Regulatory and Compliance

February 28, 2014

Jorge Rey, CISA, CISM, CGEIT
Justin Gwin, CPA, CISA

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

During the course

of this presentation….

- ✓ **HIPAA Omnibus Rule**
- ✓ **Service Organization Control (SOC) Reports – Trust Services Principles**
- ✓ **COSO 2013**

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

HIPAA OMNIBUS RULE

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Important Final Omnibus Rule Dates

- ✓ **Publication Date:** January 25, 2013
- ✓ **Effective Date:** March 26, 2013
- ✓ **Compliance Date:** September 23, 2013
- ✓ **Business Associate Agreement Compliance Date:** September 22, 2014
  For “grandfathered” BAAs

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

OMNIBUS RULE
TOP 6

- Many more entities are Business Associates
- Business Associates are now directly subject to HIPAA in many regards
- Breach notification standard is greatly changed
- Marketing rules are updated
- Individual rights are expanded, particularly with respect to ePHI and genetic information
- Monetary penalties are tiered

Business Associates Changes

Category of entities that will be considered Business Associates has been expanded to include:

- Entities that transmit and need routine access to Protected Health Information (such as Health Information Organizations, and E-Prescribing Gateways)
- Personal Health Records/Electronic Health Records who serve Covered Entities
- Subcontractors who create, receive, maintain, or transmit PHI for a Business Associate.

BREACH

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised.

Unless the PHI was unreadable or undecipherable, the risk assessment must justify not disclosing a breach.

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Transition

Business Associates need to:

- Comply with the HIPAA Privacy & Security Rule
- Implement Breach Notification Policies
- Develop a Business Associate Agreement for downstream subcontractors
- Be ready to provide access to PHI/ePHI
- Comply with OCR/HHS Investigations
- Comply with the HIPAA Privacy & Security Rule

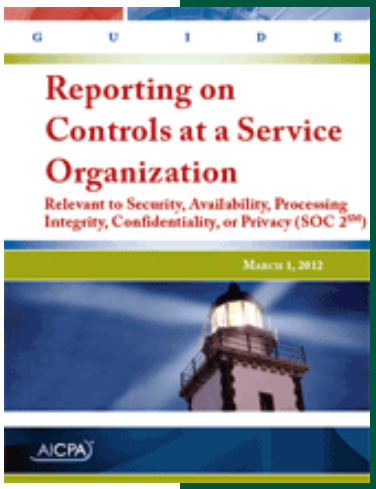
TRUST SERVICES PRINCIPLES AND CRITERIA

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Important Dates

- ✓ **SAS 70:** April 1992
- ✓ **SOC 1 / SSAE 16 & SOC 2 / 3:** April 2010
  Effective for periods ending on or after June 15, 2011.
- ✓ **Updated Trust Services:** 2009 version superseded by the 2013 version.

  Effective for periods ending on or after December 15,2014.Early implementation is permitted.



KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Why Update?

- **Restructuring of the trust services principles and criteria:** The principles and criteria for security, availability, processing integrity, and confidentiality are restructured into (1) common criteria that is applicable to all four principles, and (2) criteria applicable only to a single principle. The criteria related to the privacy principle contained in the generally accepted privacy principles (GAPP) are being revised separately.

- **Risk assessment:** To illustrate the linkage between criteria, risks, and controls, appendix B, "Illustrative Risks and Controls," was developed to provide examples of risks that may prevent the criteria from being met, as well as examples of controls that would address those risks.

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION CERTIFIED PUBLIC ACCOUNTANTS

SOC 2/SOC 3 Reports

	Operational Controls	
	SOC 2	SOC 3
Scope of system	• Infrastructure • Software • Procedures • People • Data	
Domains covered	• Security • Availability • Processing integrity • Confidentiality • Privacy	
Controls / Criteria to be tested	• Principles are selected by the service organization • Specific criteria is used instead of control objectives	

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

SOC 2/SOC 3 Trust Services Principles

Domain	*Trust Services Principle*
Security	• The system is protected against unauthorized access (both physical and logical).
Availability	• The system is available for operation and use as committed or agreed.
Processing Integrity	• System processing is complete, accurate, timely, and authorized.
Confidentiality	• Information designated as confidential is protected as committed or agreed.
Privacy	• Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

SOC 2/SOC 3 Trust Services Common Criteria

1. Organization and management
2. Communications
3. Risk management and design and implementation of controls
4. Monitoring of controls
5. Logical and physical access controls
6. System operations
7. Change management

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Transition

- Use the trust services framework to identify common risks
- Request from vendors or (if you are a vendor) provide compliance with regulations (HIPAA, GLBA), standards (ISO 27001, PCI, Cloud Controls Matrix), risks (disaster recovery)
- Use the framework for other controls (insurance)

COSO'S 2013 INTERNAL CONTROL FRAMEWORK

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS

Presentation of the COSO Model

- COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting ("Treadway Commission"), an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting.

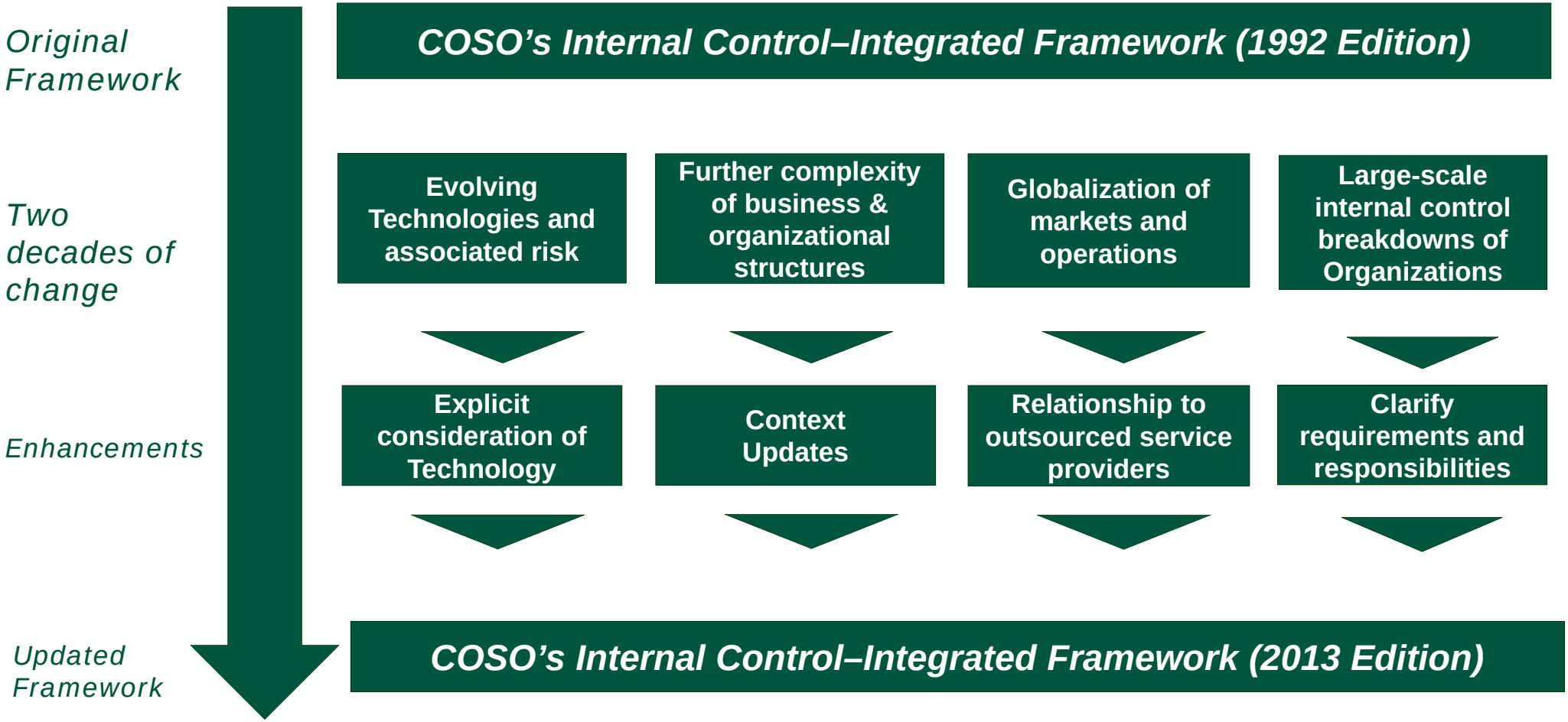
- The Treadway Commission was sponsored jointly by five major professional associations headquartered in the United States:
  - American Accounting Association (AAA);
  - American Institute of Certified Public Accountants (AICPA);
  - Financial Executives International (FEI);
  - Institute of Internal Auditors (IIA); and
  - Institute of Management Accountants (IMA).

- COSO's goal is to provide thought leadership dealing with three interrelated subjects: enterprise risk management, internal control, and fraud deterrence.

- The Treadway Commission published a report in 1987, which called for a study to develop a common framework for internal control. This resulted in the 1992 publication of COSO's *Internal Control – Integrated Framework*.

Committee of Sponsoring Organizations of the Treadway Commission

“If it ain’t broke, don’t fix it” – Why update?



Project

COSO
Board of Directors

PwC
Author &
Project Leader

COSO Advisory Council

- AICPA
- AAA
- FEI
- IIA
- IMA
- Public Accounting Firms
- Regulatory observers (SEC, GAO, FDIC, PCAOB)
- Others (IFAC, ISACA, others)

Stakeholders

Over 700 stakeholders in Framework responded to global survey during 2011

Over 200 stakeholders publically commented on proposed updates to Framework during first quarter of 2012

Over 50 stakeholders publically commented on proposed updates in last quarter of 2012

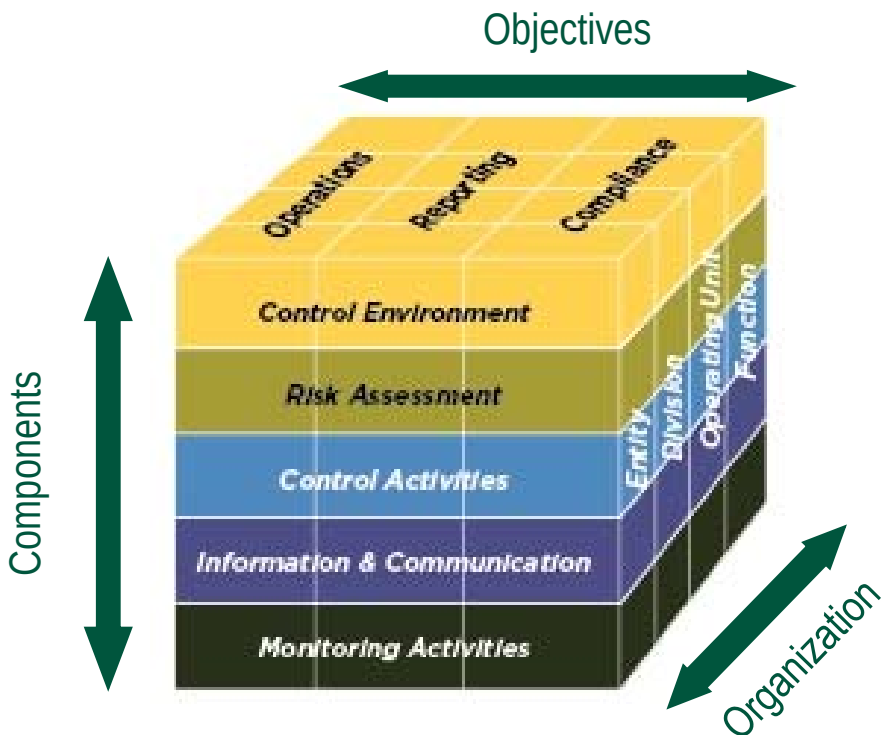
Impact

- Nearly all U.S. public companies rely on the 1992 framework to comply with internal control reporting requirements under Sarbanes-Oxley.
- Users are encouraged to transition applications and related documentation to the updated Framework as soon as feasible since the updated Framework will supersede original Framework at the end of the transition period (***December 15, 2014***)
- During the transition period, external reporting should disclose whether the original or updated version of the Framework was used.

"The longer issuers continue to use the 1992 framework, the more likely they are to receive questions about whether the continued use of the 1992 framework satisfies the SEC's requirement for a suitable, recognized control framework "

What is not changing…

- Core definition of internal control.
- Familiarity of the cube.
- Each of the five components of internal control are required for effective internal control.
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness.



What is changing…

- Fundamental concepts underlying five components articulated as principles.
- Changes in business and operating environments considered, including expanded relationships.
- Reporting objective expanded to include financial/non-financial, internal/external.
- Consideration of fraud and its relationship to internal control is more prominent.
- Increased reliance on IT controls explicitly considered.
- Enhances to Governance expectation for oversight, accountability, and competence.

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION CERTIFIED PUBLIC ACCOUNTANTS

Principles of effective internal control

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. BOD demonstrates independence & exercises oversight 3. Establishes of structure, authority, reporting lines and responsibility 4. Commitment to attract, develop, and retain competent individuals 5. Enforces accountability for internal control responsibilities
Risk Assessment	6. Specifies suitable objectives with sufficient clarity 7. Identifies and analyzes risk 8. Assesses potential fraud risk in achievement of objectives 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities to mitigate risks 11. Selects and develops general controls over technology 12. Deploys controls through establishment of policies and procedures
Information & Communication	13. Uses relevant, quality information to support function of IC 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies / takes corrective action

Example Points of Focus

11. The organization selects and develops general control activities over technology to support the achievement of objectives	- Determines dependency between the use of technology in business process and technology general controls - Establishes relevant technology infrastructure control activities - Establishes relevant security management process control activities - Establishes relevant technology acquisition, development, and maintenance process control activities
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control	- Identifies information requirements - Captures internal and external sources of data - Processes relevant data into information - Maintains quality throughout processing - Considers costs and benefits
15. The organization communicates with external parties regarding matters affecting the functioning of internal control	- Communicates to external parties - Enables inbound communication - Provides separate communication lines - Communicates with the Board of Directors - Selects relevant method of communication

Transition

STEP 5

DRIVE CONTINOUS IMPROVEMENT

STEP 4

DEVELOP AND EXECUTE COSO TRANSITION PLAN

STEP 3

FACILITATE BROAD AWARENESS AND TRAINING

STEP 2

CONDUCT PRELIMINARY IMPACT ASSESSMENT

STEP 1

DEVELOP AWARENESS, EXPERTISE, AND ALIGNMENT

Questions, Now or Later

Jorge Rey CISA, CISM, CGEIT
E: jrey@kaufmanrossin.com
P: 954.315.7178

Justin Gwin, CPA, CISA
E: jgwin@kaufmanrossin.com
P: 305.646.6088

KAUFMAN ROSSIN & CO. PROFESSIONAL ASSOCIATION
CERTIFIED PUBLIC ACCOUNTANTS