Building a Strong Foundation for your Quantitative Risk Management Program

Tim Wynkoop

FAIRCON ‘22

FAIR22 CONFERENCE

https://www.bostonglobe.com/2022/01/31/metro/historic-cape-cod-house-stilts-teetering-over-atlantic-ocean/

FAIR22 CONFERENCE

https://www.bostonglobe.com/2022/01/31/science/barrage-wind-waves-weekends-storm-pummeled-coast-cape-cod/

FAIR22 CONFERENCE

What is needed for a strong foundation?

Organizational Buy-in / Management Support

Strong Methodology

Dedicated Risk Practitioners

Organizational Buy-in

FAIR22 CONFERENCE

Gaining Organizational Buy-in

Show the alternatives

Give case studies

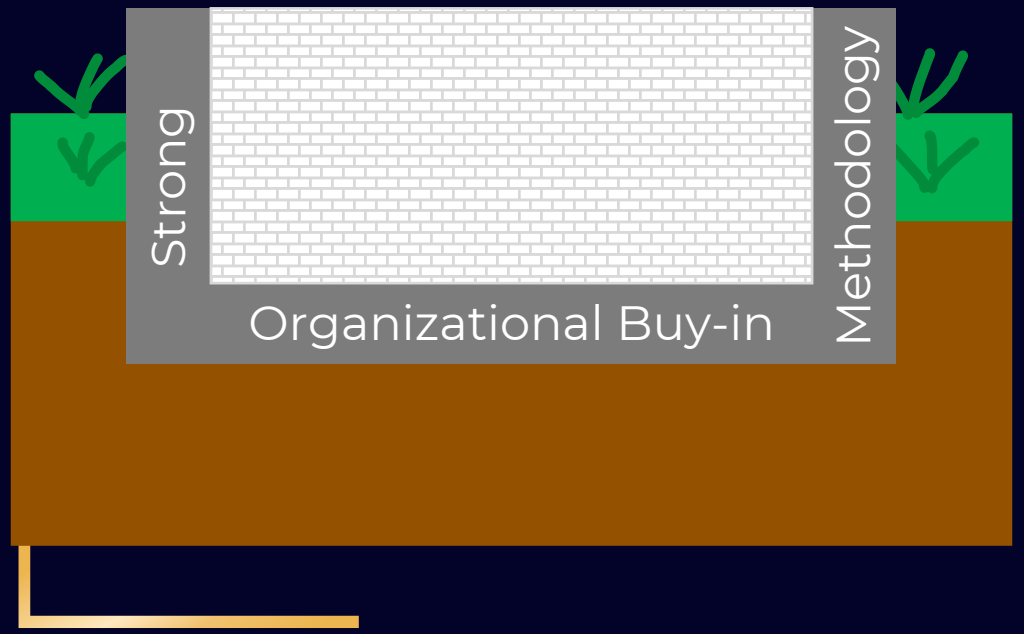
Create a North Star

North Star

”The goal of the risk management program is to enable stakeholder(s) to make forward-looking, well-informed, effective decisions by providing insight into the probable risk facing the organization, the actionable path(s) forward for addressing the risk and to enable the business to achieve an acceptable level of loss exposure”

Strong Methodology

Methodology – Definitions



- **Risk :** The probable frequency and probable magnitude of future loss
- **Risk Analysis:** A scenario analysis that includes 1 Asset, 1 Threat, 1 Effect and optionally 1 method. This is a subcomponent of a Risk Assessment.
- **Risk Assessment:** A process designed to support a decision which includes the identification many factors including 1 to many scenarios, identifying options to manage the risk issue and communicating results & recommendations to a stakeholder.
- **Risk Ownership:** The Asset Owner is considered the Risk Owner for risk events related to that asset in order to maintain an acceptable level of loss exposure.

FAIR22 CONFERENCE

Methodology – Roles & Responsibilities

Asset Owner: The person(s) responsible for ensuring the risk around the asset is managed at an acceptable level.

Generally responsible for:

- Budgetary constraints including annual cost & maintenance
- Applying controls that meet required compliance requirements
- Subject matter expert for anything related to the asset

Methodology – Roles & Responsibilities

Process Owner: The person(s) responsible for ensuring a particular process is working as intended and the risk around the process is managed at an acceptable level.

Generally responsible for:

- Ensuring proper process documentation is in place
- Having knowledge of all asset used in the process and the downstream dependencies
- Working with the associated asset owners around operational efficiencies gained by the asset

Note: The Process Owner may be the same person as the Asset Owner

Methodology – Roles & Responsibilities

Control Owner: The person(s) responsible for the design, implementation, and maintenance of a particular control to help the business manage risk at an acceptable level.

Generally responsible for:

- Ensuring the setup/design of the control aligns with the organizational compliance requirements
- Working with the Asset and Process Owners to enable operational efficiencies
- Day-to-day operation of the control

Note: This person is generally located in Information Security/Technology

Methodology – Defined Process

The risk management and assessment process is designed to allow risk to be managed at an acceptable level.

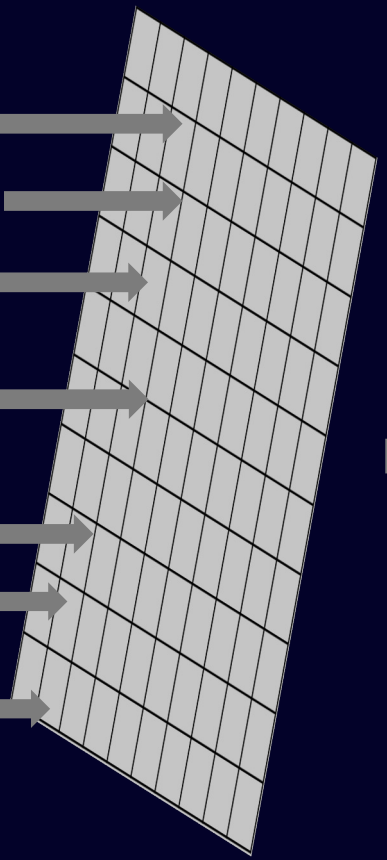
Identification / Context / Scoping	Analyze	Evaluate	Treatment	Reporting	Monitoring
What decision is being supported? What is the scope of the Risk Assessment?	What level of rigor is needed? What data is needed?	Can the risk be accepted?	Can the risk be mitigated?	What information is needed for a decision to be made?	How often should the risk be reviewed?

Identification / Context / Scoping → Analyze → Evaluate → Treatment → Reporting → Monitoring

FAIR

Issues/Concerns

- Audit Findings
- Compliance Exceptions
- Vulnerabilities
- Policy Exceptions
- Control Weakness
- Emerging Threats
- M&A

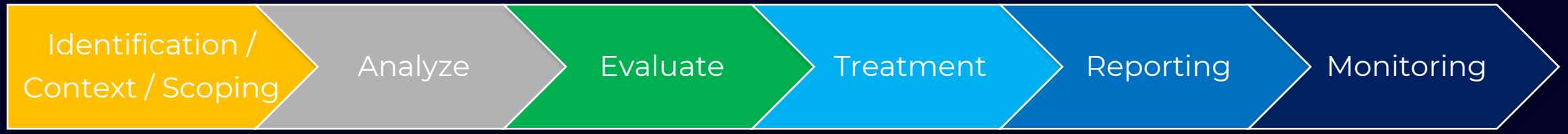


Risks

Loss Events

- Asset(s)
- Threat(s)
- Effect(s)
- Method(s)

FAIR22 CONFERENCE



SME Data

Industry Data

Cyber / Other Data

Data Libraries

FAIR Model

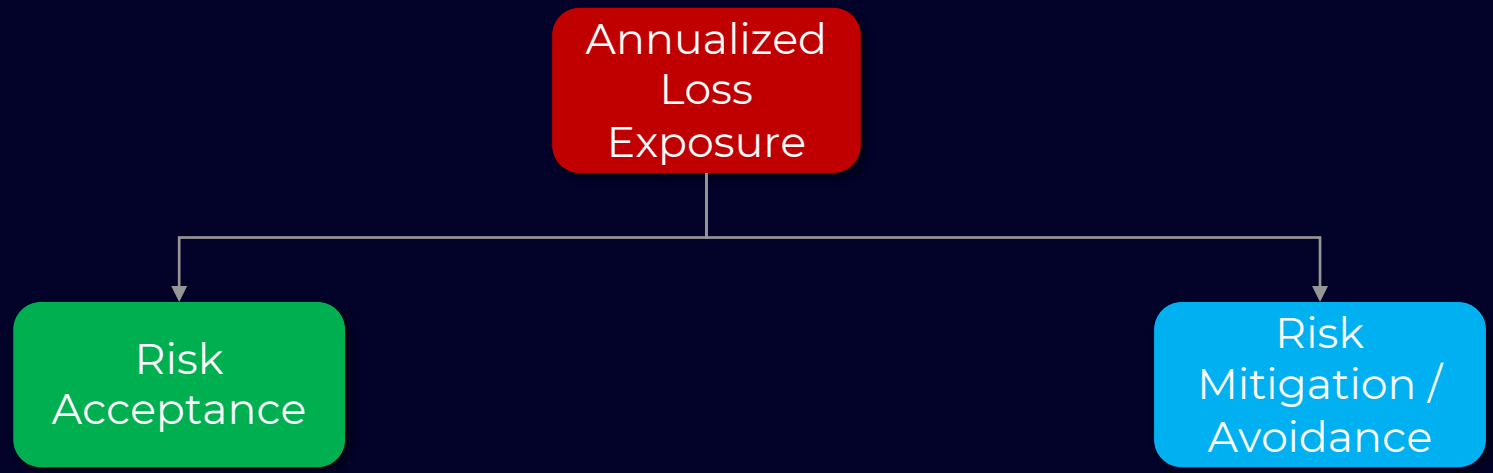
Quality Assurance & Iterations

Consistent Rationale

Tailored Reporting for the Decision Maker

Depth and Rigor of analysis is always dependent on the decision the analysis is intended to support

FAIR22 CONFERENCE



- Thresholds based upon Risk Appetite
- Approvals based by Risk Owner

- Risk Reduction opportunities (Control Improvements)
  - Timeline to implementation
  - Cost
  - Comparison Assessment
- Risk Avoidance
  - Timeline to avoid
  - Cost

FAIR22 CONFERENCE

Risk Acceptance → Reporting → Monitoring

Standardized Report
- Scope
- ALE
- Risk Acceptance
- Mitigation Options (if applicable)

Standard Monitoring Cadence

Risk Practitioners

Critical Thinking Skills

Ability to ask thought provoking questions

QUESTIONS THAT MAKE YOU THINK

What can we do as individual human beings to save the environment?

Why is it called a building if it's already built?

Why does your nose run, but your feet smell?

What do you live for?

If the universe is constantly expanding, what is it expanding into?

What's your idea of heaven?

What letter is silent in scent – S or C?

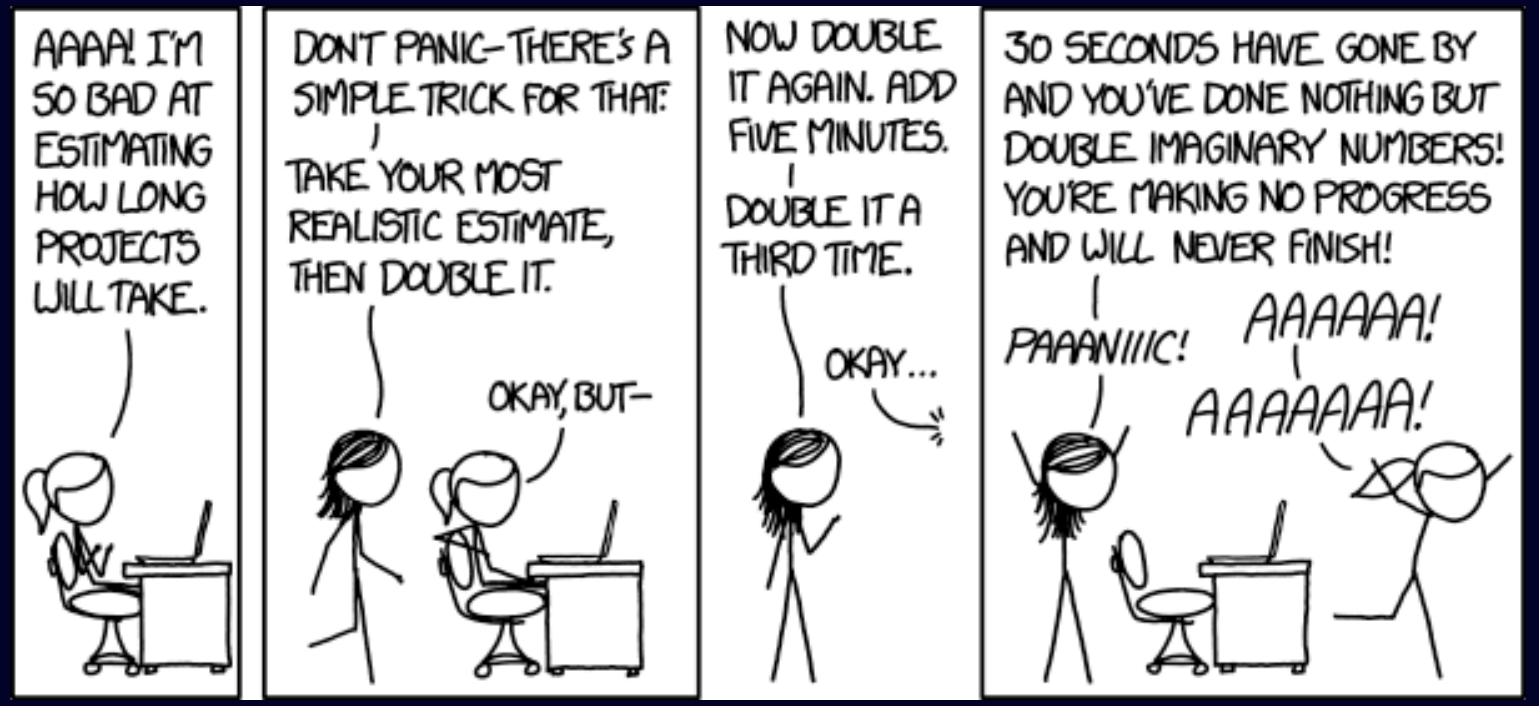
What came first – the fruit orange or the color orange?

If you hire a guy to kill you, will it be ruled as suicide or murder?

Where do our thoughts come from?

The Pleasant Conversation

Trained in Calibration

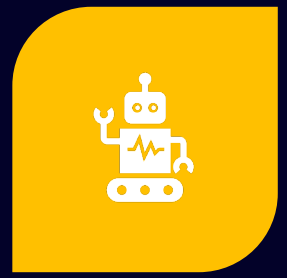


FAIR22 CONFERENCE

Be comfortable with basic probability and numbers

FAIR22 CONFERENCE

Training



SCOPING, SCOPING, SCOPING

HOW DOES LOSS UNFOLD IN THE EVENT?

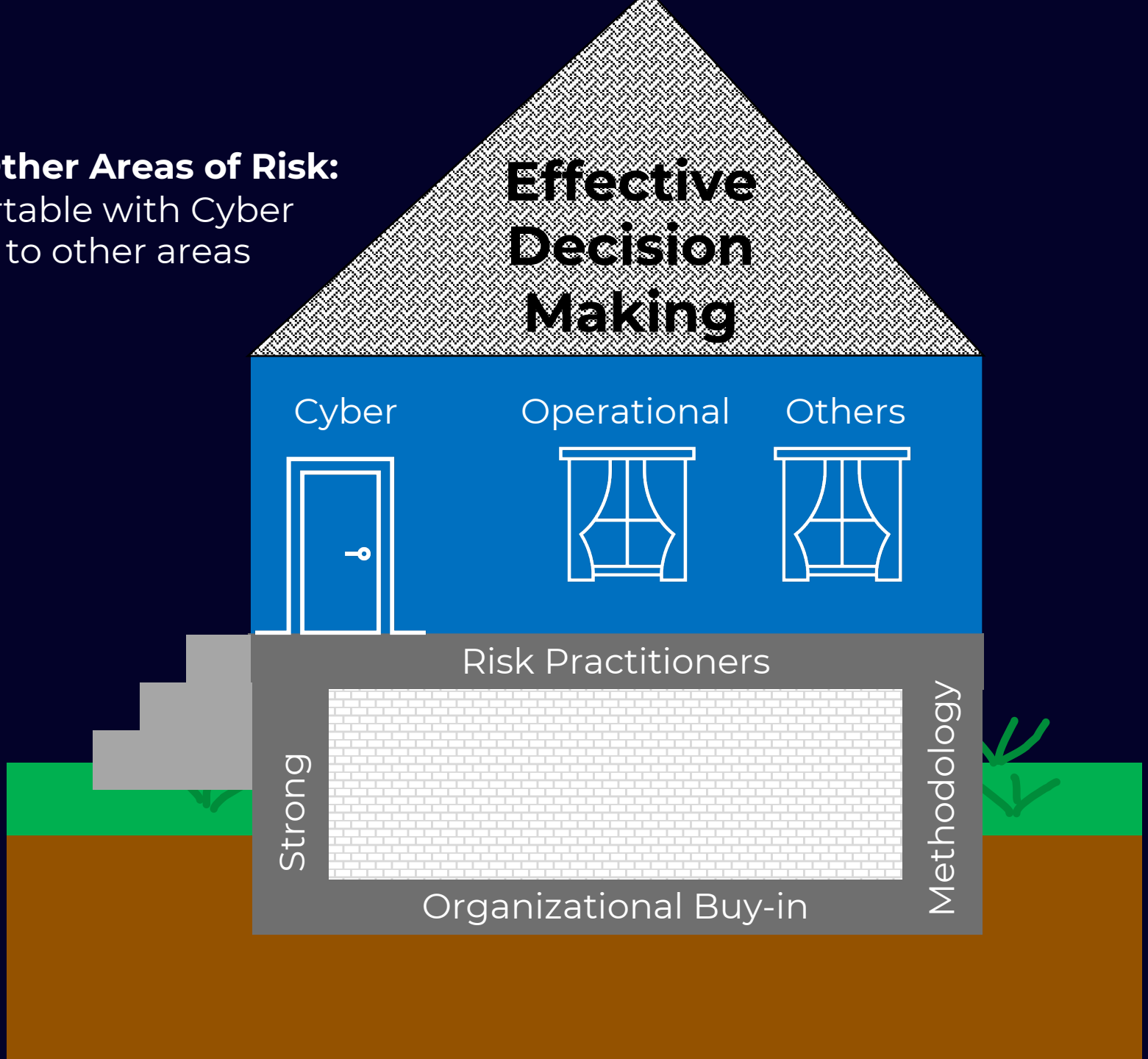
ANALYST CHALLENGES – SIMULATE REAL WORLD SCENARIOS

DATA GATHERING SHADOWING

FAIR22 CONFERENCE

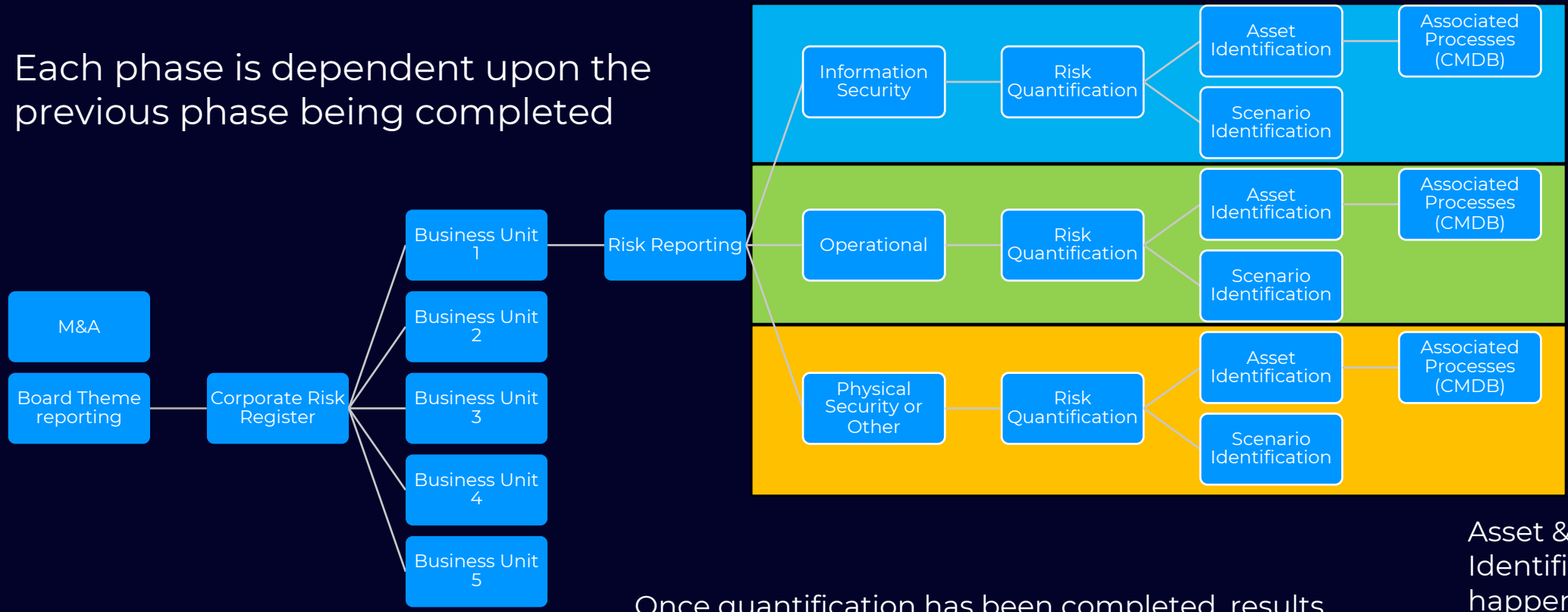
Evolving to Other Areas of Risk:

- Get Comfortable with Cyber
- Then move to other areas



FAIR22 CONFERENCE

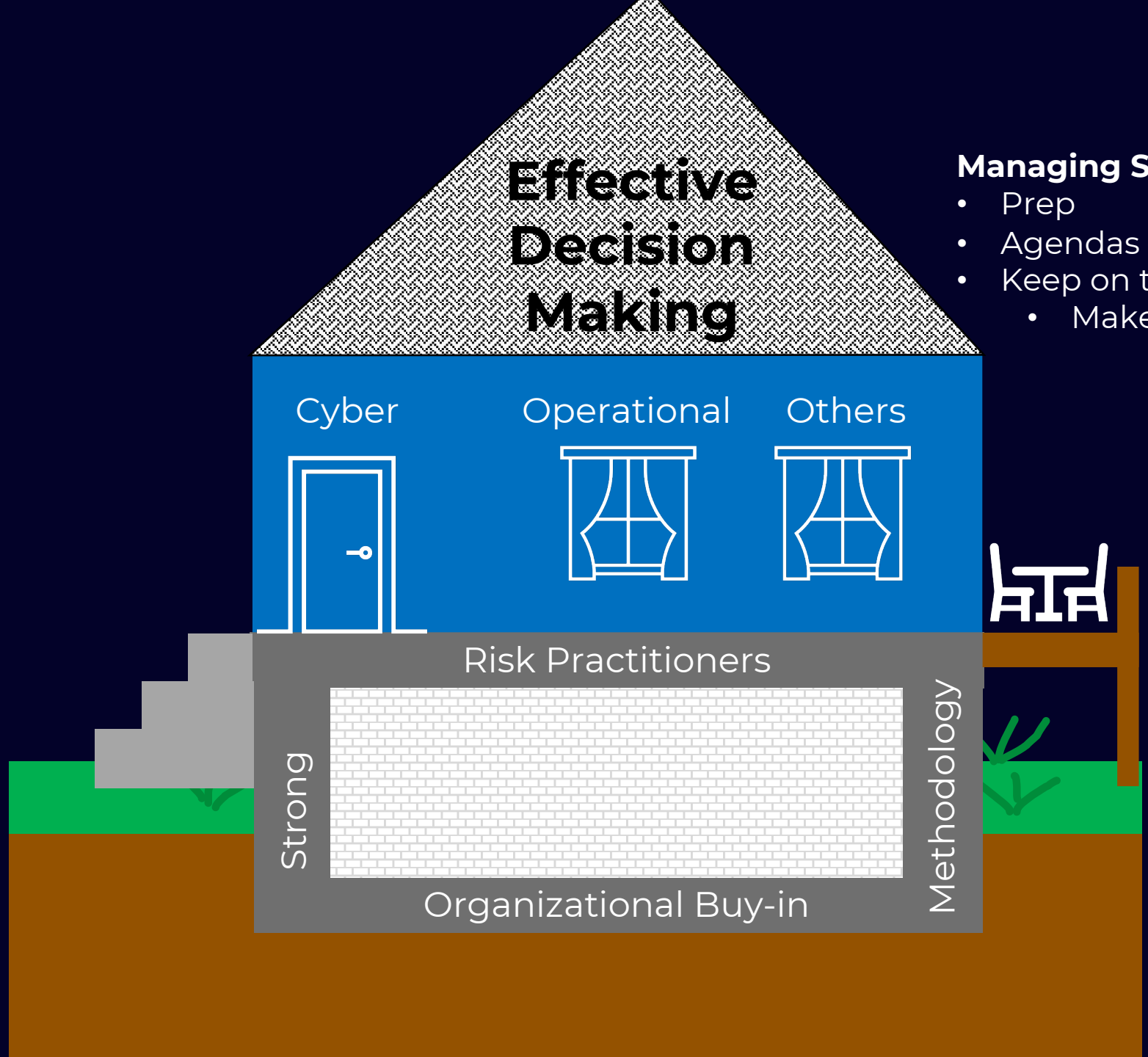
Each phase is dependent upon the previous phase being completed



Asset & Scenario Identification may happen in tandem

Once quantification has been completed, results will be presented quantitatively to the appropriate stakeholder. This completes the phase.

FAIR22 CONFERENCE



Managing Stakeholder Burnout

- Prep
- Agendas – SEND WITH INVITE
- Keep on topic
  - Make sure they feel heard

FAIR22 CONFERENCE

Questions

FAIR CONFERENCE 22