AFERM

Association for Federal Enterprise Risk Management

ERM From a COSO Perspective

Thought Leadership for Your Organization

Eighth Annual Federal Enterprise Risk Management Summit

November 3-4, 2015

Robert Hirth, Chairman

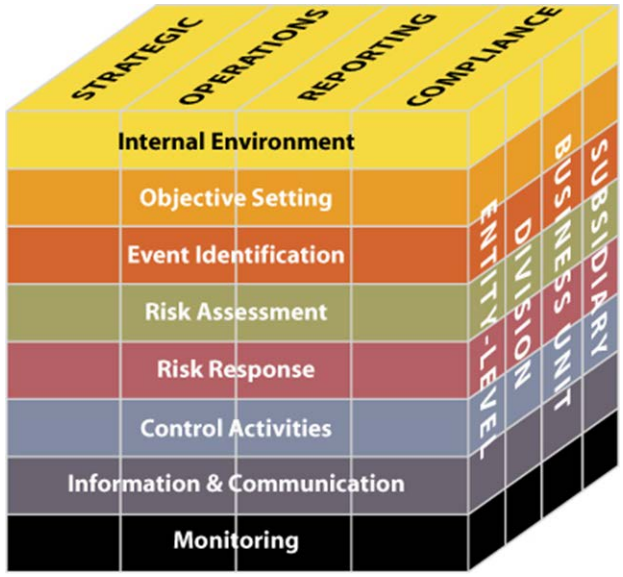
COSO

I welcome your comments, observations, critique, complaints, encouragement, questions and support…

Incrementalism…

“How would you like to meet more of your objectives more of the time? “

Our Next Challenge and Opportunity



ERM Really Not Required?

"Disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure."

Some Great Examples…

Walmart

usbank

Or Should it Be ?

- Improves Transparency
- Addresses change and challenges
- Enhances governance
- Helps facilitate better internal control
- Deepens understanding of operations
- Better communication of the strategy
- Reduces losses and mistakes

Public vs. Private Sector… Not so Different ?

Yes, You have Your Challenges…

- How to get started, value proposition, funding
- Support from leadership and tone at and from the top
- Changes in Leadership
- Conflicting priorities
- What methods and approaches to use
- Communication and information
- Monitoring- how's it going- is it making a difference?

COSO Can Help ALL Organizations!

A Suitable Model Everywhere…

Is this the Real Reason for ERM?...

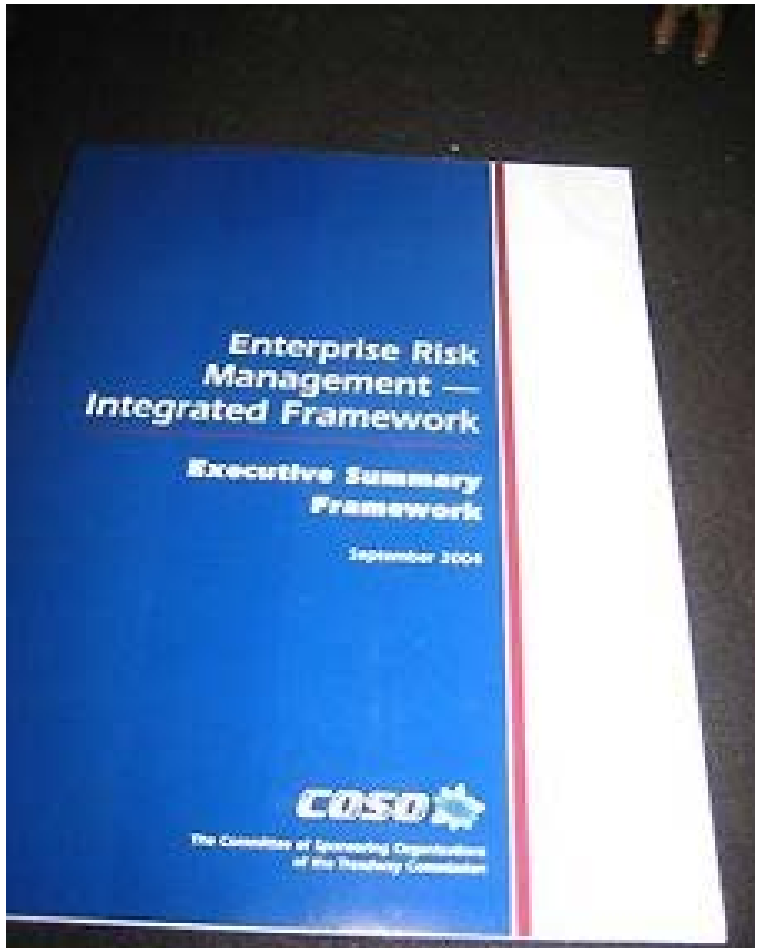
COSO Announces Project to Update *Enterprise Risk Management- Integrated Framework*

- **NEW YORK, October 21, 2014** -- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) today announced a project to review and update the 2004 *Enterprise Risk Management–Integrated Framework* (Framework).
- The Framework, originally published in 2004, is a widely accepted framework used by management to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase stakeholder value.
- This initiative is intended to enhance the Framework's content and relevance in an increasingly complex business environment **so that organizations worldwide can attain better value from their enterprise risk management programs.** The initiative also will develop tools to assist management in reporting risk information and in reviewing and assessing the application of enterprise risk management.

Why Update the Framework Now?

- Concepts and practices have evolved
- Lessons learned
- Bar raised with respect to enterprise risk management
- Business and operating environments more complex, technologically driven, and global in scale
- Stakeholders more engaged, seeking greater transparency and accountability
- Risk discussions increasingly prominent at the board level

We Are Updating This…



Not This…

Important Summarization

- Every entity exists to provide value for its stakeholders
- All entities face uncertainty
- The challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value
- Uncertainty presents both risk and opportunity
- ERM enables management to effectively deal with uncertainty and associated risk and opportunity

Value is maximized when managements sets strategy and objectives to strike an optimal balance between growth and related risks, and efficiently and effectively deploys resources in pursuit of an entity's objectives.

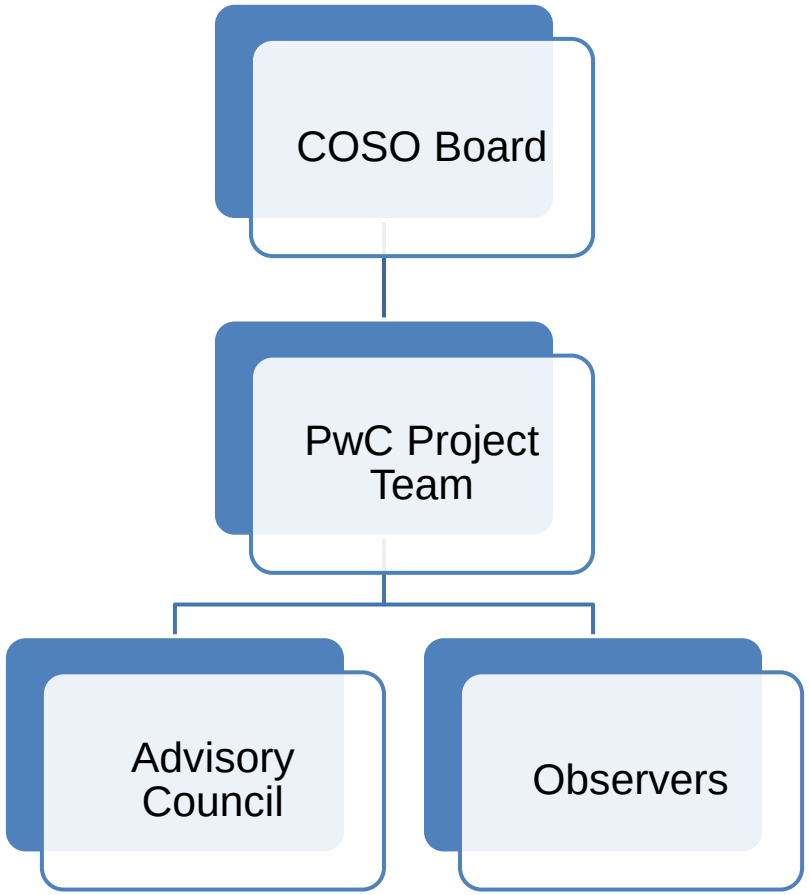
Included in 2004 COSO ERM…

- Aligning Risk Appetite and Strategy
- Enhancing Risk Response Decisions
- Reducing Operational Surprises and Losses
- Identifying and Managing Multiple and Cross-enterprise Risks
- Seizing Opportunities
- Improving Deployment of Capital

In Case You Had Forgotten…

"Enterprise Rick Management is a process affected by an entity's board of directors, management and other personnel, applied in a strategic setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

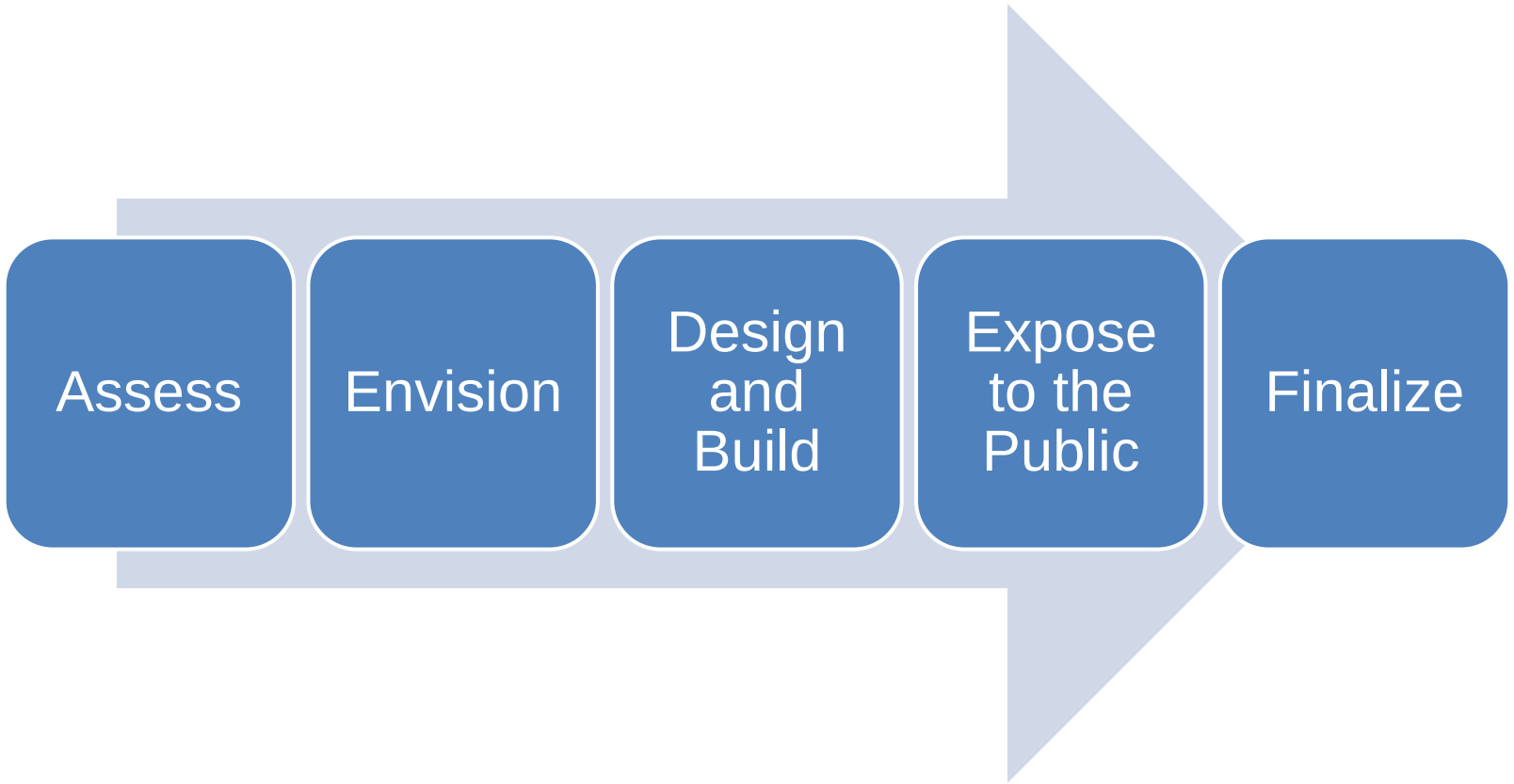
Project Governance



Advisory Council and Observers:

- Consists of over 25 professionals
- Provides input, expertise, feedback, insight, and ideas throughout the update.
- Obtains and synthesizes feedback from their respective constituency, organization, industry

Project Approach



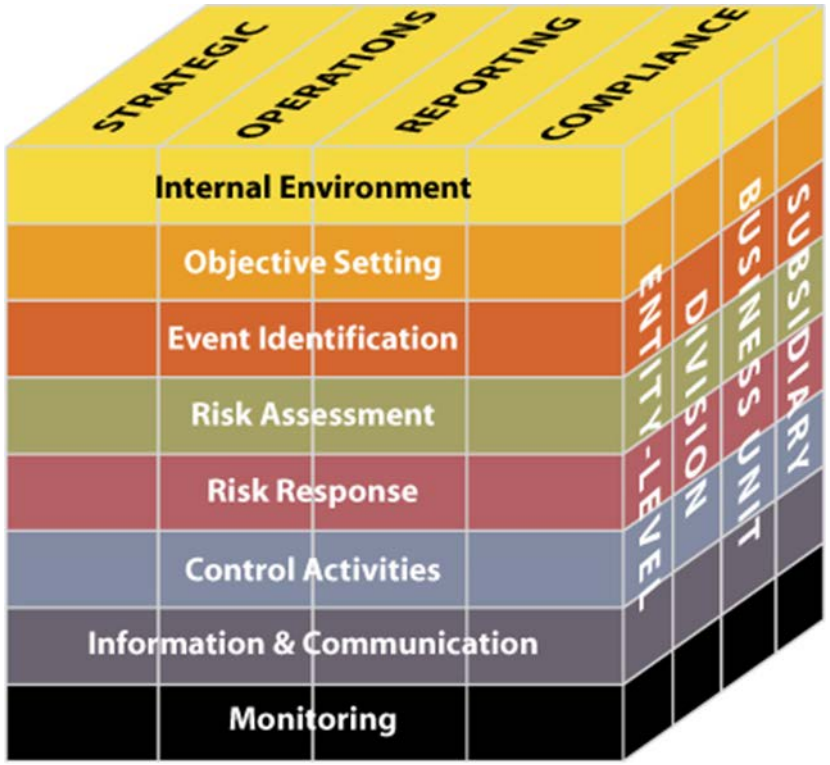
Advisory Council

- **CRO's**
- Risk Luminaries
- Risk Management, ERM University Professors
- Chief Audit Executives
- Accounting Firm Risk Practice Partners
- Board Members
- Public Sector
- Company Executives

Official Observers

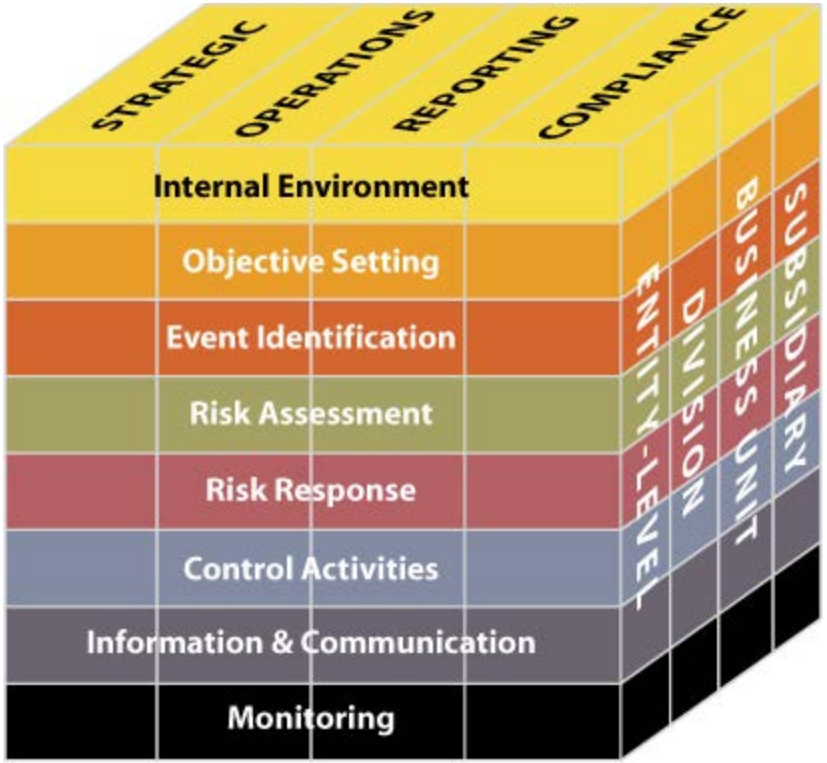
- FDIC
- OIG
- IMA
- IFAC
- RIMS
- ISACA
- China Ministry of Finance (Special)
- SEC- declined
- PCAOB determined to not be relevant given no audit requirements

The 2004 ERM Cube…



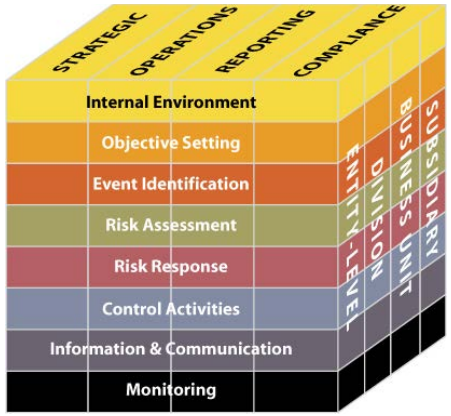
Key Goals

- Usefulness
- Clarity
- Value Proposition
- Relevance
- Suitability
- Effectiveness



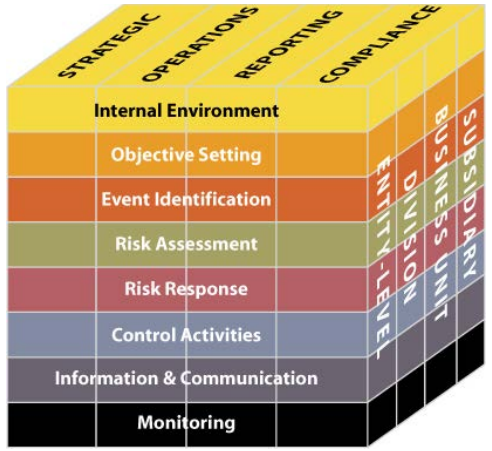
Key ERM Framework Questions

- What is your ideal view of ERM?
- What are the 3 strengths of the 2004 framework?
- What are the 3 most significant areas for update and revision?
- What should the framework do to stay relevant for the next 10 years?
- What would improve user acceptance?



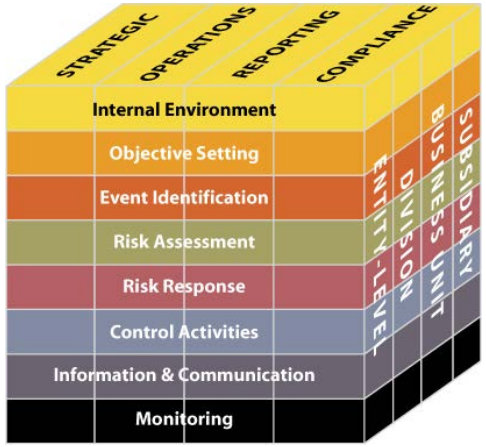
What is Your Ideal View of ERM?

- Baked in, imbedded, not a bolt-on
- Accelerates growth and success
- Improves decision making and performance
- Discipline, not a process
- Ability to take on more risk
- Continuous, identifiable, structured
- ERM is NOT a roll-up, aggregation of risk at lower levels



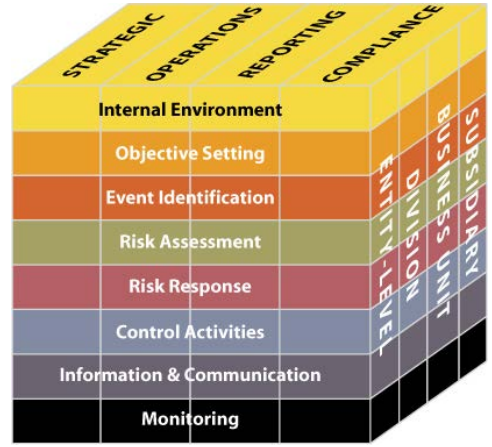
What are the 3 Strengths of the 2004 Framework?

- Link to Strategy setting
- Linkage to objectives
- 4 buckets(S, O, F, C)
- Risk response/treatments
- Linkage to internal control
- Evaluation/Attestation criteria concept
- Board oversight
- Due process
- The Cube?



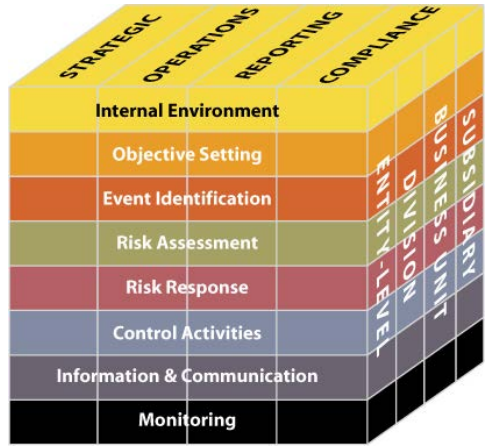
What are the 3 Most Significant Areas for Update and Revision?

- Principles and points of focus
- Definition ?
- Usefulness
- Maturity models
- Format, structure, length, complexity
- Opportunity side of risk



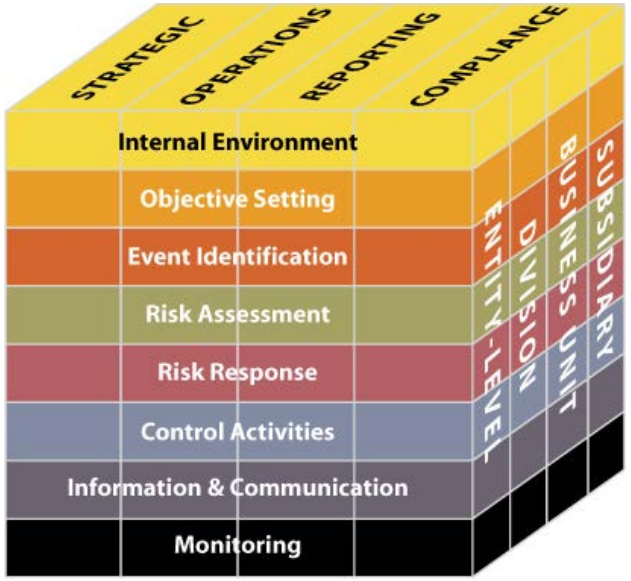
What Should the Framework Do to Stay Relevant for the Next 10 years?

- Maturity Model
- Sustainability
- Governance
- Principles
- Stay a framework
- Add update materials, papers

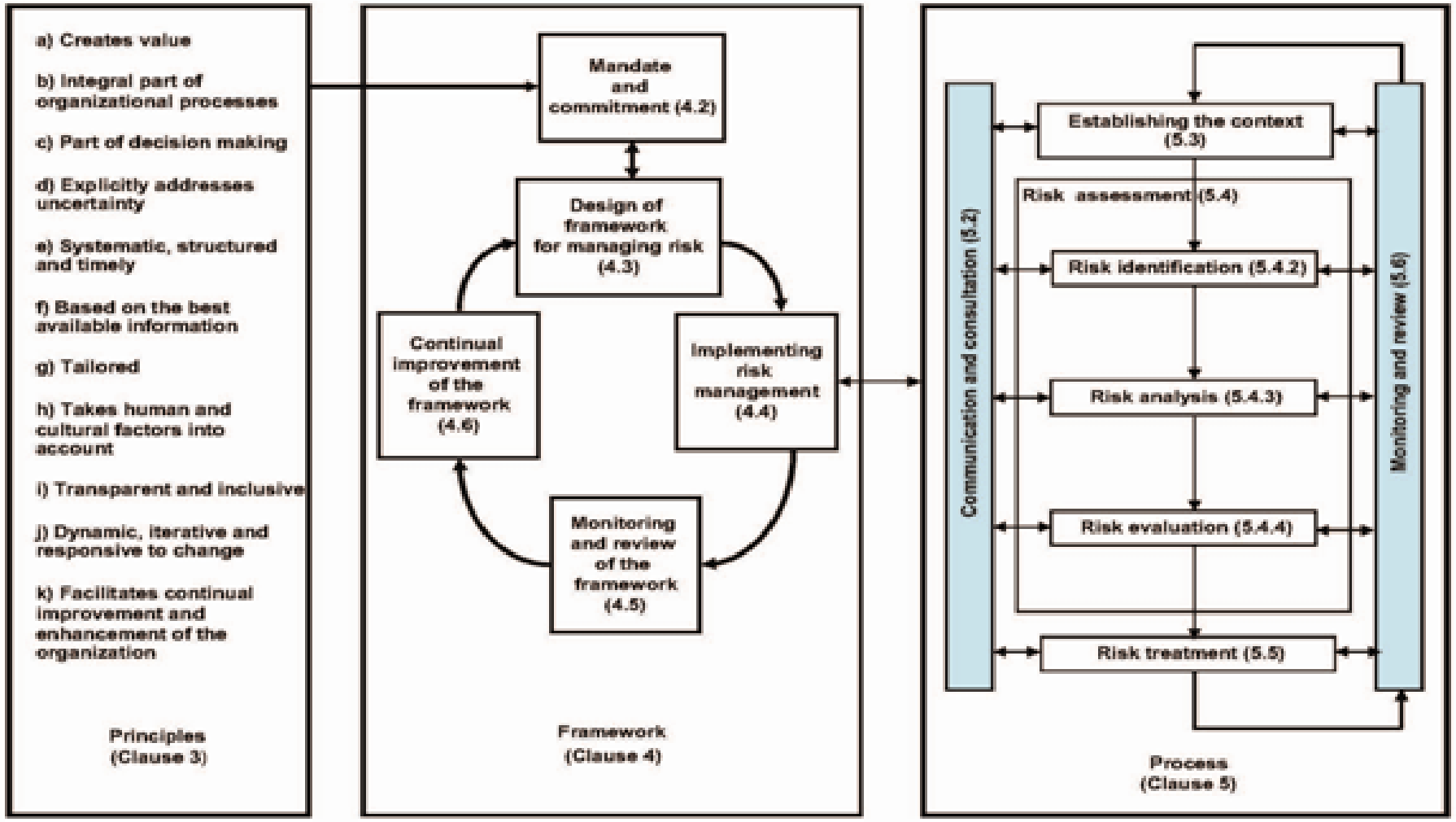


What Would Improve User Acceptance?

- CEO and Board buy-in
- Case studies
- Example successes
- Improve value proposition
- More and better promotion
- Regulatory requirement



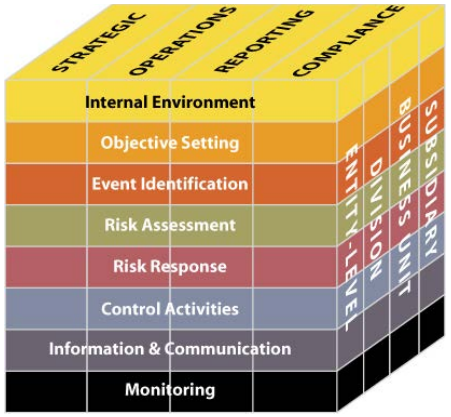
Comparison of ISO and COSO



Bridging Between ERM and Internal Control Frameworks

Document Structure

- We anticipate that the updated Framework **will apply principles and points of focus**
  - The 2004 Framework contained over 100 key principles in an appendix. The updated Framework will significantly reduce this number
- The Project Team will also be review aspects of the update including:
  - Components
  - Categories of objectives
  - The business model

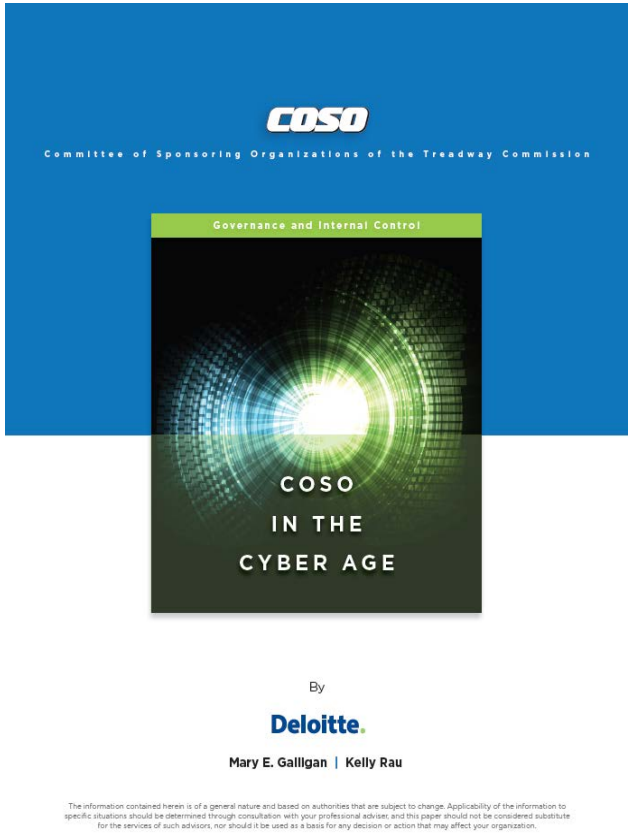


An Enhanced View…

"ERM is a discipline and mindset **imbedded throughout an organization** which **improves decision making** in governance, strategy setting, operations, reporting and compliance. It helps to **accelerate growth and enhance performance** by **more closely linking objectives to risk** and opportunity in a more formal and structured manner which **better protects and creates organizational value**. "

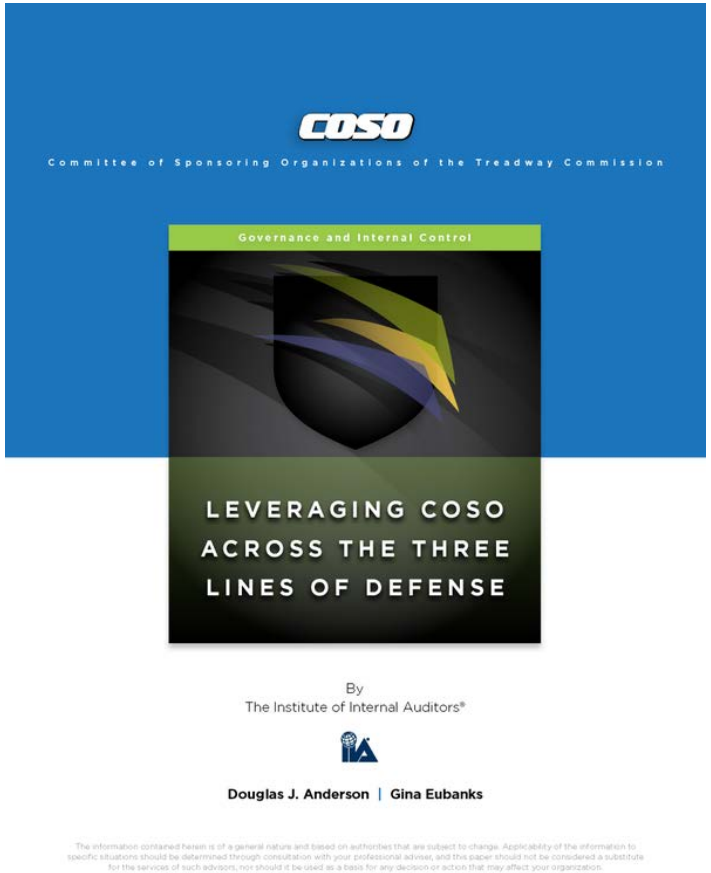
Incrementalism…

“How would you like to meet more of your objectives more of the time? “



COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has released COSO in the Cyber Age, a thought leadership paper that provides direction on how the Internal Control-Integrated Framework (2013) and the Enterprise Risk Management-Integrated Framework (2004) can help organizations effectively and efficiently evaluate and manage cyber risks.

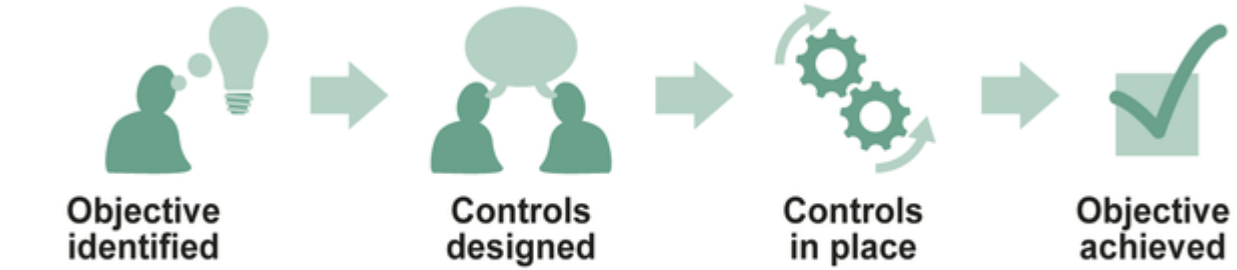


Leveraging COSO Across the Three Lines of Defense:

Advocates for clearly defining responsibilities for three aspects of risk: risk ownership, risk monitoring, and risk assurance. Respectively, functions that own and manage risks are the first line. Various risk control and compliance functions that monitor risks are the second line. Internal audit, which provides independent assurance on the effectiveness of control and compliance functions, is the third line.

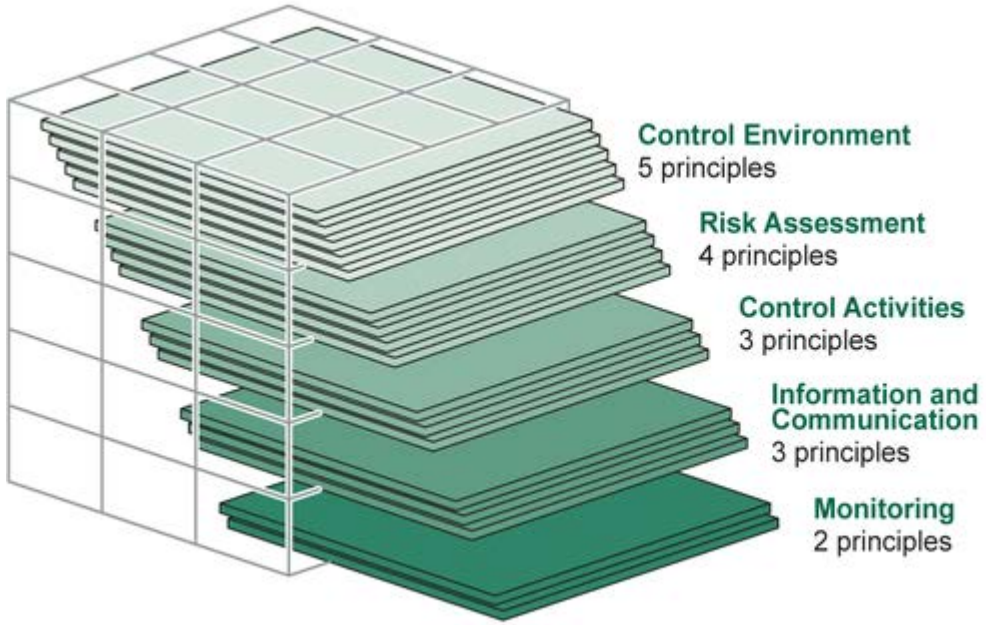
I'd Be Remiss…

.



Source: GAO. | GAO-14-704G

t.



Source: GAO. | GAO-14-704G


thank you
tenki
ขอขอบคุณคุณ
takk
спасибо
kam sah hamnida
je
hvala
הדות
dhanyavadagalu
tack
дзякуй
dziękuję
bedankt
blagodaram
mèsi
xièxie
tanemirt
gracias
rahmet
enkosi
mochchakkeram
trugarez
dank
djere dieuf
danke
kop khun krap
faafetai lava
arigatô
akun
shukriya
ありがとう
kia ora
dankon
děkuji
manana
diolch
gràçie
kiitos
spas
ačiū
grazzi
mamnun
barka
शुक्रिया
tau
dankie
gràcies
bayarlalaa
σας ευχαριστώ
teşekkür ederim
obrigada
chnorakaloutioun
tapadh leat
dhanyavad
gratias ago
sulpáy
sagolun
murakoze
taiku
mahalo
didi madloba
chokrane
rahmat
sukriya
obrigado
dakujem
misaotra
welalin
najis tuke
terima kasih
mercé
köszönöm
asante
grazie
謝謝
mersi
sobodi
nanni
vinaka
mauruuru
nandri
merci
go raibh maith agat
matondo
cảm ơn bạn
paldies
ngiyabonga