J. W. Mayo
CONSULTING

jwmc-llc.com

J. W. Mayo CONSULTING

Threat Modelling

Joseph W. Mayo

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

joseph.mayo@jwmc-llc.com

Agenda

J. W. Mayo CONSULTING

- Threat Taxonomy
- Threat Modeling in Today's Environment
- Critical Asset Protection Solution (CAPS)
- Best-in-class Threat Modeling
- Opportunity Analysis & Rationalization Solution (OARS)
- Q&A

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

conferences i/o

We're going to be using a product called Conferences i/o that will allow you to engage with us during this session. **All responses are anonymous!**

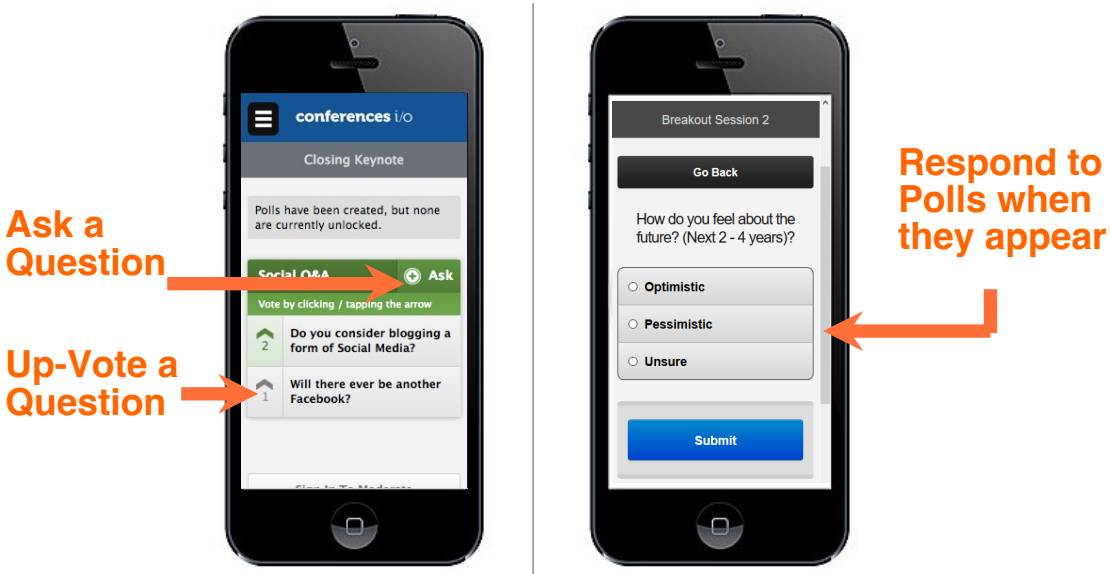
If you have a mobile device (smartphone, tablet, laptop, etc.) please take a moment now, and go to https://taoofrisk.cnf.io

The Conferences i/o app allows you to ask questions, up-vote questions other attendees asked and respond to polls when they appear on your device, all in real time!

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

WEBSITE ADDRESS: **TaoOfRisk.cnf.io**



Note: Responses and submissions are anonymous

joseph.mayo@jwmc-llc.com

Threat Taxonomy

J. W. Mayo CONSULTING

- **Asset** – Something used to meet organizational goals
- **Vulnerability** – Weakness that exposes an asset to potential damage
- **Threat** – Anything that can destroy or diminish asset value
- **Threat agent** – Entity capable and motivated to exploit an asset's vulnerability
- **Threat event** – Threat agent attempts to exploit asset's vulnerability
- **Threat vector** – Tool or technique used to exploit a vulnerability
- **Loss event** – Threat agent successfully exploits an asset's vulnerability

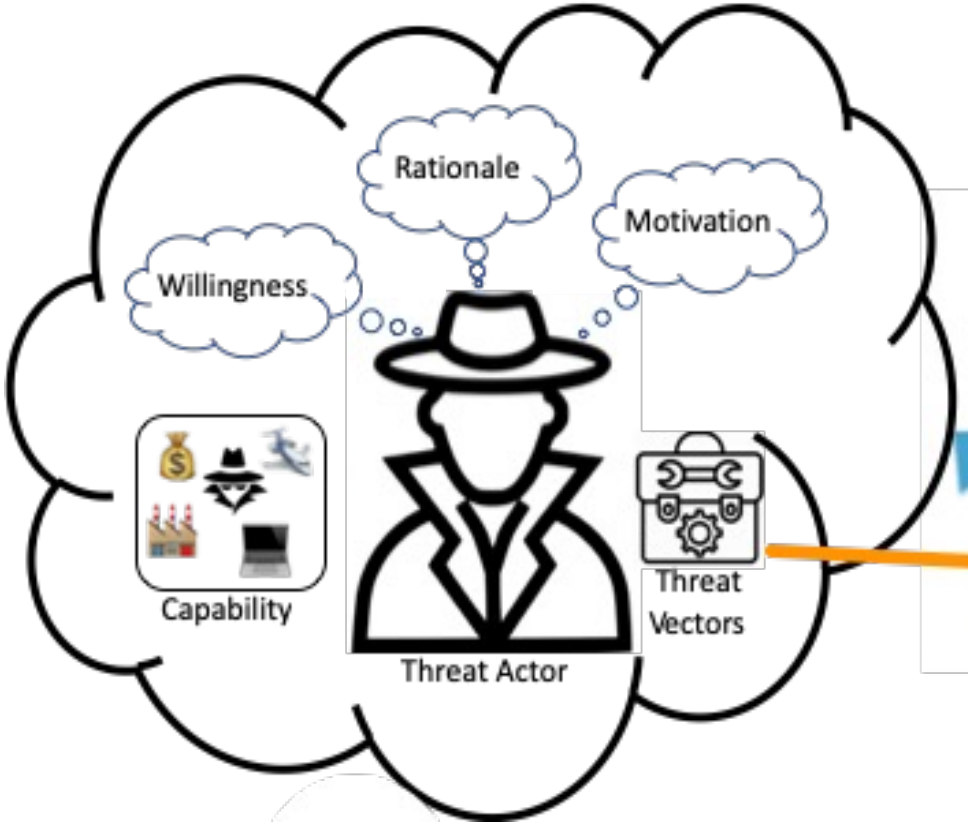
Threat events only occur if a threat agent has motivation and skill to exploit a vulnerability

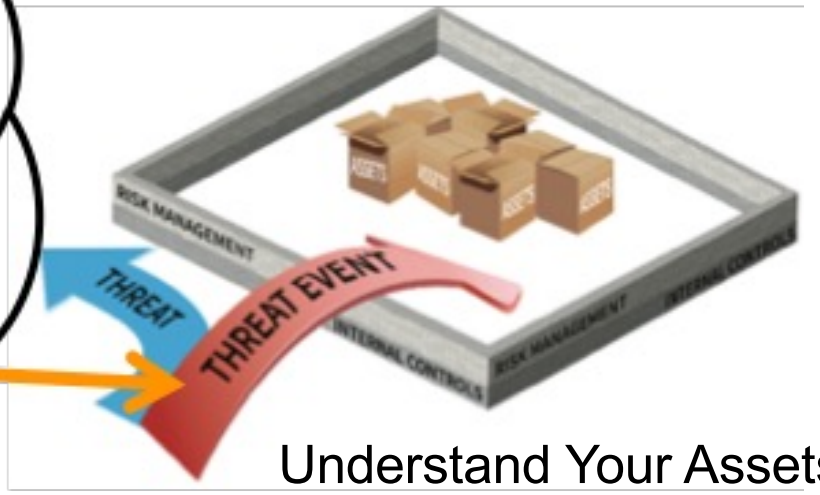
joseph.mayo@jwmc-llc.com

Threat Modeling in Today's Environment

J. W. Mayo CONSULTING

Understand The Threat





Understand Your Assets

- ✓ Vulnerabilities
- ✓ Controls
- ✓ Treatment Options
- ✓ Priority based on mission criticality
- ✓ Impact to business objectives
- ✓ Value

joseph.mayo@jwmc-llc.com

Live Content Slide

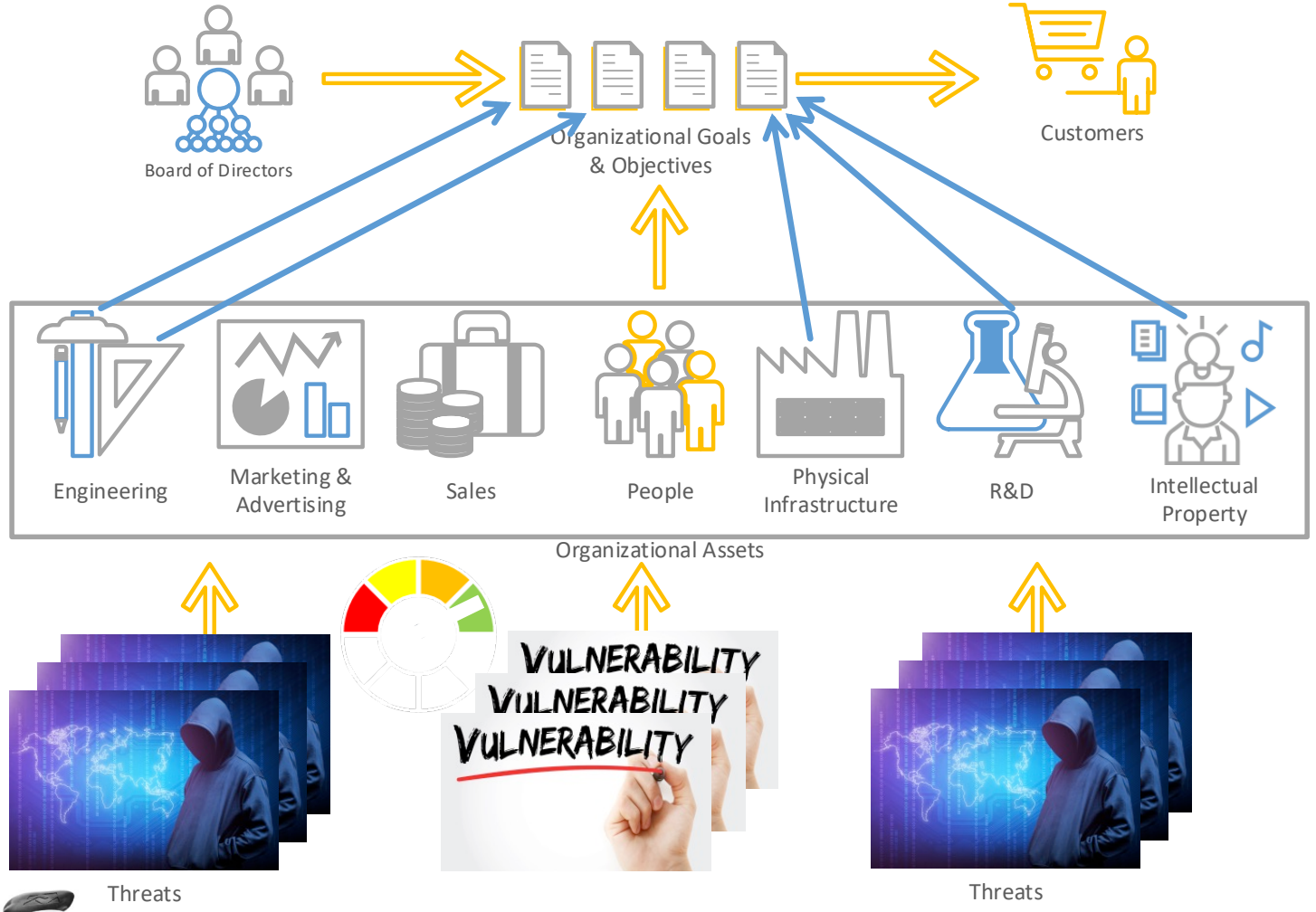
When playing as a slideshow, this slide will display live content

Poll: Which of the choices best describes your asset inventory?

joseph.mayo@jwmc-llc.com

Threat Modeling in Today's Environment

J. W. Mayo CONSULTING



joseph.mayo@jwmc-llc.com

Best-in-class Threat Modelling

J. W. Mayo CONSULTING

Critical Asset Protection Solution (CAPS)

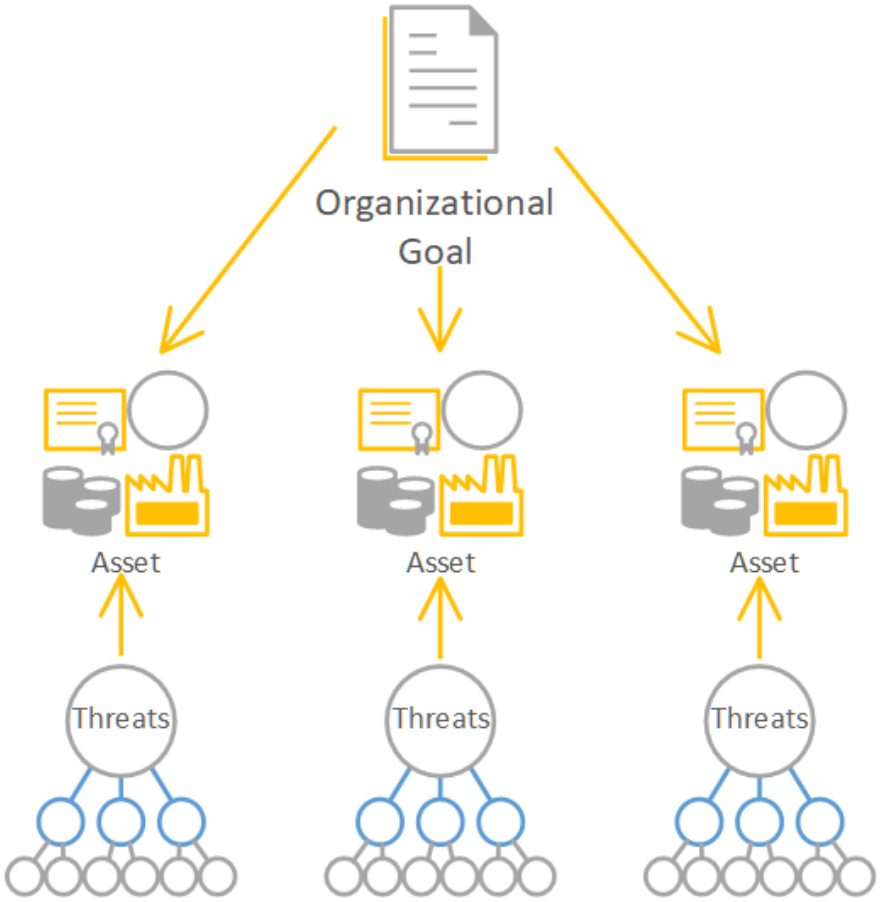
- Asset oriented
- Ties critical assets to organizational goals and business functions
- Creates an inventory of critical organizational assets
- Highlights low-value assets that should be replaced or eliminated
- Models the impact of total asset loss and impaired assets

Extend Threat Models

- Include all types of risk and not just cyber threats
- Use a hybrid approach
  - Attack trees (includes both IT & non-IT threats)
  - Persona non Grata (impact of insider threats)
  - Security Cards (threat rationale & motivation)
  - Octave (asset oriented, less abstract methods)

joseph.mayo@jwmc-llc.com

Best-in-class Threat Modelling



joseph.mayo@jwmc-llc.com

Opportunity Analysis and Rationalization Solution (OARS)

- Opportunity analysis is effectively speculative risk management
  - Resources are expended with no guarantee of a return
- Structured techniques exist
- Improves communication with Senior Stakeholders and The Board
- Critical success factor for organizations in the 4IR
- Proactive opportunity analysis is critical to 4IR risk management

joseph.mayo@jwmc-llc.com

Opportunity Analysis and Rationalization Solution (OARS)

J. W. Mayo CONSULTING

Bayesian statistics

- Mechanism for using subjective beliefs in a problem
- All that is needed is knowledge of existing environment

Decision tree (aka EMV)

- Graphical display
- Quantitative results

Monte Carlo Simulation

- Easy to use
- Software enables nearly unlimited simulation runs

Preliminary hazard analysis (PHA)

- Carried out early in the lifecycle when limited design or operating procedures information exists
- Able to be used when there is limited information

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Live Content Slide

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

Poll: Does your organization conduct formal threat modeling activities?

joseph.mayo@jwmc-llc.com

Opportunity Analysis and Rationalization Solution (OARS)

J. W. Mayo CONSULTING

Multi-criteria decision analysis (MCDA)

- Objectively assess the overall worthiness of a set of options
- Useful where multiple and sometimes conflicting objectives exist
- Helps rationally consider problems where tradeoffs must be made

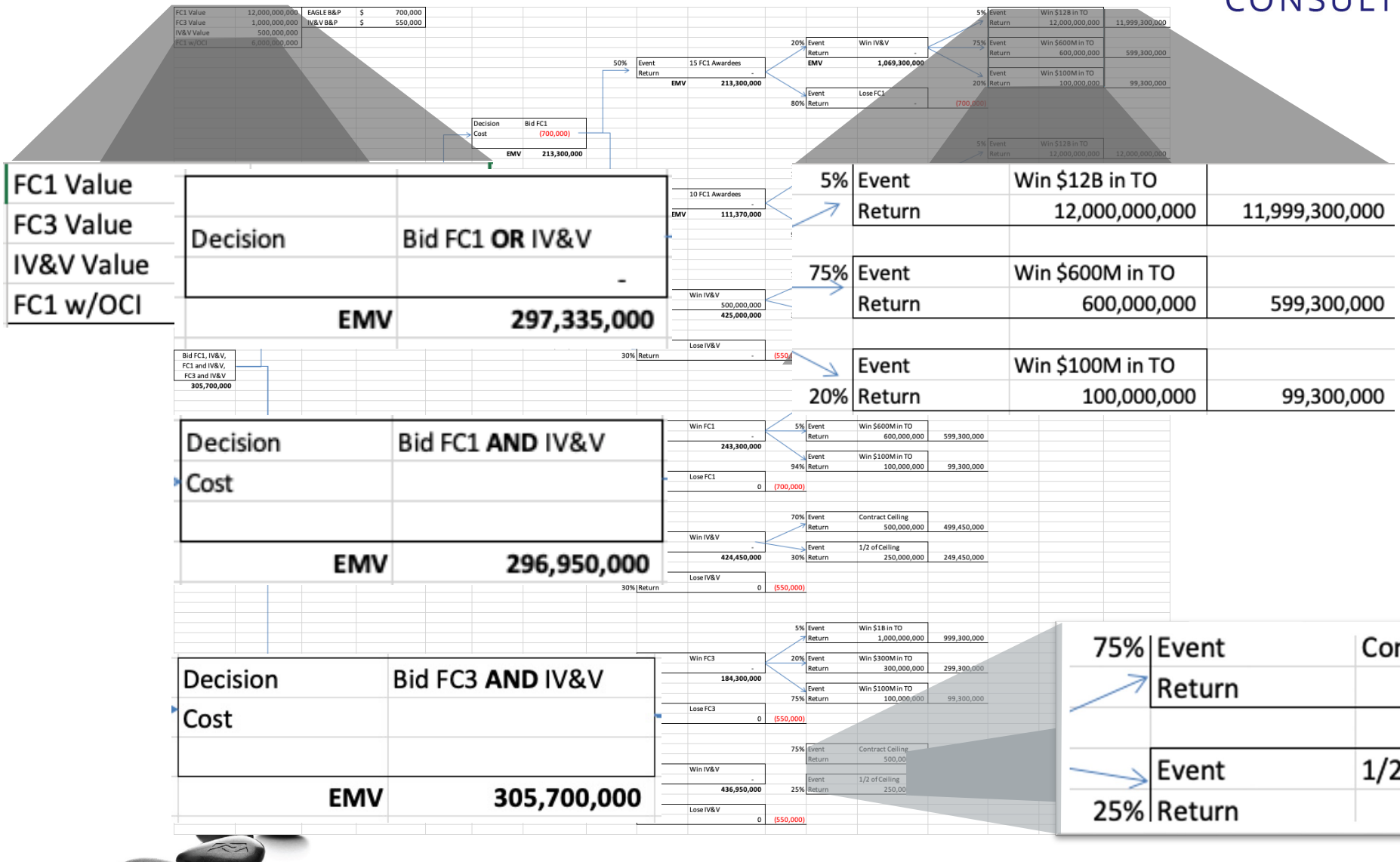
F_n Curves

- AKA - As Low As Reasonably Practicable (ALARP)
- Highlights events impacting a large segment of the population with a high frequency of occurrence which may be socially or politically unacceptable
- Can be constructed using data from past losses or calculated from simulation model estimates

joseph.mayo@jwmc-llc.com

Opportunity Analysis and Rationalization Solution (OARS)

J. W. Mayo CONSULTING



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