FAIR Overview

RiskLens®

Bernadette “Bernie” Dunn (She/Her/Hers)

Trainer, RiskLens Academy (bdunn@risklens.com)

- Risk Management Experience in Healthcare, Financial Services, U.S. Federal Government, and Technology & Digital Services
- Developer of Enterprise Risk Management Software Platform Training
- 15 Years Enterprise Software Solutions Executive
- Certified OpenFAIR Trainer, RiskLens
- B.A., Organizational Communications, University of Cincinnati, 2001
- Certificate of Mastery, Rhetorical Theory, University of Cincinnati, 2001
- Certified Leadership Development Coach and Trainer, Next Level Trainings (2015) Deep Coaching Institute (2018)
- DEI Advocate & Co-Chair, RiskLens Diversity Empowerment Council

RiskLens

1. The **Communication** Challenge
2. Moving from **Qualitative** to **Quantitative Risk Management**
3. **FAIR** Risk Model and Importance of Consistent **Terminology**
4. **RiskLens Platform**: Our **Next Steps** Moving Forward
5. Questions

RiskLens

The Communication Challenge

RiskLens

Qualitative vs. Quantitative Measurement Methods

RiskLens®

Risk Management Evolution

Fear, Uncertainty & Doubt → Compliance Checklists/ Maturity Models → Qualitative Impact Assessments → Quantitative Risk Analysis

RiskLens

Subjectivity

Verbal descriptions of probability and impact may not be interpreted equally

Translate each label into a probability

- **Certain = 100%**
- **Highly likely =**
- **Probable =**
- **Unlikely =**
- **Extremely unlikely =**

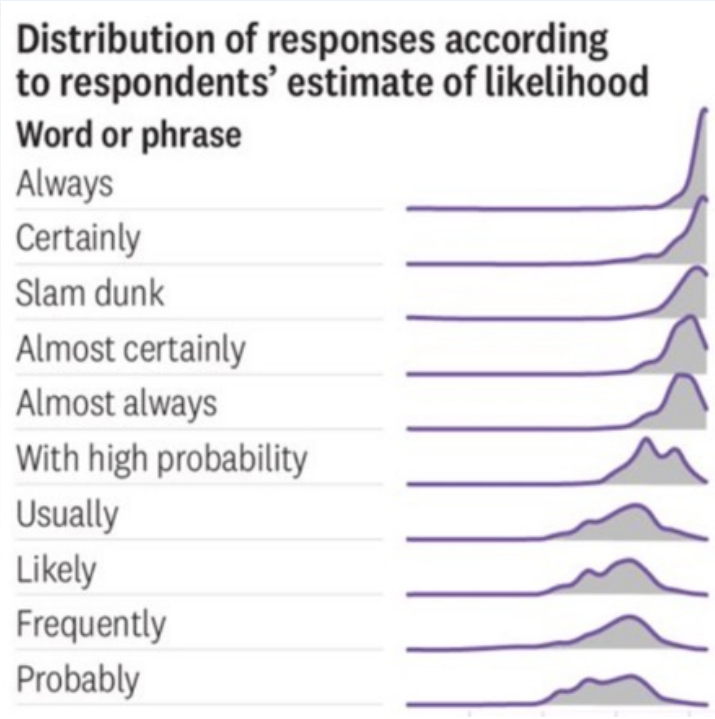
"Not only are [such] probabilistic terms subjective, but they also can have widely different interpretations. One person's "**pretty likely**" is another's "**far from certain**"

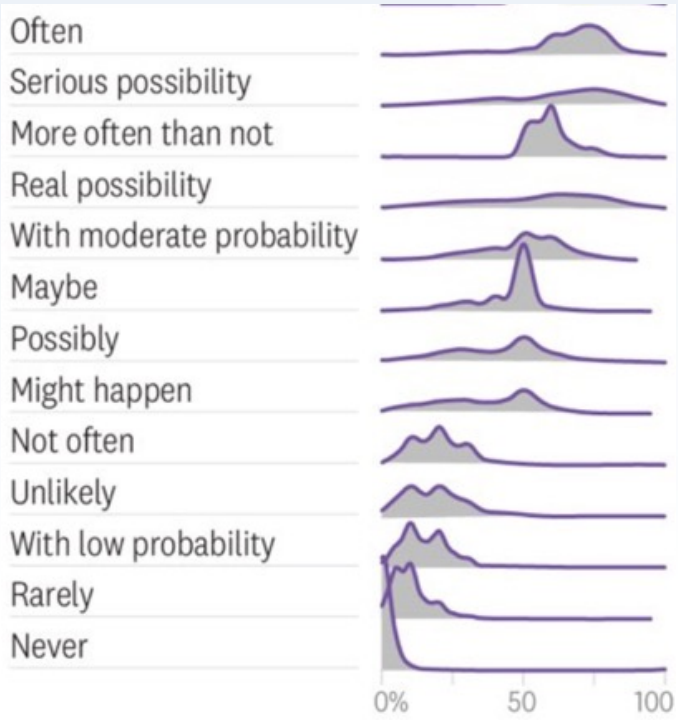
-Andrew and Michael Mauboussin

data scientist at Twitter; professor at Columbia Business School, respectively
authors of the cited HBR article

RiskLens

Subjectivity (continued)





Source: Harvard Business Review

RiskLens

Impact/Likelihood Range Compression

When you break a continuous scale into discrete buckets you lose fidelity and decrease the ability to make meaningful comparisons.

Scenario	Est. Prob.	Est. Impact	Expected Value	Prob. Rating	Impact Rating	Risk Score
A	15%	$500,000	$75,000	2	3	6
B	20%	$800,000	$160,000	2	3	6

This problem is even worse when "High Impact" means > $x.

RiskLens

Flaws with Implying Certainty

- Assigning a single value doesn't allow for expression of uncertainty
- "Supply chain disruption" could last an hour, a day, 8 months…
- We need a forecasting method that shows us a range of probable outcomes

RiskLens

Traditional methods have logical flaws, which prevent us from answering some important risk-based questions.

RiskLens®

Unanswerable Questions

- **How much money might we lose from this event over the next year?**
- **How much risk do we face across the department/ business/enterprise?**
- **Should we invest in this new control? Is the risk reduction worth the cost?**

RiskLens

Quantitative Approach to Risk Management

Instead of this…

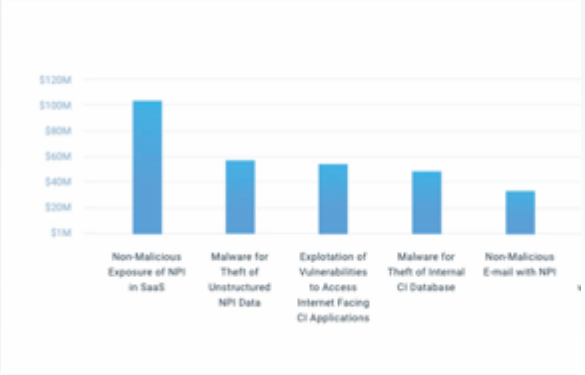
Medium Likelihood	High
Scenario A	High Impact

Medium Likelihood	High
Scenario B	High Impact

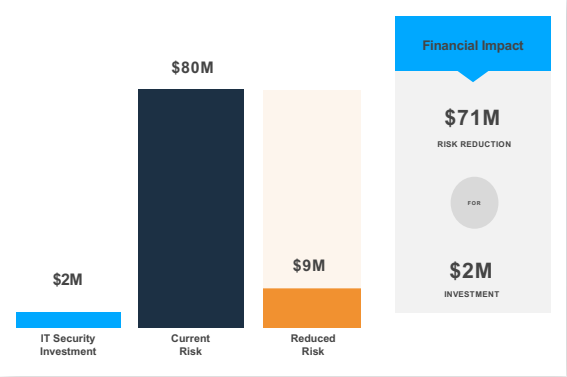
*"We need to prioritize **multiple scenarios** for remediation because we're currently at high risk of experiencing a data breach. They are both rated **high** since the likelihood is medium and the impact is high."*

We could have this:

FOR ILLUSTRATIVE PURPOSES ONLY



Top Risks

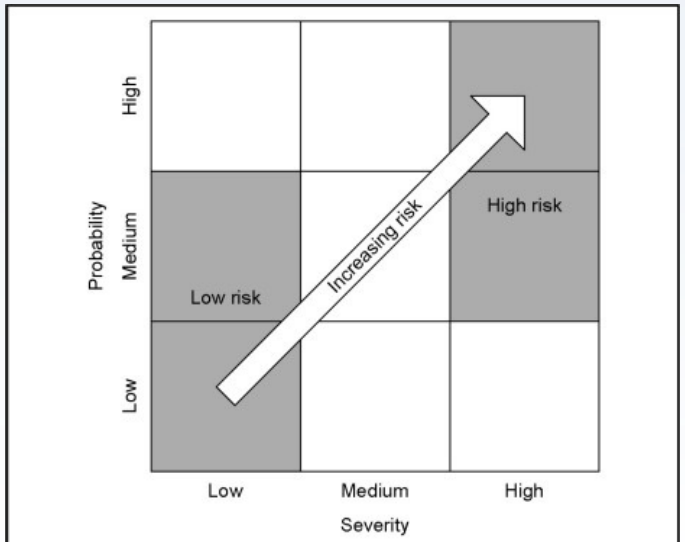


Cost Benefit

FAIR enables cost-benefit analysis and effective prioritization of risks in financial terms

RiskLens

Prior to FAIR, answers looked like this:

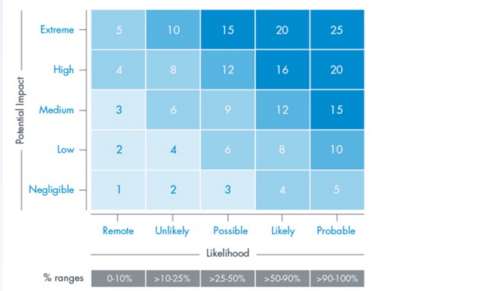


A quick method of assessing risk

A simple 3 x 3 matrix can rapidly show where risk is and help to set priorities. Identify a risk, consider the potential effect (high, medium or low), consider the probability of the risk (high, medium or low) and you have an immediate assessment of the risk.

Impact

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

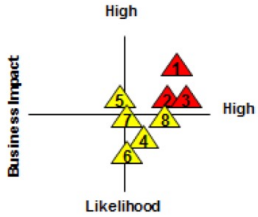


Source: Risk assessment for mid-sized companies: tools for developing a tailored approach to risk management. Scott McKay, AICPA, 2011

Observations

1. Service Level Agreements not defined and incorporated into ADP contract
2. Business case and project charter not formally documented
3. Business requirements definitions for reporting not consistently communicated to ADP
4. In-house understanding of ADP security structure does not appear to be adequate
5. Shared user accounts exist in the ADP system with Supervisor access
6. Read-only access not administered properly
7. Lack of monitoring around accounts with Supervisor access
8. Testing approach and test plan not defined and formally documented

Priority Risk Map



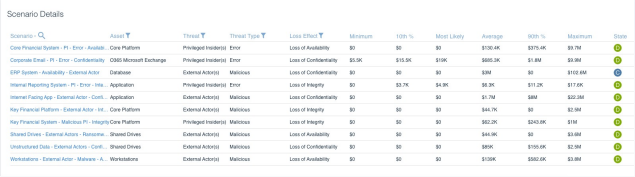
- Observations in the top right quadrant are given high priority.
- Observations in the bottom left quadrant are given low priority.
- Observations in the top left and bottom right quadrants are given medium priority.

RiskLens

RiskLens Reports by Role

Cyber Risk Analyst

Deliver Accurate and Defensible Cyber Risk Assessments

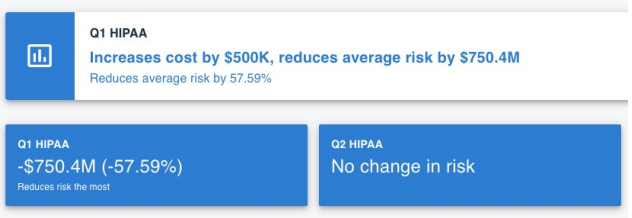


CRO

Build a Highly Effective Cyber Risk Management Program

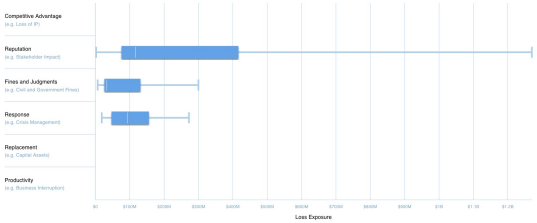
CISO

Manage Cybersecurity from the Business Perspective



Board and Business Executives

Understand the Financial Impact of Cyber Risk



RiskLens

The FAIR Risk Model & Terminology

RiskLens®

Definitions of Risk

Dictionary: “a situation involving exposure to danger”

COSO ERM: “the possibility that events will occur and affect the achievement of objectives”

ISO Guide 73: “the effect of uncertainty on objectives”

NIST-CSF: “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.”

IRM: “the combination of the probability of an event and its consequences”

RiskLens

FAIR's Definition: RISK

FAIR defines risk as a measurement of the probable frequency and probable magnitude of future loss.
Risk is expressed quantitatively, in amounts of future loss and their probabilities over a given timeframe. (Almost always over the next year)

RISK FORECASTED ALE
(ANNUALIZED LOSS EXPLOSURE)

=

LOSS EVENT FREQUENCY # OF TIMES

x

LOSS MAGNITUDE $$$/EVENT

RiskLens

Which of these are risks?

- Data Confidentiality
- Hacktivists
- Cloud Computing
- Phishing / Social Engineering
- Insider Threat(s)
- Fraud
- Cyber Criminals
- Mobile Malware
- Application Vulnerabilities
- Business Continuity

Typical Top 10 Technology Risk List

NONE!

Application Vulnerabilities	Control Deficiencies
Cloud Computing	Asset
Insider Threat(s)	Threat
Phishing / Social Engineering	Method

RiskLens

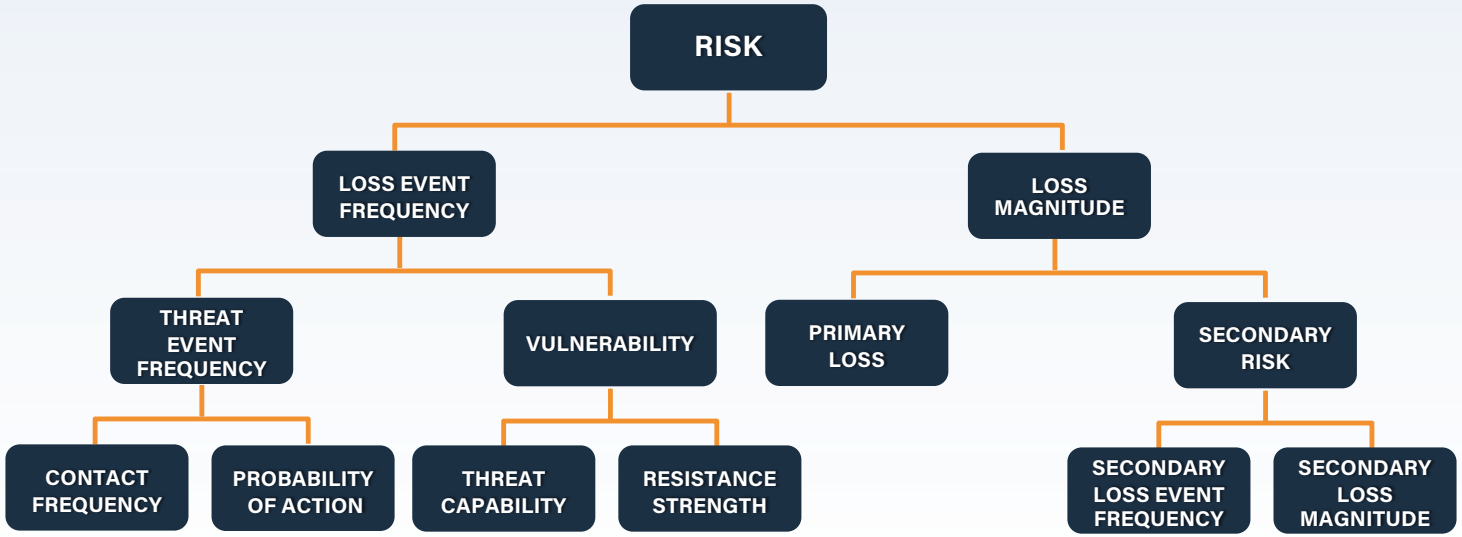
The FAIR Model

Factor Analysis of Information Risk

A model and method for defensible quantitative analysis of risk that produces results in financial and probabilistic terms, enabling cost-effective management of risk across the organization/enterprise.

RiskLens

FAIR: A Standard Risk Analytics Model



Accredited as an Industry Standard by

Complementary to Risk Frameworks

Supported by a Fast Growing Community

Wide Industry Adoption 30% Fortune 1000

FAIR Book Inducted in Cybersecurity Canon

RiskLens

Here's How Loss Unfolds

Loss Event

Anything, actor or agent, capable of acting against an asset in a manner that can result in loss

Anything of value that can be affected in a manner that results in loss

How loss materializes within a given asset

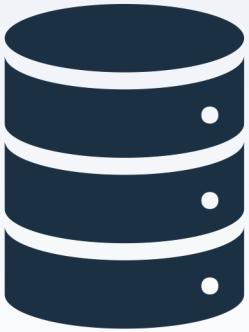
Risk = A measurement of the **probable frequency** and the **probable magnitude** of **future loss**.

RiskLens

Risk Scoping Scenario Example

External Malicious

Breaches PII
(**Confidentiality Effect**)
from



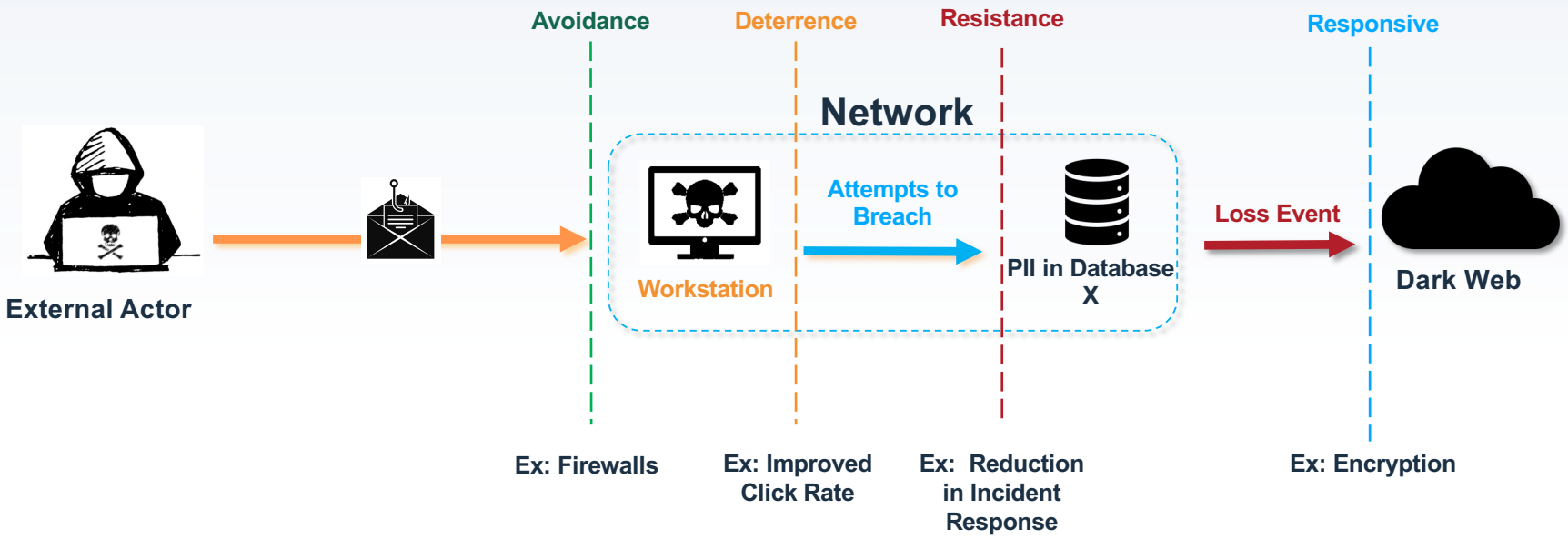
Database X

How much risk do we face from
cybercriminals breaching the **confidentiality**
of sensitive data **(PII)** in **Database X**

RiskLens

How Will This Loss Unfold?

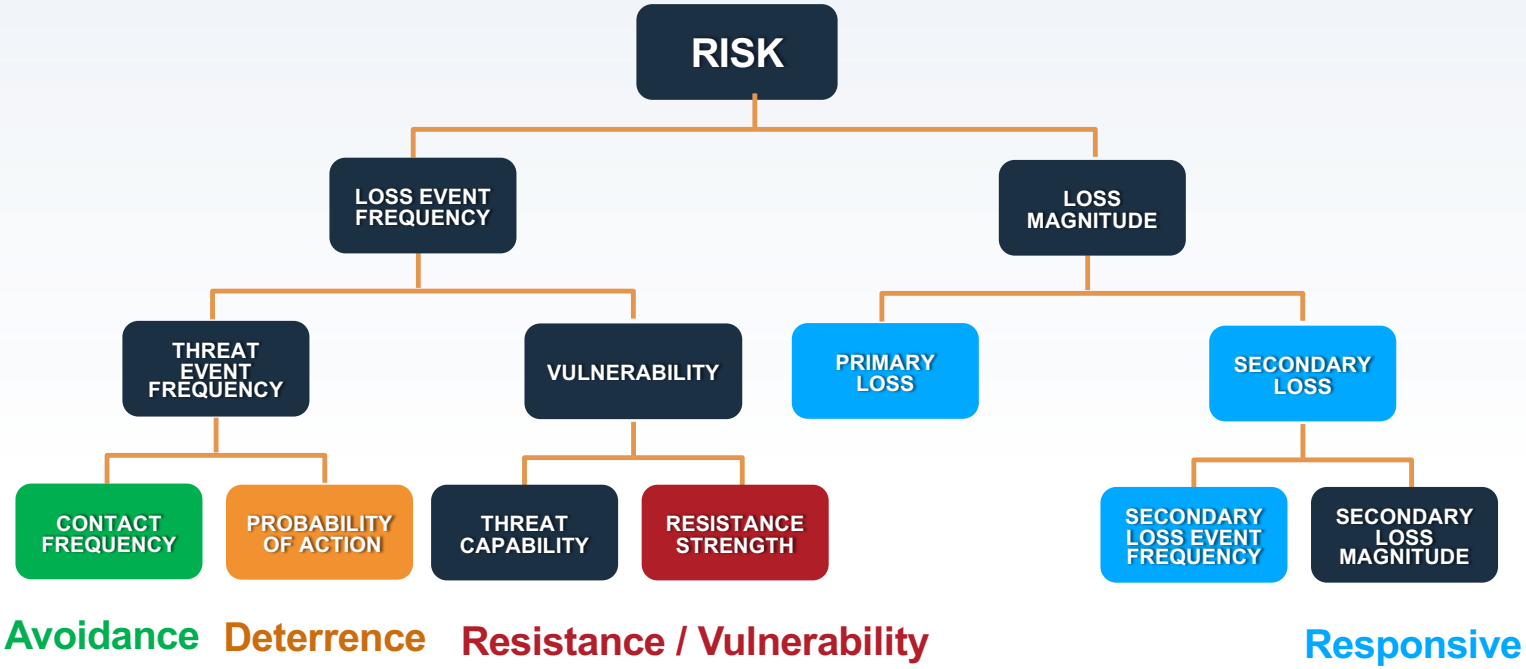
Scenario: Breach of PII from Database X by External Malicious Actor



RiskLens

Where Controls Map to FAIR

In FAIR, controls are used to **reduce the frequency** of an event happening or **reduce the loss magnitude** once the loss event happens.



RiskLens

Six Forms of Loss

Productivity

Reduction in an organization's ability to generate its primary value proposition (producing goods or services, etc.)

Response

Expenses associated with managing or responding to a loss event

Replacement

Capital expense associated with replacing or repairing lost or damaged assets

Competitive Advantage

Losses associated with competitors obtaining and using trade secrets

Fines and Judgments

Losses from legal or regulatory actions levied against an organization through civil, criminal, or contractual actions.

Reputation

Losses associated with an external perception that an organization's value, competency, or ethics have diminished.

RiskLens

Data Collection and Probable Estimation

RiskLens®

Measurement Concepts

Knowing or stating the *probability* of an outcome or event *does not = a prediction*.

Probability vs. Prediction

Anything is possible, especially on a long enough timeline. Focusing on time-bound probabilities will help inform decisions.

Possibility vs. Probability

Not binary concepts, they exist on a spectrum. Goal: *drive toward objectivity in analyses* with an external frame of reference.

Subjectivity vs. Objectivity

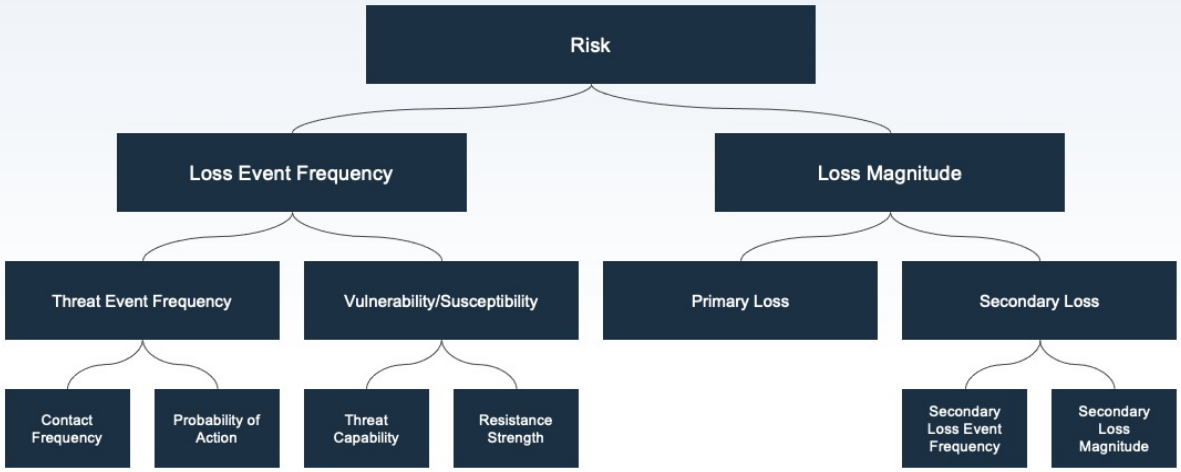
Accuracy is King. Goal*: accuracy* (i.e. correctness) *with a useful degree of precision*.

Accuracy vs. Precision

RiskLens

Measuring Risk Refresher

The FAIR Model



Probability Distributions

Estimates in FAIR analysis are expressed using probability distributions.

4-Part Estimates

- Minimum Probable Value
- Maximum Probable Value
- Most Likely Value (MLV)
- Confidence Level (MLV) is more probable than other values in the range

Calibration Estimation

Measurement technique that produces **accurate ranges** with a **useful degree of precision**

Calibrated Estimation Process:

1. Start with an **absurd** range
2. Eliminate **highly unlikely** values
3. Reference **what you know** to narrow the range further
4. Play a **calibration** game (equivalent bet test)

RiskLens

The goal is to *calibrate* all estimates to 90% confidence intervals.

When it's too hard for you to choose between the range and the spinner, you've found your calibrated estimate.

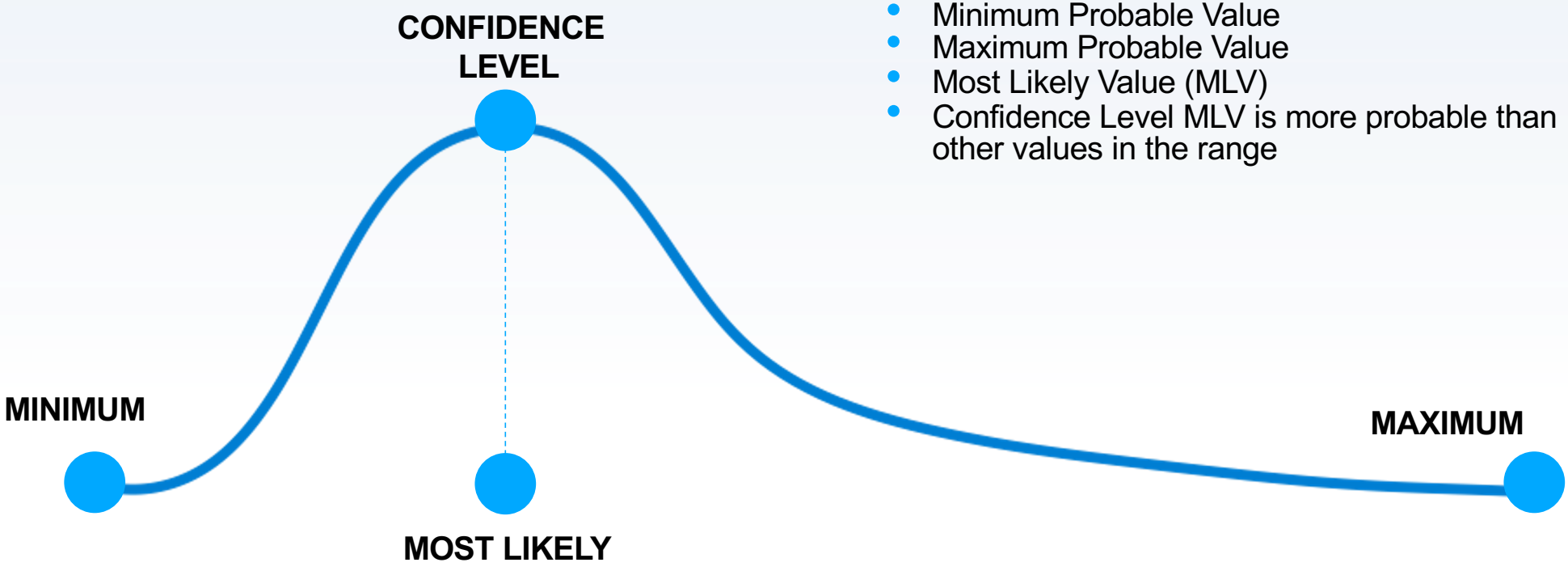
10% chance you lose!

90% chance you win!

RiskLens

Probability Distributions

Estimates in FAIR analysis are expressed using probability distributions.



4-PART ESTIMATES

- Minimum Probable Value
- Maximum Probable Value
- Most Likely Value (MLV)
- Confidence Level MLV is more probable than other values in the range

RiskLens

Calibration Estimation

Measurement technique that produces **accurate ranges** with a **useful degree of precision**

Calibrated Estimation Process:

1. Start with an **absurd** range
2. Eliminate **highly unlikely** values
3. Reference **what you know** to narrow the range further
4. Play a **calibration** game (equivalent bet test)

The goal is to *calibrate* all estimates to 90% confidence intervals.

When it's too hard for you to choose between the range and the spinner, you've found your calibrated estimate.

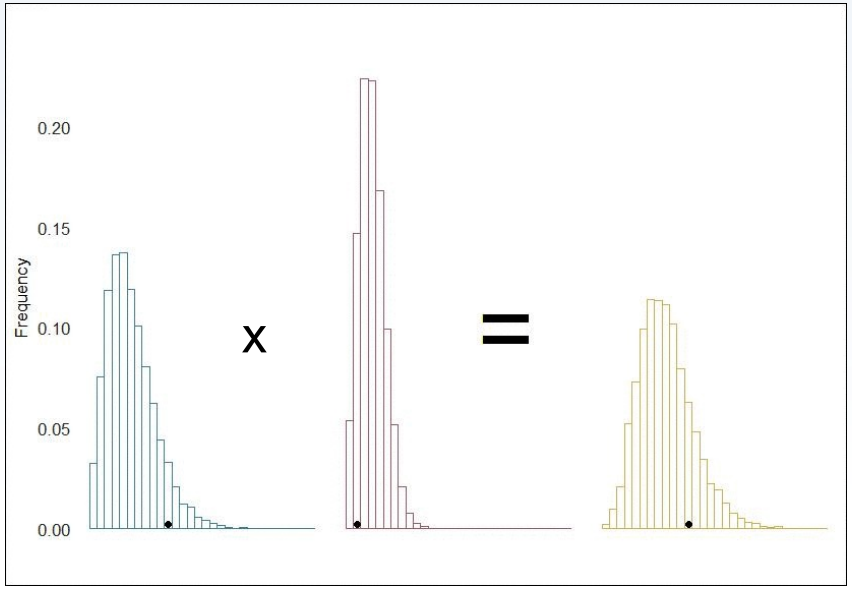
10% chance you lose!

90% chance you win!

RiskLens

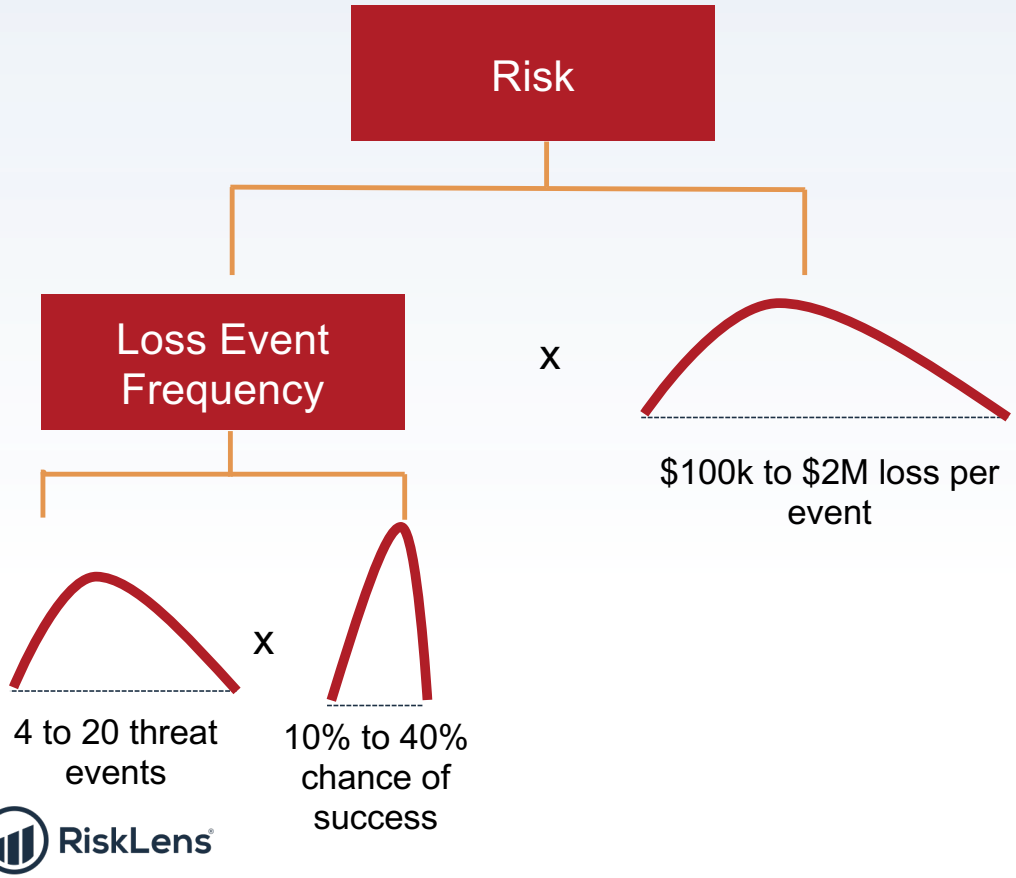
Monte Carlo Simulations

- "Monte Carlo simulations perform repeated random sampling to obtain numerical results. The output of Monte Carlo simulations used in risk analysis is shown as probability distributions. The primary advantage of using Monte Carlo simulations in risk analysis is the ability of the method to perform thousands of calculations on random samples, allowing risk analysts to create a more accurate and defensible depiction of probability given the uncertainty of the inputs."
  OpenFAIR Standard

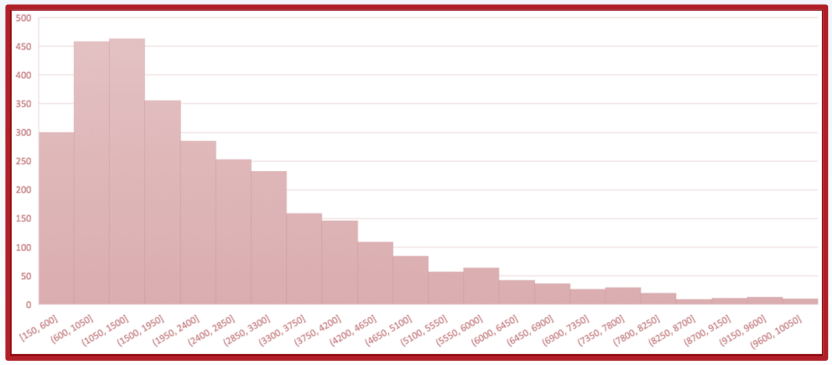


https://roh.engineering

QA The FAIR Factors After Results



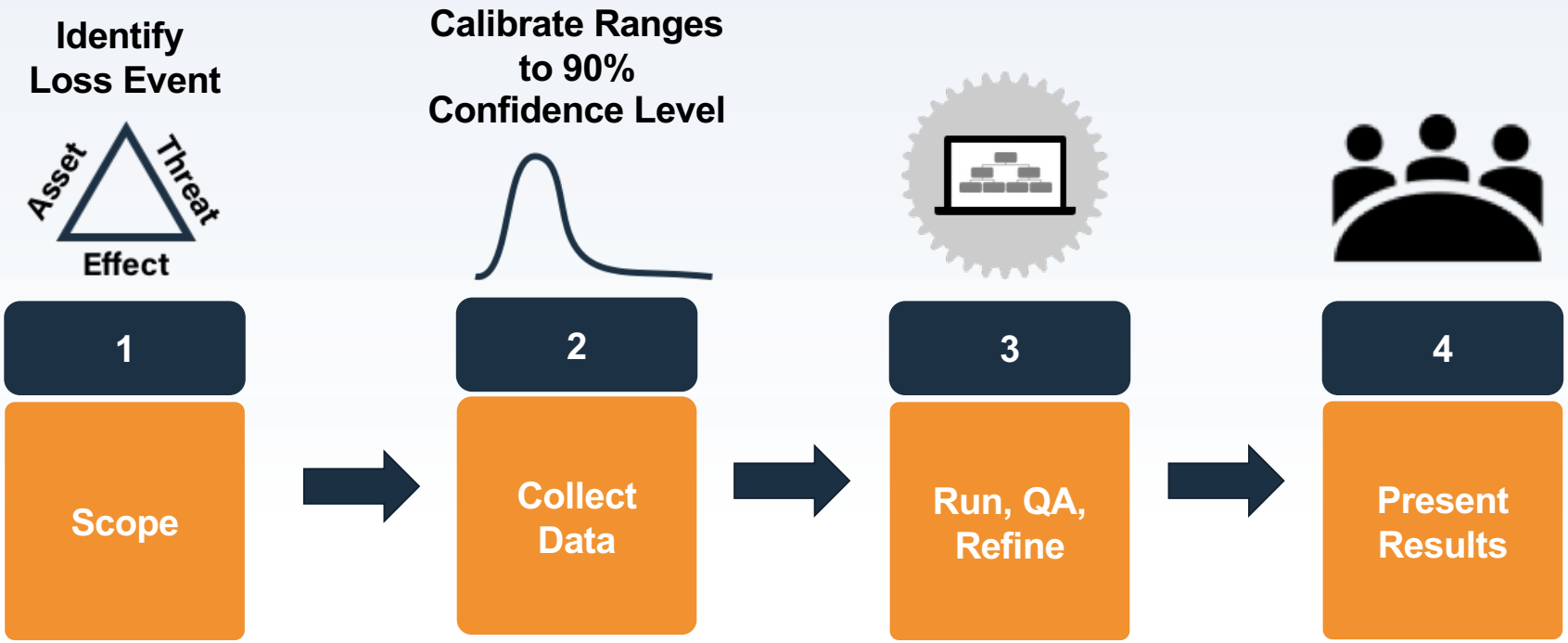
RESULTS



Monte Carlo allows us to account for uncertainty and see the relative probabilities of different outcomes

RiskLens

FAIR-Based Risk Analysis Process

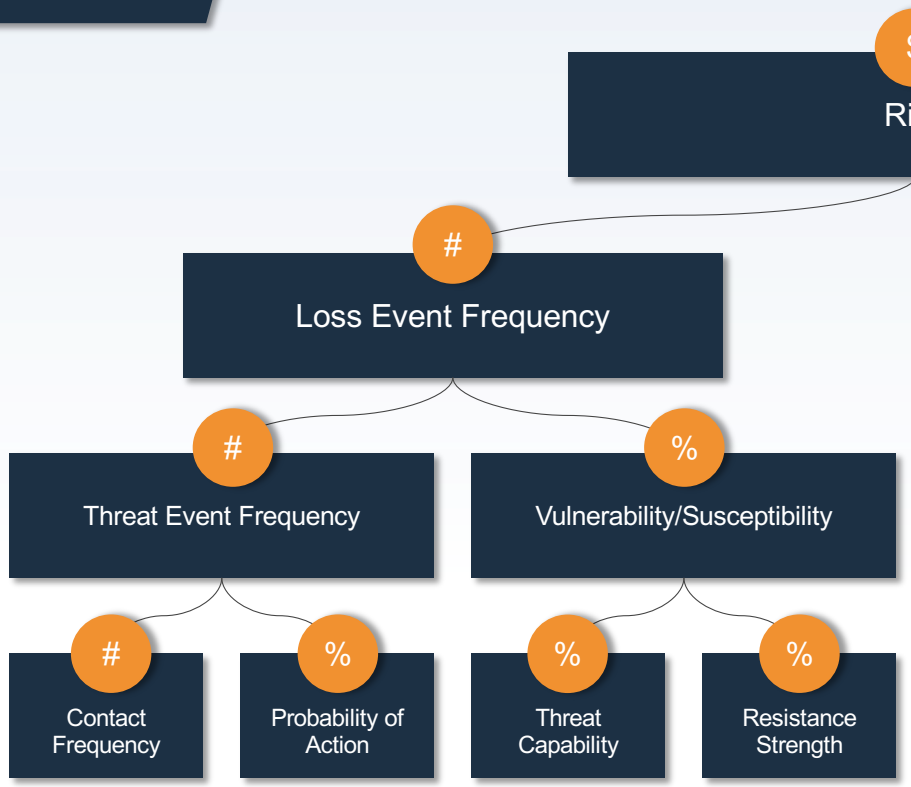


RiskLens

2

Input Data

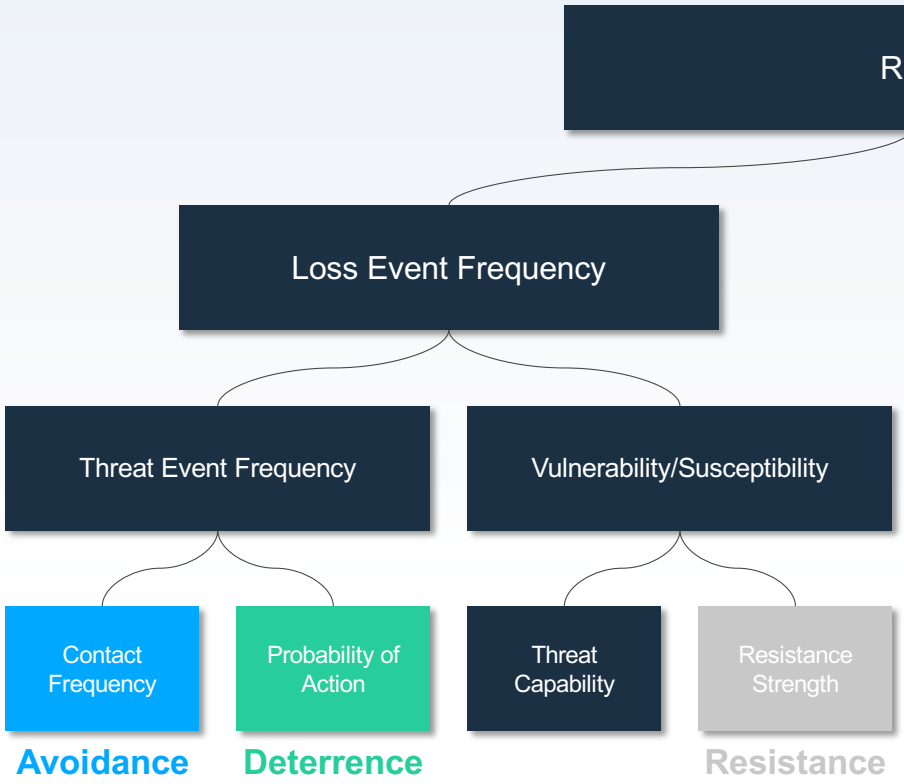
The FAIR Model – Frequency Side



Start at the top where you have the best available data, then provide calibrated 4-part estimates.

RiskLens

Controls Mapping to FAIR



In FAIR, controls are used to **reduce the frequency** of an event happening (or reduce the loss magnitude once the loss event happens).

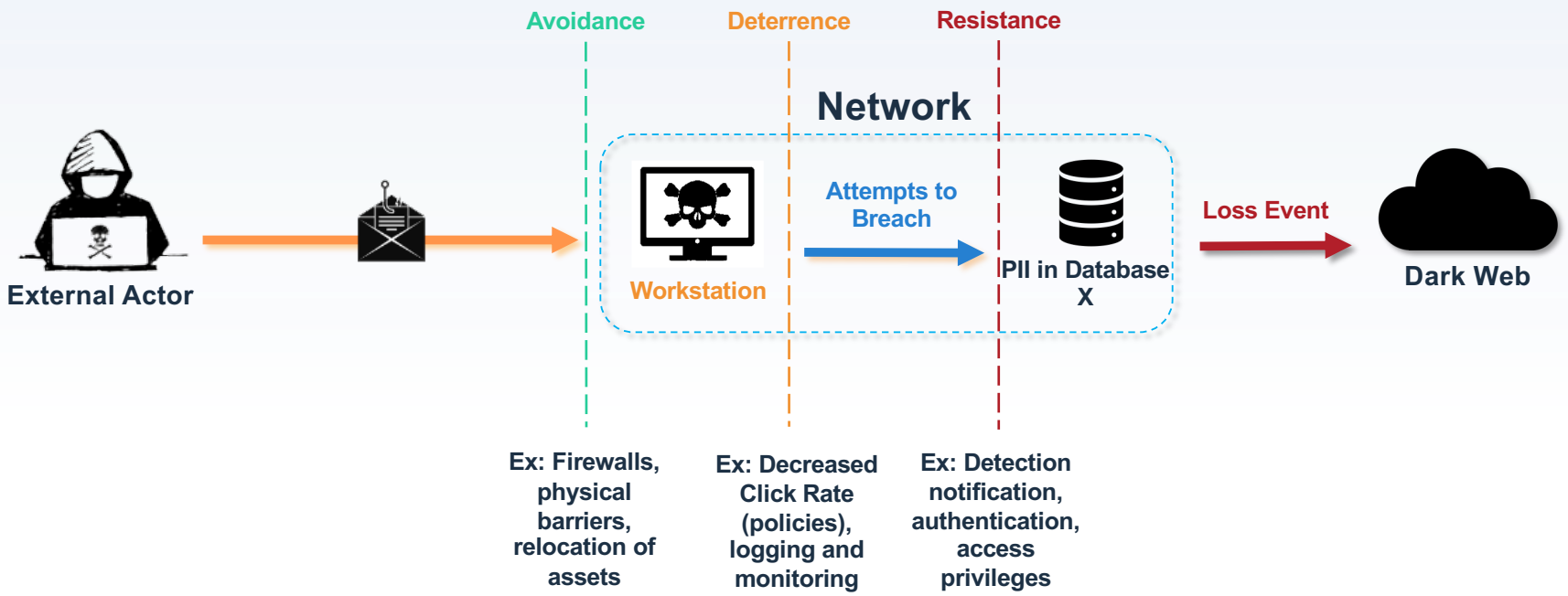
Types of Controls for Frequency:

- Avoidance
- Deterrence
- Resistance

RiskLens

How Will This Loss Unfold?

Scenario: Breach of PII from Database X by External Actor

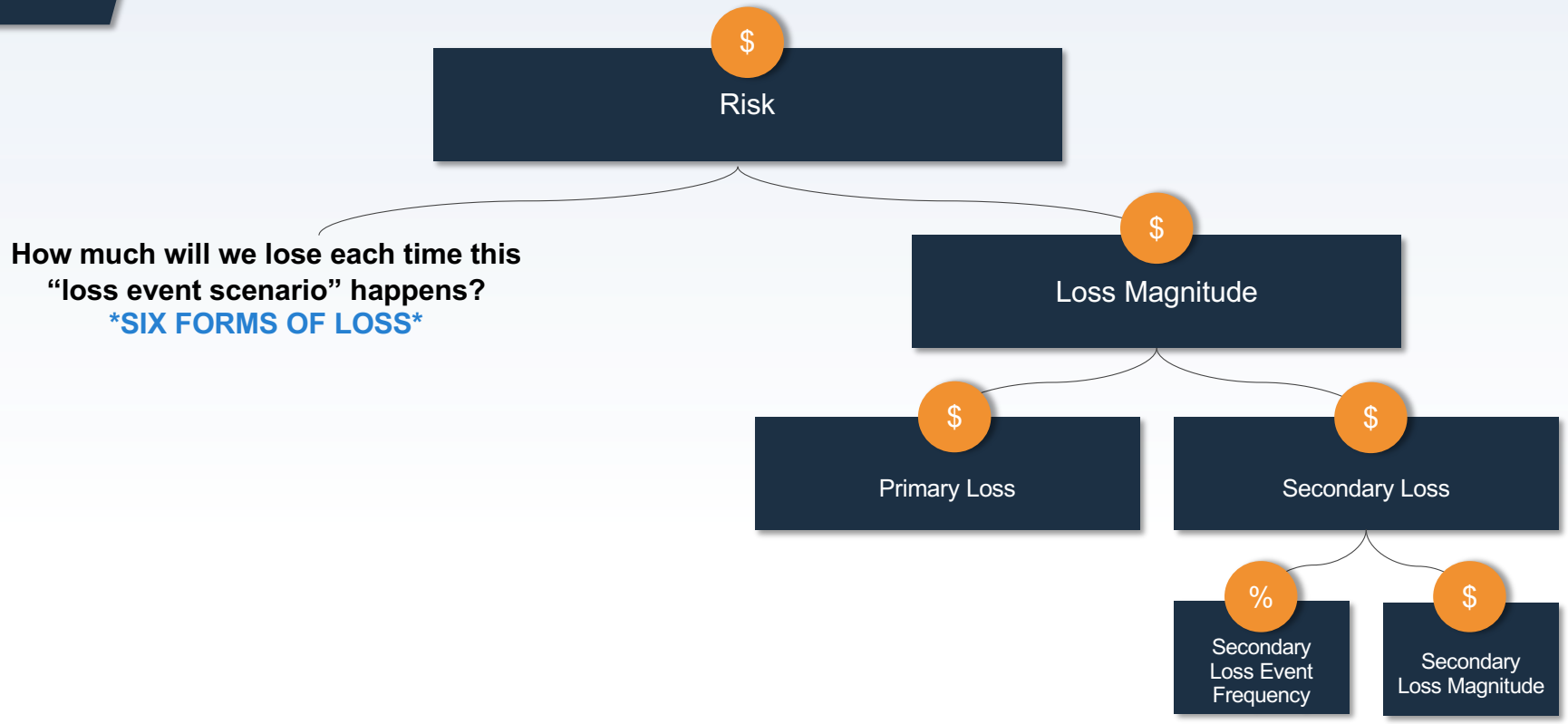


RiskLens

2

Input Data

The FAIR Model – Loss Magnitude Side



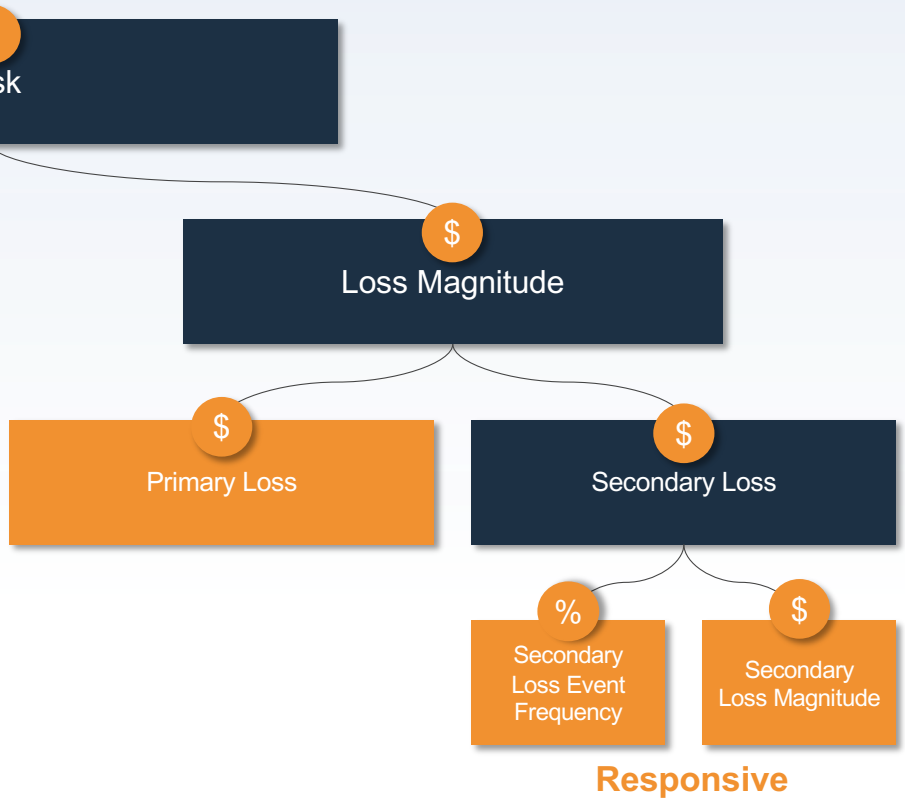
RiskLens

Controls Mapping to FAIR Continued

In FAIR, controls are used to **reduce the frequency** of an event happening or **reduce the loss magnitude** once the loss event happens.

Type of Control for Loss Magnitude:

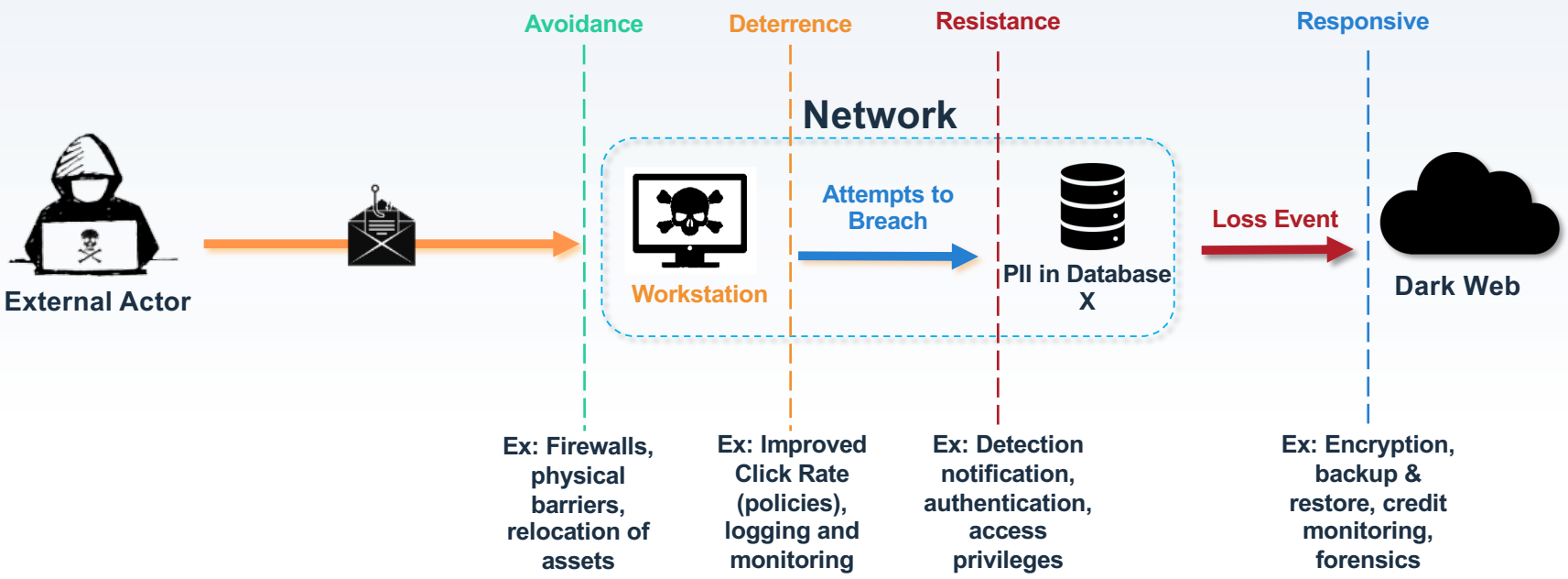
- Responsive



RiskLens

How Can Loss Magnitude Be Reduced?

Scenario: Breach of PII from Database X by External Actor



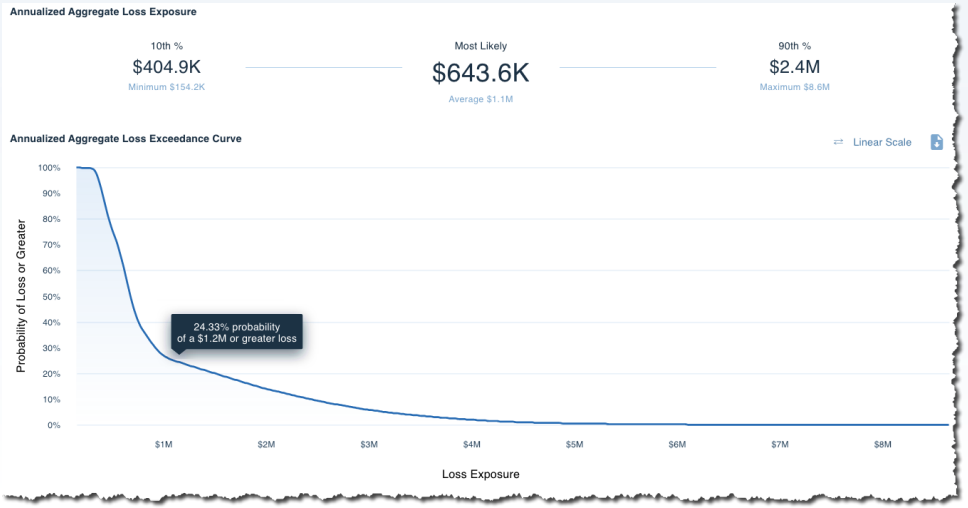
RiskLens

3

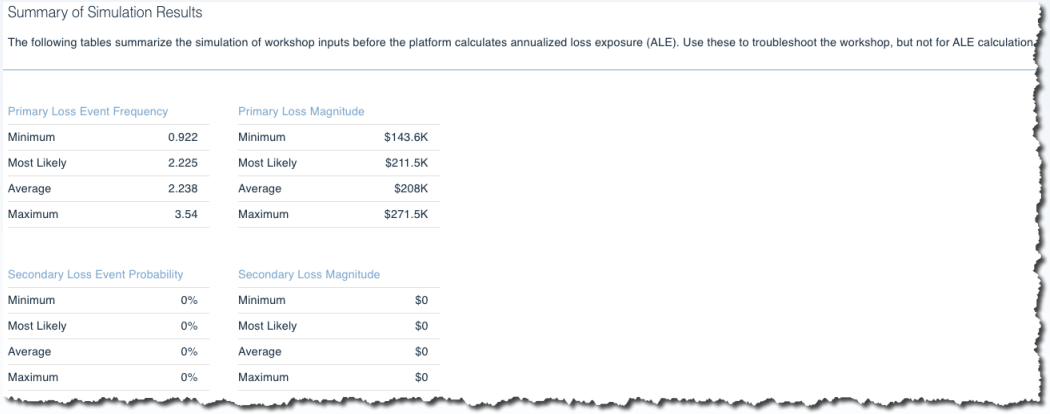
QA

Results

- For single-scenario analyses, focus on two sets of results:



Loss Exceedance Curves show what % of simulations met or exceeded a given amount of loss in the simulated year.



Summary of Simulation Results

The following tables summarize the simulation of workshop inputs before the platform calculates annualized loss exposure (ALE). Use these to troubleshoot the workshop, but not for ALE calculation.

Primary Loss Event Frequency	
Minimum	0.922
Most Likely	2.225
Average	2.238
Maximum	3.54

Primary Loss Magnitude	
Minimum	$143.6K
Most Likely	$211.5K
Average	$208K
Maximum	$271.5K

Secondary Loss Event Probability	
Minimum	0%
Most Likely	0%
Average	0%
Maximum	0%

Secondary Loss Magnitude	
Minimum	$0
Most Likely	$0
Average	$0
Maximum	$0

Summary of Simulation Results shows the probable frequencies and probable magnitudes of primary and secondary loss events.

RiskLens

4

Report

Report the Results to the Stakeholder

- RiskLens provides out-of-the-platform “risk statements” to support translating the results to stakeholders.
- Which statement(s) would your stakeholder want to hear when reporting how much risk for a specific scenario?
- RiskLens provides additional reports for risk assessments.

2.24 loss events are forecasted per year with an Average Per Event Loss of **$208K**

2.24 loss events forecasted per year	$208K Average Per Event Loss	$465.8K Average Annualized Loss Exposure	Exceed $1M every 1612.9 years
100% forecasted within a year	Non-annualized, assumes secondary losses		0.06% annualized probability of exceeding threshold

Annualized Loss Exposure

10th %	Most Likely	90th %
$239.8K	$424.2K	$672.7K
Minimum $148.2K	Average $465.8K	Maximum $1.1M

Scenario Outcomes Summary Statements

- 2.24 loss events are forecasted per year with an average annualized loss of $465.8K ($148.2K - $1.1M).
- A single non-annualized loss event with full secondary losses is forecasted to have an average loss of $208K ($143.6K - $271.5K).
- Loss events exceeding $1M are forecasted every 1612.9 years (0.06%).
- You are forecasted to be vulnerable to threat events in this scenario 14.9% of the time.

RiskLens

4

Report

Single Scenario Reporting

- How often are you reporting on a single scenario?
- What do you do next?
- What is really being asked of you as it relates to translating “How much risk do we have?”
- FAIR gets you started, RiskLens completes the process for Risk Assessments.

RiskLens

4

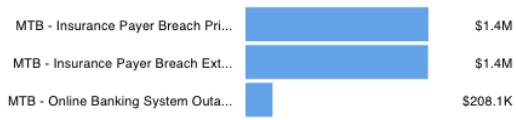
Report

RiskLens Top Risk Report

Top Risks Report

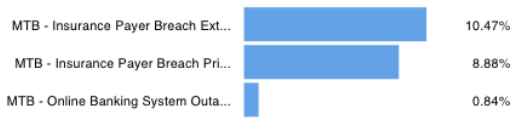
$1.4M	Most Severe Event

Top Risks - Average Per Event Loss Magnitude



10.47%	Highest Probability to Exceed $1M

Top Risks - Probability of Annualized Loss Exceeding $1M



$593.6K	Top Annualized Risk

Top Risks - Average Annualized Loss Exposure

Scenario Details

Scenario	Asset	Threat	Threat Type	Loss Effect	Minimum	10th %	Most Likely	Average	90th %	Maximum	State
MTB - Insurance Payer Breach External A...	MTB - Insurance Payer Data...	External Actor(s)	Malicious	Loss of Confidentiality	$0	$0	$0	$250.5K	$1.1M	$5.7M	C
MTB - Insurance Payer Breach Privileged...	MTB - Insurance Payer Data...	Privileged Inside...	Malicious	Loss of Confidentiality	$0	$0	$0	$212K	$830.7K	$5.4M	C
MTB - Online Banking System Outage Pri...	MTB - Online Banking System	Privileged Inside...	Error	Loss of Availability	$154.2K	$385.1K	$645.8K	$593.6K	$828.4K	$1.3M	C

RiskLens

4

Report

RiskLens Cost Benefit Analysis Report

Encryption

Increases cost by $500K, reduces average risk by $424.8K

Reduces average risk by 40.23%

Network Segmentation

-$209K (-19.79%)

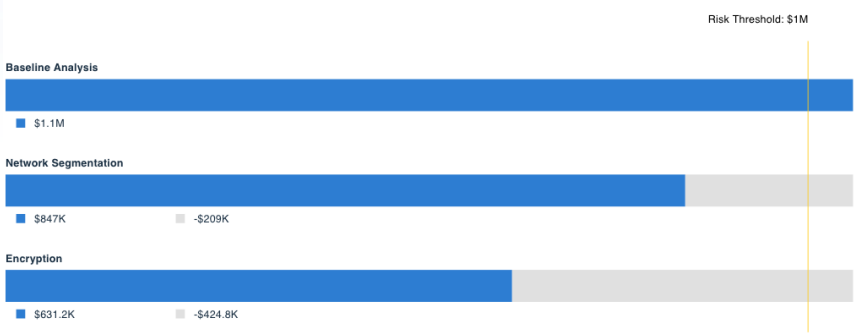
Encryption

-$424.8K (-40.23%)

Reduces risk the most

Comparison Results

Comparison by Average Annualized Loss Exposure



Analyses

Baseline Analysis

	Minimum	10th %	Most Likely	Average	90th %	Maximum
Analysis Results	$154.2K	$404.9K	$643.6K	$1.1M	$2.4M	$8.6M

Network Segmentation

	Minimum	10th %	Most Likely	Average	90th %	Maximum
Analysis Results	$154.2K	$395.7K	$643.6K	$847K	$1.7M	$7.6M
Increase Or Reduction	$0	-$9.2K	$63	-$209K	-$757.4K	-$1M
Cost-Benefit Summary	$0	0$	$0	-$10	-$38	-$50

Encryption

	Minimum	10th %	Most Likely	Average	90th %	Maximum
Analysis Results	$162.7K	$396.7K	$645.3K	$631.2K	$863K	$5.9M
Increase Or Reduction	$8.6K	-$8.2K	$1.8K	-$424.8K	-$1.6M	-$2.7M
Cost-Benefit Summary	$0	0$	$0	-$1	-$3	-$5

RiskLens

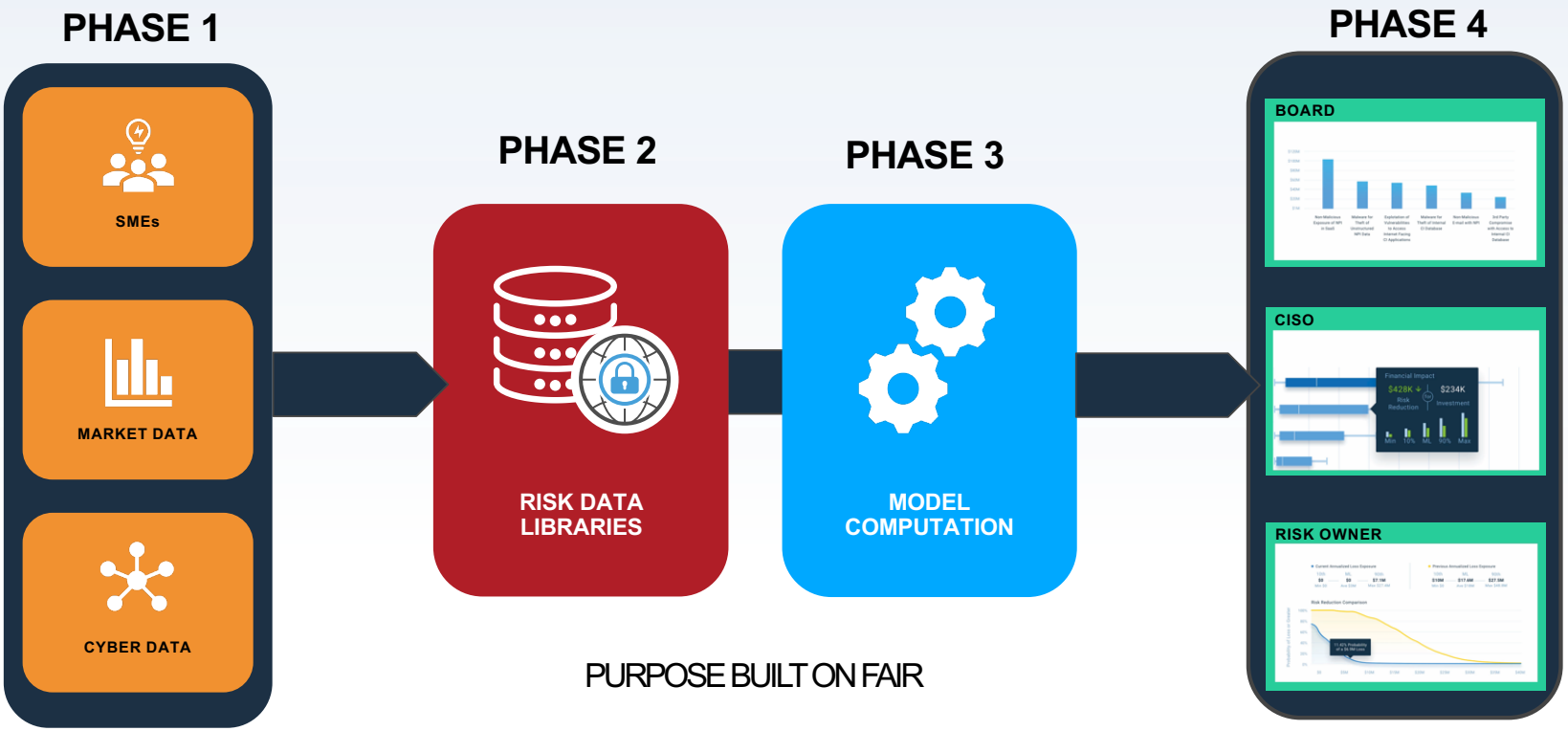
Thank you!
Questions?

RiskLens®

Next Steps with the RiskLens Platform

RiskLens®

RiskLens Platform



PURPOSE BUILT ON FAIR

RiskLens