FAIR INSTITUTE

Enabling Risk Economics

Helping organizations measure
Information & Operational Risk and the
cost-effectiveness of risk mitigation activities

About the FAIR Institute

The FAIR Institute is a non-profit expert organization dedicated to enabling business-aligned and cost-effective risk management

Based on the Open FAIR Standard

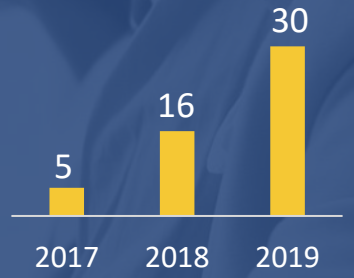
Education | Collaboration | Best Practices

9,300+
Members

23 Local Chapters

Workgroups

Universities offering FAIR courses



Leadership & Board Members

Jack Jones
Chairman, FAIR Institute
Chief Risk Scientist, RiskLens

Sounil Yu
Author
Cyber Defense Matrix

James Lam
Board Member
eTrade

Chris Porter
CISO
Fannie Mae

La'Treall Maddox
Strategy Risk Manager
Cisco

Kim Jones
Director, Security Operations
Intuit

Donna Gallaher
CEO
New Ocean Enterprises

Omar Khawaja
CISO
Highmark Health

Wade Baker
Founder Cyentia Institute
Prof. Integrated Security, VA Tech

Jack Whitsitt
SVP & FAIR Team Lead
Bank of America

Nicola (Nick) Sanna
President FAIR Institute
CEO RiskLens

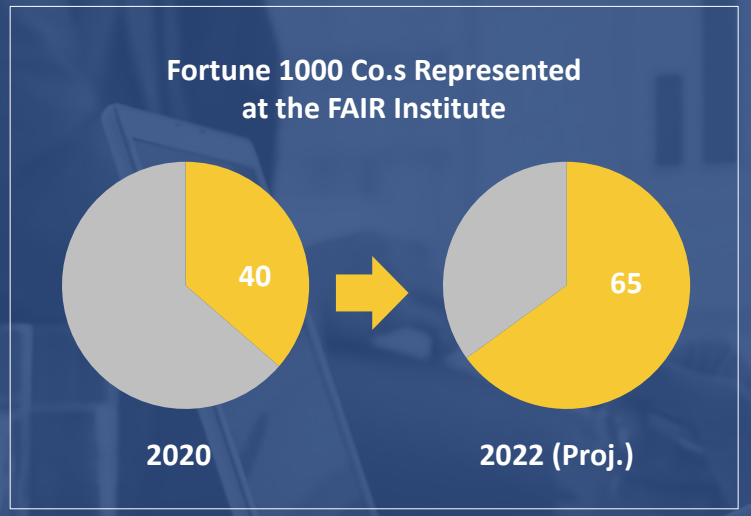
Evan Wheeler
VP of Risk Management
NVDR, Inc

FAIR Institute Recognized by SC Magazine As One of Three Most Important Industry Organizations of the Last 30 Years

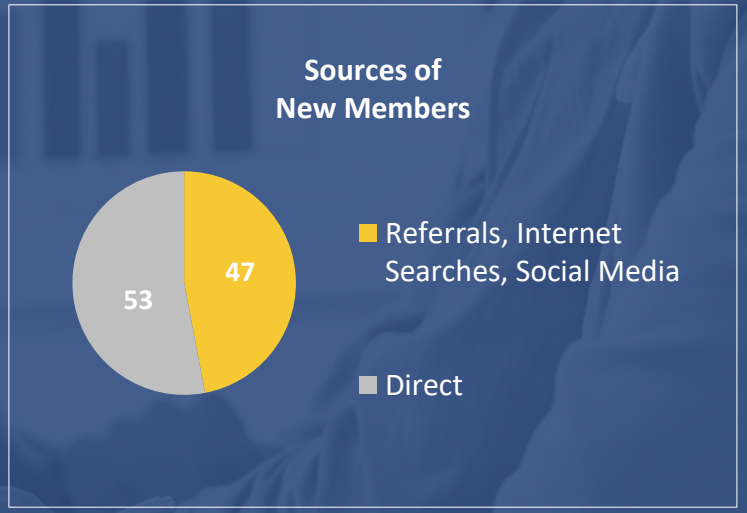
FAIR Sweeping the Industry

STRONG MEMBERSHIP GROWTH

FAIR EMERGING AS RISK MODEL OF CHOICE



FAIR SPREADING VIRALLY

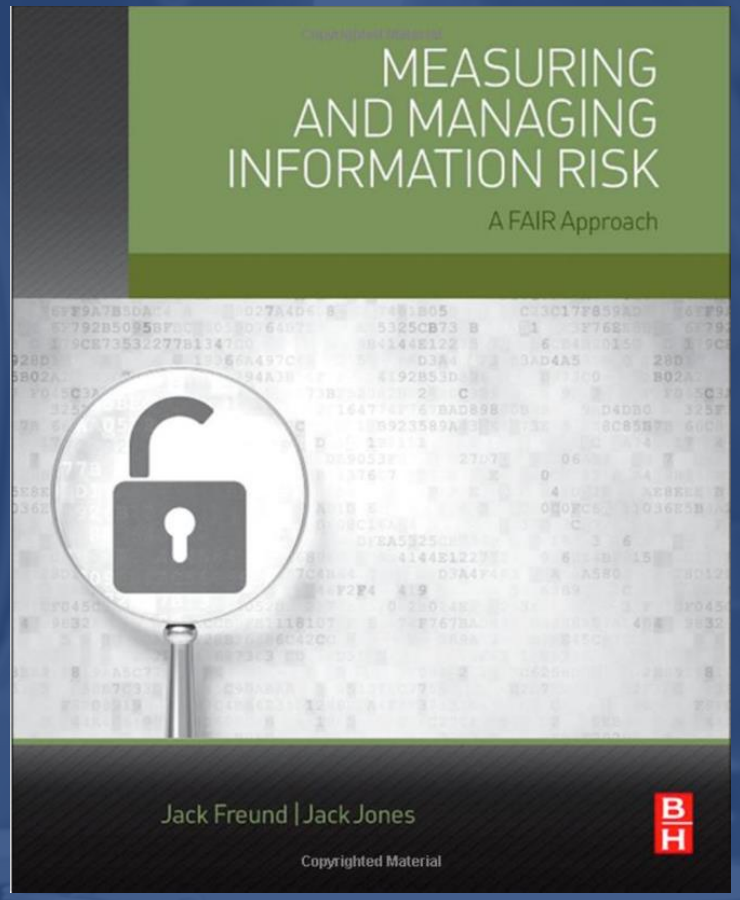


What is FAIR?

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative analysis model for information security and operational risk

- A Standard Taxonomy for Information and Operational Risk
- A Methodology for Quantifying and Managing Risk in Financial Terms in Any Organization
- A Complementary Analytics Model to existing Risk Frameworks, such as NIST CSF, ISO 31000, COSO
- A Standard of The Open Group

History of FAIR



- Jack Jones began research in 2001 at Nationwide Insurance
- Model perfected over 19+ years of operational use
- FAIR established as a global risk analysis standard by The Open Group in 2013
- FAIR Book is published in 2014
- FAIR Institute is founded in 2016
- NIST recognizes FAIR as a complementary standard to the CSF in 2019

EXPECTATIONS FOR CYBER RISK REPORTING HAVE CHANGED

FEAR, UNCERTAINTY & DOUBT → COMPLIANCE CHECKLISTS → MATURITY MODELS → CYBER RISK ECONOMICS

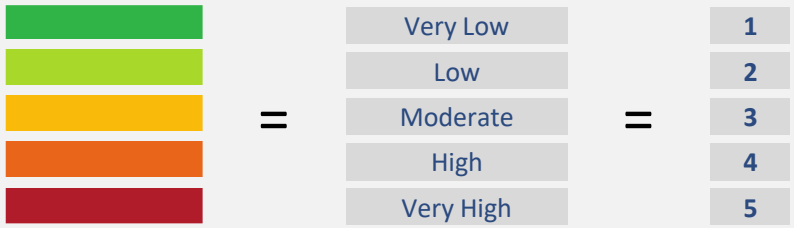
THE COMMUNICATION CHALLENGE

COMPLIANT… BUT STILL IN THE DARK

1 Qualitative Checklists & Excel

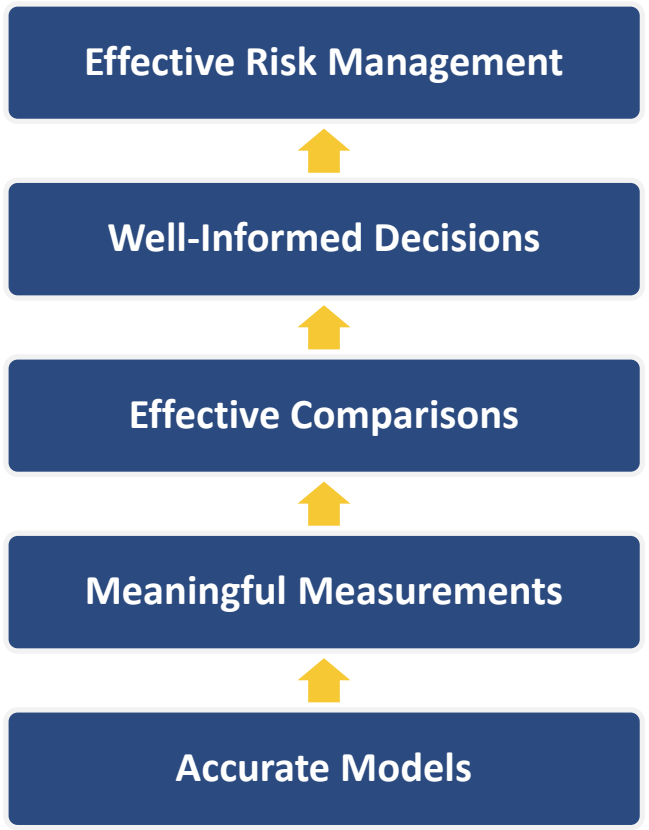
2 Governance, Risk & Compliance Tools

No embedded risk analytics capabilities in most GRC tools



The way most organizations measure risk today fails to quantify information and operational risk in terms the business can understand and use

EFFECTIVE RISK MANAGEMENT



The combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure.

Source: "Measuring and Managing Information Risk: A FAIR Approach"

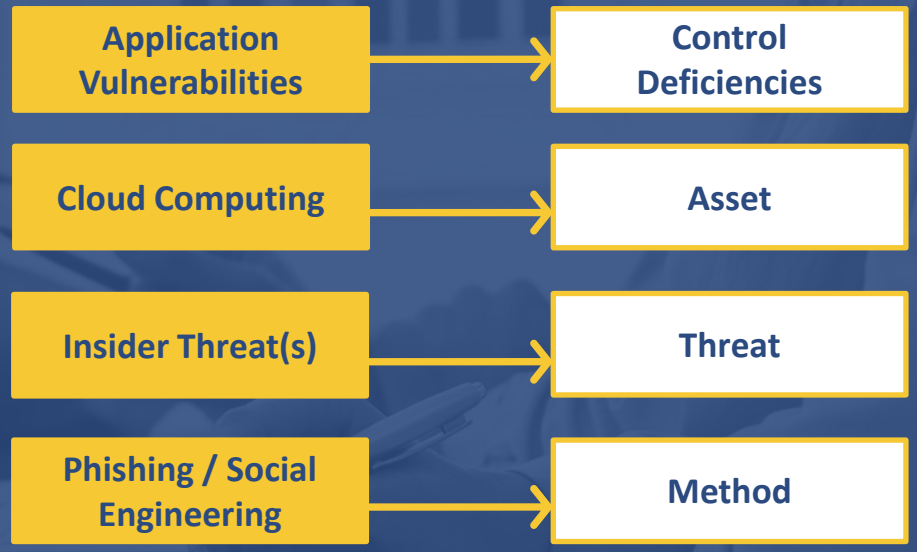
RISK MODELS MATTER

Which Of These Are **Risks?**

Point of Sale Attacks	Hacktivists
Cloud Computing	Phishing / Social Engineering
Insider Threat(s)	Third-party Risk
Cyber Criminals	Mobile Malware
Application Vulnerabilities	Business Continuity

Typical Top 10 Technology Risk List

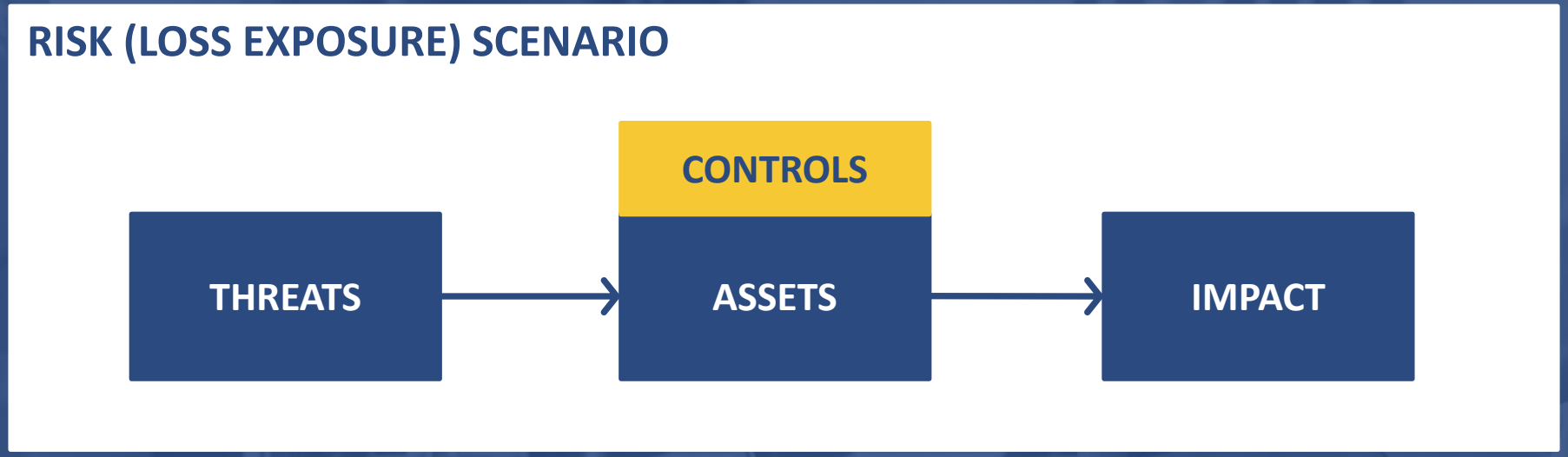
None!



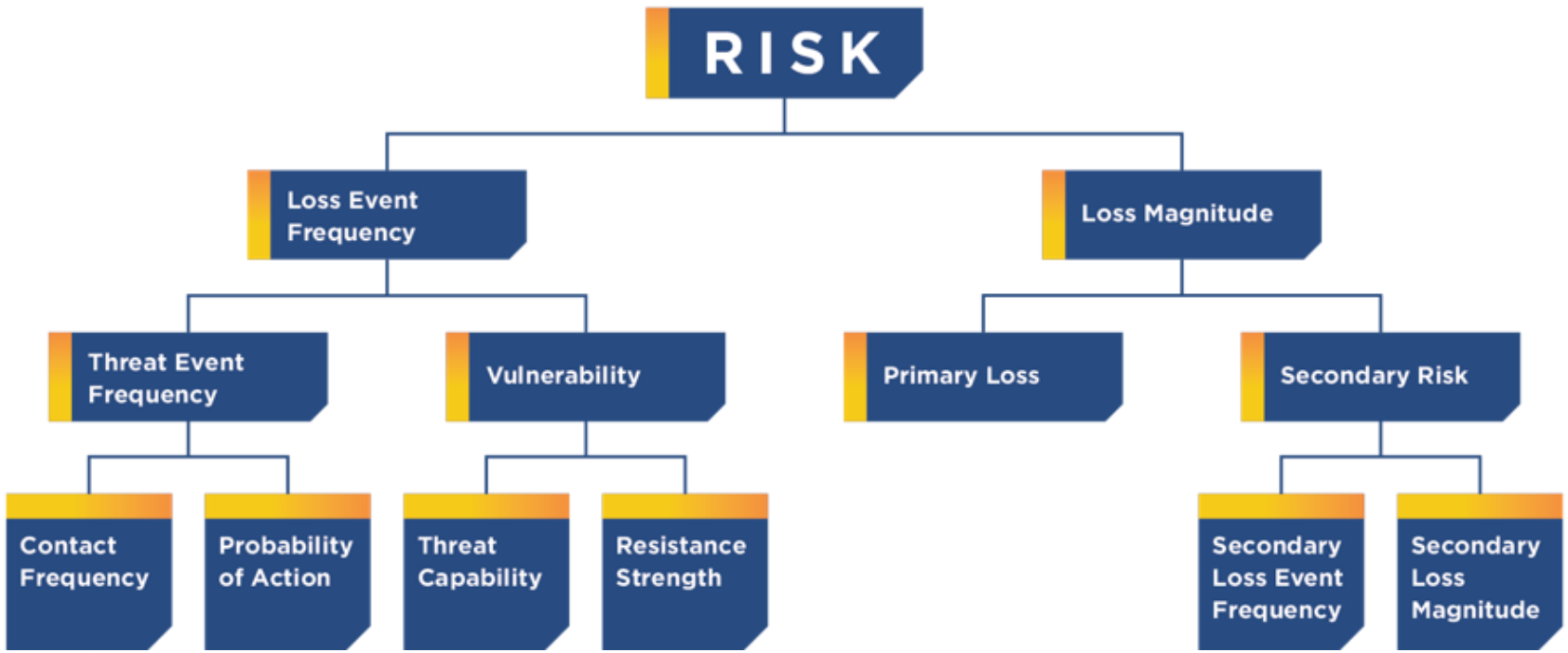
FAIR INSTITUTE

FAIR: A STANDARD RISK SCOPING MODEL

We Can Only Assess The Risk Of **Loss Events**



FAIR: THE STANDARD RISK ANALYTICS MODEL



Accredited as an Industry Standard by

THE Open GROUP
FAIR Foundations Risk Standard

Complementary to Risk Frameworks

ISO 27001 Certified

NIST

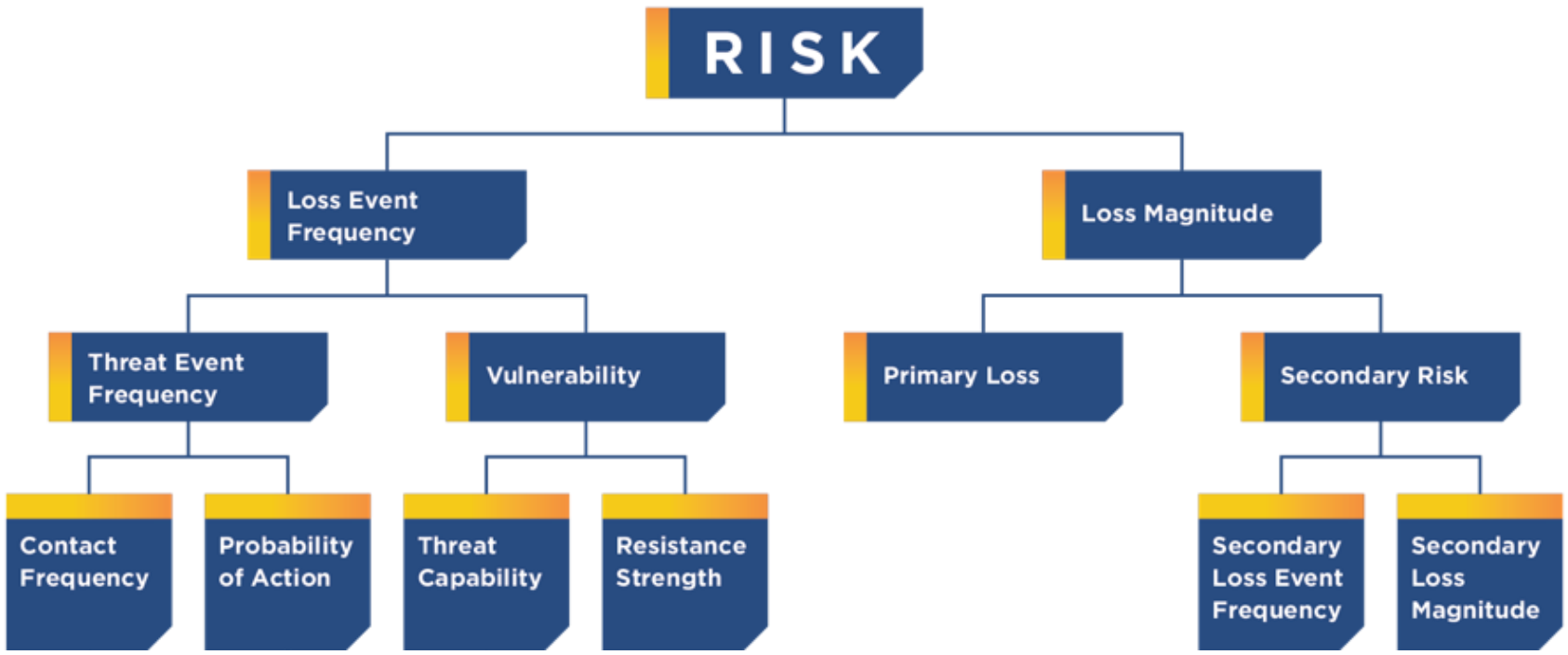
Supported by a Fast Growing Community

FAIR INSTITUTE

FAIR Book Inducted in Cybersecurity Canon

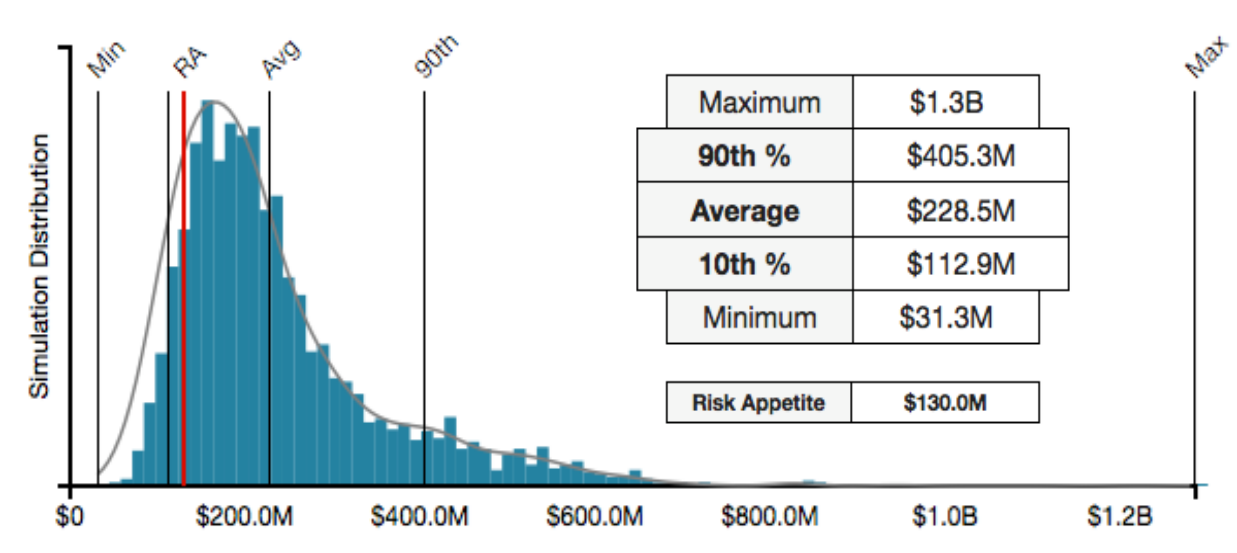
FAIR INSTITUTE

FAIR: THE STANDARD RISK ANALYTICS MODEL



- Designed to support risk quantification
- Supports quantitative measurement scales for risk factors
- Integrates into quantification solutions for calculating risk in financial terms
- Embraces Uncertainty: Inputs and Outputs are all statistical ranges
- Use of Monte Carlo simulations for more statistically accurate results

Measuring Information & Operational Risk in Financial Terms

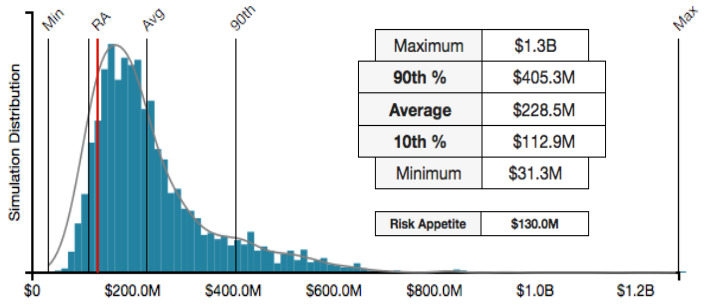


Sample Annual Loss Exposure Report
(Source: RiskLens – Technical Advisor of the FAIR Institute)

- FAIR is designed to support risk quantification
- It supports quantitative measurement scales for risk factors
- Integrates into computational engines (such as RiskLens) for calculating risk in financial terms, dollars and cents

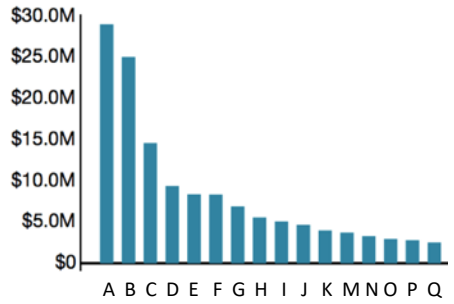
Communicating Risk in Financial Terms

"HOW MUCH RISK DO WE HAVE?"



Maximum	$1.3B
90th %	$405.3M
Average	$228.5M
10th %	$112.9M
Minimum	$31.3M
Risk Appetite	$130.0M

"WHAT ARE OUR TOP RISKS?"

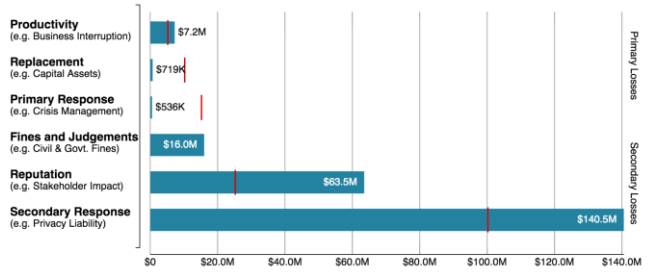


"HOW IS OUR RISK TRENDING VS. APPETITE?"

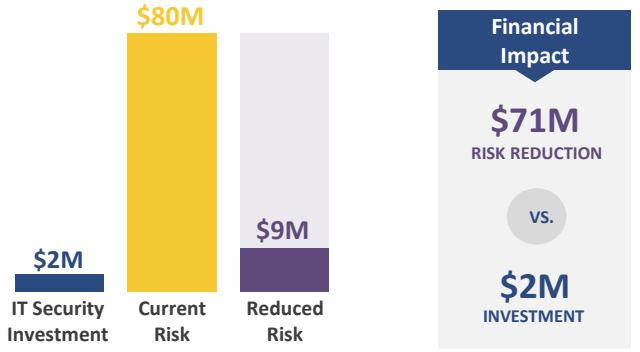
"HAVE WE REDUCED RISK?"

Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum
Annual Baseline Enterprise Analysis	Quarter 1 2014	$31.3M	$112.9M	$228.5M	$405.3M	$1.3B
Quarterly Updated Enterprise Analysis	Quarter 3 2014	$9.4M	$58.3M	$137.8M	$254.7M	$781.5M

"WHAT TYPE OF LOSS CAN WE EXPECT?"



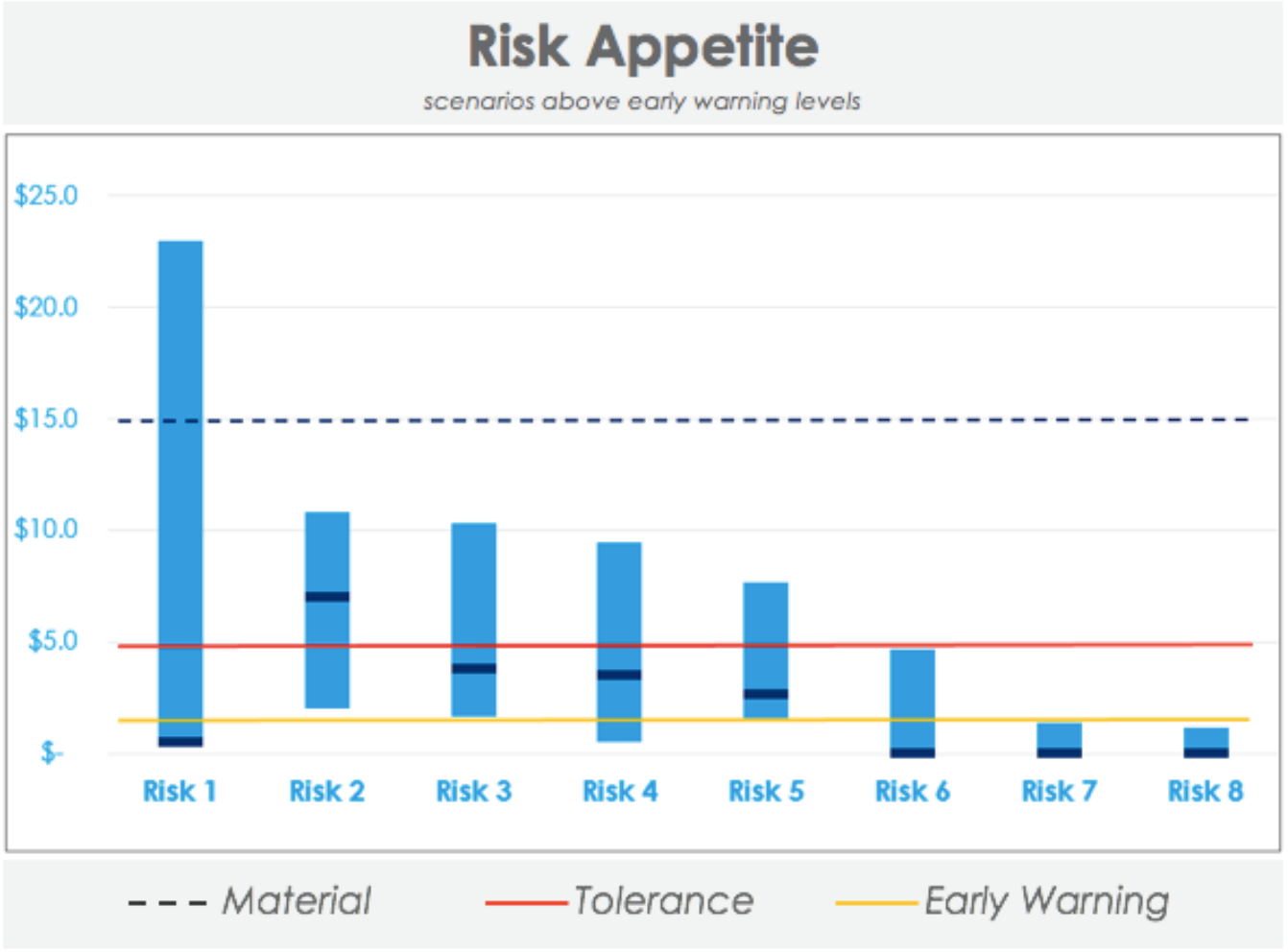
"WHAT IS THE COST/BENEFIT OF THIS PROJECT?"

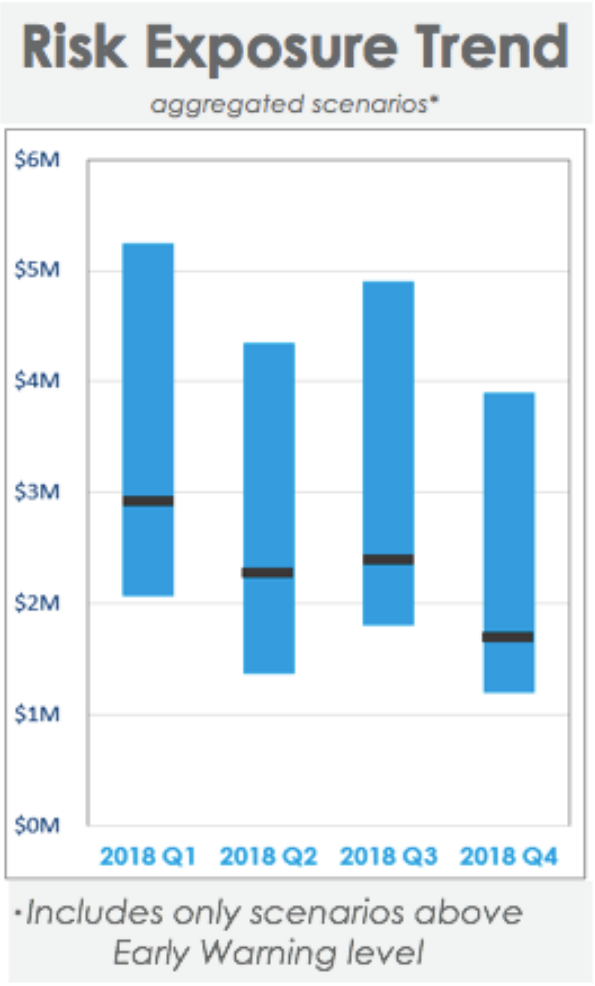


(Source: RiskLens)

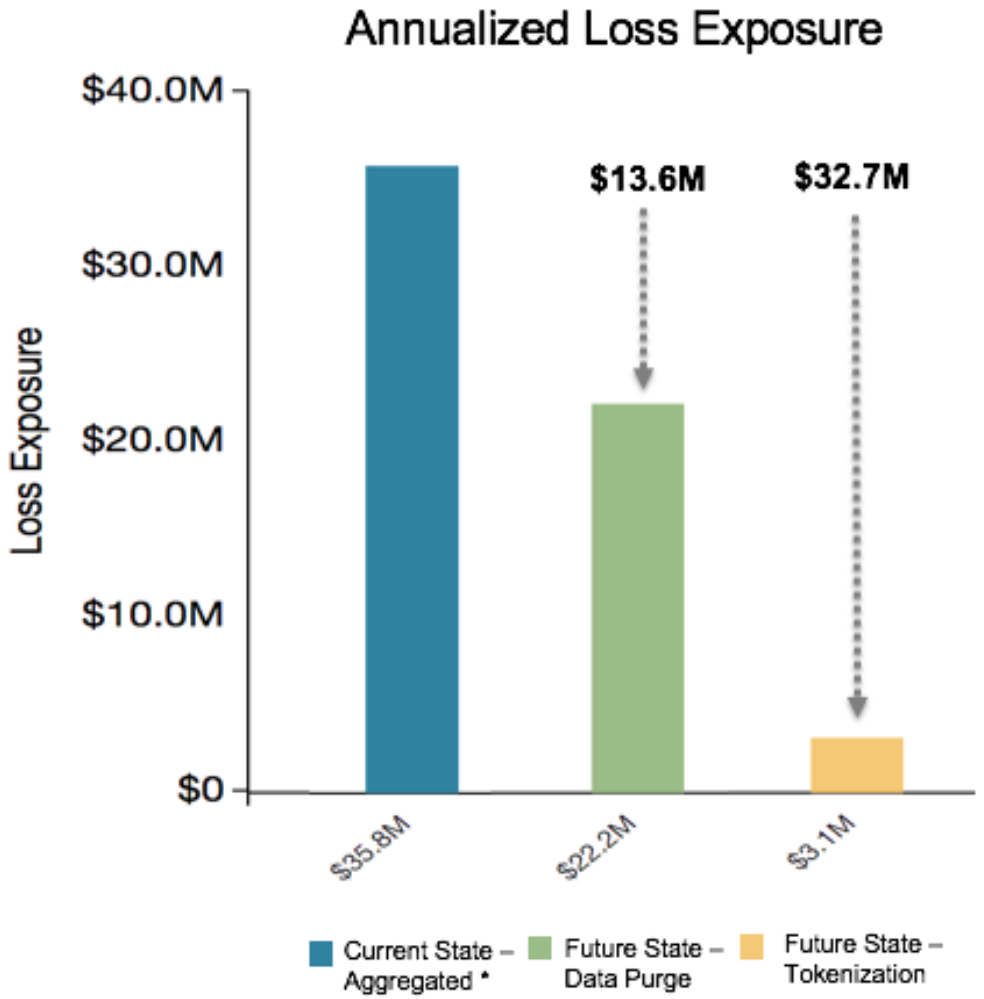
FAIR INSTITUTE

Risk Assessment – A Quantitative View





COMPARING RESULTS: DATA PURGE vs. TOKENIZATION



Key Drivers – Data Purge

Reduction of potential PII records stolen

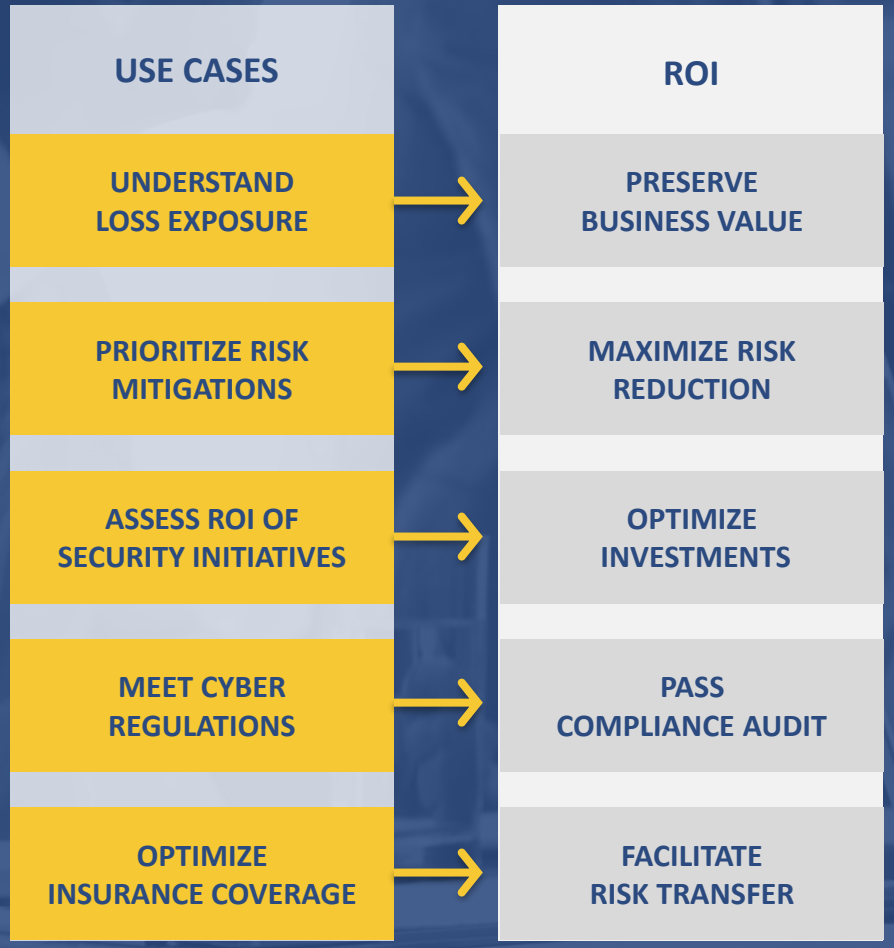
- Maximum of 1.8M (1. 2M reduction) for file shares
- Maximum of 6M (4M reduction) for database cluster

Key Drivers – Tokenization

Reduction in likelihood of secondary fall-out

- Reduction in Secondary Loss Event Frequency as the remaining data would be "phone book" data

MULTIPLE DIMENSIONS OF ROI



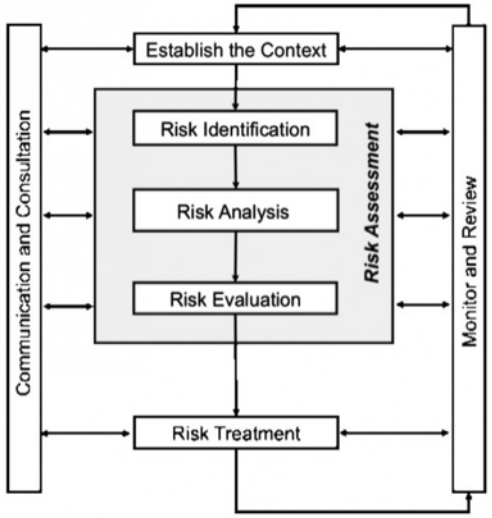
DRIVING
SMARTER INVESTMENTS
THAT ENHANCE
BUSINESS RESILIENCE

Complementary to Risk Mgmt. Frameworks

COSO Cube

NIST Cybersecurity Framework

ISO31000 Risk Mgmt. Process

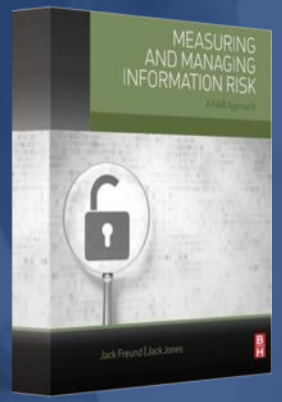


Most risk mgmt. frameworks **do not prescribe a specific approach** to identifying, analyzing and prioritizing risk and leave it to the risk practitioners to select their preferred analytics model.

This is where FAIR comes in and can be used to:

- **Identify top risks,** according to the FAIR risk scenario definitions
- **Quantify risk,** in monetary terms
- **Evaluate the efficacy of treatment options,** in terms of possible risk reduction
- **Communicate risk in a language than everyone understands,** including at board level

FAIR RESOURCES



FAIR BOOK

FAIR BLOG

RESOURCE LIBRARY

FAIR TRAINING & CERTIFICATION

FAIR-U TOOL

FAIR UNIVERSITY CURRICULUM

2020 FAIR Conference

October 6 & 7, 2020
A Virtual Experience

FAIRCON20 brings leaders in information and operational risk management together to explore best FAIR practices that produce greater value and enable business-aligned communication.

- Explore best risk management practices that align with business goals
- Discover new FAIR-based products and services to help your program
- Expand your industry wide network

Reserve your Seat Today: http://www.fairinstitute.org/faircon20

For more information, become a member at www.FAIRInstitute.org