GRC and the New COSO Framework

Whole being greater than the sum of parts –

A holistic view of integration benefits and challenges

Presented By
Swami RV – Senior Director BFSI
Maclear
New COSO Framework and GRC Triad

What’s all the talk about…

Mission: Improve organizational performance and governance

- Align GRC [Governance, Risk and Compliance]
- IC Focused [Internal Controls]
- POF [Principles of Focus]
Control Environment

Principles advocated under the framework

- Commitment to Integrity and ethical values [T.A.T]
- Oversight responsibility of the board [SOX]
- Responsibilities through reporting lines [SOX / ISAE / PCAOB]
- Commitment to the workforce
- Accountability
Risk Assessment

Principles advocated under the framework

- Specify appropriate Objectives
- Identify and analyse Risks
  - EVALUATE FRAUD RISKS
- Identify and analyse changes that significantly impact internal controls
Control Activities

Principles advocated under the framework

- Control activities should *mitigate* risks
- Develop control activities throughout the entity and in all functions
- Policy and Procedures should drive control activities
Control Title Principles

Control Environment
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Risk Assessment
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication
13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies
Changes Driven by Updates …

Environment changes have driven Framework updates

- Expectations for governance oversight……
- Globalization of markets and operations……
- Changes and greater complexity in business…. 
- Demands & complexities in laws, rules regulations, & standards………..
- Technology / Assessment of Fraud
COSO Enables GRC or Vice Versa?

- COSO and GRC – Synonyms or subset?
- Internal controls elements / ERM / COSO – How they gel together with GRC
- Regulatory compliance – Is there enough mention in the new COSO framework?
- COSO more focused on the ‘G’ and the ‘R’ than the ‘C’ – Devil is in the details – ISO 31000
Bringing it all Together ....

- ERM / COSO
- SARBANES OXLEY
- PCAOB - AS 5
- ISAE 3402
- ISO 31000
- ITGC / COBIT / ITIL
- INTERNAL CONTROL – INTEGRATED FRAMEWORK

Enterprise Governance Risk Compliance
By Domain .... COSO and GRC

Tools for assessing effectiveness of System of Internal control (COSO 2013)

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

13. Uses relevant information
14. Communicates internally
15. Communicates externally

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Policy Management, Overall Dashboards for Oversight

Risk Management Framework

Control Management, Third Party Assessments

Communication through notifications, dashboards and alerts

Monitoring Dashboards
Key Challenges...

- Lack of a formal ongoing ethics program
- Not communicating expectations of integrity and ethics to third parties /OSPs
- Not considering the relevant types of fraud when performing risk assessment
- Inappropriately considering residual risk as against inherent risk
- Not performing OSP risk assessments
Key Challenges... Continued;

- Lack of a detailed, thoughtful risk assessment
- Increased potential for overrides
- Inadequate segregation of incompatible duties
- Lack of a data governance strategy – policies, standards defining control expectations
Conclusion

- No ‘One size fits all’ approach – holistically viewed at each entity level.
- New framework incorporates many business/regulatory driven changes that enable comprehensive e-GRC – GRC 2.0!!
- Effective Tone at the top / Steering Committee critical for successful transition
- Do not rush unless there is readiness at all levels – Communication / Updates is critical