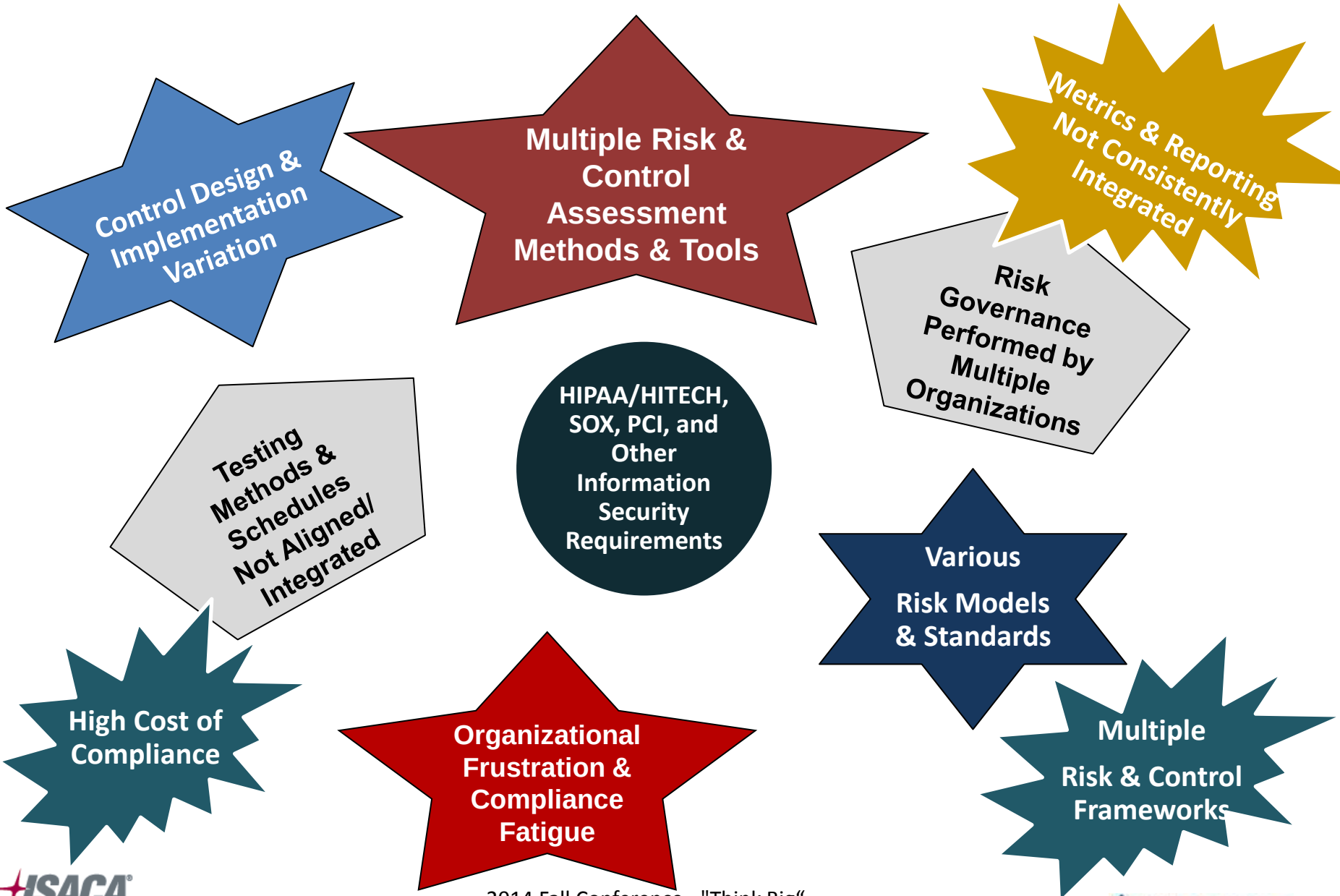

*2013 Cost of Data Breach Study:United States, Benchmark research sponsored by Symantec, Independently Conducted by Ponemon Institute LLC; May 2013*

# Data Breach Investigations Analysis




*2014 Verizon Vertical Insight - Data Breach Investigations Report HEALTHCARE*

# The Regulatory Compliance Challenge



# Day in the Life

A Conversation With the Information Consumers

## All of the change is just too much!

- **Competing priorities –** *protect the information while maintaining reasonable access*
  - We are a health care company.
  - Electronic protected health information (ePHI) is a vital component of our every-day jobs.

# Day in the Life (cont'd)

## A Conversation With the Information Consumers

- **Confusing landscape –** *confusing direction*
  - Convoluted, technical and conflicting requirements (HIPAA, SOX, PCI).
  - Too many policies, procedures and rules to meaningfully understand them all.
  - Resources not able to spend time doing what they were hired to do.

# Day in the Life (cont'd)

A Conversation With the Information Consumers

- **The Needs of the Information Consumers –** ***seem to have been forgotten***
  - Should be considered when proposing anything that may impact our access to the data.


# Integrating Technology Risk Management and Compliance at KP (HIPAA/SOX/PCI)

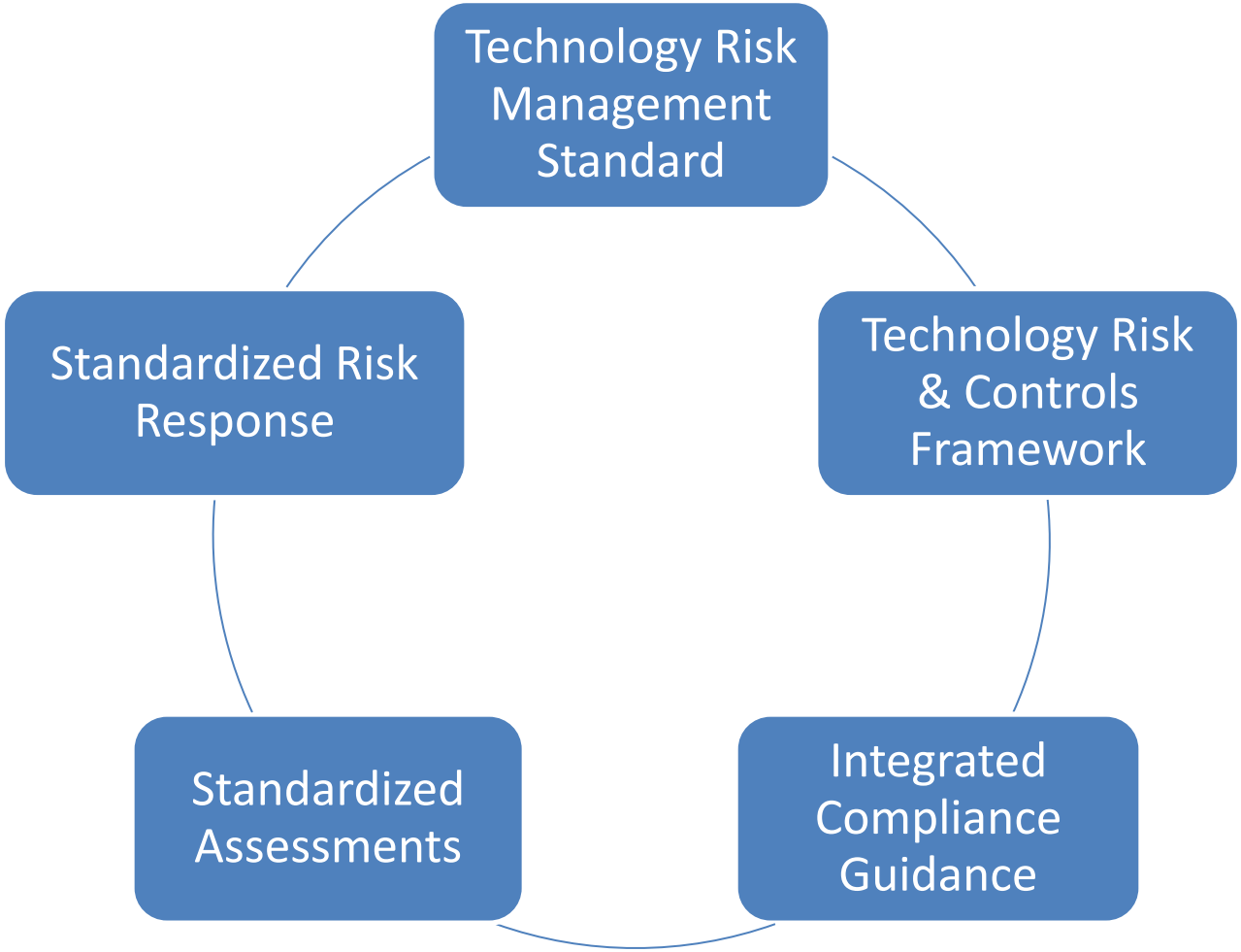
- **What do we mean by integrated?**

  An approach that aligns the guidance and methods to address the three primary regulatory requirements into a cohesive framework and delivery model.

- **Why integrate?**
  - Reduce redundancy, resource contention and compliance fatigue.
  - Consistently align compliance requirements.
  - Improve compliance results.
  - Improve risk decision making.
  - Reduce cost of technology risk management and compliance.

# An Integrated Approach

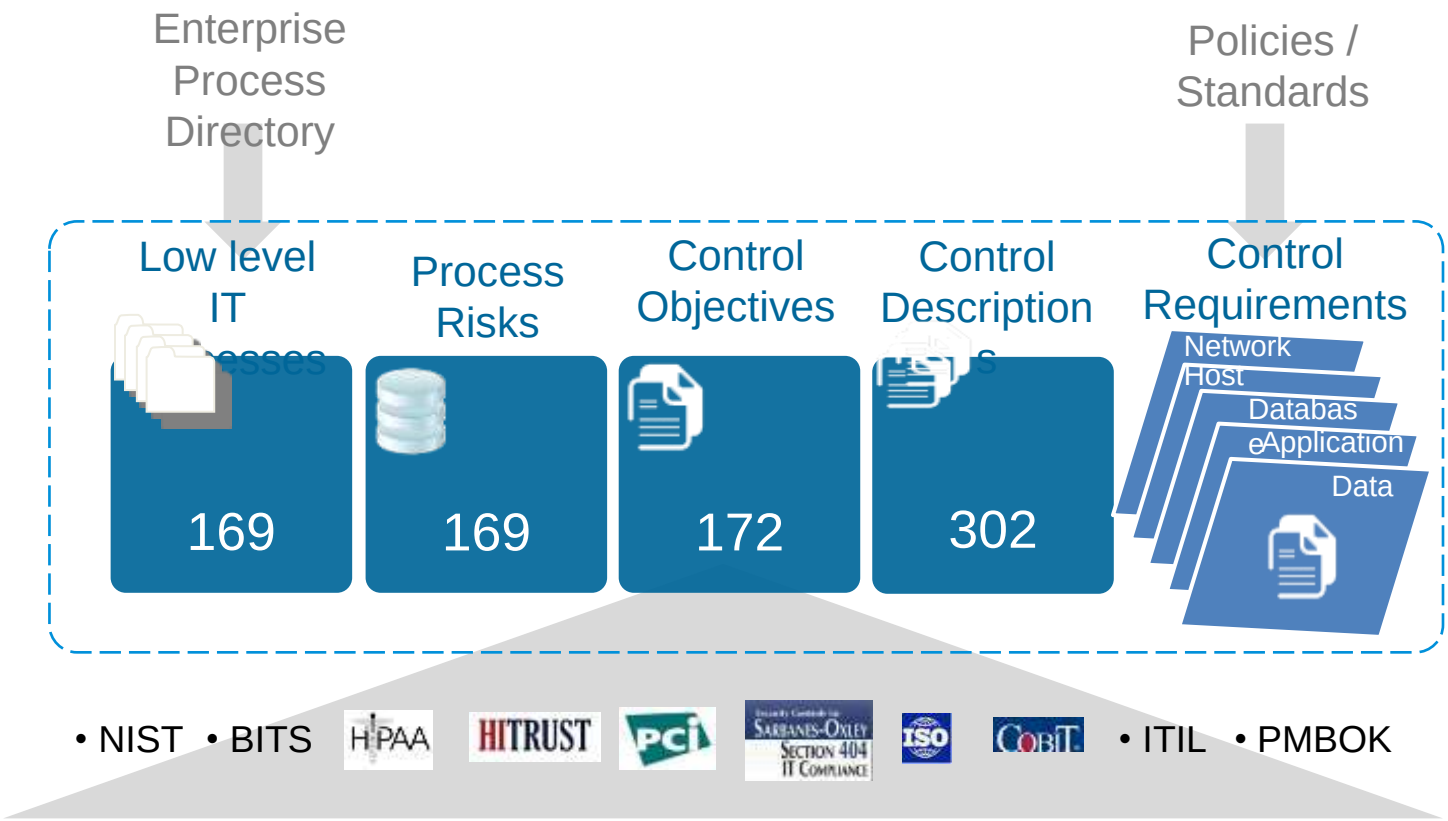
To Technology Risk Management and Compliance (HIPAA/SOX/PCI)



# Technology Risks and Controls Framework

Technology Risks and Controls (TRC) Framework

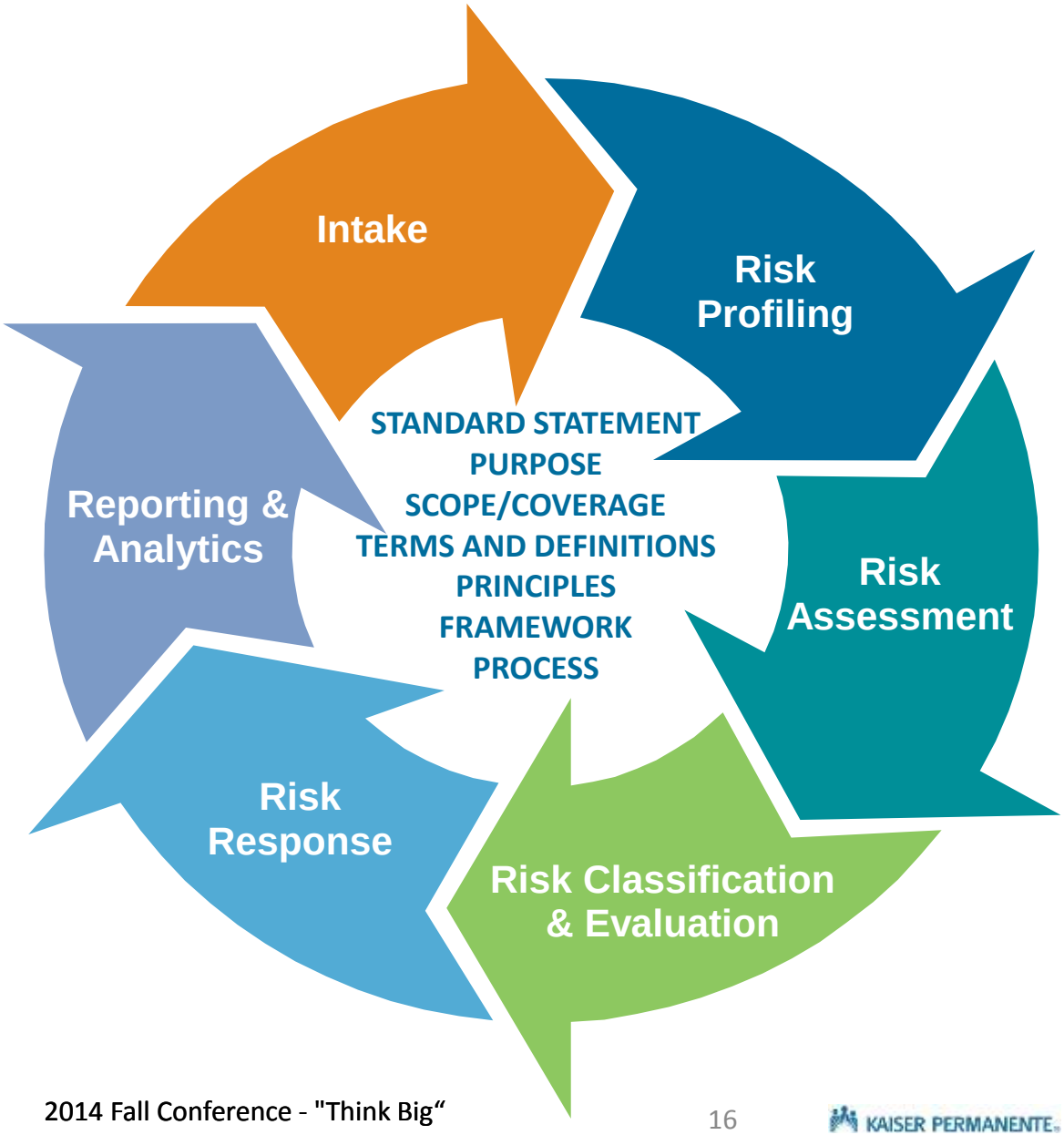
A hierarchical catalog of KP technology processes, risks and controls.
Reference architecture for risk aggregation, analysis and reporting.
Aligned to KP policies, applicable laws, regulations, and leading industry practices.



# Technology Risk Management Standard

The standard provides:

- *terminology related to the words used*
- *life cycle processes by which risk management is carried out*
- *organization structure and managing framework for risk management*
- *objective, scope and principles for risk management*



# Integrated Compliance Guidance

Multiple Inputs Evaluated to Create an Integrated Baseline in a Set of Compliance Manuals for HIPAA, SOX, and PCI

**Collaborate with Stakeholders**

Identify relevant HIPAA Standards/ Implementation Specifications

Develop HIPAA-SOX-PCI Compliance Baseline

Draft and Develop HIPAA-SOX-PCI Interpretation of Requirements

**Language** | **Objective**

Socialize HIPAA-SOX-PCI Guidance

Deliver Integrated Compliance Guidance (ICG) Manual

- HITRUST
- HIPAA Security Rule

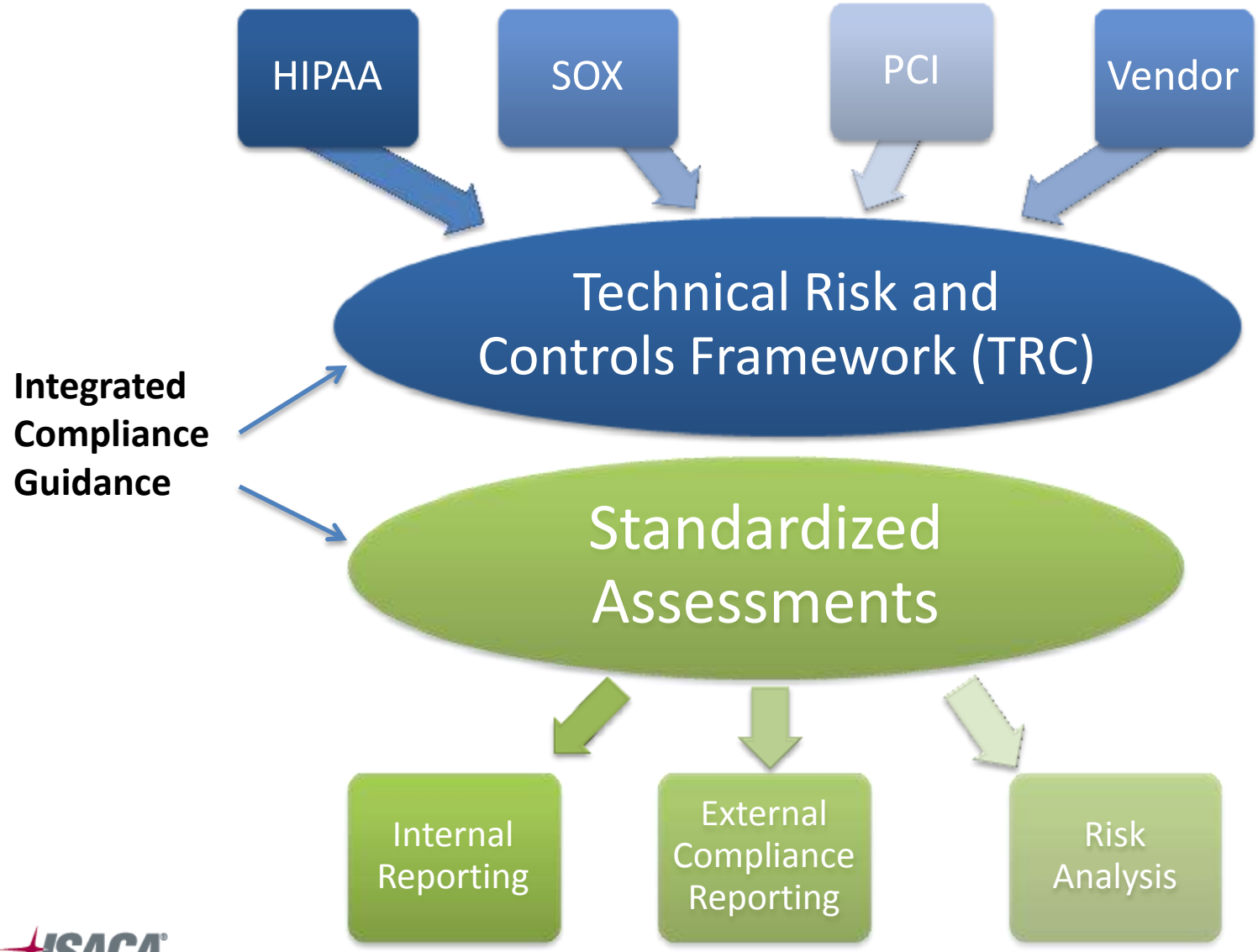
- TRC Framework
- SOX, PCI

- Other Authoritative Sources (HITRUST, ISO 27002, NIST 800-53, NIST 800-66)
- Internal Policy & Standards

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

# Standardized Assessments

Test Once, Use Many



# Standardized Risk Response

Risk Treatment

- **Risk Response**
  - Process, activities, and decisions for managing risk that has been assessed and classified.
- **Management chooses to remediate or pursue risk acceptance considering:**
  - Compliance goals.
  - Business goals.
  - Risk tolerance.

# Value Proposition

By integrating Technology Risk Management and compliance we are delivering real value to the enterprise.

- Improved program integration and alignment.
- Decreased frustration.
- Improved visibility into the risk landscape.
- Decreased cost of technology risk management and compliance.

# Lessons Learned

- Restructuring was required to incorporate in sustaining organizations.
- Program integration and alignment is a long-term proposition.
- It’s challenging to change the engine on the plane while you’re flying it.

# Q&A