Practical Risk Quantification
It changes things...

Jack Jones, CISSP, CISM, CISA

What we'll cover...

- Why would change be a good thing?
- Why has quantification been so hard?
- Common concerns
- There's quantitative and then there's "quantitative"
- Practical risk quantification
- Q&A

Why change?

Example...

- Engaged a “Big Four” firm to conduct an attack and penetration exercise
  - Among their findings, several issues were rated “high risk”
  - After conducting a risk analysis, they conceded that none of those issues actually represented high risk

Example...

- Risk issue needed to be addressed
  - Evaluated three mitigation approaches
    - “Best practice”
    - And two atypical options
  - After analysis, option “B” (not “best practice”) was expected to be as effective as the best practice solution, but at ~$250,000 less per year
  - Guess which one management chose...

What management cares about...

- How much risk do we have?
- If I spend this money, how much less risk will I have?
- What benefit am I getting from the money I'm already spending?
- Which are my most cost-effective options?

Why has quantification been so hard?

You can't measure what you haven't defined

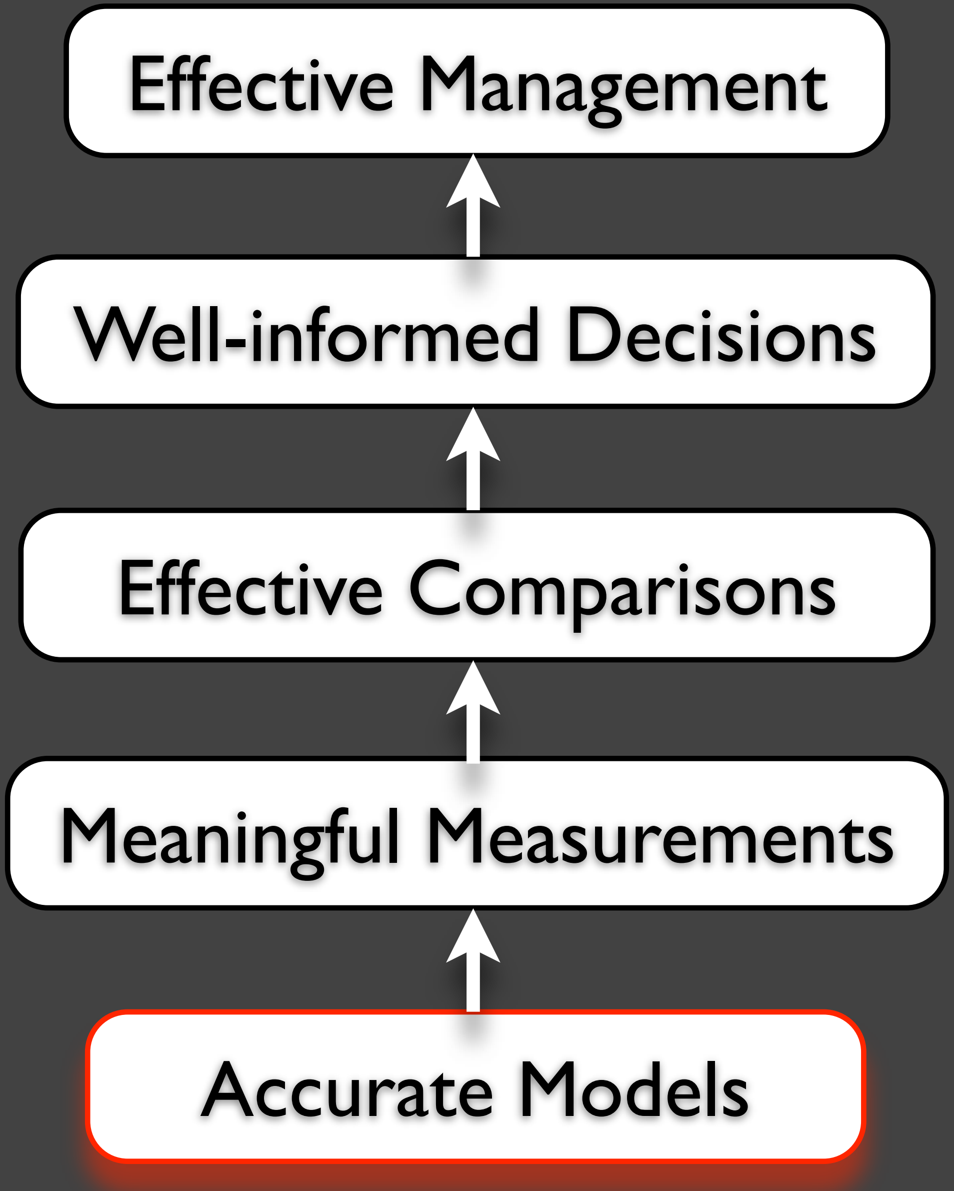
Which of these are “profits”?

- Customers
- A supply chain
- Marketing material
- Product development
- An accounts payable system
- A customer account representative

Which of these are “risks”?

- A weak password
- A disgruntled employee
- A poorly trained employee
- An unencrypted backup tape
- An unpatched Internet-facing server
- A database full of sensitive information

The missing ingredient



Effective Management

Well-informed Decisions

Effective Comparisons

Meaningful Measurements

Accurate Models

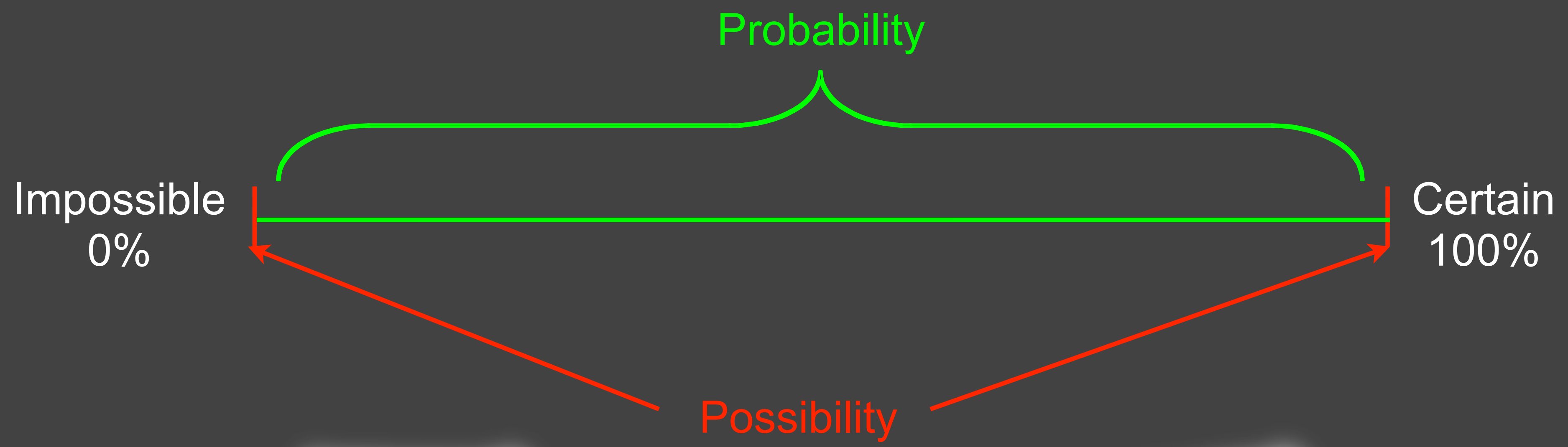
Risk...

The probable frequency and probable magnitude of future loss

In other words...

How often bad things are likely to happen,
and how bad they're likely to be when they do happen

Probability vs. Possibility



Probability

Impossible
0%

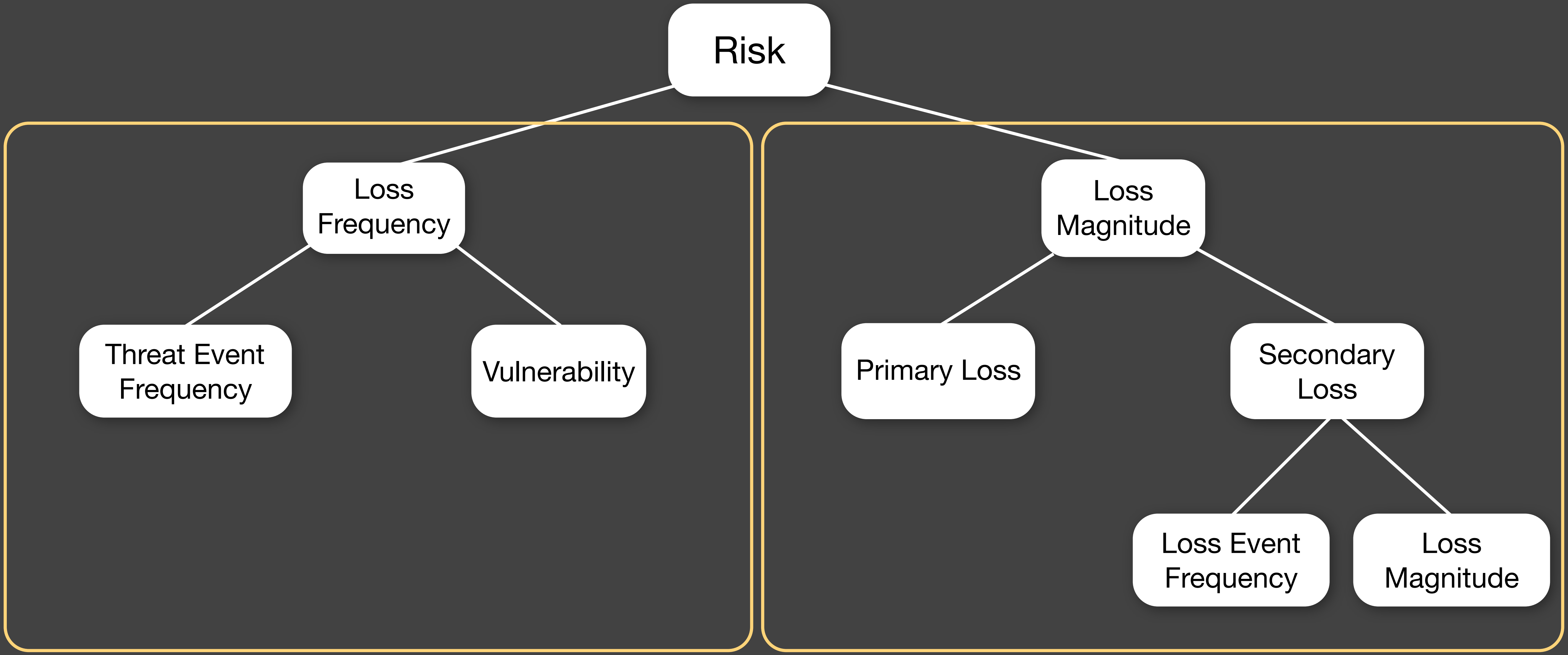
Certain
100%

Possibility

~17%

~100%

The FAIR taxonomy



Risk

Loss Frequency

Threat Event Frequency

Vulnerability

Loss Magnitude

Primary Loss

Secondary Loss

Loss Event Frequency

Loss Magnitude

Loss Event Frequency

Loss Magnitude

Common Concerns

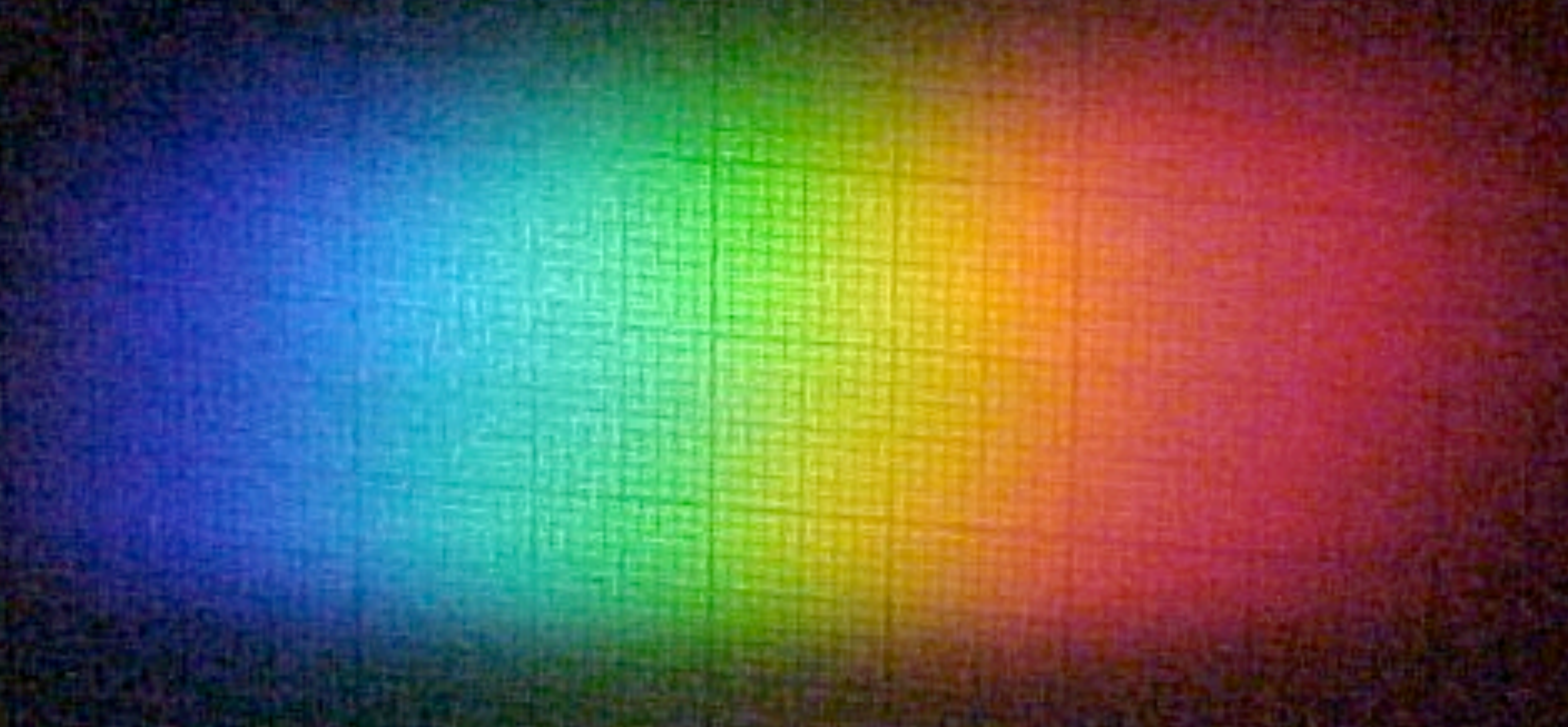
- Prediction
- Subjectivity vs. objectivity
- Accuracy vs. precision
- Data? What data?
- Quantification takes too much time

Prediction

“Prediction is very difficult,
especially about the future.”

(Niels Bohr, Nuclear Physicist and Nobel Laureate)

The dirty word of measurement: **SUBJECTIVITY**

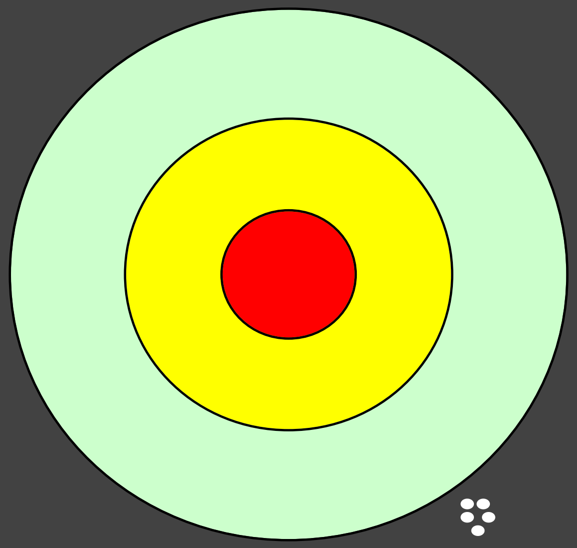


Subjectivity and Objectivity

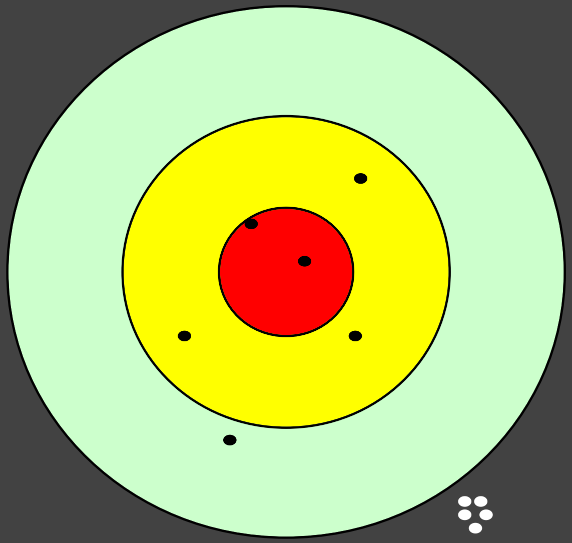
They’re not binary. It’s a spectrum!

- How tall am I?
    - Is that subjective or objective?
- What’s your favorite flavor of ice cream?
    - Is that subjective or objective?
- If you’re approaching a stoplight that’s turning yellow, should you slow down or speed up?
    - Is that subjective or objective?

Precision



Accuracy



Management invariably prefers (and expects) accuracy rather than precision

Data? What data?

- But we don't have enough good data to support quantitative analyses!! Do we?
  - Actually, much of the data is there to be had if we know where to look for it
  - Also, we don't need that much data in order to make well-reasoned quantitative estimates

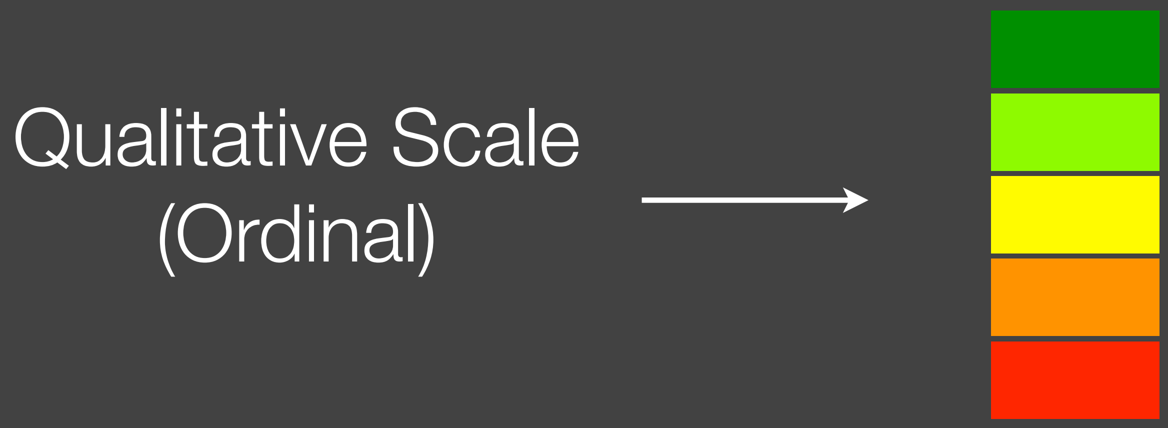
Quantification is too hard!

Quantifying risk CAN take a lot of time and effort...

...but it doesn't HAVE to

There’s quantitative and
then there’s “quantitative”

There’s quantitative and then there’s “quantitative”



Qualitative Scale
(Ordinal)

What does 🟩 x 🟧 equal?

What does 🟨 + 🟩 equal?

Ordinal scales...

What’s the difference?

Scale

🟩
🟩
🟨
🟧
🟥

=

Scale

- Very Low
- Low
- Moderate
- High
- Very High

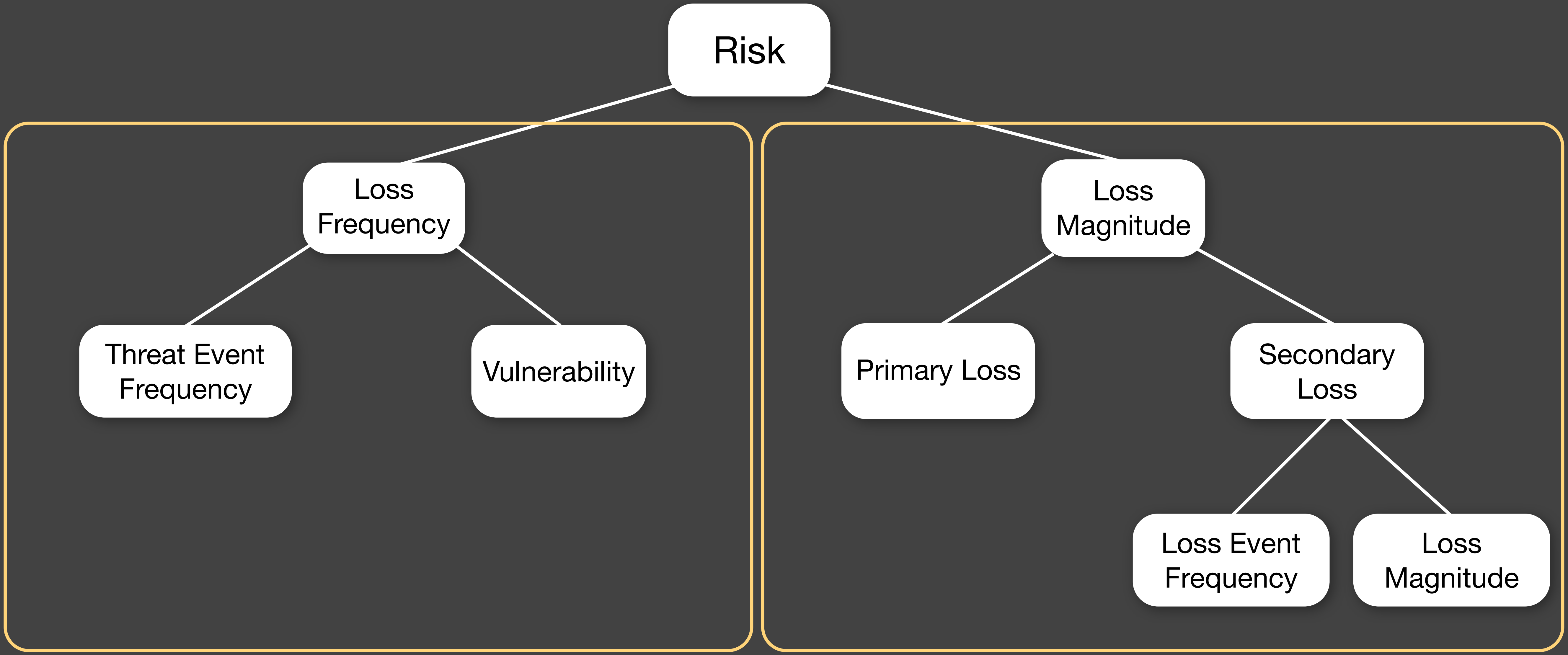
=

Scale

- 1
- 2
- 3
- 4
- 5

Practical risk quantification

Start with an accurate risk model



Loss Event Frequency

Loss Magnitude

Calibrate!

...because you’re never going to have perfect data

What is calibration?

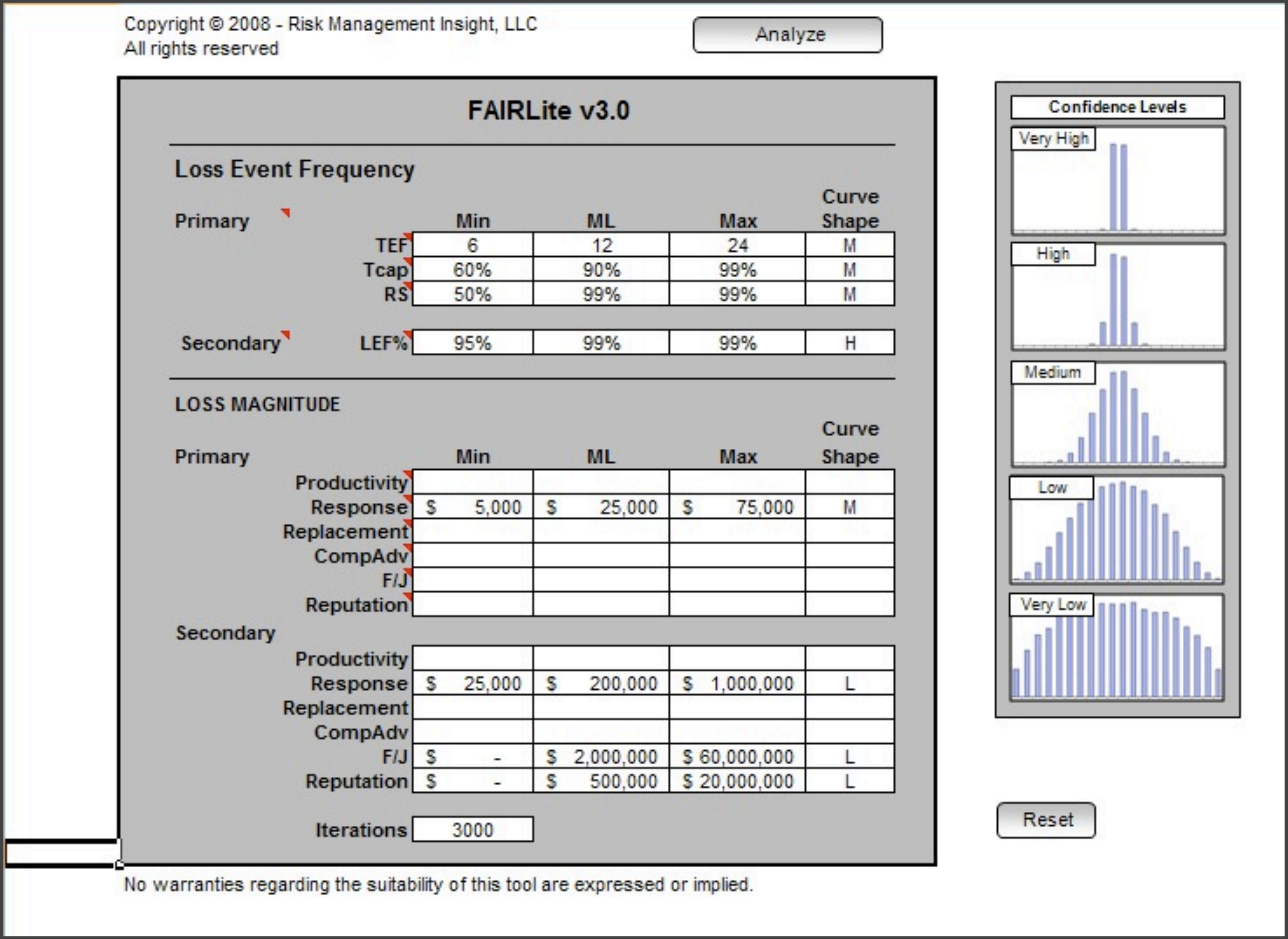
A method for gauging and improving an individual's ability to make good estimates

Why calibration?

- Garbage in, garbage out...
- The ability to estimate effectively varies from person to person
- People can be trained to estimate more effectively

Leverage Monte Carlo!

...because you’re always going to have uncertainty



FAIRLite v3.0

Loss Event Frequency

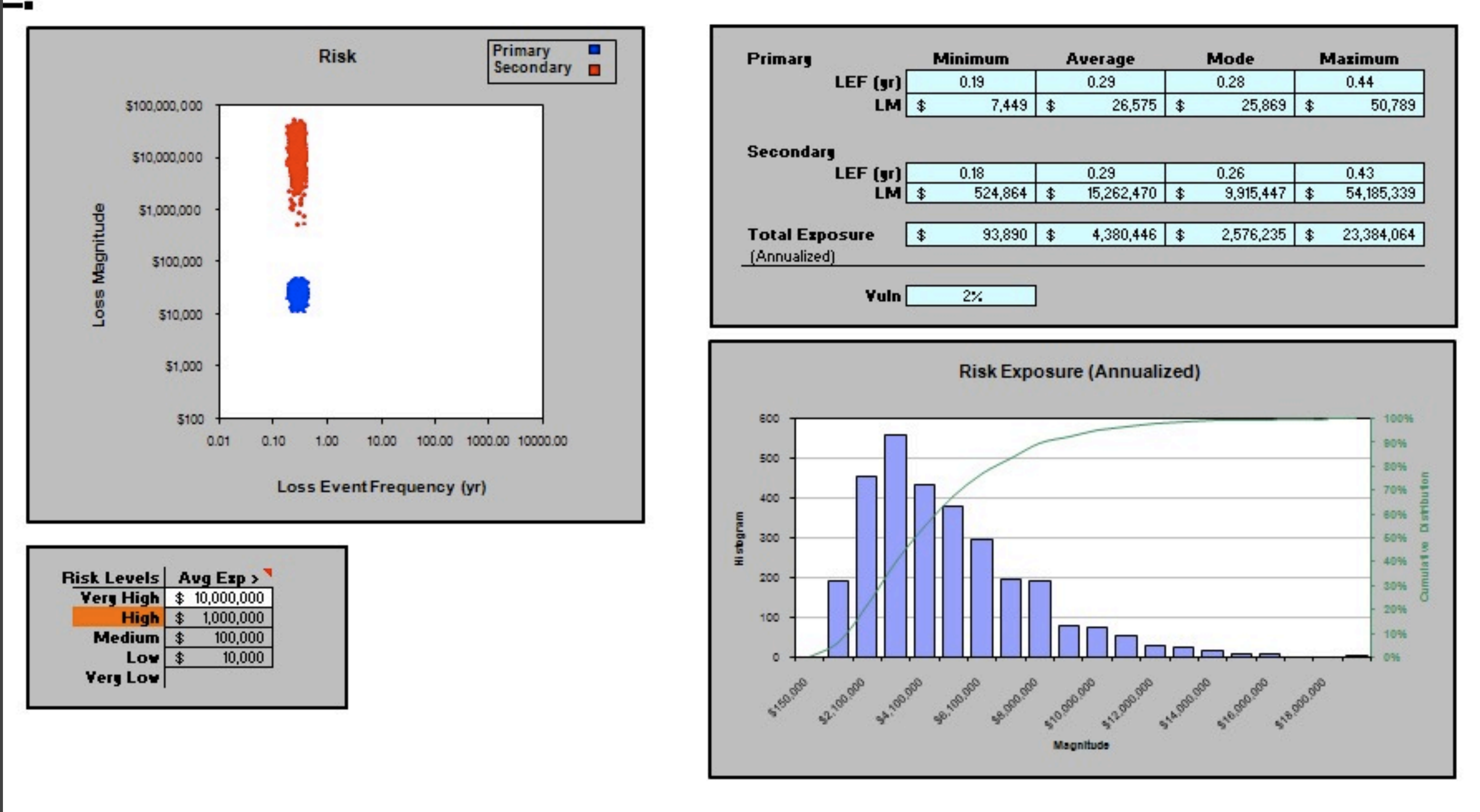
Primary		Min	ML	Max	Curve Shape
	TEF	6	12	24	M
	Tcap	60%	90%	99%	M
	RS	50%	99%	99%	M
Secondary	LEF%	95%	99%	99%	H

LOSS MAGNITUDE

Primary		Min	ML	Max	Curve Shape
	Productivity				
	Response	$ 5,000	$ 25,000	$ 75,000	M
	Replacement				
	CompAdv				
	F/J				
	Reputation				
Secondary					
	Productivity				
	Response	$ 25,000	$ 200,000	$ 1,000,000	L
	Replacement				
	CompAdv				
	F/J	$ -	$ 2,000,000	$ 60,000,000	L
	Reputation	$ -	$ 500,000	$ 20,000,000	L

Iterations 3000

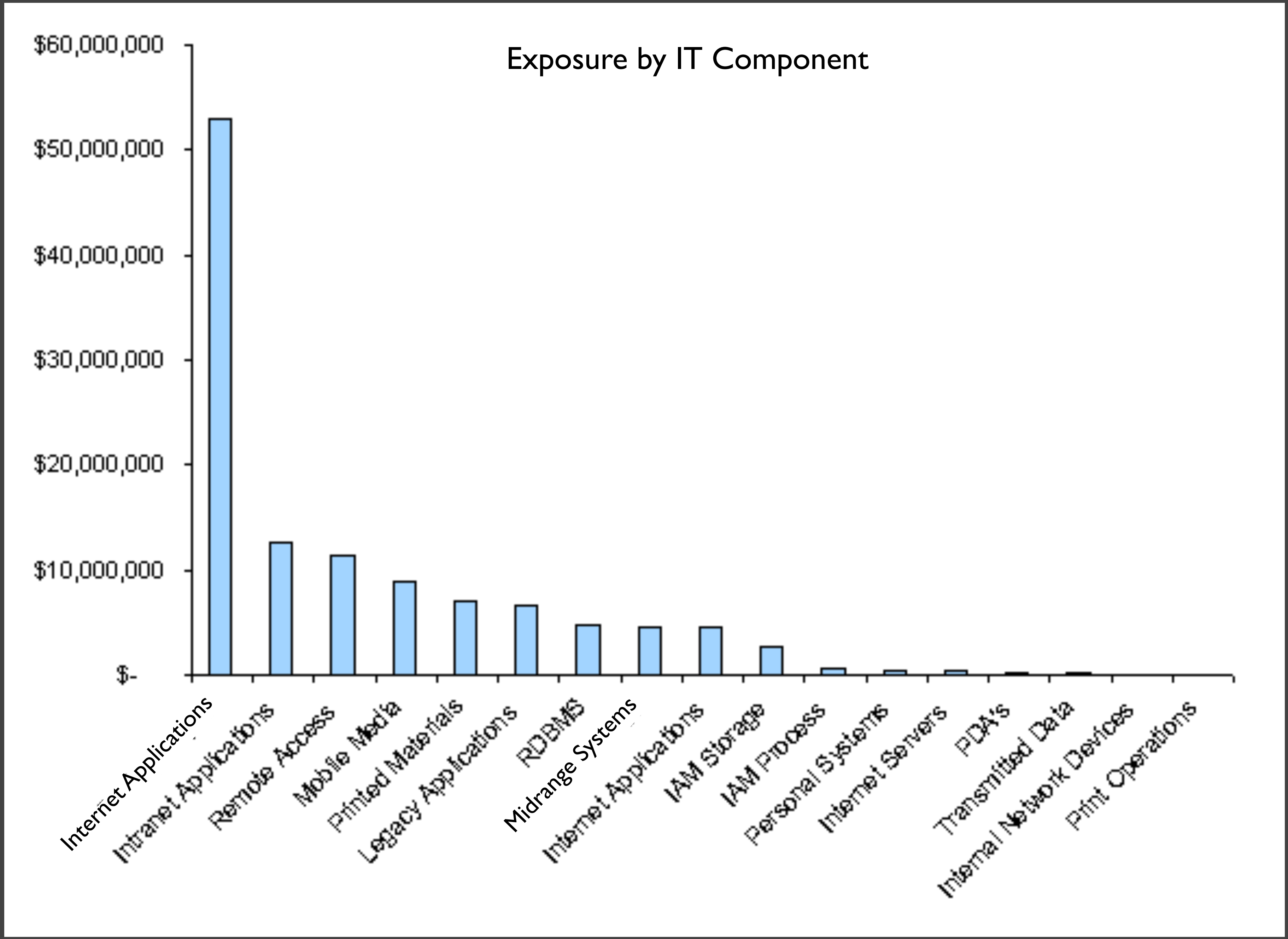
No warranties regarding the suitability of this tool are expressed or implied.



		Minimum	Average	Mode	Maximum
Primary					
	LEF (yr)	0.19	0.29	0.28	0.44
	LM	$ 7,449	$ 26,575	$ 25,869	$ 50,789
Secondary					
	LEF (yr)	0.18	0.29	0.26	0.43
	LM	$ 524,864	$ 15,262,470	$ 9,915,447	$ 54,185,339
Total Exposure (Annualized)		$ 93,890	$ 4,380,446	$ 2,576,235	$ 23,384,064
	Vuln	2%			

Risk Levels	Avg Exp >
Very High	$ 10,000,000
High	$ 1,000,000
Medium	$ 100,000
Low	$ 10,000
Very Low	

Ability to Focus



In summary...

- Management cares about risk - not security
  - Risk management is the only value proposition for security
  - When you focus on the context management cares about (risk), the relationship with management changes
- Risk is a probability issue (vs. possibility)
- Ordinal scales are not quantification
- You have to have accurate models
  - Start with a clear and useful definition of risk...
- Leverage well-known methods for dealing with imperfect data and uncertainty

Good Risk Resources

- Factor Analysis of Information Risk (FAIR)
  - http://riskmanagementinsight.com
- The Open Group
  - http://www.opengroup.org/bookstore/catalog/c081.htm
- How to Measure Anything
  - http://www.howtomeasureanything.com/

Questions?