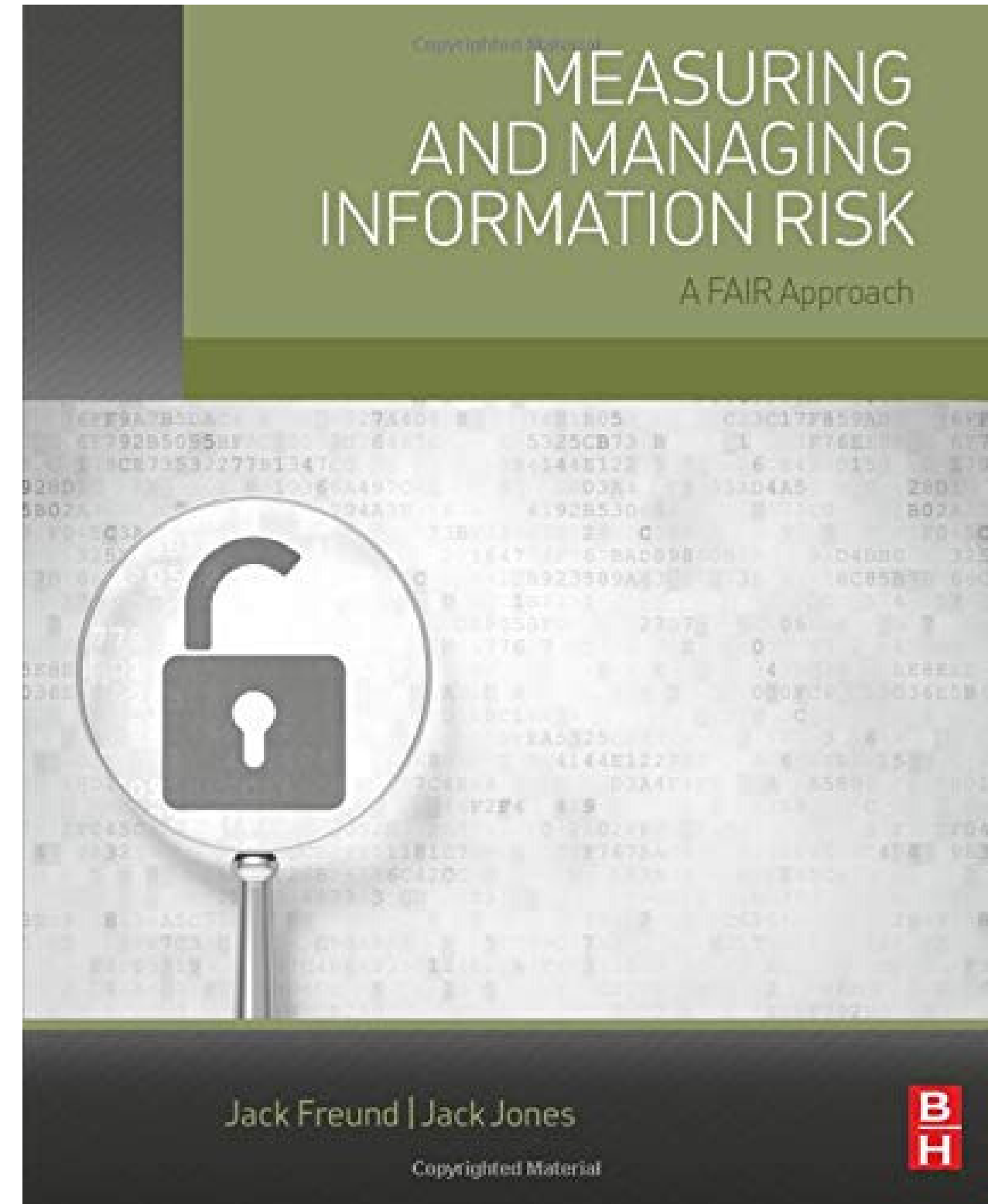


BOOK CLUB

Measuring and Managing Information Risk

Part 4: Chapters 8 - 9



...

What Will We Cover Today?

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

Chapter 8

Risk Analysis Examples

Chapter 9

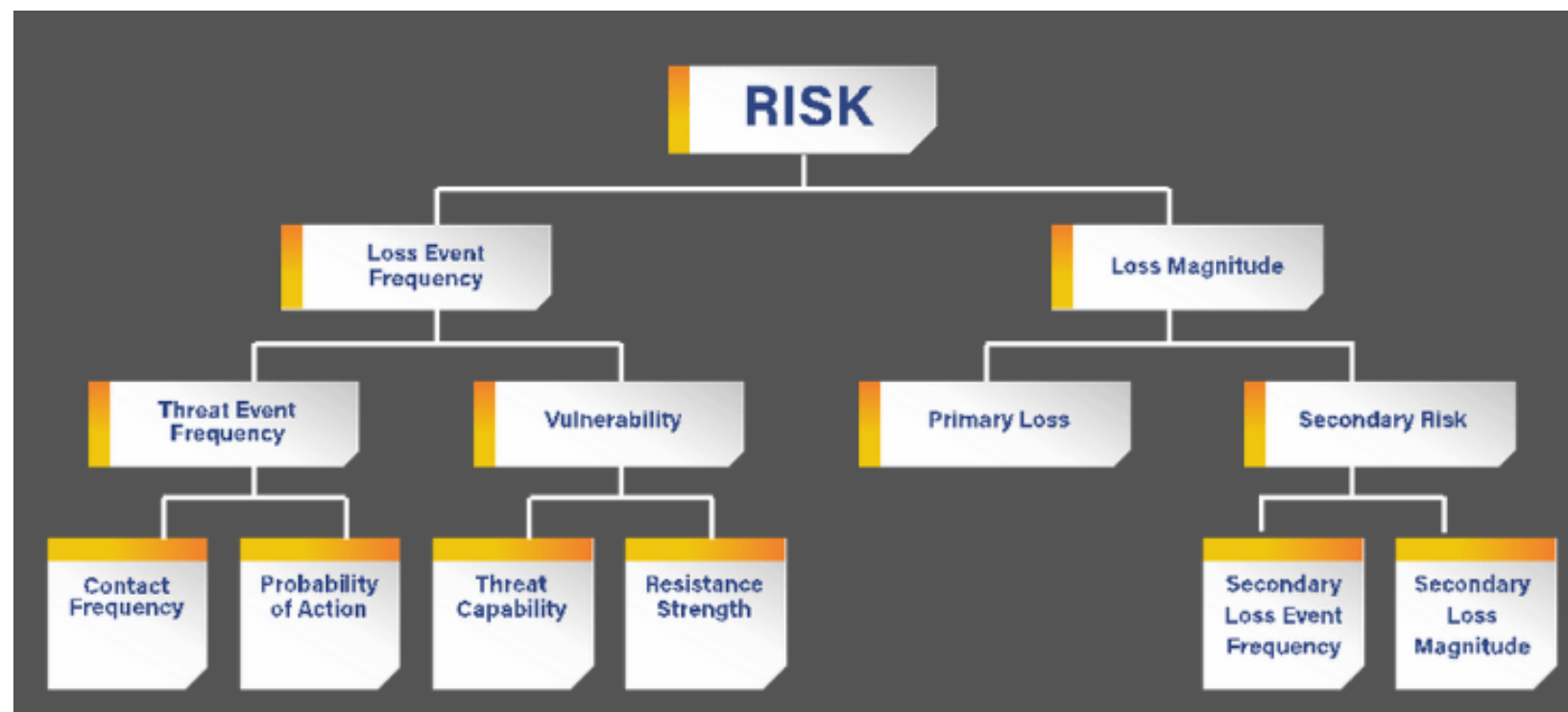
Thinking about Risk Scenarios Using FAIR

Chapter 8 - Risk Analysis Examples

Applying Our Knowledge

You may or may not have read through the examples but this guide is going to focus on applying an example to what you would actually measure in practice. We will start with scoping and go through the data gathering phase together to come up with our analysis!

You can break up in groups and agree on a scope, scope it out together as a team, or work individually and come back together for a review and debrief!



Bringing it *All* Together

Next few pages will cover the following topics...

- **Scoping**
- **Data Gathering**
 - Frequency
 - Vulnerability
 - Primary Magnitude
 - Secondary Magnitude
- **Reviewing Reporting**



Quick Tip: There is a free tool online to use FAIR in action - use throughout this activity to guide your data inputs. Find the link [here](#) or search for FAIR-U online.

Scoping

Step 1: Pick a concern in your organization - *I will provide my example throughout*

Note: If using FAIR-U you are able to work in the CIA Triad. If your scenario is operations focused you can still select one of the effects and just use FAIRu because it works directly at the model.

Asset

What is the thing of value we are concerned with?



Ex: *Customer Database containing PII*

Threat

Who is taking action against our asset?



Ex: *External Malicious Actor*

Effect

What loss effect will they cause? (pick 1)

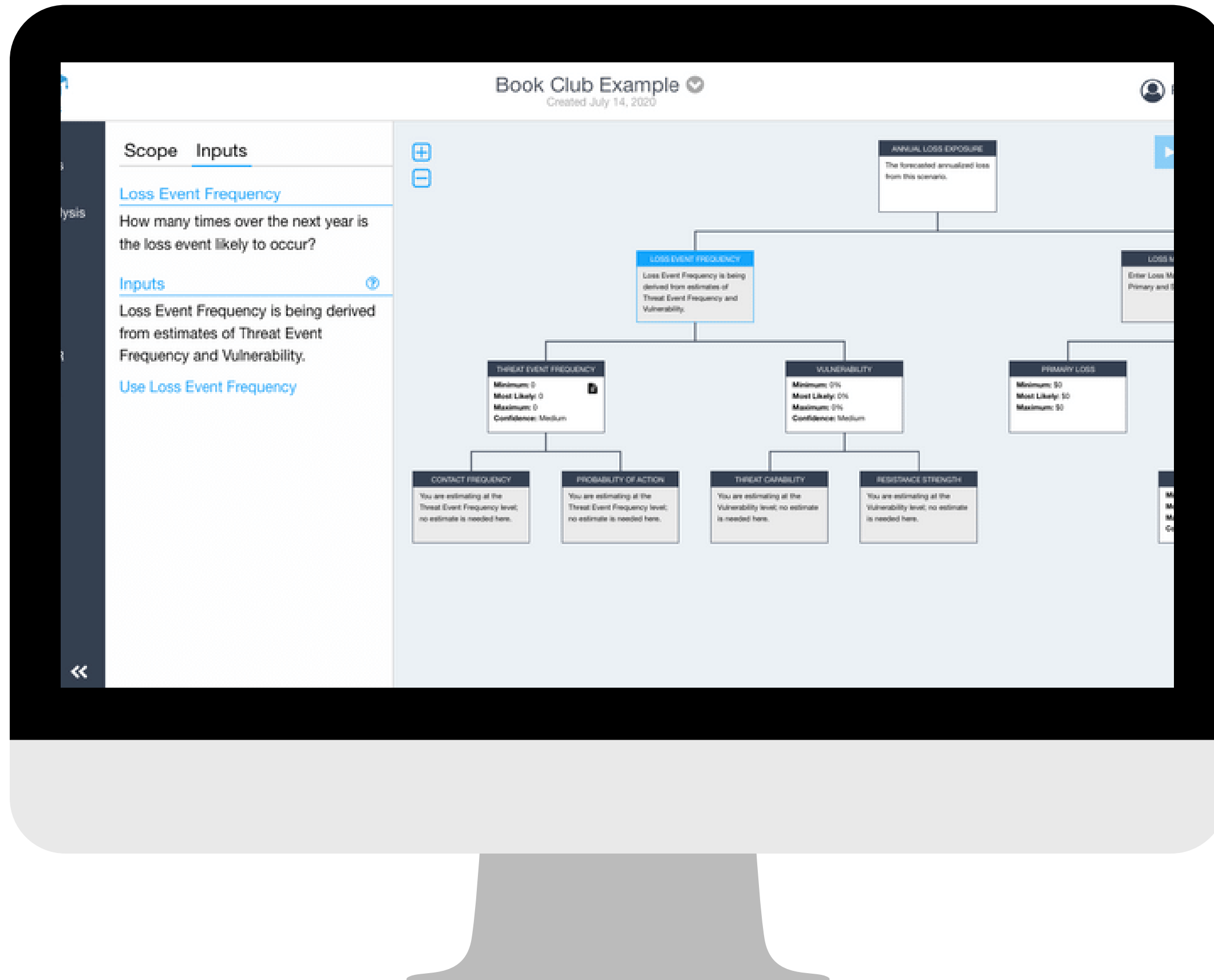


Ex: *Confidentiality*

Update your scope in FAIR-U (or use RiskLens if you have it)

What does your loss event represent?

In my example it is a breach of the Customer Database via an External Malicious Actor!



Step 2 - Frequency

Top Down Approach

Remember FAIR is a top down approach - start at your loss event frequency and work your way down. You work where you have the best readily available data.

Example - Decomposing the Problem

*I have **never** seen a successful breach of the Customer Database via an External Malicious Actor. I've been at the organization for 5 years.*

I was able to review a recent Incident Response report and we see around 10 - 24 incidents per year. We can also use an industry data report to further refine this number and according to the CrowdStrike report 2019, 25% of incidents are related to confidentiality. To account for the unknown we will consider 25 - 50% of our incidents as breach related attempts.

Quick Tip: For the purposes of our case study I would recommend using calibrated ranges and estimates.



Update Frequency Data

Where did you work in the model?

In my example I *did not know* about any successful events so I worked at **Threat Event Frequency**.

Data Inputs (#)

Min: 2.5

- **Rationale:** 10 incidents x 25% (Based CrowdStrike Data)

Max: 12

- **Rationale:** 24 incidents x 50% (Based on CrowdStrike data - but increased for uncertainty)

Skewed most likely towards the minimum.

Scope Inputs

Threat Event Frequency

How many times over the next year is the threat event likely to occur? How many times will the asset face a threat action?

Inputs

Minimum	Most Likely	Maximum
2.5	5	12

Confidence: **Medium**

Rationale

Min: 2.5
 Rationale: 10 incidents x 25% (Based CrowdStrike Data)
 Max: 12

LOSS EVENT FREQUENCY
 Loss Event Frequency is being derived from estimates of Threat Event Frequency and Vulnerability.

THREAT EVENT FREQUENCY
 Minimum: 2.5
 Most Likely: 5
 Maximum: 12
 Confidence: Medium

VULNERABILITY
 Minimum: 0%
 Most Likely: 0%
 Maximum: 0%
 Confidence: Medium

CONTACT FREQUENCY
 You are estimating at the Threat Event Frequency level; no estimate is needed here.

PROBABILITY OF ACTION
 You are estimating at the Threat Event Frequency level; no estimate is needed here.

THREAT CAPABILITY
 You are estimating at the Vulnerability level; no estimate is needed here.

Step 3: Vulnerability











Map out key controls that would stop a success attack from happening!

Typically I look at my 10 key controls and then build my vulnerability estimate around the efficacy of those controls.

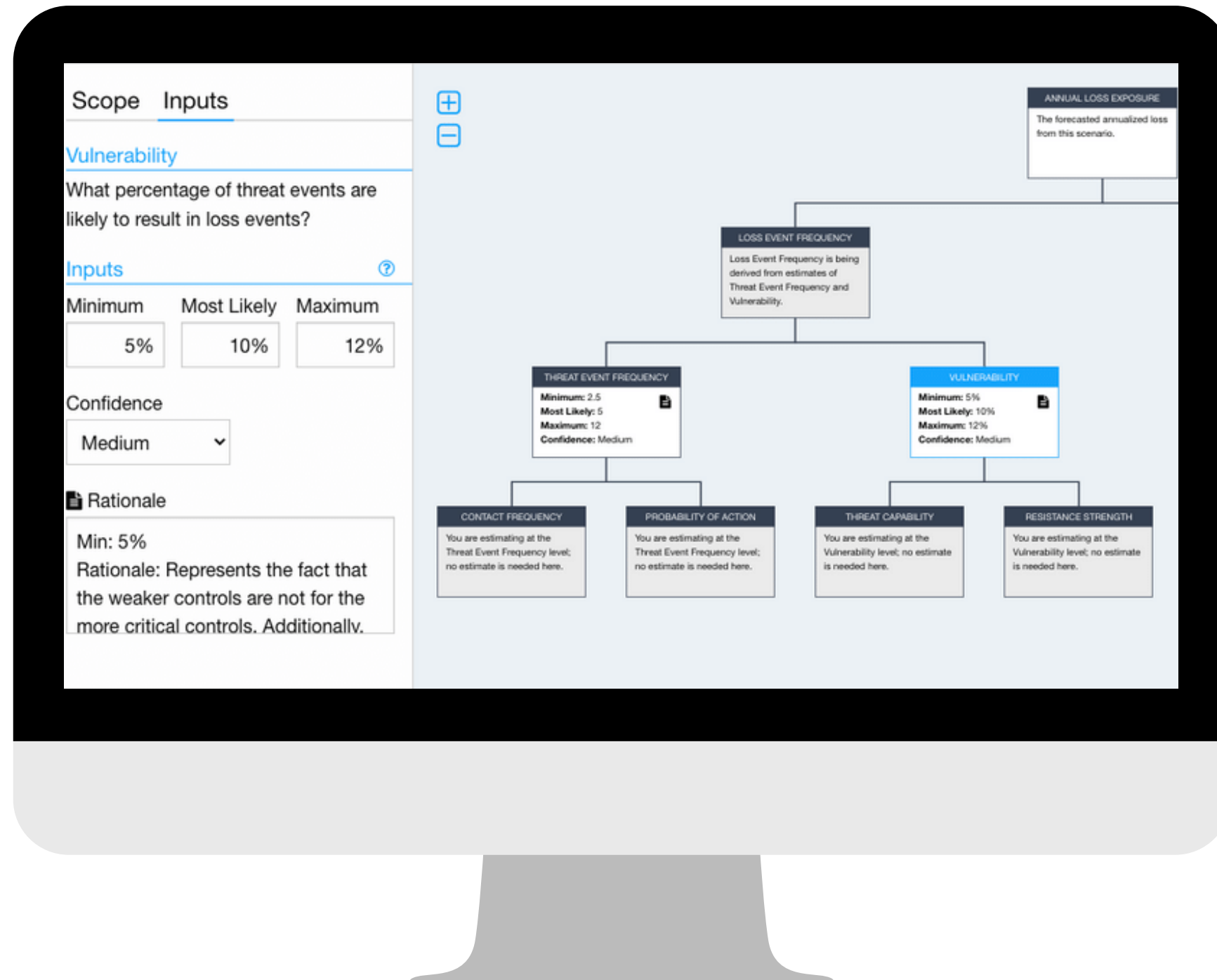
If they are operating as intended they get a checkmark and if not they get a minus.

For example to the right my **Vulnerability = 10%**

This is just one way to estimate it but I find it to be useful!

-  Multi-Factor Authentication
-  Patching - not compliant
-  Appropriate Privileged Users
-  Phishing Awareness Campaigns
-  CrowdStrike in place
-  Proofpoint - email filtering
-  Pen Testing - few issues
-  User Behavior Tools
-  FireEye Detection
-  Honeypots set up for key systems

Update Vulnerability Data



Where did you work in the model?

In my example I worked at the highest option on the vulnerability side - you can work lower if you please!

Data Inputs (%)

Min: 5%

- **Rationale:** Represents the fact that the weaker controls are not for the more critical controls. Additionally, we have never seen a successful breach.

M/L: 10%

- **Rationale:** Based on key control assessment.

Max: 12%

- **Rationale:** Accounting for uncertainty within range.

...

Step 4: What will materialize?

Forms of Loss to Consider

Primary Response

Incident response, investigations, 3rd Party investigations, etc.

Secondary Response

Sending letters to our 10m customers, involving PR, sending credit monitoring options to customers, additional audits, etc.

Secondary Fines & Judgments

F&J imposed by regulators and customers.

Secondary Reputation

Our customers are locked in so we do not expect much - if any - reputation damage. Will consider at the max end.

Update Magnitude Data

What forms of loss did you use?

In my example I thought through the losses that would materialize for a breach of 10m PII records.

Data Inputs (\$)

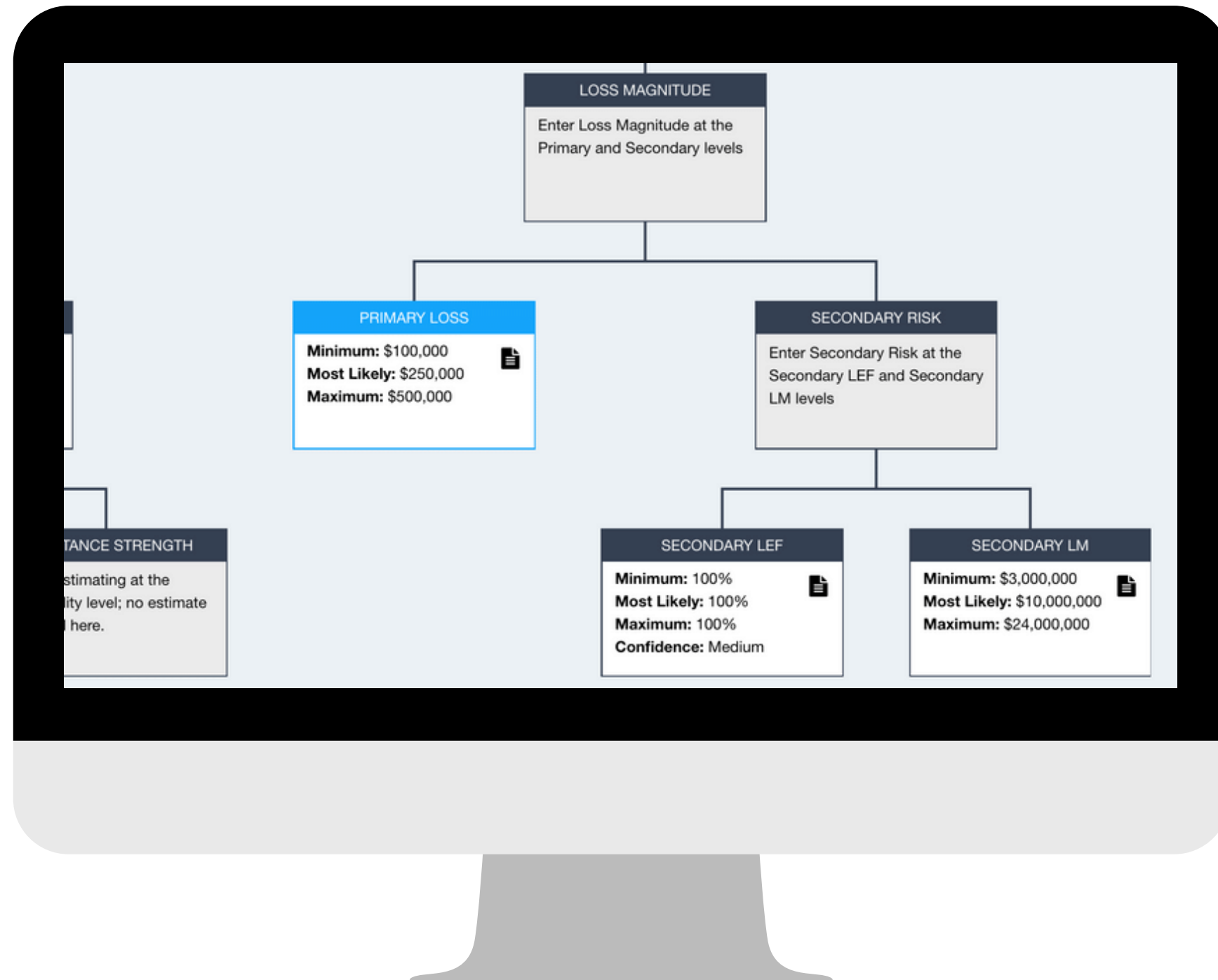
Primary Response: \$100k - 500k

Secondary Response: \$2m - \$10m

Secondary F&J: \$1m - \$10m

Secondary Reputation: \$0 - \$4m

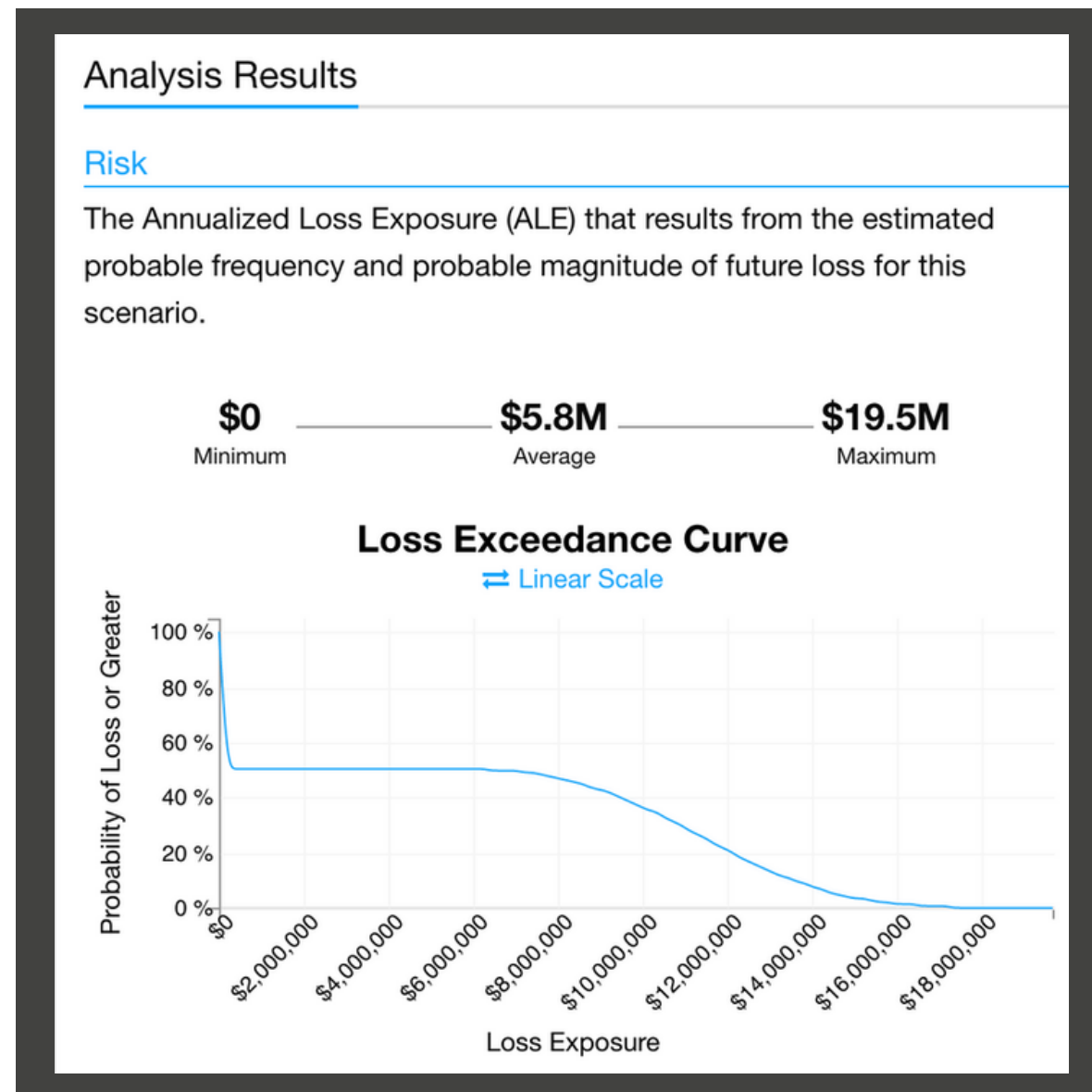
SLEF: 100% - all records are PII



Understanding Reporting

Analysis Results

The report below tells us our Annualized Loss Exposure (ALE). Essentially, this is the frequency times the magnitude.



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.51	1
Loss Magnitude	\$105.1k	\$267.3k	\$490.5k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.51	1
Loss Magnitude	\$4.3M	\$11.2M	\$19.7M

Vulnerability 8.89%

Per Event Metrics

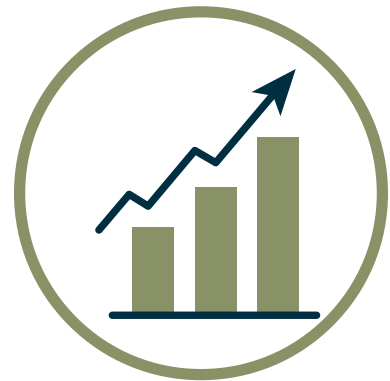
The report above tells you how frequently (loss events/year) this *could* happen and how much it could cost per event (magnitude).



Project Prioritization



Vulnerability Management



Cost Benefit Analysis



Reporting to the Board

Chapter 9

Thinking about Risk Scenarios Using FAIR

We've walked through a few examples throughout the guides - have you begun to think about how your department, team, or even organization can begin to use FAIR to make decisions?

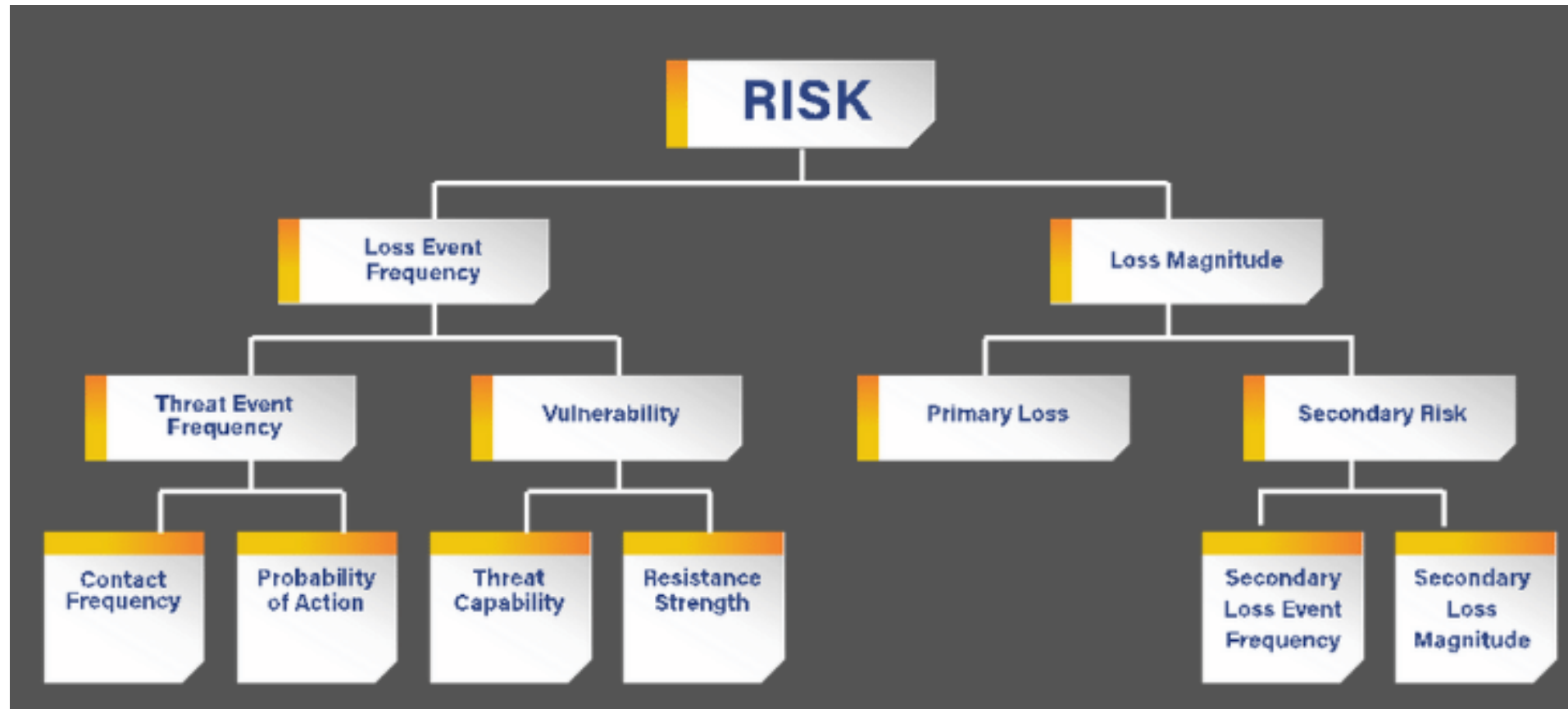


The FAIR Institute

Ohhh oh...you're
halfway there.

Bon Jovi

*We are now halfway through book club
- keep on going and let us know if
you're enjoying the guides.*



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!](#)