ISACA The Institute of Internal Auditors

2017GRC

Where Governance and Risk Management Align for Impact

CS 1-3: How Risk Culture Affects Compliance and Internal Controls

Joseph W. Mayo, President, J.W. Mayo Consulting, LLC

Agenda

2017GRC

- Organizational Culture
- Case Study – Sigma Pharmaceuticals
- Heuristic Auditing
- Conclusion
- Q&A

Bio

- Joseph Mayo
- PMP, RMP, CRISC
- 3 decades of industry experience
- Author
  - Chaos to Clarity
  - Cultural Calamity
- Creator
  - Risk Hurricane

2017GRC

ORGANIZATIONAL CULTURE

Disaster Sequence Pattern

- Disaster Sequence Pattern[1]
  - Equilibrium
  - Precipitating event
  - Adjustment periods
  - Re-established equilibrium

[1]Carr, L. J. (1932, September). Disaster and the Sequence-Pattern Concept of Social Change. *American Journal of Sociology*, *38*(2), 207-218.

Polling Question #1

Has your organization experienced a precipitating event?

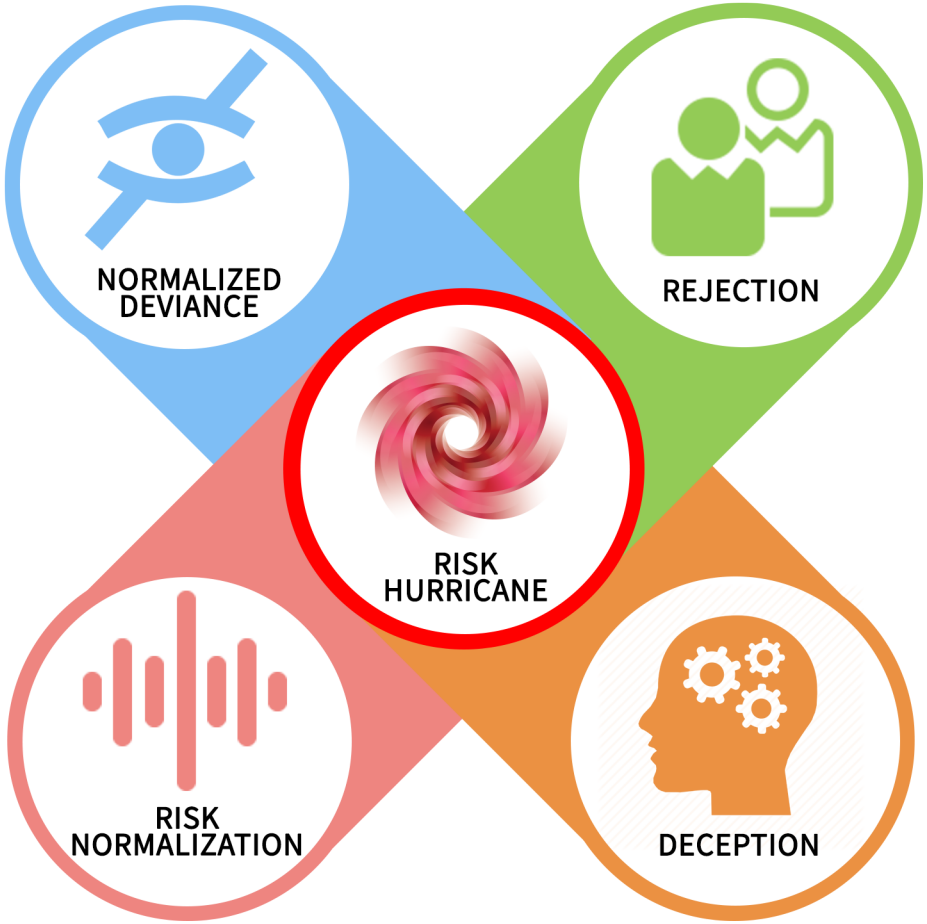
2017GRC

Disaster Warning Signs

- Cultural patterns that precede disasters[2]
  - Rigidities in perception
  - Decoy problems
  - Disregard for nonmembers
  - Information difficulties
  - Involvement of strangers
  - Regulatory non-compliance
  - Minimizing emergent danger

[2]Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, *21*(3), 378-397.

Risk Hurricane



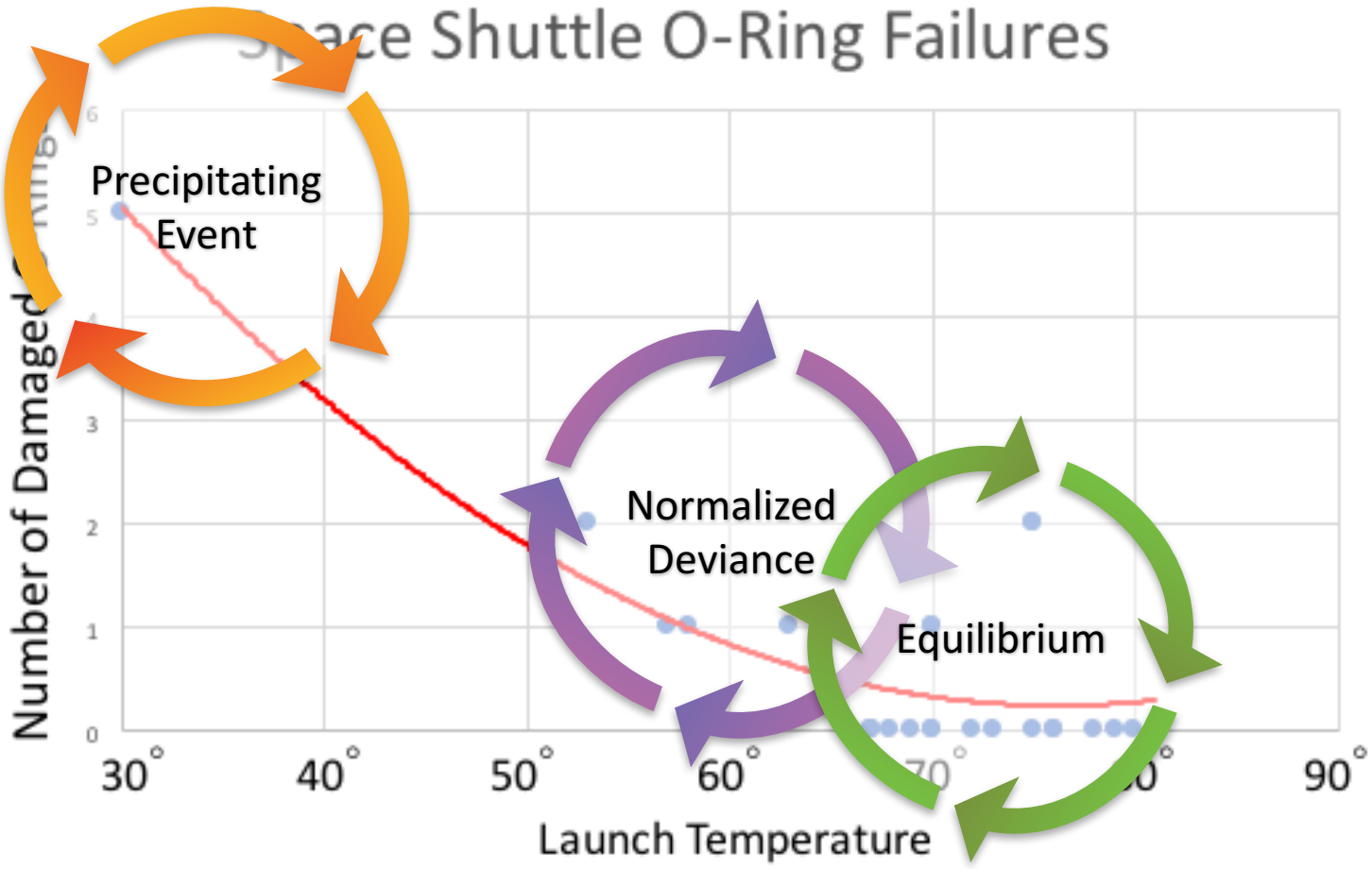
Risk hurricane illustrates organizational culture traits that can lead to disaster

Polling Question #2

Does your organization have a risk hurricane brewing?

2017GRC

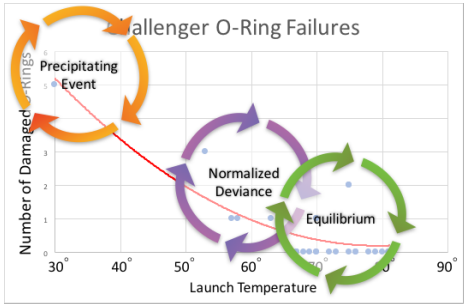
Recipe for Disaster



Normalized Deviance and Rejection

2017GRC

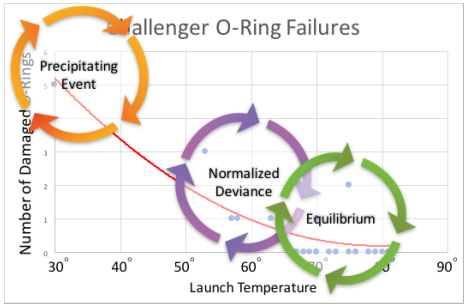
- Space Shuttle Columbia Disaster
  - 1981: Initial launched
  - 1988: Foam debris acknowledged as flight safety risk
  - 1992: Launch allowed with outstanding debris anomalies
  - 2002: ”Major debris event”
  - 2003: Columbia breaks up during reentry



Normalized Deviance and Rejection

2017GRC

- GM ignition switch defect
  - 2001: Defect detected in pre-production testing
  - 2003: Defect noted again during testing
  - 2004: Management notified of defect once again
  - 2005: Management rejects corrective action, too costly
  - 2005: Engineer advises GM to correct defect, Management rejects proposal
  - 2005: First death attributed to defect
  - 2015: 124 deaths, 275 injured, $4.1 billion



Reestablishing Equilibrium

- Reestablishing equilibrium is challenging
- 30 years after the Challenger disaster NASA has not yet exited the re-adjustment period
- Hewlett Packard
  - Equilibrium lasted more than 40 years
  - Precipitating event occurred in 1999
  - Today, 18 years later, HP still hasn't reestablished equilibrium

Polling Question #3

Can your organizational culture quickly reestablish equilibrium after a precipitating event?

2017GRC

CASE STUDY – SIGMA PHARMACEUTICALS

Sigma Pharma

2017GRC

- Very robust ERM program
- Tightly coupled ERM and management accounting information system (MAIS)
- Comprehensive framework to identify, assess and manage risk across the enterprise
- Established a Risk & Audit Committee (RAC)
- RAC was heavily compliance focused on near-term risk events
- Regular internal and external audits
- Monthly reporting to the Board

Sigma Pharma

- Supreme confidence ERM and MAIS would provide early warning for emerging risk event
- February 2010 Sigma shares plummeted 58% in one day and ultimately collapsed nearly 80%
- Sigma shares were suspended from trading and Sigma was nearly bankrupt overnight
- The cause was a low probability, high impact risk that had been reported for quite some time

Sigma Pharma

- The problem
  - Multiple risk events simultaneously
  - Risk events occurred out of sequence
  - Risk events were low probability
  - Tightly coupled ERM and MAIS did not detect these events
  - Blind faith in ERM process and Compliance-based approach set the stage for a devastating domino effect

Polling Question #4

Is internal audit highly focused on compliance?

2017GRC

What We Learned From Sigma

- Tight coupling can lead to a domino affect impossible to stop
- Non-linear complexity of risk can result in unpredictable behavior and results
- Normalized deviance and other risk hurricane characteristics can have devastating results
- Pure compliance-based auditing is insufficient

Polling Question #5

Is internal audit tightly coupled with the risk management process?

2017GRC

What Do We Do Now?

- Migrate from compliance-based auditing to heuristic auditing
- Challenge the status quo
  - Are we doing enough?
  - Are we doing the RIGHT things?
  - Just because we have always done it this way, is this the right thing to do?”
  - Are we running on trust (and being lucky) or are we really protected

HEURISTIC AUDITING

Heuristic Approach

2017GRC

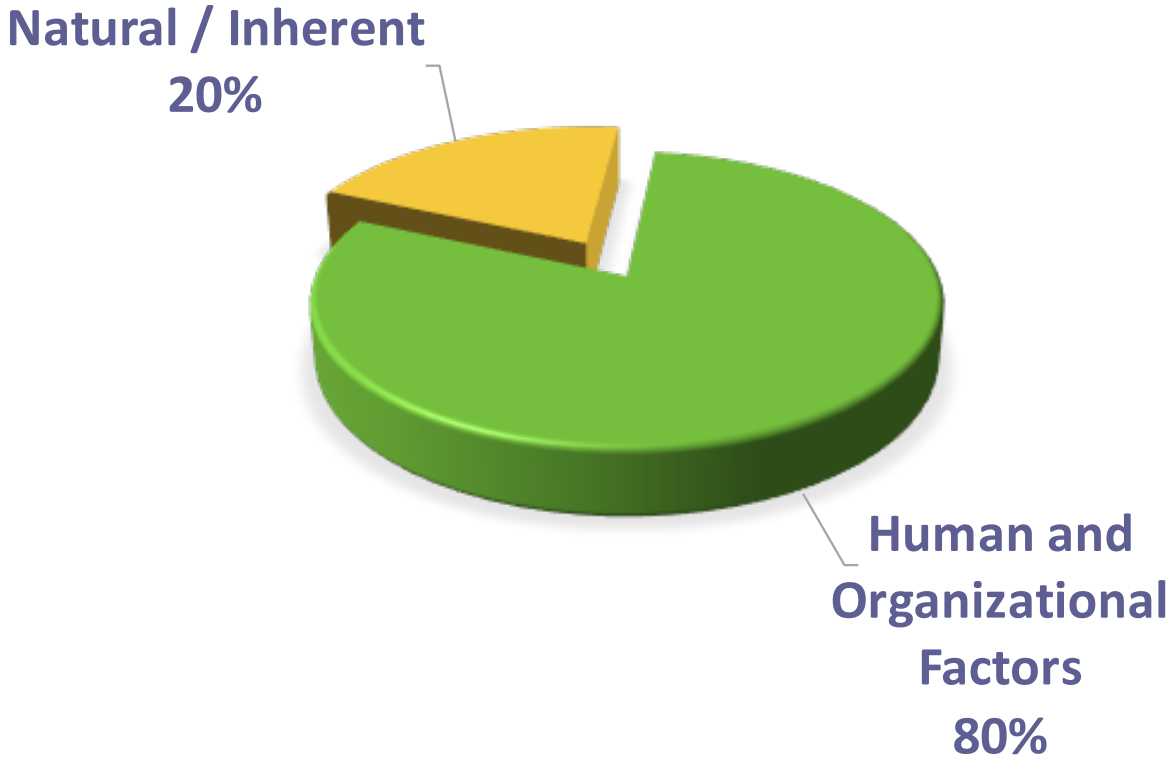
Heuristic (adjective | heu·ris·tic | \hyu̇-ˈri-stik\)

1. involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-an-error methods
2. of or relating to exploratory problem-solving techniques that utilize self-educating techniques to improve performance

Heuristic. (n.d.). Retrieved April 22, 2017, from https://www.merriam-webster.com/dictionary/heuristic

Major Failure Causes

MAJOR FAILURE CAUSES



According to Bea, a study of 600 major failures indicated that 80% were caused by human and organizational factors (HOF)

Bea, R. (2006). *APPROACHES TO ACHIEVE ADEQUATE QUALITY AND RELIABILITY*. Berkely, CA: Center for Catastrophic Risk Management.

Heuristic Auditing

2017GRC

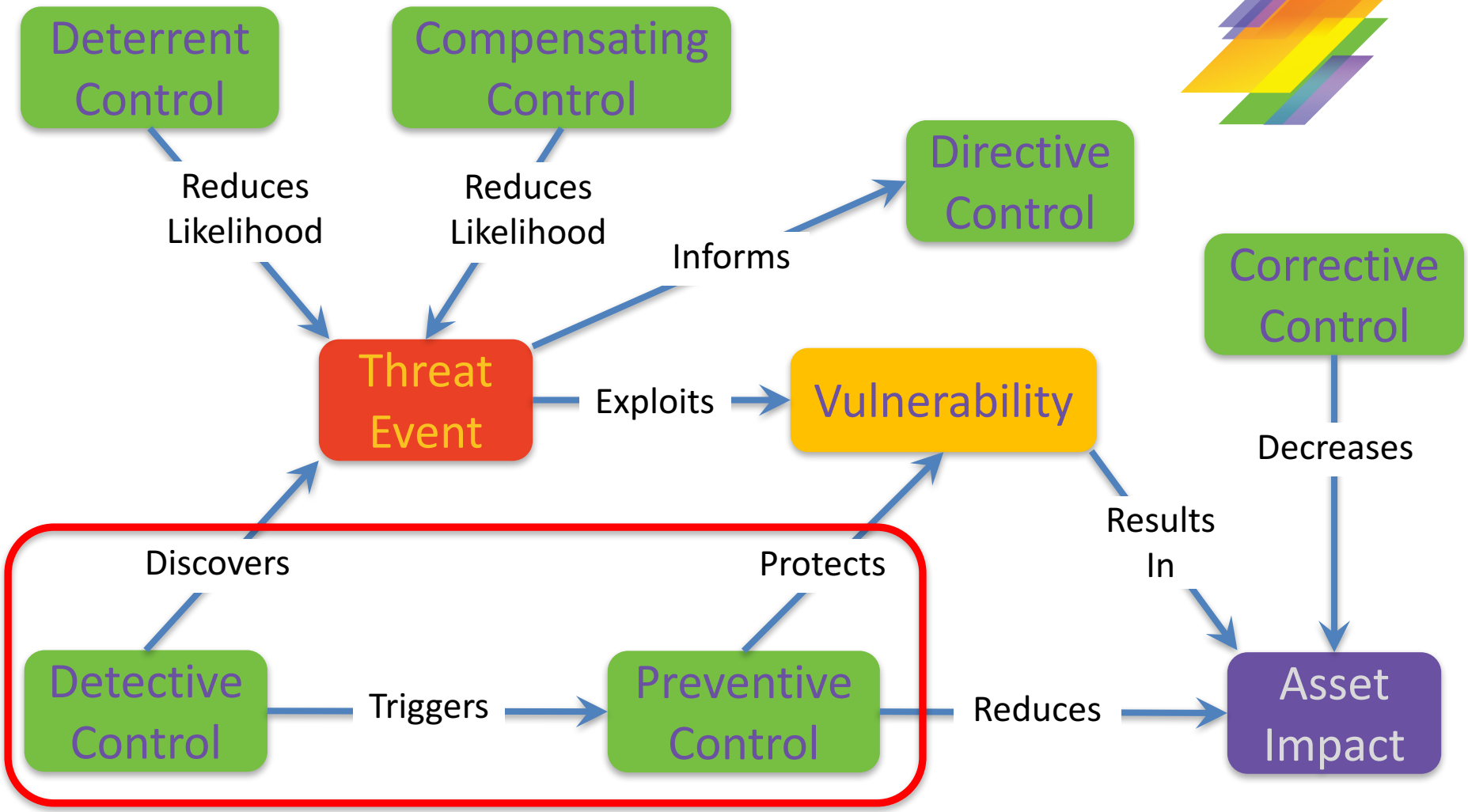
- Primary focus is asset protection
- De-emphasize compliance-based audits
- Follow your nose approach
  - Consider incidents and near-misses as learning opportunities
- Beware of risk hurricanes
  - Normalized deviance, rejection and deception mask HOF
- HOF often give rise to “quiet failures”
  - Quiet failures go unnoticed, for awhile
  - Loud failures attract public and media attention

Polling Question #6

Will your organizational culture support heuristic auditing?

2017GRC

Control Environment



Polling Question #7

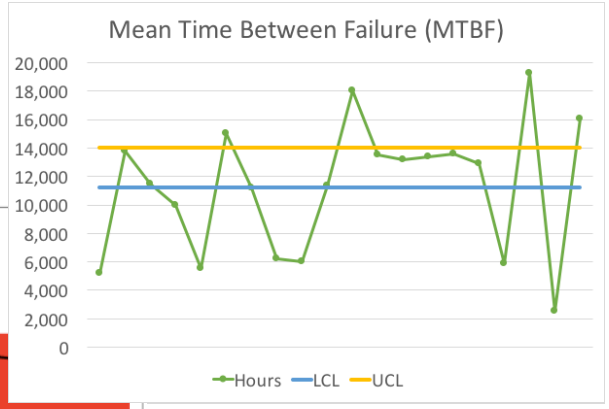
What percentage of your internal controls are detective controls?

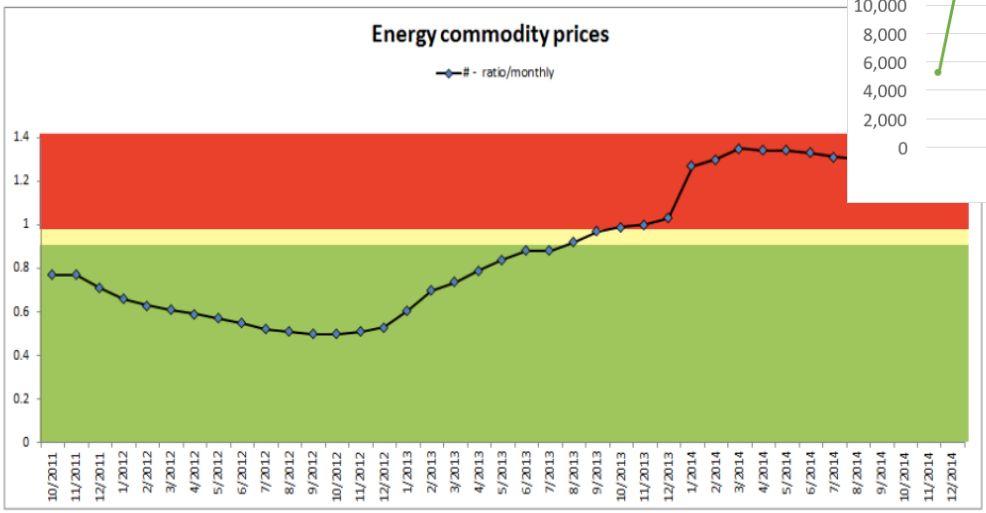
2017GRC

Detective Controls and KRIs

2017GRC

- Key Risk Indicator (KRI)
  - Critical for detective controls
  - Control charts
  - Trend analysis





Boyd, S. R., Moolman, J. A., & Nwosu, N. J. (N.D.). *Risk Reporting & Key Risk Indicators A Case Study Analysis* . Raleigh, NC: Enterprise Risk Management Initiative.

CONCLUSION

Conclusion

2017GRC

- Organizational culture and normalized deviance can cloud decision maker's judgement
- Incidents, near-misses, and accidents are leading indicators of impending disaster
- Beware of risk hurricanes
- Utilize heuristic auditing & KRIs to identify looming risk hurricanes
- Be wary of tightly integrated ERM solutions
  - Software vendors are driving tightly coupled ERM and MAIS as a best practice

Q & A

Thank You!

2017GRC

Joseph Mayo, PMP, RMP, CRISC

- www.jwmc-llc.com
- joseph.mayo@jwmc-llc.com
- @TaoOfRisk
- https://www.linkedin.com/in/josephmayo/