

# The Risk-Compliance Connection



Angel Lee  
Director, Ethics and Compliance  
Chipotle Mexican Grill



Gerry Zack  
CEO, RiskTrek, LLC  
Former CEO, SCCE & HCCA

# Session Agenda

- The importance of a risk-compliance connection
- Understanding risk relationships
- Improving risk scales to improve risk assessments
- Not all risks are created equal
- From assessment to action
- Practical lessons for building alignment

- Alignment of risk functions (compliance, ERM, HR, IT, etc)
- What do we mean by alignment?
  - Proper positioning of components for coordinated functioning
  - A state of agreement or cooperation among persons or groups with a common cause
  - It does NOT mean:
    - Doing things identically across each function
    - One of these functions being subordinate to another
- Results should enable the capability of an organizational view of risk

# The Risk-Compliance Connection

- Right-sizing risk management in your organization
- What does a healthy risk-compliance connection look like?
- Common breakdowns in the risk-compliance connection

# Understanding Risk Relationships

- Compliance risks rarely exist in isolation
  - Usually exist in a relationship with other risks, such as HR, IT, fraud, operational, etc
- Who “owns” each risk?
  - The owner rarely has the ability to control each aspect of it
- Identifying risk (and control) relationships can lead to:
  - Increased collaboration across functional teams
  - Improved organizational view of risk
  - Greater efficiencies in supporting efforts, such as internal audit

- Oh no, it's a 3 !!!
  - How did we get here ??
- Considerations for making risk scales more useful:
  - Incorporate strategic metrics
  - Qualitative vs quantitative
  - Customize for specific risk categories
- Why?
  - Helps turn risk management into a strategic function, not an exercise
  - Assists in building cross functional collaboration
  - Positions compliance as a strategic asset

- Oh no, it's a 3 !!! Now what ???
- Do your risk scales and risk framework reflect risk appetite?
  - The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value (COSO)
- Does your organization even discuss risk appetite?
  - At what level?
- Consider risk appetite by category or by risk (i.e. risk-centric appetite) before establishing scales and thresholds for mitigation

# From Assessment to Action

- How are results prioritized?
- How are mitigation plans assigned?
- How are risks tracked over time?
- How are updates reported to leadership or the board?

# Lessons in Alignment

- Common definitions
- Scales that facilitate consolidation with other risk functions
- Be realistic – the key is buy-in and usability, not perfection
  - Remember the compliance mantra of “continuous improvement”
  - Aim for improvement over time and prioritize where to make improvements strategically
- Consider risk relationships
- Leveraging existing work
- Relate your work to strategic priorities of the organization

# Thanks !

Angel Lee

Director, Ethics and Compliance

Chipotle Mexican Grill

Angel.Lee@Chipotle.com

Gerry Zack

CEO, RiskTrek, LLC

Former CEO, SCCE & HCCA

Gerry@Risk-Trek.com