2020

DIVING INTO RAPID RISK ASSESSMENTS

USE CASES, BENEFITS AND CASE STUDY

Presented by: **Teresa Suarez** | August 26th 2020

RiskLens®

AN INTRODUCTION TO THE PRESENTER

Who? **Teresa Suarez**, Senior Manager – Professional Services Architect

What role? Help design, develop, and deliver the RiskLens Services team offerings

What work? Since joining in 2016, has had the opportunity to work with dozens of customers including both international and Fortune 100 organizations. Delivery experience includes: FAIR trainings, Proof of Concepts, Top Risk Identification Workshops, Rapid Risk Assessments, Board Reports, Risk Management Program Builds etc.

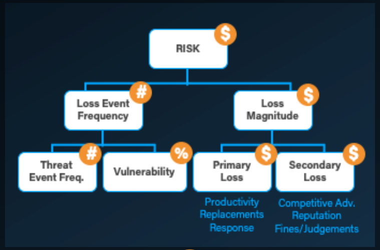
Fun Fact(s)

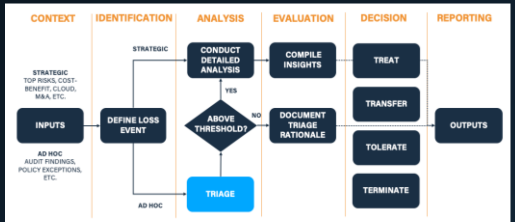
- Have Jack Jones as a mentor
- Wrote the RiskLens Culture Code

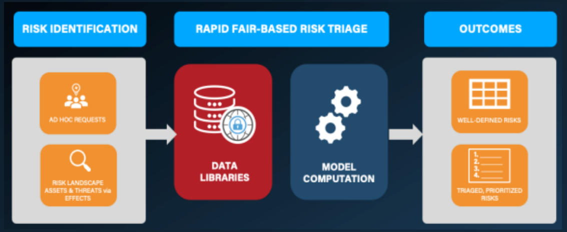
WEBINAR OVERVIEW

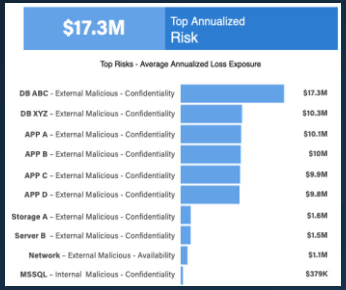
Why - How - Where

Process – Sample Outcome









Establishing Context

Rapid Risk Assessment Example

ESTABLISHING CONTEXT: WHY, HOW, & WHERE

WHY: RISK ASSESSMENT CHALLENGES

REQUESTS CAN STEM FROM:

C - SUITE

AUDIT COMMITTEE

NEW CISO

PRODUCT OWNERS

ANALYTS HAVE LIMITED TIME TO CONDUCT RISK ASSESSMENTS

THE CHALLENGE

Organizations need a way to **efficiently** and **meaningfully** assess risk to enable well-informed risk decisions and effective resource prioritization in complex and dynamic risk landscapes.

WHY: RAPID RISK ASSESSMENT USE CASES

- The C-Suite or Board, uneasy about loss exposure or regulatory compliance
- Audit committee or regulators requiring identification of top risks
- Business leaders evaluating a new digital initiative
- A new CISO eager to get up to speed
- Rapid identification of top risks that require additional detailed analysis and treatment
- Policy Exception Request Reviews
- Emerging Threat Analysis
- Plan of Actions & Milestones (POA&Ms) prioritization

RiskLens®

Responding to the Challenge:
RiskLens Rapid Risk Assessment

Do You Know Your Top Cyber Risks?

Could You Present Them to your CEO Next Week?

Visit: Rapid Risk Assessment

WHY: QUALITATIVE RISK ASSESSMENT METHODS ARE PLAGUED WITH:

COMMUNICATION CHALLENGES

CFO: *"How much risk do we have? Are we spending too little or too much on mitigation?"*

AUDIT: *"Did you fix all those high-risk issues?"*

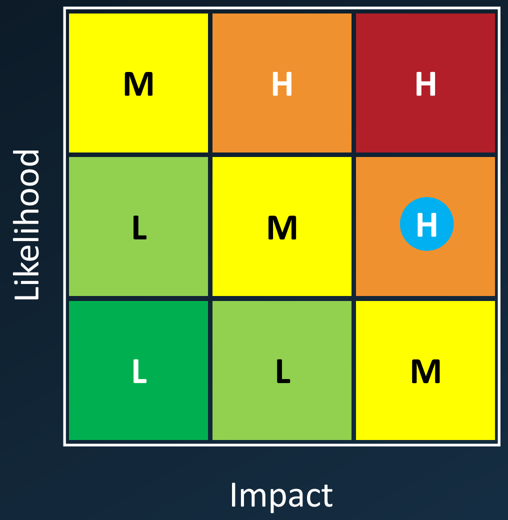
CISO: "Εχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό"

CYBERSECURITY VALUE??

CIO: *"Are we spending our cybersecurity budget on the right things? What is the ROI?"*

BOARD: *"We don't want to be in the headlines as a cybercrime victim. Are we doing enough to minimize risk?"*

MEANINGLESS MEASUREMENTS

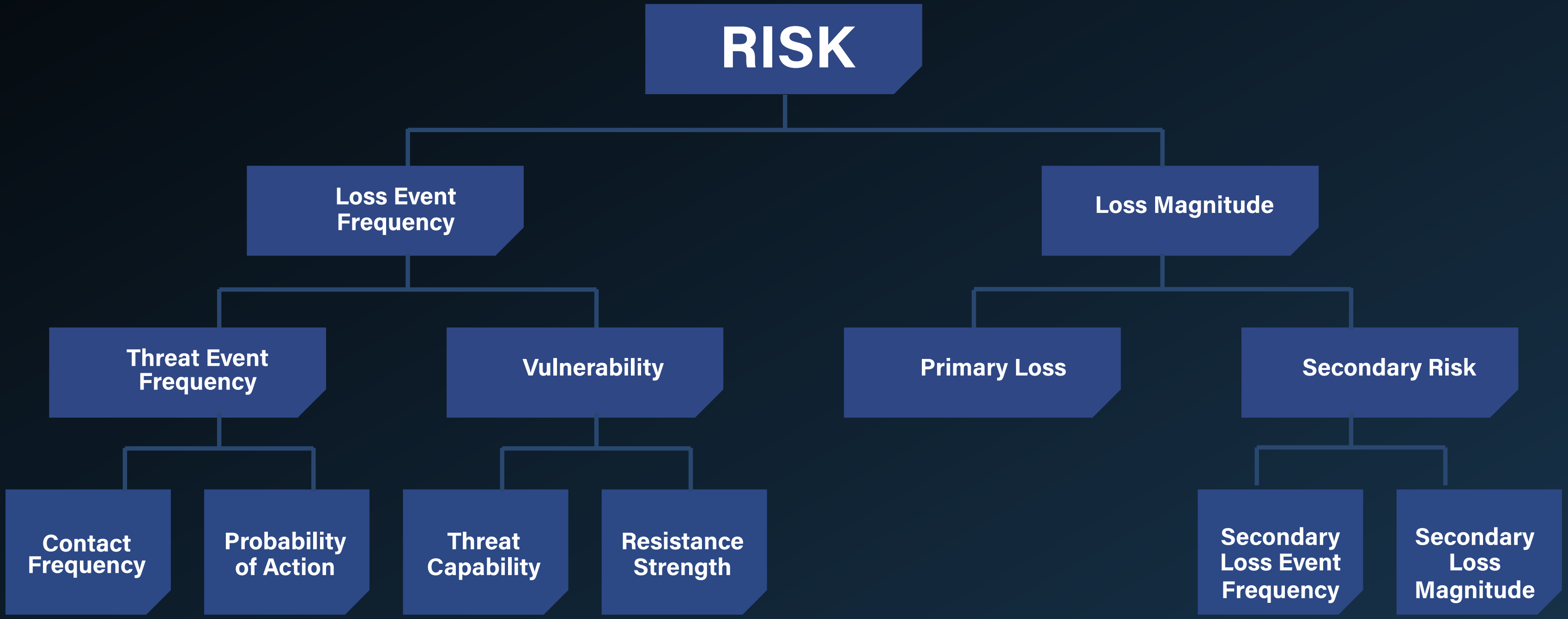


M	H	H
L	M	H
L	L	M

INCONSISTENT DEFINITIONS

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

HOW: FAIR: A STANDARD ANALYTICS MODEL



RISK

Loss Event Frequency

Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss

Secondary Risk

Contact Frequency

Probability of Action

Threat Capability

Resistance Strength

Secondary Loss Event Frequency

Secondary Loss Magnitude

Accredited as an Industry Standard by

Complementary to Risk Frameworks

Supported by a Fast Growing Community

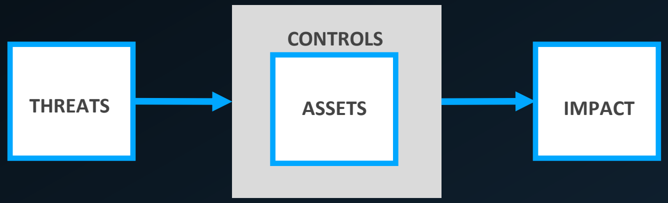
Wide Industry Adoption 30% Fortune 1000

FAIR Book Inducted in Cybersecurity Canon

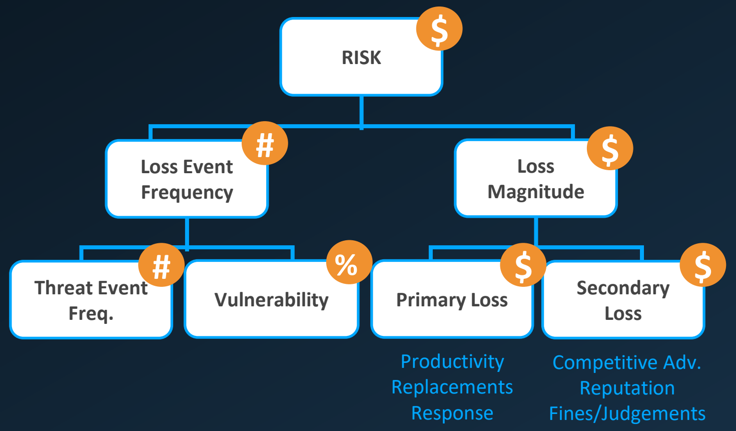
HOW: VALUE OF FAIR-BASED TRIAGE

The FAIR standard provides the taxonomy and analytic model that enables risk to be quantitatively:

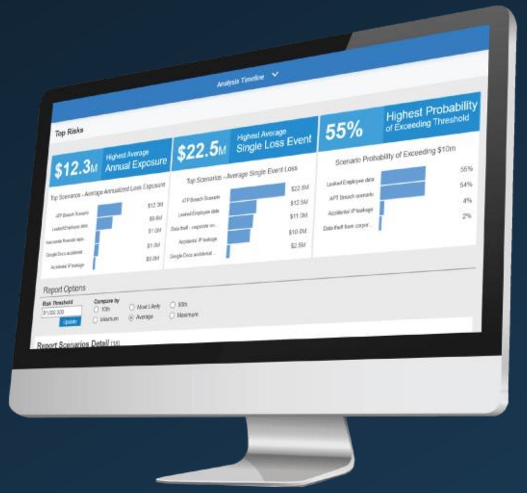
DEFINED



MEASURED

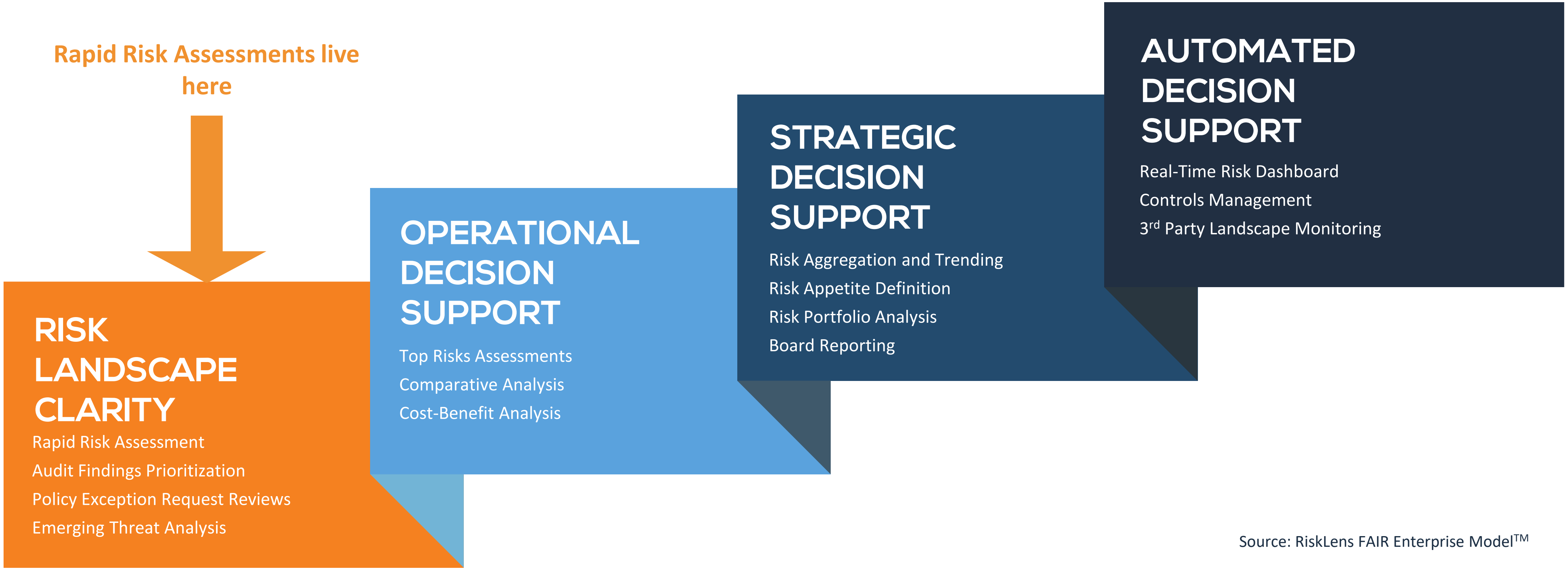


PRIORITIZED


Analysis Timeline
Top Risks
$12.3M Highest Average Annual Exposure
$22.5M Highest Average Single Loss Event
55% Highest Probability of Exceeding Threshold
Top Scenarios - Average Annualized Loss Exposure
Top Scenarios - Average Single Event Loss
Scenario Probability of Exceeding $10m
Report Options
Risk Threshold
Compare by
Update
Report Scenarios Detail

RiskLens Rapid Risk Assessment capability enables the rapid analysis and prioritization.

WHERE RRA FITS IN THE MATURITY SPECTRUM



Rapid Risk Assessments live here

RISK LANDSCAPE CLARITY

Rapid Risk Assessment

Audit Findings Prioritization

Policy Exception Request Reviews

Emerging Threat Analysis

OPERATIONAL DECISION SUPPORT

Top Risks Assessments

Comparative Analysis

Cost-Benefit Analysis

STRATEGIC DECISION SUPPORT

Risk Aggregation and Trending

Risk Appetite Definition

Risk Portfolio Analysis

Board Reporting

AUTOMATED DECISION SUPPORT

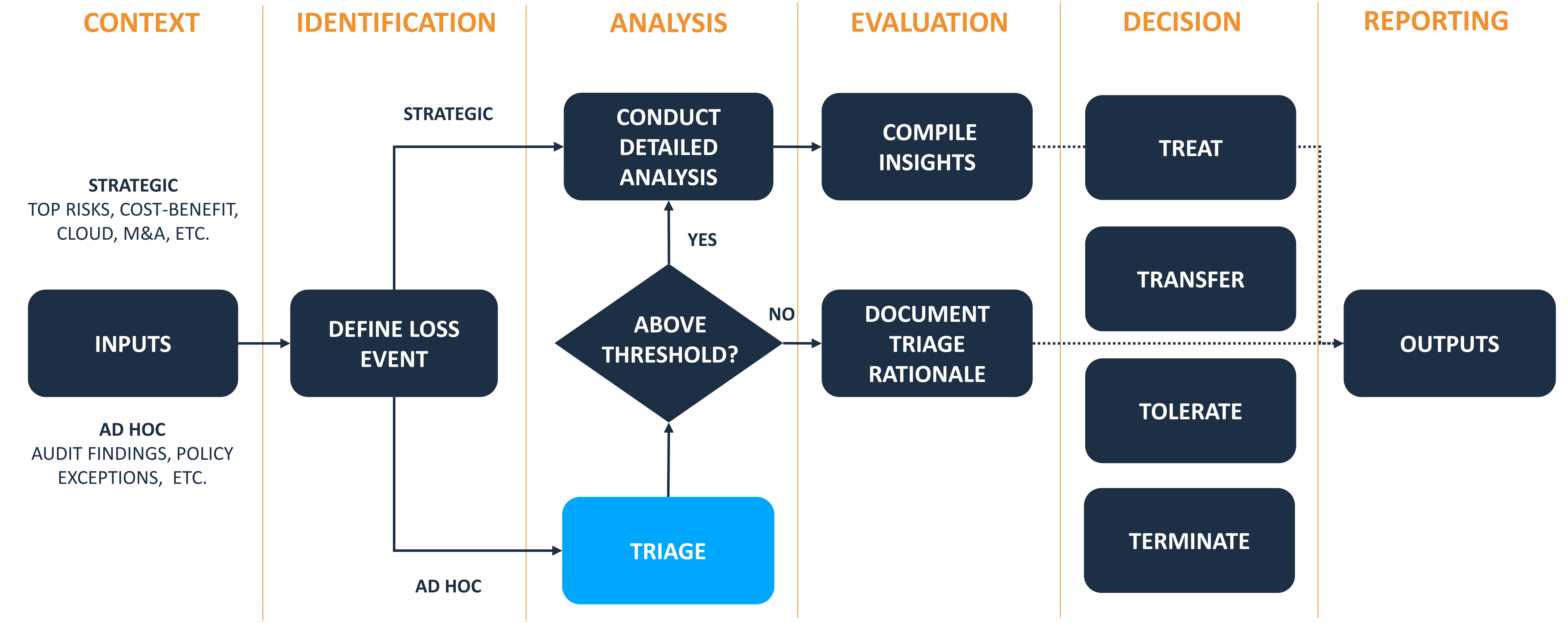
Real-Time Risk Dashboard

Controls Management

3rd Party Landscape Monitoring

Source: RiskLens FAIR Enterprise Model™

WHERE RRA FITS IN THE RISK MANAGEMENT PROCESS



Rapid Risk **ASSESSMENT** Example

RAPID RISK ASSESSMENT OVERVIEW

SCOPE RISK SCENARIOS

Scoping Via Drop-down Menus

Leveraging Asset List Completed during Onboarding

ANSWER ASSESSMENT QUESTIONS

Complete Frequency & Magnitude Workshop

Use of Risk Data Libraries Configured during Onboarding

MONTE CARLO SIMULATIONS

Save and Press Run Button

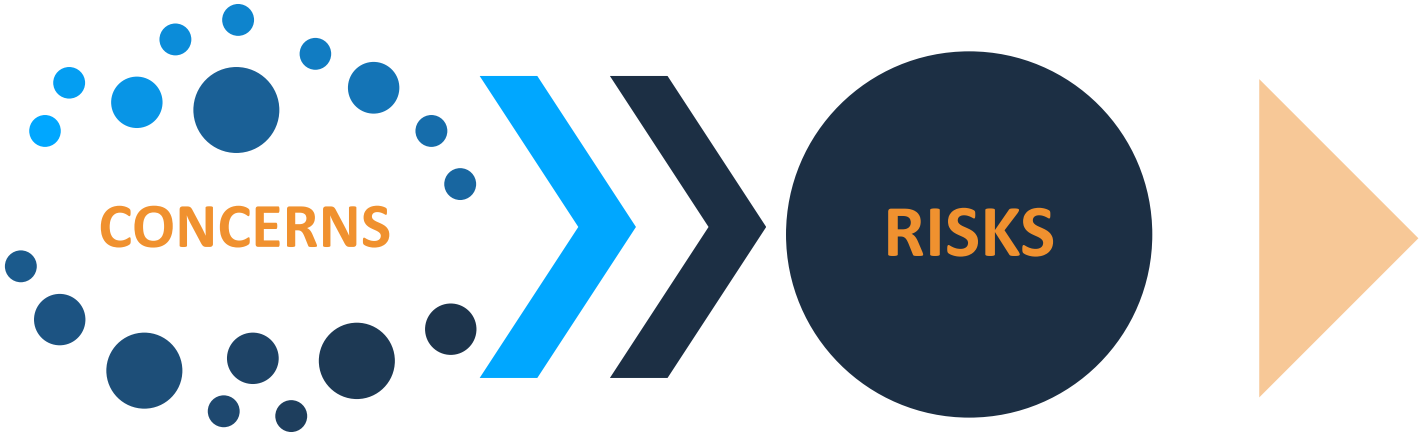
RiskLens Automatically Runs 10,000 Monte Carlo simulations

EVALUATE ASSESSMENT RESULTS

Review Rapid Risk Assessment Results

RiskLens Automatically Generates Risk Reports

IDENTIFICATION PHASE: LEVERAGE FAIR TERMINOLOGY

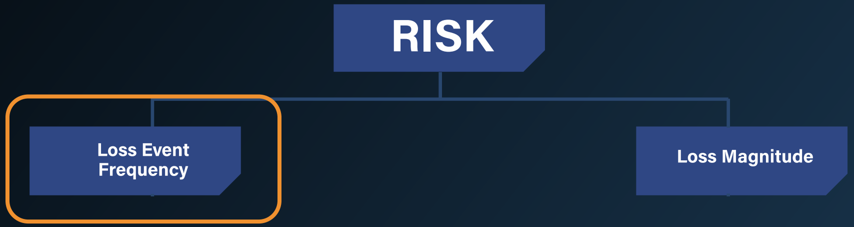


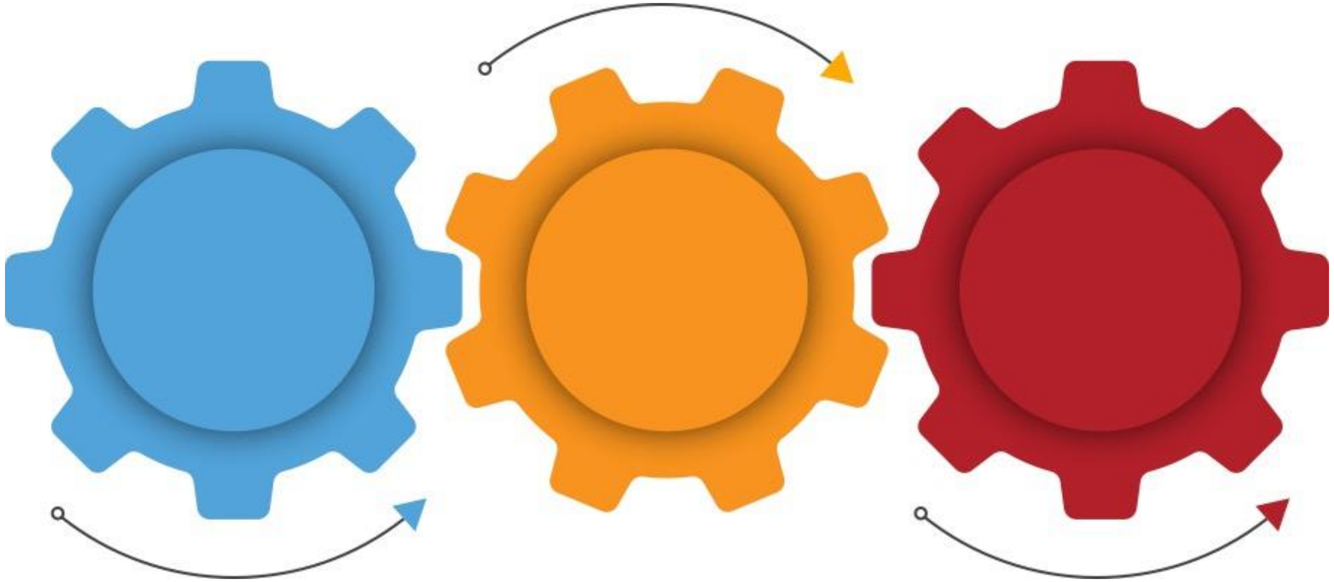
Breach of Customer PCI data from POS-related systems

Loss of Systems Availability due to malicious insider

Theft of Customer PII data through application attacks

TRIAGE: HOW RISKLENS HELPS ANSWER FREQUENCY





Simple, non-quant ninja questions

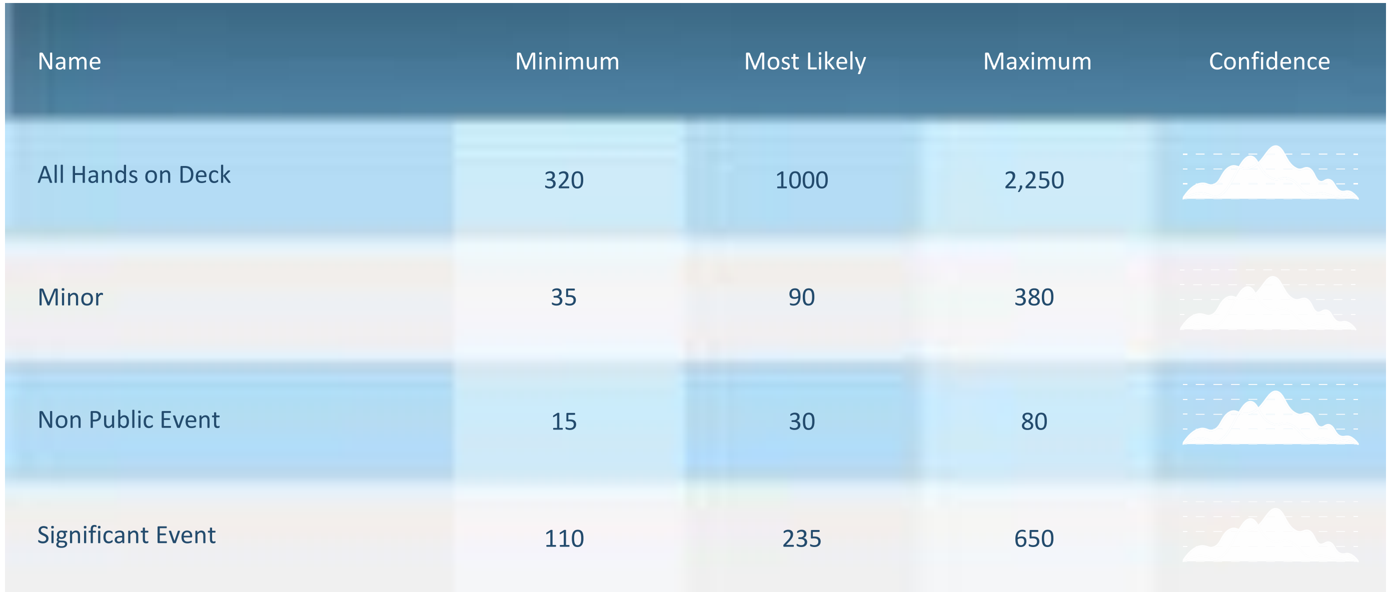
“Triage”= high-level, rapid analysis

Platform translates answers into quantitative range to answer “how often”

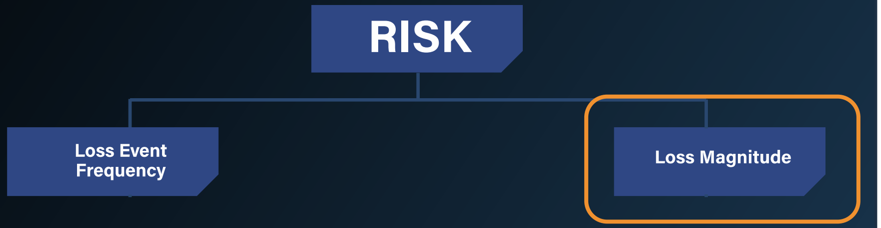
TRIAGE: HOW RISKLENS HELPS ANSWER LOSS MAGNITUDE

Data Helpers & Loss Tables Drive Efficiency & Consistency

Illustrative Example



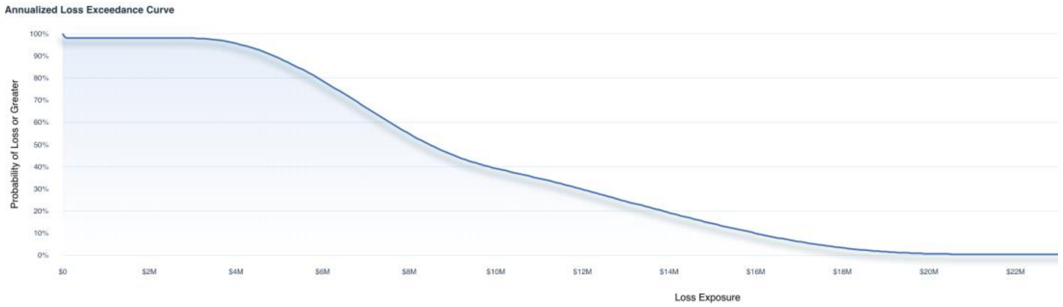
Name	Minimum	Most Likely	Maximum	Confidence
All Hands on Deck	320	1000	2,250	
Minor	35	90	380	
Non Public Event	15	30	80	
Significant Event	110	235	650	



TRIAGE: HOW RISKLENS COMPUTES DISTRIBUTIONS

Embedded Monte Carlo Simulations

- Problem solving technique used to approximate the probability of certain outcomes by automatically running thousands of trial runs, called simulations, using random inputs from the data ranges provided
- Monte Carlo is used by RiskLens at every branch of the FAIR model
- Same techniques are used in other enterprise risk domains to assess market risk, credit risk, etc.



Distributions Provide a Range of Outcomes

Report By

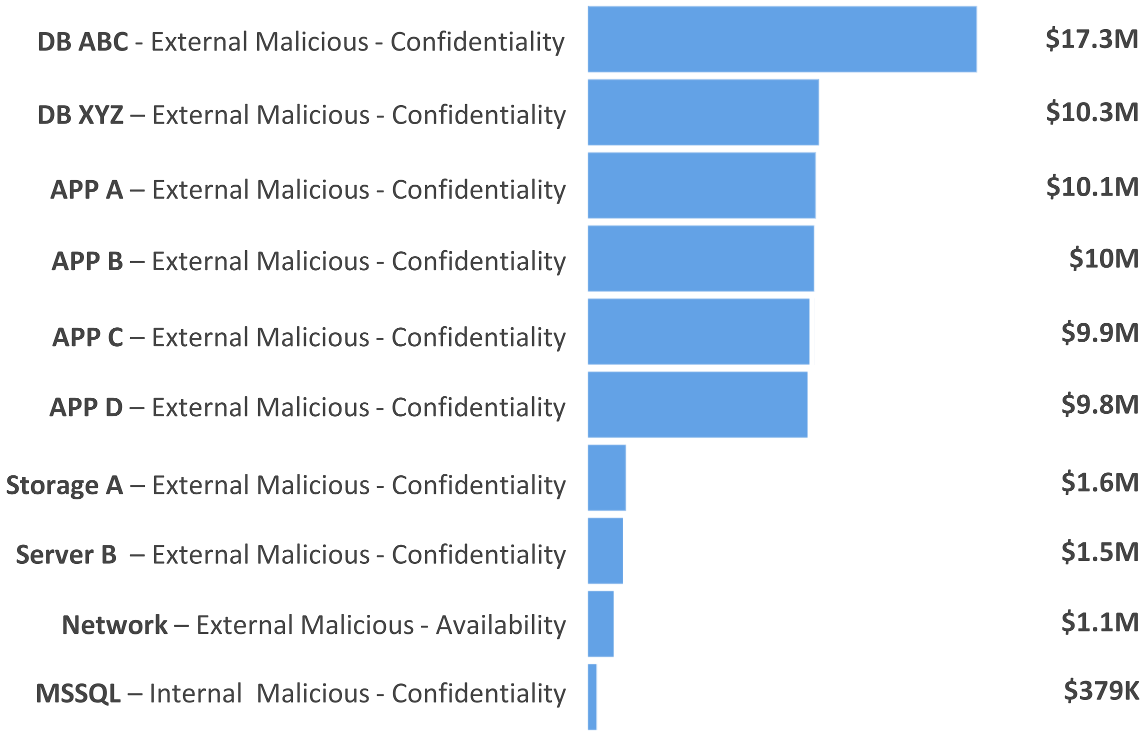
- Most Likely
- Minimum
- Average
- Maximum
- Etc.

OUTCOME EXAMPLE: TOP 10 TRIAGED LOSS EVENTS

Annualized Loss Exposure Average

Definition:
Top 10 scenarios with the largest average annualized loss exposure

$17.3M Top Annualized Risk


Top Risks - Average Annualized Loss Exposure

Thank you! - Q & A

RiskLens®

WORKSHOP: SCOPE OF THE IDENTIFICATION PHASE

40 Individual Scenarios Identified

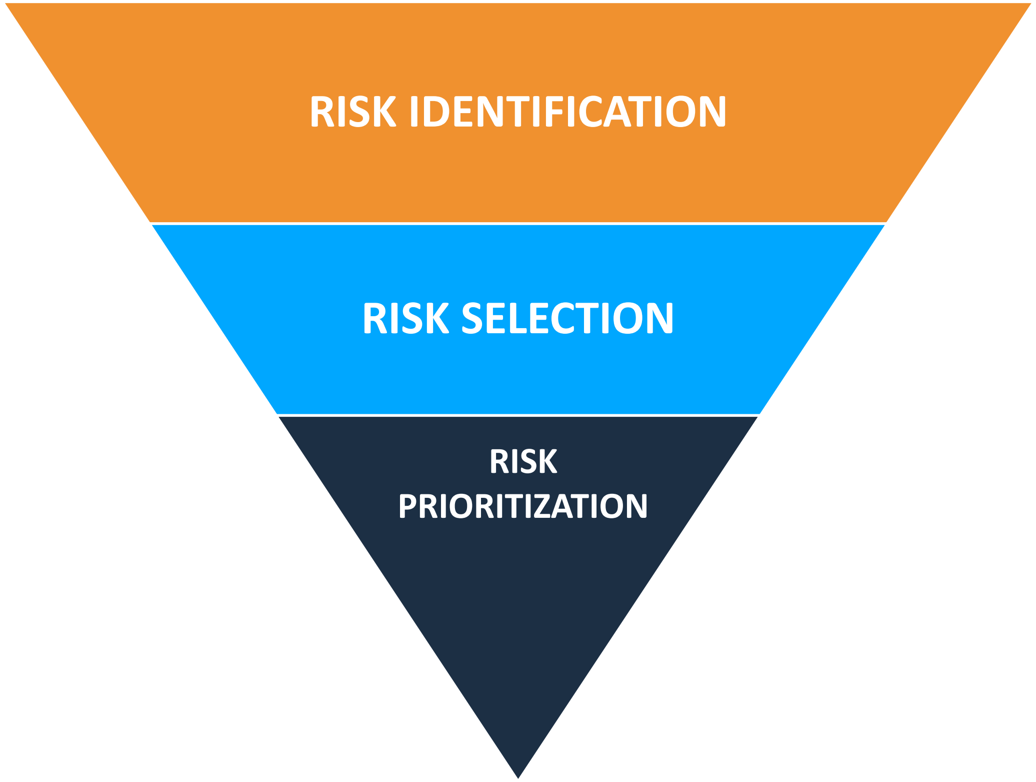
20 Selected for Triage Analysis

10 Unique Assets

- DB ABC
- DB XYZ
- APP A

5 Threat Communities

3 Effects


RISK IDENTIFICATION
RISK SELECTION
RISK PRIORITIZATION