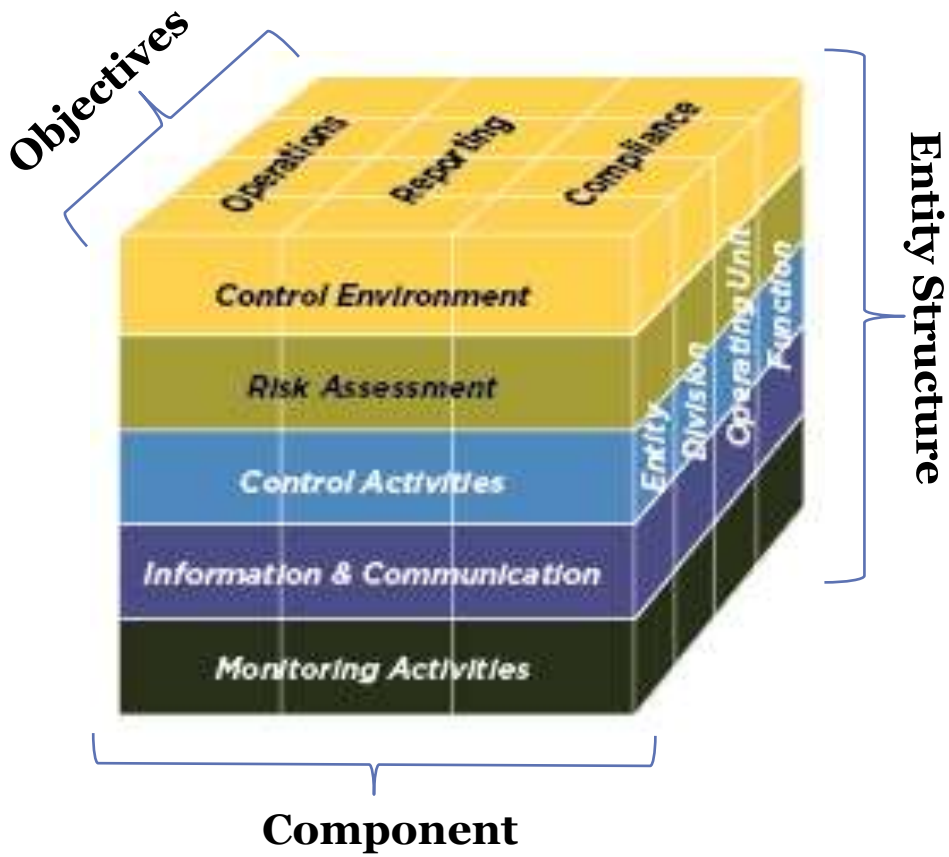
Implementing COSO, Part II: Leveraging the Control Framework Beyond ICFR

Kenneth Blomster, Partner, Risk Assurance, PwC
Aaron Garcia, Director, Risk Assurance, PwC

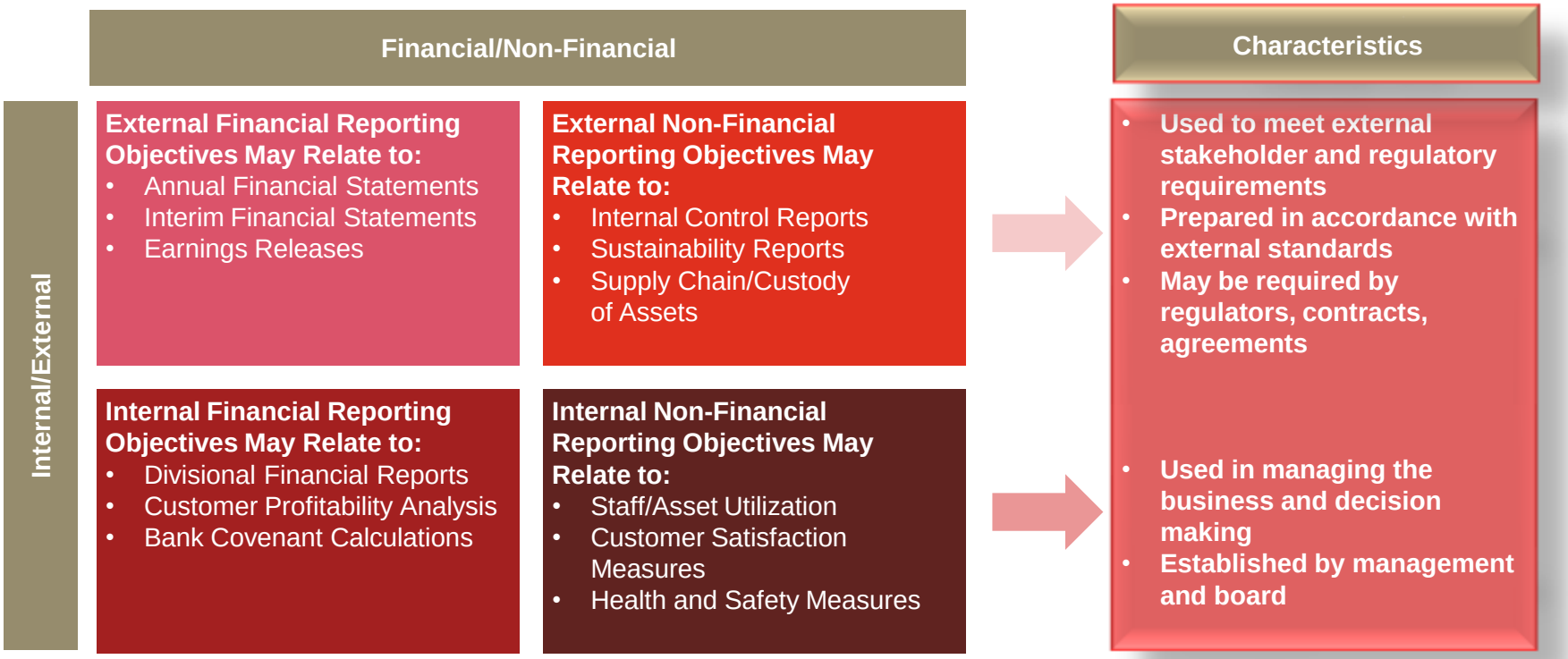
pwc

2013 COSO internal controls cube

- **Five Components**
- **Multiple Units:**
  - **Entity**
  - **Divisions**
  - **Operating Units**
  - **Functions**
- **Three Categories of Objectives (can be applied narrowly or broadly)**



The "reporting" objective is further divided into four sub-objectives



Broadening the scope of applying the 2013 framework

Operations and Compliance Objectives

Operations Objectives:

- Examples Include
  - Productivity Objectives
  - Sustainability Goals
  - Safeguarding of Assets

Compliance Objectives:

- Examples Include
  - Foreign Corrupt Practices Act (FCPA) Compliance
  - Sector-Specific Regulations
  - Compliance w/Employment Laws
  - Environmental Laws

Non-ICFR Reporting Objectives

External Non-Financial Reporting Objectives:

- Examples Include
  - Internal Control Reports
  - Sustainability Reports
  - Supply Chain/Custody of Assets Reports

Internal Financial Reporting Objectives:

- Examples Include
  - Divisional Financial Reports
  - Customer Profitability Analysis
  - Bank Covenant Calculations

Internal Non-Financial Reporting Objectives:

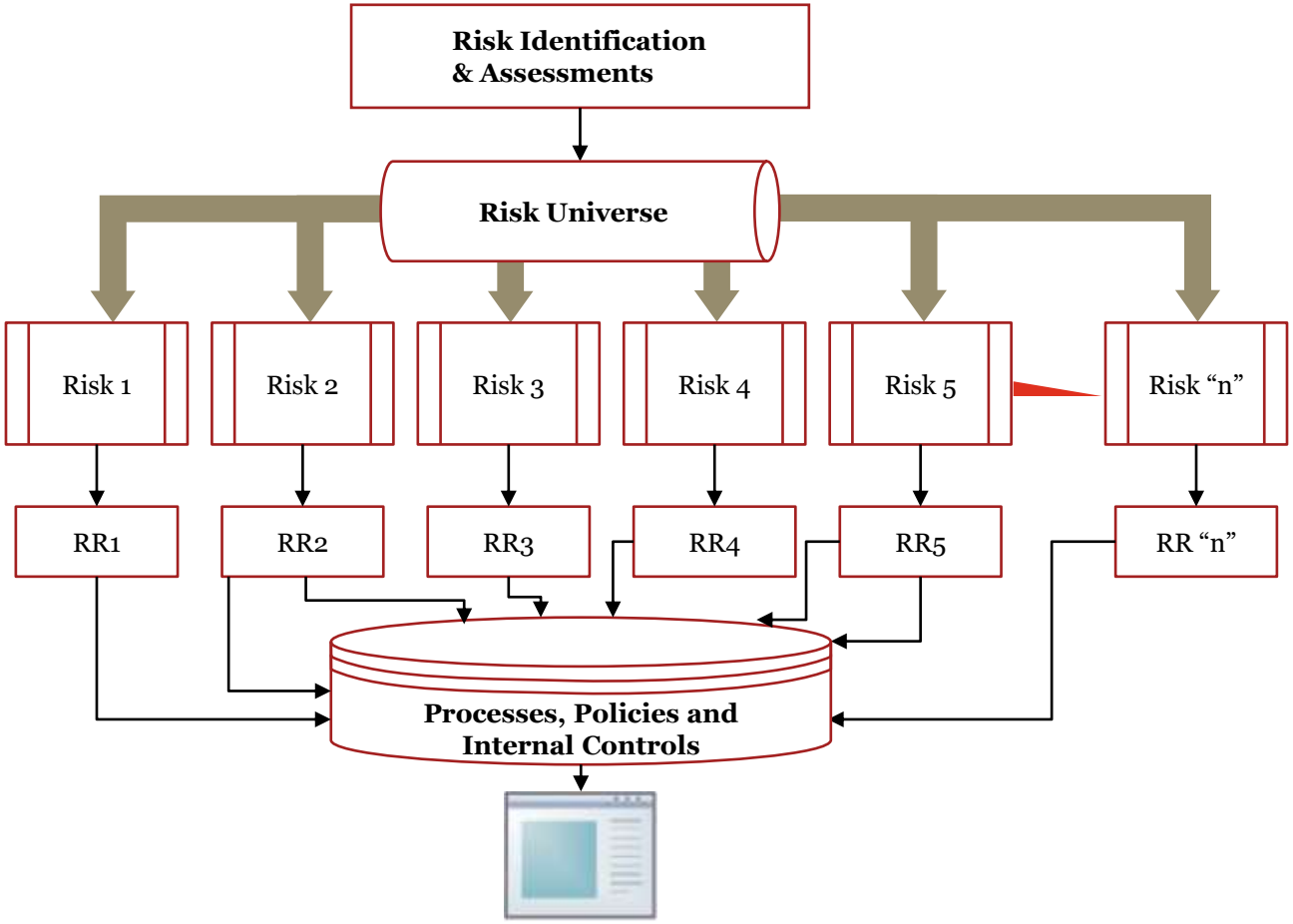
- Examples Include
  - Staff/Asset Utilization Measures
  - Customer Satisfaction Measures
  - Health and Safety Measures

Accumulating Risk Responses

Risk Responses

Gather and Collate Risk Response, including Assessments

GRC Dashboard



Questions for management to consider

Expectations of internal control have been expanding, demanding that organizations design systems of internal controls responsive to an exceedingly complex universe of risks. Such a broader view underpins COSO's revised Internal Control Framework. The updated Framework lays a foundation for organizations to integrate internal control systems throughout the organization. By aligning internal control with the organization's most important operational, reporting and compliance objectives, companies can achieve numerous synergies and establish a common framework for evaluating internal controls throughout the organization.

Has your company historically used the COSO Internal Control Framework for purposes of reporting on Sarbanes Oxley (SoX)?

Is your monitoring of internal controls designed to achieve compliance, operations and internal reporting objectives aligned with your monitoring of internal controls over external financial reporting?

Is your organization subject to numerous regulations? Have you developed processes and controls to ensure compliance with those regulations?

Are your organization's non- Internal Control Over Financial Reporting (ICFR) controls subject to regulatory criteria (e.g., Health Insurance Portability and Accountability Act (HIPAA), Basel)?

How effective are your organization's IT governance processes at effectively producing strategic business value and meeting the needs of my business and my customers?

Does management employ disparate financial and planning systems (e.g., Financial Systems, Enterprise Resource Planning, Customer Relationship Management (CRM), multiple spreadsheets with multiple interfaces, etc.) in managing the business?

Change-Drivers: Has your organization experienced:

Major Business Changes - Growth, restructurings, new markets, products, and partners - which introduce new risks?

Increasing Regulatory Oversight and Scrutiny - Increasing regulator expectations as to the strength of operating effectiveness of Enterprise Risk Management (ERM) frameworks?

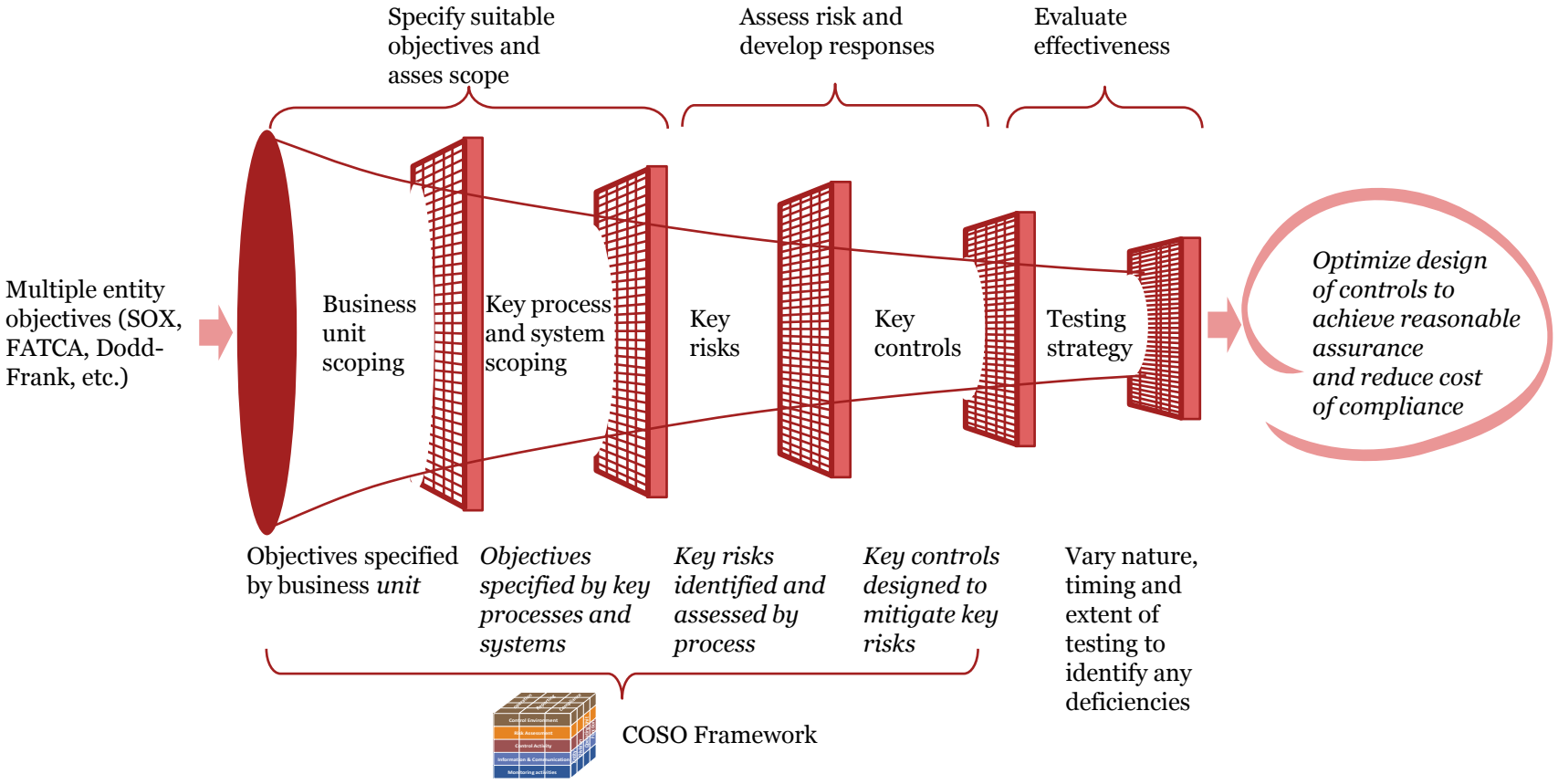
Greater Complexity in Operating Models and Structures - Taking on new service providers or other partners which change the company's risk profile?

Increased Reliance on Technology - New uses of existing technology and new tech investments which may impact risks?

New and Evolving Expectations for Non-Financial Reporting - Stakeholders and regulators seek greater transparency and confidence in reporting processes?

Business Failures and Reputational Risk Events - Businesses in many industries need to re-build trust with customers and stakeholders?

2013 framework describes a process for designing, operating and evaluating effective internal control for multiple objectives



Sample sector-specific objectives other than ICFR

Pharma & LS

- Physician transparency reporting (i.e., Sunshine Act) for state and federal disclosures
- Trade compliance
- Pharmacy 340b compliance (Medicaid rebate)
- HIPAA and International privacy laws
- Annual Pharma fee (for manufacturers or importers of branded prescription drugs)
- Medical Device Excise Tax (MDET) – 2.3% excise tax on sale of certain medical device products
- Unique Device Identification (UDI) – FDA regulation requiring specific labeling and identification requirements to improve recall process

Defense

- FCPA and anti-corruption risk
- Regulatory cost issues
- Financial/contract management requirements of federal contracting
- Export control regulations for tangible and intangible exports
- Int'l Traffic in Arms Regulations/Export Administration Regulations
- DCAA Audit Coordination
- Contractor Responsibility Standards
- Certified Cost or Pricing Data
- Contractor code of business ethics

HC Providers

- Overall Compliance program effectiveness
- Value based purchasing and quality reporting
- Readmission Reduction program
- ICD-10
- Electronic Health Record (EHR) implementations and clinical transformation, including:
  - Meaningful Use Attestation
  - Impact on Revenue Cycle
  - Impact on Clinical Applications
- HIPAA Omnibus/HITECH Compliance (Privacy/Security)
- Cyber-Security
- Five Star Quality Rating System

Fin'l Services

- Fraud - including Anti Money Laundering, Know Your Customer and Trading Fraud
- Model Governance/ Validation– Design and Documentation
- Third Party Risk Management (TPRM)
- US Own Risk and Solvency Assessment (ORSA)
- Principals based life reserving (PBR)
- Dodd-Frank Initiatives: Federal Insurance Office, Systemic Risk and Insurance Thrifts
- Analytics and big data in underwriting, pricing and claims

Illustrative output – mapping policies, processes and controls to risks and principles

Objective Category =>	External Financial Reporting	External Non-Financial Reporting		Internal Financial Reporting		Internal Non-Financial Reporting		Operations		Compliance	
Objective =>	Accuracy & Completeness of releases, quarterly and annual financial reporting	Sustainability Reporting	Reporting Proxy Information	Divisional Financial Reports	Bank Covenant Calculations	Staff/Asset Utilization Measures	lth and Safety Meas	Cyber-Security	Customer Experience	Sector-Specific Regulations	
Risks/ Opportunities =>	Inaccurate or Incomplete Financial Reporting	Conflicts Minerals Reporting	Inaccurate Information in Proxy	Risk of Fraudulant Internal Reporting	Changes to Financing and Capital Availability	High Employee Turnover Rate	Work Site Inspection	Confidential Data Protection	Deterioration in Customer experience	Occupational Health and Safety Regulations	Health Insurance Portability and Accountability Act
Principle											
1	C1, C3, C9, C10	C5, C9, C12	C5, C9, C12	C4, C25, C28	C17, C21, C21	C11, C22, C45	C44, C64	C33, C65	C88	C18, C21, C36	C1, C19, C22, C95
2	C10, C12, C67	C15, C20	C18, C32, C55	C45, C80	C28, C35	C14, C22, C26	C45, C90, C92	C35, C79	C21, C24	C2, C15, C25	C24, C55, C63
3	C10, C15, C25	C5, C23, C92	C27, C43	C66, C91	C32, C34	C56	C52, C72	C45, C90, C92	C15, C20	C13, C39, C43	C28, C35
4	C11, C22, C45	C18, C21, C36	C4, C8	C30, C45	C28, C39, C63	C14, C19, C36	C18, C25, C43	C13	C12, C43, C87	C60, C86	C4, C8
V V	V V	V V		V V	V V	V V	V V	V V	V V	V V	V V
17	C3, C15, C28	C14, C22, C26	C19, C54, C90	C24, C55, C63	C40, C51, C57	C13, C48	C51, C65	C6, C7, C35	C18, C24	C3, C15, C28	C28, C39, C63

Illustrative output – Internal control design/documentation assessments

				Assessment of design		Assessment of documentation		Overall assessment
Control Number	**Control Description**	**Highest Risk Rating (a)**	**Location of Control**	**Assessment**	**Date of Assessment**	**Assessment**	**Date of Assessment**	**Strength of Control (b)**
C1	*Insert control description*	Low	Location D	*Insert assessment of Design*	1/19/2012	*Insert assessment of documentation*	6/16/2012	Strong
C2	*Insert control description*	Moderate	Location A Location D Location F	*Insert assessment of Design*	4/1/2012	*Insert assessment of documentation*	11/14/2012	Medium Strong Minor
C3	*Insert control description*	High	Location A	*Insert assessment of Design*	1/5/2012	*Insert assessment of documentation*	9/26/2012	Medium
C4	*Insert control description*	Moderate	Location R	*Insert assessment of Design*	4/5/2012	*Insert assessment of documentation*	6/27/2012	Strong
C5	*Insert control description*	High	Location H	*Insert assessment of Design*	2/12/2012	*Insert assessment of documentation*	10/10/2012	Strong
V	V	V	V	V	V	V	V	V
V	V	V	V	V	V	V	V	V
V	V	V	V	V	V	V	V	V
C100	*Insert control description*	Moderate	Location C	*Insert assessment of Design*	2/24/2012	*Insert assessment of documentation*	6/2/2012	Medium

Note (a): Because a given control may be mapped to multiple Risks or Opportunities, this column reflects the highest risk rating for those Risks/Opportunities to which the control is mapped.

Note (b): After considering the description, and assessing the design and documentation of the control, this column captures management's overall assessment of the strength of the control in achieving the underlying principle(s) assuming it is functioning effectively.

Illustrative output – Operating effectiveness assessments

				Assessment of operating effectiveness		
Control Number	**Control Description**	**Highest Risk Rating (a)**	**Location of Control**	**Assessment**	**Testing Results (1-10; 10 best)**	**Date of Assessment**
C1	*Insert control description*	Low	Location D	*Insert detailed assessment*	6	1/9/2012
C2	*Insert control description*	Moderate	Location A	*Insert detailed assessment*	10	4/1/2012
			Location D		9	6/3/2012
			Location F		8	8/5/2012
C3	*Insert control description*	High	Location A	*Insert detailed assessment*	10	1/5/2012
C4	*Insert control description*	Moderate	Location R	*Insert detailed assessment*	7	4/5/2012
C5	*Insert control description*	High	Location H	*Insert detailed assessment*	5	2/12/2012
V	V	V	V	V	V	V
V	V	V	V	V	V	V
V	V	V	V	V	V	V
C100	*Insert control description*	Moderate	Location C	*Insert detailed assessment*	9	2/24/2012

Leveraging ICFR for other suitable objectives

Optimize potential synergies in designing processes and controls intended to support multiple objectives to enhance effectiveness and efficiency

Principles in COSO framework (2013)	Potential synergies
1. Demonstrates Commitment to Integrity and Ethical Values	High
2. Exercises Oversight Responsibility	High
3. Establishes Structure, Authority, and Responsibility	High
4. Demonstrates Commitment to Competence	High
5. Enforces Accountability	High
6. Specifies Suitable Objectives	Low
7. Identifies and Analyzes Risk	Low
8. Assesses Fraud Risk	Moderate
9. Identifies and Analyzes Significant Change	Moderate
10. Selects and Develops Control Activities	Low
11. Selects and Develops General Controls over Technology	Moderate
12. Deploys through Policies and Procedures	Low to Moderate
13. Uses Relevant Information	Low to Moderate
14. Communicates Internally	High
15. Communicates Externally	High
16. Conducts Ongoing and/or Separate Evaluations	High
17. Evaluates and Communicates Deficiencies	High

Take a fresh look at ICFR and other applications using the 2013 framework

Focusing on ICFR

Conduct preliminary assessment of ICFR vs. COSO Framework (2013)

Take action to remediate any deficiencies before evaluation required by SOX

Optimize design of ICFR

Take a fresh look at design and operation of ICFR to enhance effectiveness and reduce cost of compliance

Making the most of it

Use COSO Framework to implement/enhance and evaluate effectiveness of internal control supporting objectives beyond ICFR

- Using COSO Framework (2013) for SOX reporting supports the business case for using a common approach for all suitable objectives
- Rigorous design and operation (and documentation) of entity's ICFR and SOX program may not be necessary for other objectives

Thank you

Kenneth Blomster, partner, risk assurance, PwC
kenneth.blomster@us.pwc.com

Aaron Garcia, director, risk assurance, PwC
aaron.garcia@us.pwc.com