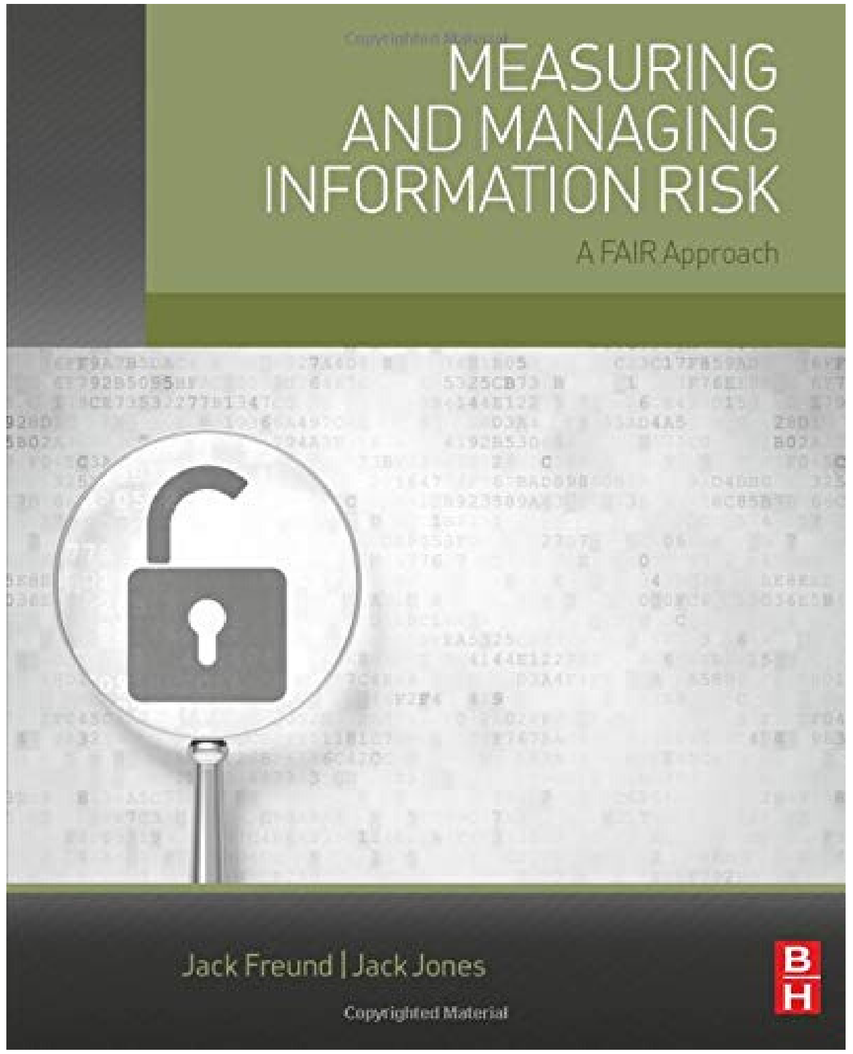
BOOK CLUB

# Measuring and Managing Information Risk

Part 3: Chapters 6 - 7



# What Will We Cover Today?

Use the following guide during your book club to drive discussion around the chapters outlined

## Chapter 6

Analysis Process

## Chapter 7

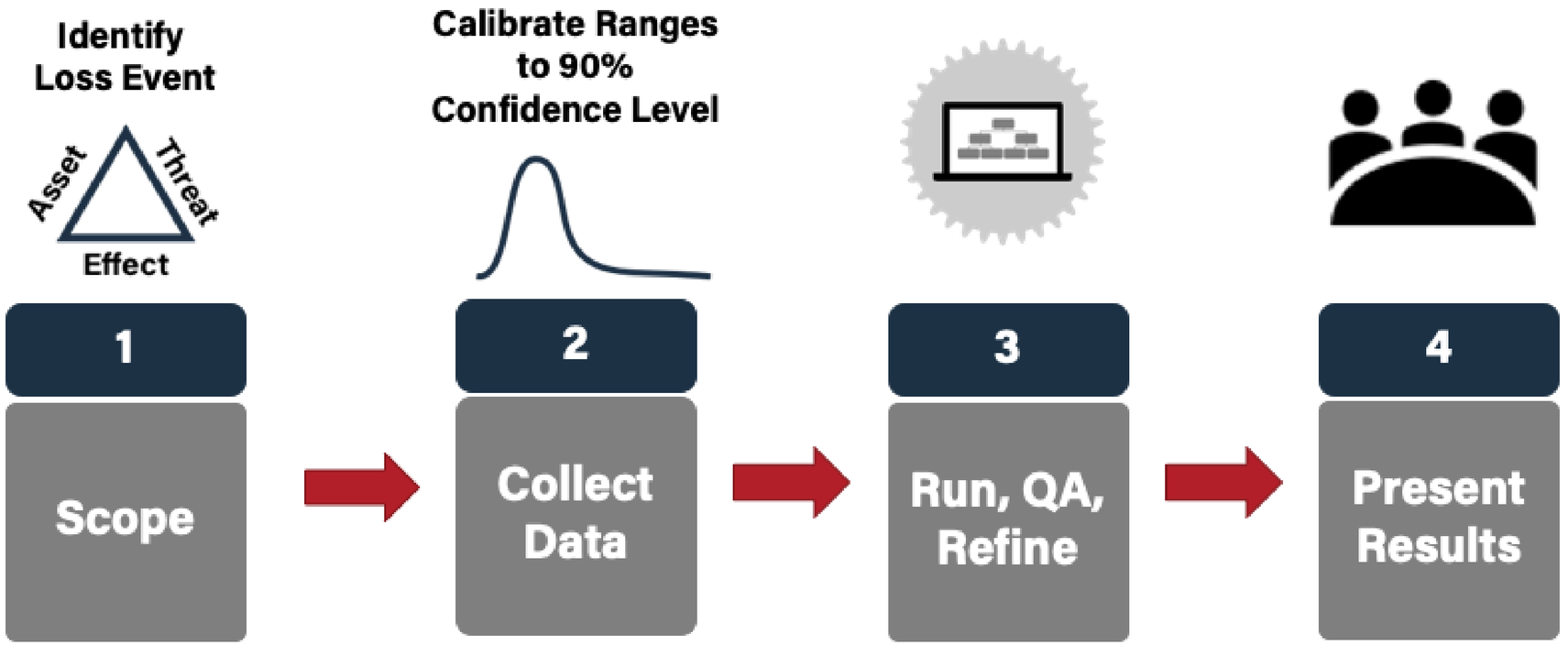
Interpreting Results

# Chapter 6: Analysis Process

FAIR is a nomenclature, ...for thinking through complex scenarios clearly and confidently, and it is a way to explain how you came to your conclusions.

*Measuring and Managing Information Risk*

# How to Apply the FAIR Model?



# Scoping a Scenario

As a group - decide on a common concern the organization has. This could be a crown jewel database, the cloud, manufacturing plants, etc.

I'm going to use the Crown Jewel DB as an example

### *Define an Asset*

What is the thing of value you're concerned with.
**Ex:** Crown Jewel DB containing PII and PCI

### *Define a Threat*

Who is acting on your asset to cause a loss?
**Ex:** External Malicious Actor

### *Define an Effect*

What loss are they causing?
**Ex:** Confidentiality

### *Define the Method (optional)*

How will this actor cause the loss event?
**Ex:** Successful Phishing Attack

# Scope Creep

How did the case study go? Did you find yourself expanding the scope to something that seems impossible to measure?

Word of advice - **start small** - get comfortable with something you know then expand from there!

# Reusing Data

What forms of loss would materialize in each scenario? Do you see areas where you can reuse data across scenarios?

What is different - severity of scenario?

Breach of DB containing PII via an External Malicious Actor.

Outage of the VPN due to System Failure (capacity overload).

Breach of a Customer Application via a Malicious Insider.

Outage of the Online Customer Portal via an Insider Error.

Tip: There are similar losses - like responding to customers, productivity loss, responding to the event - that we could reuse!

# Maybe you're wondering why we talk about scoping so much...

*Any entire chapter? Really?*

Well my guess is that any FAIR practitioner would say SCOPING is the most important part of the analysis process.

**You cannot measure what you CANNOT define!**


THOUGHTS?

# Chapter 7: Understanding Results

1. *Focus with the end in mind*

When delivering results, you should first go back to WHY you did the analysis. Is this answering that question you started with?

There are many different graphs and reports shown in the book - are there any that stick out to you? Any you enjoy or just don't understand?

*2. What would your audience best understand?*

I know we give heatmaps a hard time, but if your audience is use to seeing heatmaps and colors defining your risk then this is an opportunity to take your defensible quantitative figures and put them into something they can digest - this is not a sin - we will not be mad at you.

Do you think you'll need to continue with your current reporting approach for some time?

# ALE (Annualized Loss Exposure)

*Total Loss Exposure*

**If you're reading this on a Friday (or any day) you may be thinking we are about to go drink a beer. We completed our analysis now time to celebrate!**

Actually this represents how much loss exposure (or risk) we could have within a given year. FAIR will annualize our risk to help us understand how much risk we could have this year but also the probability of incurring x amount of loss in years to come.

## Frequency x Magnitude

In simple words, ALE = frequency x magnitude in the FAIR Model. ***When do you think this would be helpful to report on?*** In the book it is referred to as 'Total loss exposure' and you can see it displayed in a range of potential outcomes - ***do you think your management would enjoy seeing the results in financial terms***?

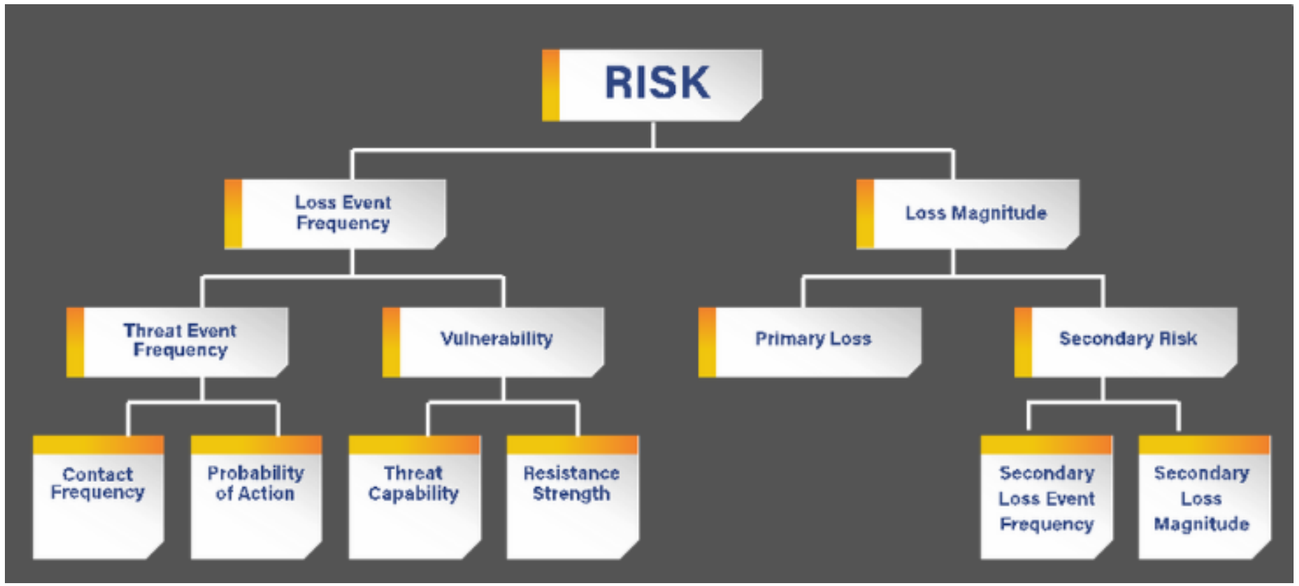
# Wrap-Up

*It's time to finish you ALE's and talk through any final thoughts.*

Anything in the book I missed? What do you as a group find to be a challenging area thus far?

### *FAIR Certification Exam Hint:*

Study and memorize the stable and unstable conditions if you plan to take the exam. My favorite is to think through an example to help me remember!




# Final Thoughts?

Open discussion...

Join the Book Club discussion online! Share your club's insights, your feedback to the Guide or pose a question at the FAIR Institute's LINK community site (FAIR Institute membership and LINK signup required).

Join the Book Club discussion online!