J. W. Mayo
CONSULTING

jwmc-llc.com

J. W. Mayo CONSULTING

Asset Oriented Risk Management

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Case Study – Sigma Pharmaceuticals

joseph.mayo@jwmc-llc.com

Sigma Pharmaceuticals

- 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)
- Regular internal and external audits
- Monthly reporting to the Board

joseph.mayo@jwmc-llc.com

Sigma Pharmaceuticals

- Supreme confidence ERM and MAIS would provide early warning for emerging risk event
- RAC was heavily compliance focused on near-term risk events
- 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

joseph.mayo@jwmc-llc.com

Sigma Pharmaceuticals

J. W. Mayo CONSULTING

What went wrong?

- 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

joseph.mayo@jwmc-llc.com

What We Learned From Sigma

J. W. Mayo CONSULTING

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

joseph.mayo@jwmc-llc.com

What Do We Do Now?

J. W. Mayo CONSULTING

Focus on asset protection

Process compliance is necessary but is secondary

- Assets include
  - People (employees, suppliers, customers, contractors)
  - Intellectual property (patents, processes, methods, etc.)
  - Property (buildings, fleets, IT, real estate, etc.)
  - Data
  - Reputation

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

joseph.mayo@jwmc-llc.com

Heuristic Auditing

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

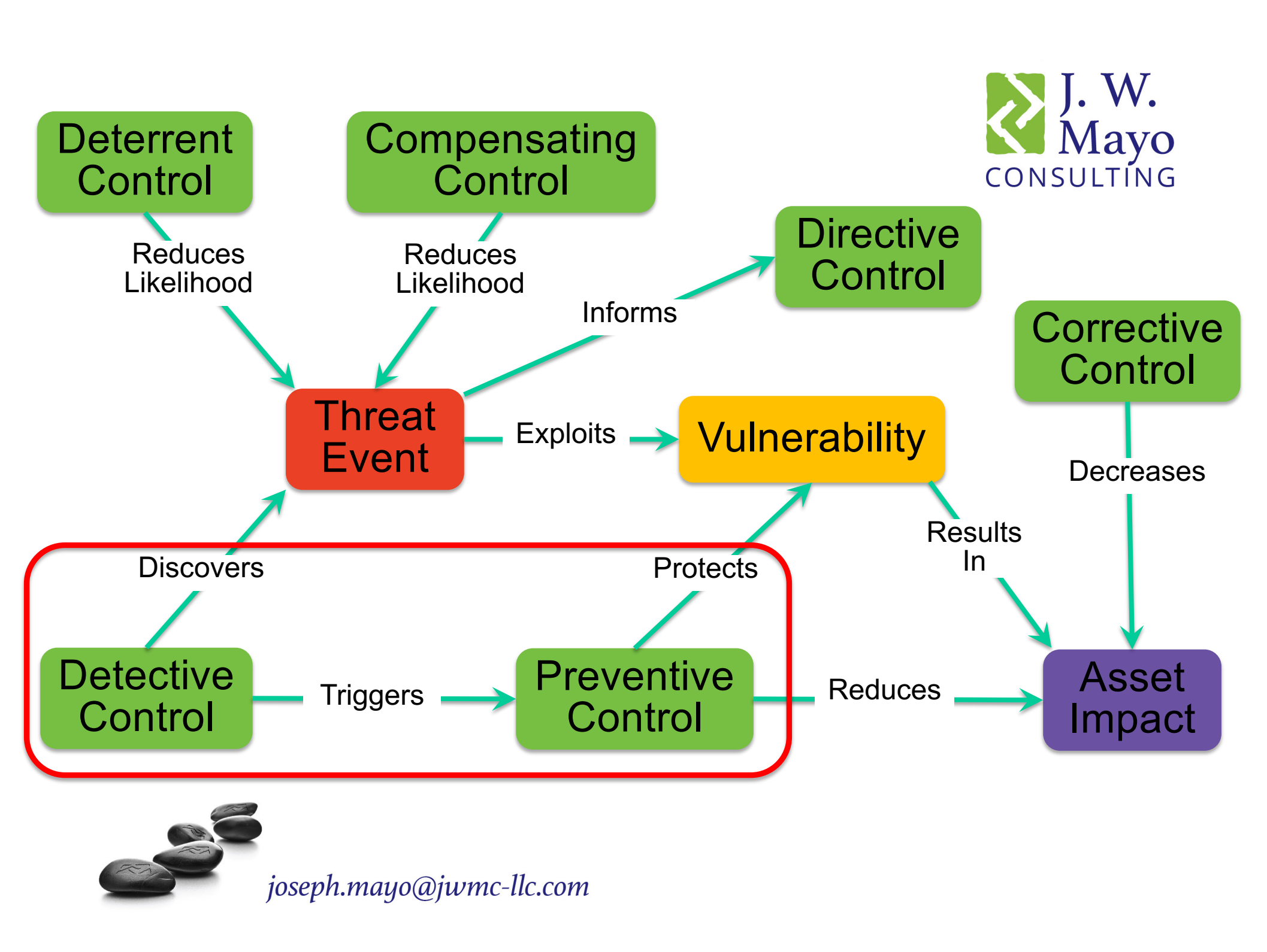
1. involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-an-error methods
2. of or relating to exploratory problem-solving techniques that utilize self-educating techniques to improve performance

Primary focus is asset protection

Follow your nose approach

Consider incidents and near-misses as learning opportunities

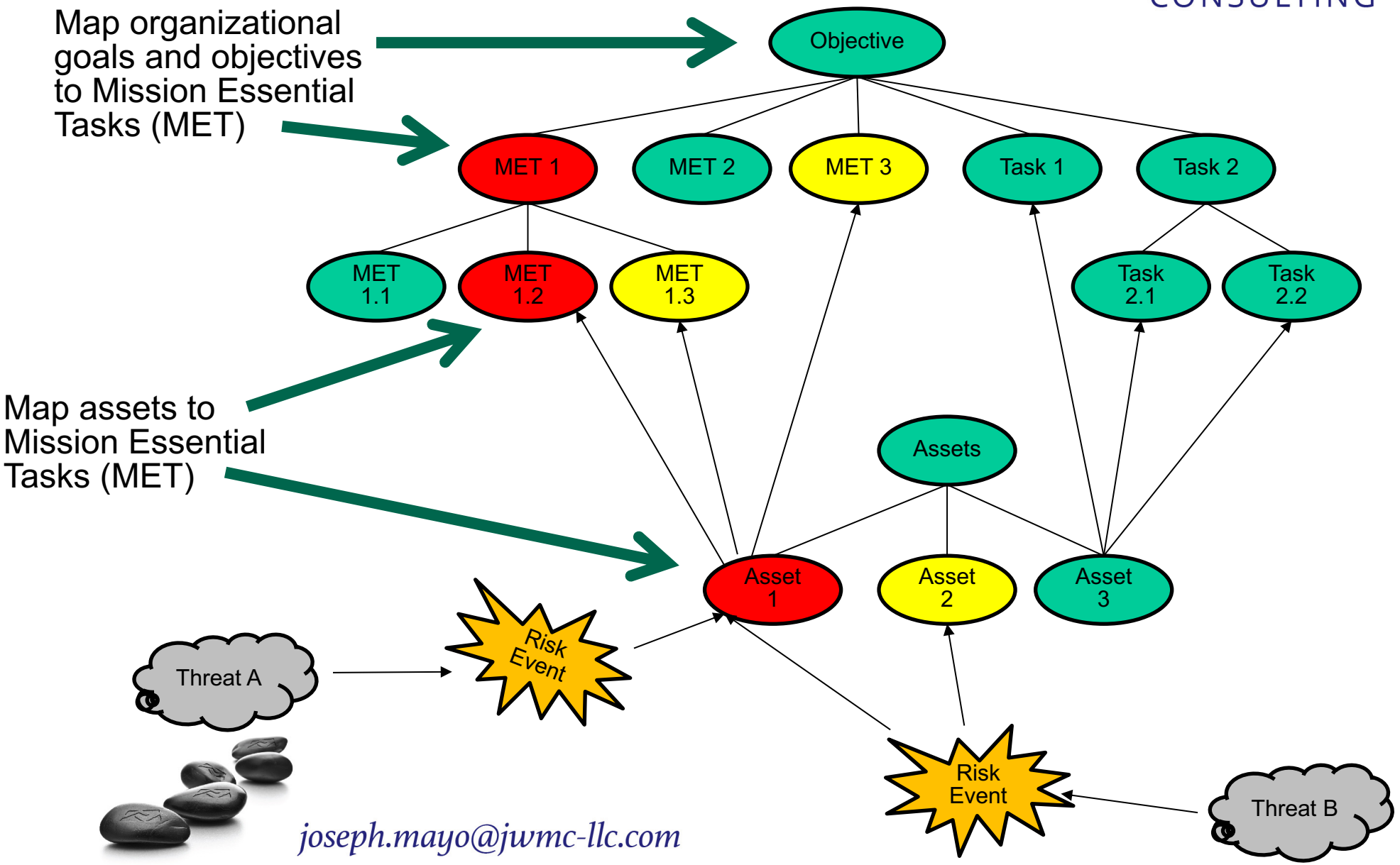
joseph.mayo@jwmc-llc.com



J. W. Mayo CONSULTING

joseph.mayo@jwmc-llc.com

Crown Jewel Analysis (CJA)



Conclusion

We must revolutionize current risk management practices

Risk management must evolve from a defensive strategy to an offensive strategy

Sun Tzu - Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive.

- A defensive strategy avoids losing
- An offensive strategy allows winning

Increase use of detective controls and KRIs to provide early warning of problems

Detective controls, KRIs, and heuristic auditing will protect more assets and avoid a repeat of Sigma Pharmaceuticals

joseph.mayo@jwmc-llc.com

Live Content Slide

When playing as a slideshow, this slide will display live content

Social Q&A for ISACA Maryland Chapter Virtual Conference

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Thank You!

• • •

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

@TaoOfRisk