J. W. Mayo
CONSULTING

jwmc-llc.com

Implementing the Risk Process

Joseph W. Mayo

J. W. Mayo Consulting, LLC

joseph.mayo@jwmc-llc.com

Agenda

- Purpose of Risk Management
- Tone at The Top
- Focus on Assets
- Case Study
- Risk Framework

joseph.mayo@jwmc-llc.com

Purpose of Risk Management

J. W. Mayo CONSULTING

The purpose of risk management is to protect assets so we can meet personal or organizational goals and objectives

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Tone at the Top

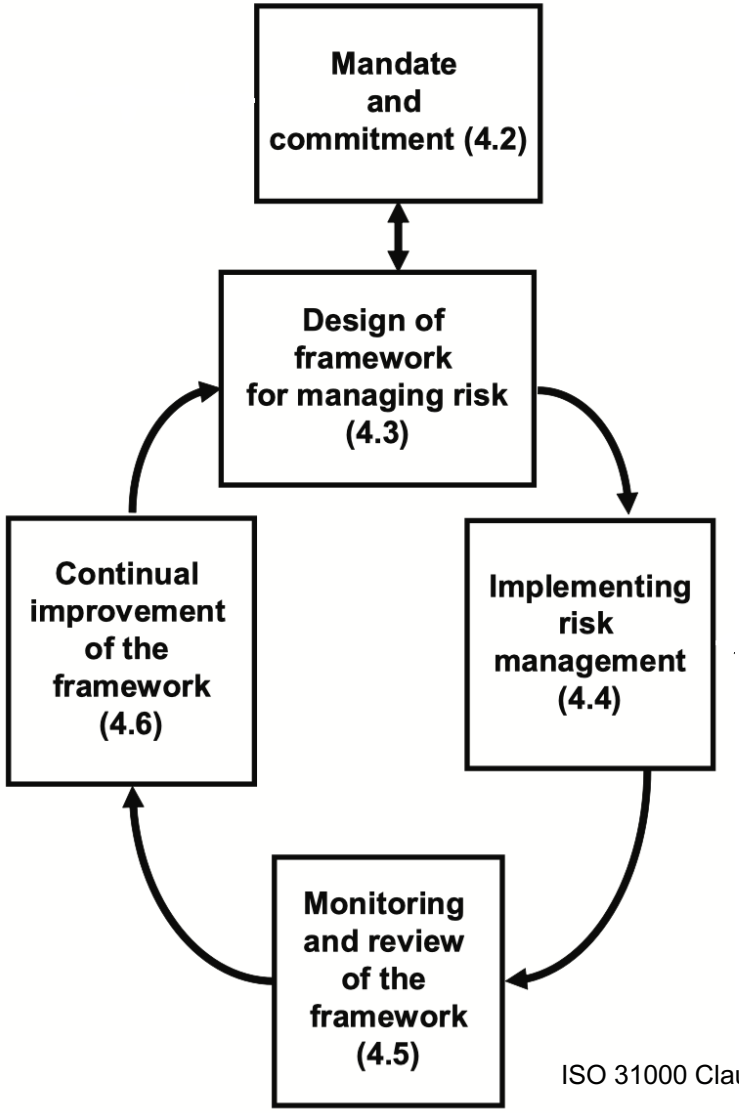
joseph.mayo@jwmc-llc.com

Start at the Top

- Tone at the Top
  - Begins with the risk policy
  - Further refined by appetite and tolerance
- Align culture with risk policy
- Focus on organizational assets
  - Align goals and objectives with assets

joseph.mayo@jwmc-llc.com

Start at the Top



ISO 31000 Clause 4

joseph.mayo@jwmc-llc.com

Risk Policy Statements

J. W. Mayo CONSULTING

Our risk management systems aim to ensure that:

- Our managers have an up to date and accurate understanding of the material risks relevant to their areas of responsibility …
- Policies and procedures are developed to guide our actions...
- Appropriate risk management education and training is provided ...
- Risk management processes and practices are diligently applied by our employees.
- Regular evaluation and improvement of our risk management approaches ...
- Information regarding the status of a range of risks is regularly presented and reviewed ...

joseph.mayo@jwmc-llc.com

Risk Policy Statements

<Company> strives to:

- Use best practice in RM to support and enhance activities…
- Embed a common culture throughout the organization…
- …promotes awareness of potential exposures and opportunities created by risk.
- Ensure RM is an integral part of all our decision making processes.
- Train our people to implement RM effectively.
- Continually improve RM practices.

joseph.mayo@jwmc-llc.com

Risk Policy Statements

- It is our policy to integrate risk management into the every day business, making it systematic and Company wide.
- Our use of risk management will be documented, consistently applied and cost effective.
- We will foster a ‘no blame’ culture …
- We will encourage everyone to report risks and potential issues …
- We aim to anticipate, and where appropriate, deal with risks in advance, …
- Our approach includes the development of contingency plans that will allow us to contain the negative effect of unlikely events …
- We aim to have total transparency as far as possible …
- All risk management will be aligned to the delivery of relevant objectives and targets:

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Focus on Assets

joseph.mayo@jwmc-llc.com

Focus on Assets

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

Determine asset's role in organizational goals

- Helps prioritize risk

joseph.mayo@jwmc-llc.com

Focus on Assets

J. W. Mayo CONSULTING

Quantitatively measure risk impact

- FAIR ontology is an excellent tool

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

J. W. Mayo CONSULTING

Focus on Assets

Heuristic Auditing

joseph.mayo@jwmc-llc.com

Heuristic Auditing

J. W. Mayo CONSULTING

Primary focus is asset protection

Follow your nose approach

- Consider incidents and near-misses as learning opportunities

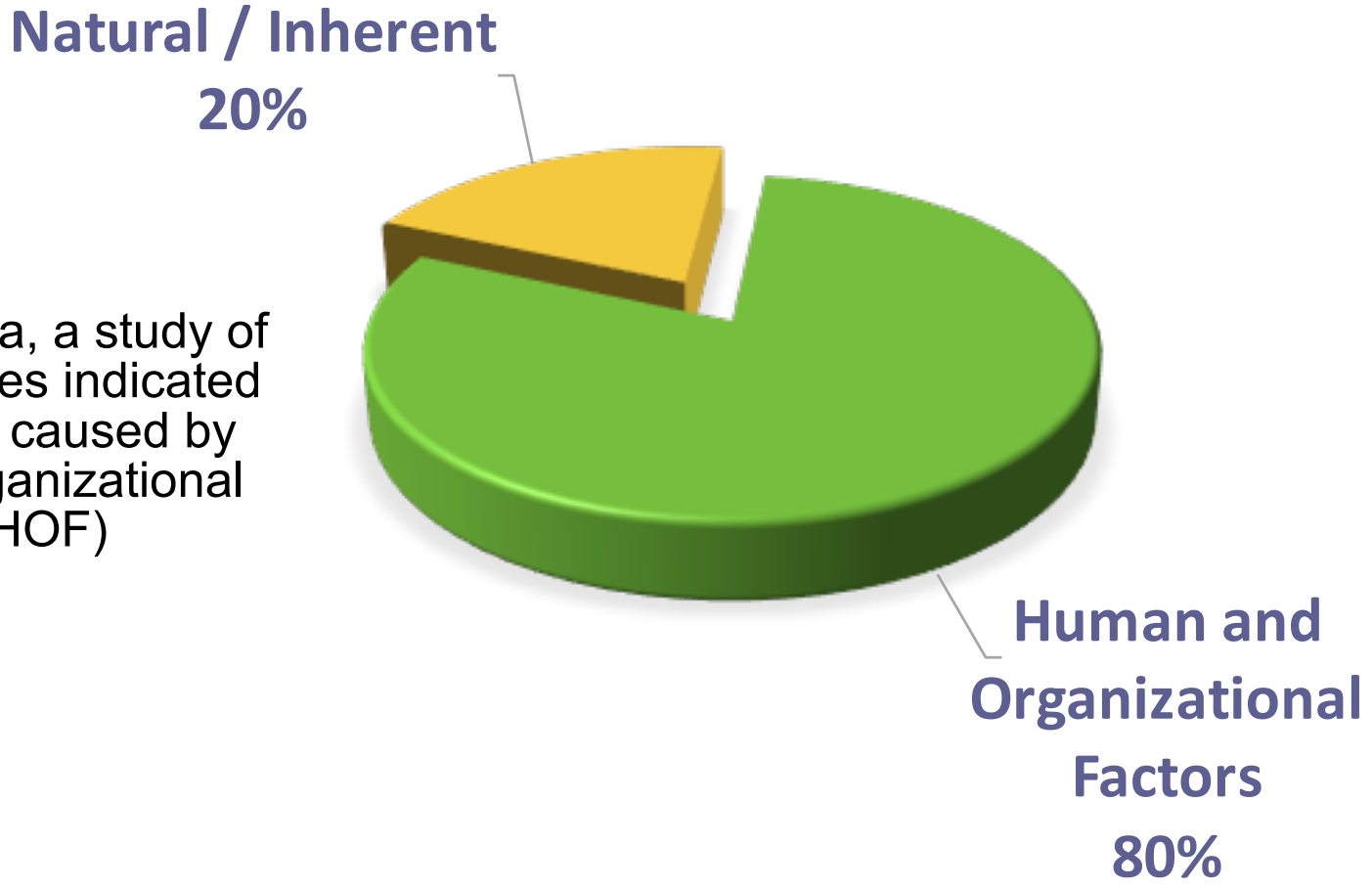
Human and Organizational Factors (HOF) often give rise to “quiet failures”

- Quiet failures go unnoticed, for awhile
- Loud failures attract public and media attention

joseph.mayo@jwmc-llc.com

Major Failure Causes

J. W. Mayo CONSULTING



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

R. (2006). *APP*

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Case Study

joseph.mayo@jwmc-llc.com

FAIR Ontology

J. W. Mayo CONSULTING

Frequency Analysis for Information Risk (FAIR)

FAIR taxonomy

- Threat
- Threat event
- Vulnerability
- Loss event
- Risk
- Asset

joseph.mayo@jwmc-llc.com

FAIR Example

J. W. Mayo CONSULTING

Scenario

- A component in a technology system has a mean time between failure (MTBF) of 13,000 hours (approximately 18 months of continuous use)
- Lead time to procure replacement is 6 months
  - Replacement orders must be placed 12 months after installation
- 50% were failing early, 30% within 8 months

joseph.mayo@jwmc-llc.com

FAIR Example

J. W. Mayo CONSULTING

Mission (MTBF scenario)

- Asset – technology system
- Threat – poor design
- Vulnerability – 50% fail before MTBF
  - Early failure – 50%, normal failure – 30%, late failure – 20%
- Threat event – system implementation (unavoidably introduced due to mission requirements)
- Loss event – lost productivity caused my technology failure

joseph.mayo@jwmc-llc.com

FAIR Example

J. W. Mayo CONSULTING

Mission (MTBF scenario)

- Risk – Mission
- Appetite
  - How many systems are you willing to have inoperable?
- Treatment:
  - Low risk appetite – 50% spares @ $200K each
    - Nearly 100% availability based on current data
    - Requires $8.2M contingency reserve
  - High risk appetite – 20% spares @ $200K each
    - 70% availability
    - Requires $3.3M contingency reserve

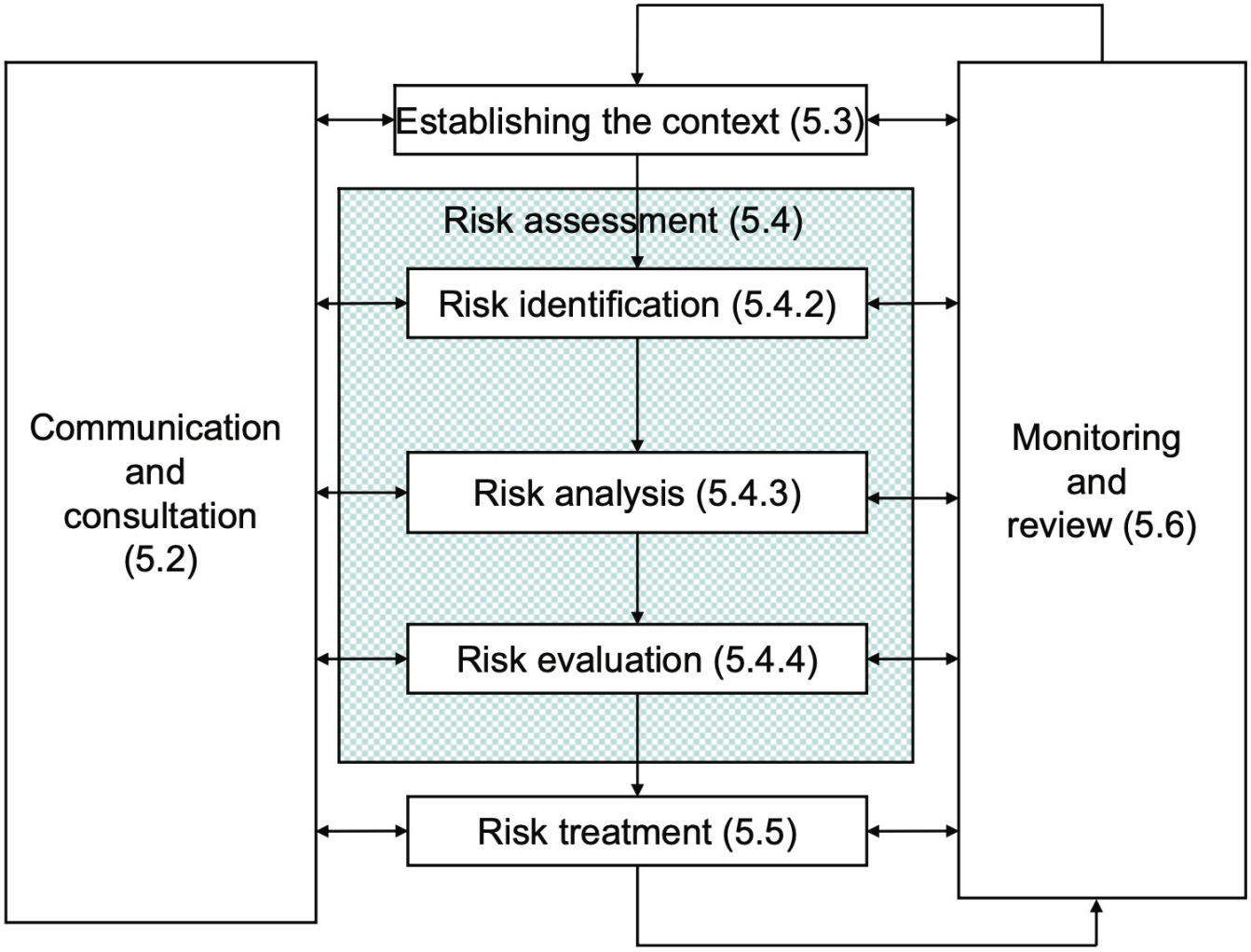
joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Risk Framework

joseph.mayo@jwmc-llc.com

Design Risk Framework



ISO 31000 Clause 5

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