SAN JOSÉ STATE UNIVERSITY

DEPARTMENT OF ECONOMICS

The Open Factor Analysis of Information Risk, a Standard for Cyber Risk

Mike Jerbic
stephen.jerbic@sjsu.edu

Today’s Main Ideas

As cyber risk becomes a board governance concern, management is increasingly making cyber risk part of operational risk management

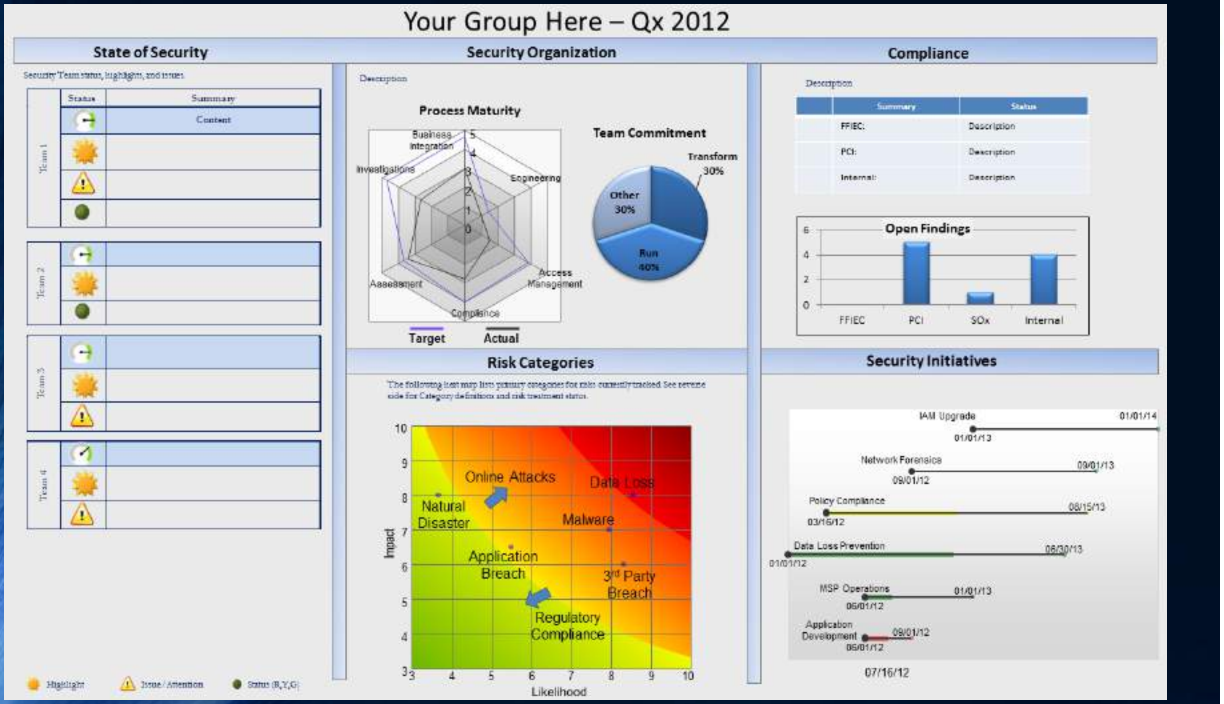
- For most organizations, cyber risk is not measured to the same standards as other risks
- Today, though we discuss how it can be by
  - Asking the right question
  - Using industry standard methods
  - Working through practical concerns and application
- This is an overview only
  - The references, though will give you a lot of self-study

How We Inform Cyber Risk Decision Makers

- “My data is a high risk”
- “Malware is a huge risk”
- “My passwords and firewalls are a risk”
- “Definitely, my employees are risks”
- “Earthquakes, fires, tornadoes, hurricanes are risks”

When asked, most executives believe cyber risk cannot be measured

Measuring Cyber Risks Today (Mostly)



Your Group Here – Qx 2012

State of Security

Security Team status, highlights, and issues.

	Status	Summary
Team 1	◔	Content
	☀	
	⚠	
	●	
Team 2	◔	
	☀	
	●	
Team 3	◔	
	☀	
	⚠	
Team 4	◔	
	☀	
	⚠	

● Highlight ⚠ Issue / Attention ● Status (R,Y,G)

Security Organization

Description

Risk Categories

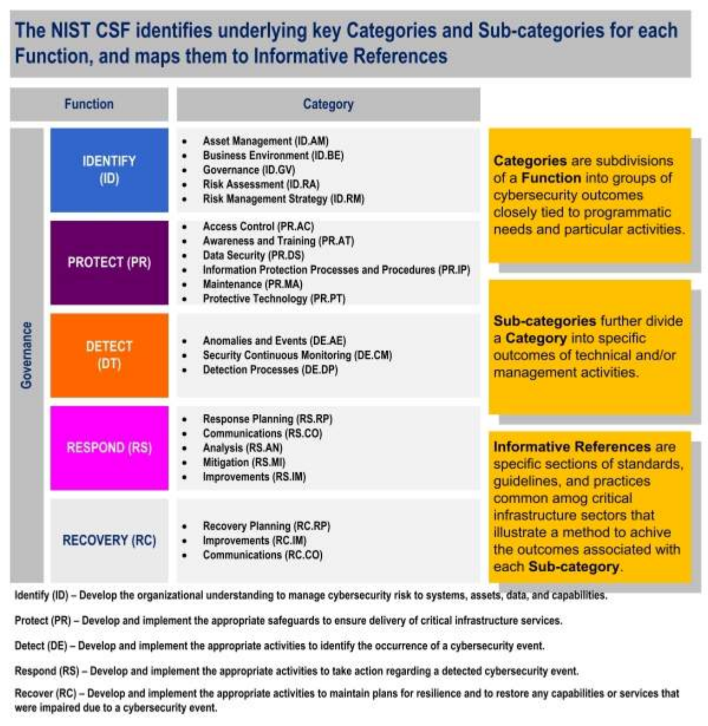
The following heat map lists primary categories for risks currently tracked. See reverse side for Category definitions and risk treatment status.

Compliance

Description

	Summary	Status
	FFIEC:	Description
	PCI:	Description
	Internal:	Description

Security Initiatives



The NIST CSF identifies underlying key Categories and Sub-categories for each Function, and maps them to Informative References

	Function	Category
Governance	IDENTIFY (ID)	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM)
	PROTECT (PR)	Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)
	DETECT (DT)	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)
	RESPOND (RS)	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)
	RECOVERY (RC)	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)

Categories are subdivisions of a **Function** into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Sub-categories further divide a **Category** into specific outcomes of technical and/or management activities.

Informative References are specific sections of standards, guidelines, and practices common amog critical infrastructure sectors that illustrate a method to achive the outcomes associated with each **Sub-category**.

Identify (ID) – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect (PR) – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect (DE) – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond (RS) – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover (RC) – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

But Elsewhere, Risk is Defined and Measured

- Risk: defined as the likelihood and severity of loss, loss exposure in dollars per year
  - Credit risk
  - Market risk
  - Operational risk
- Through well developed models to estimate and quantify risk
  - Domain-specific models
  - Through simulation
- Quantified results support effective management decisions
  - Capital requirements
  - Disclosure
  - Regulatory compliance
  - Cost-Benefit analysis of alternatives
    - Assessment
    - Insurance / Transfer
    - Project cost-benefit analysis and prioritization

Boards Need Standardized Risk

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
- Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
- Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
- Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Source: Cyber-Risk Oversight, Director's Handbook Series 2014, National Association of Corporate Directors, available at https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688

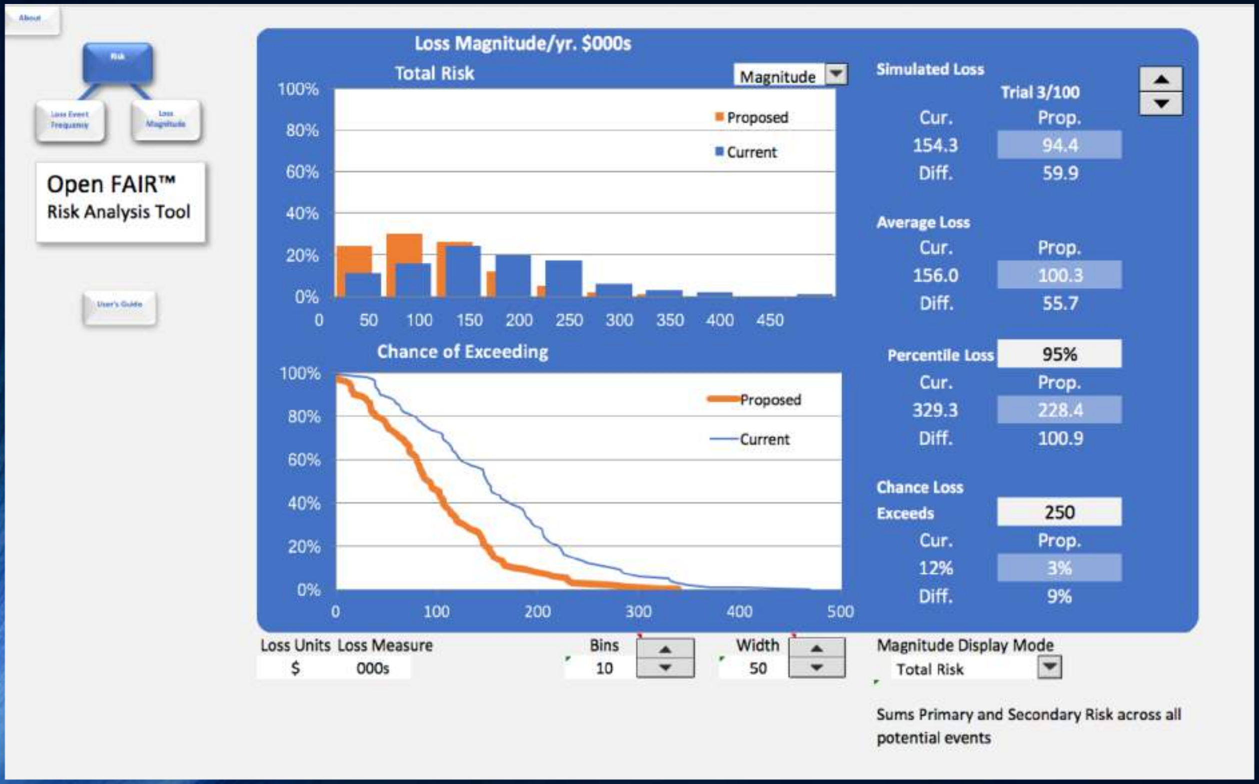
What a Risk Standard Does For Us

- Answer common questions / solves common problems once
  - Terms
  - Definitions
  - Relationships
- When combined, can form a “generally accepted body of knowledge”
- Once developed, no cost to reuse: resource efficient
- Enable interoperability of practitioners, systems, information

Risk Standards Now

Central Question	Credit Risk	Market Risk	Cyber Risk
	Banks Managing Risk associated with loans	**Traders managing Risk associated with trading financial assets**	**Risk associated with running information systems**
How often do bad things occur?	Probability of Default	Probability a loss exceeds a tolerable threshold	Probable Loss Event Frequency
How bad are they when they do?	Loss Given Default	Defined loss tolerance threshold	Probable Loss Magnitude

Most Importantly, Risk is a Distribution of Estimated Outcomes



Open FAIR™
Risk Analysis Tool

Simulated Loss

Trial 3/100

Cur.	Prop.
154.3	94.4
Diff.	59.9

Average Loss

Cur.	Prop.
156.0	100.3
Diff.	55.7

Percentile Loss 95%

Cur.	Prop.
329.3	228.4
Diff.	100.9

Chance Loss Exceeds 250

Cur.	Prop.
12%	3%
Diff.	9%

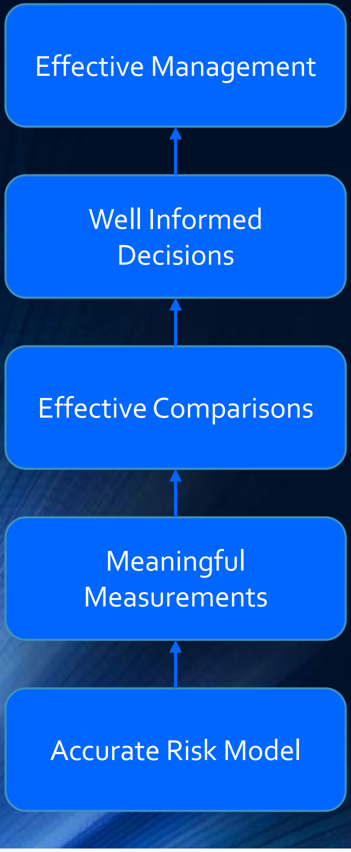
Loss Units	Loss Measure	Bins	Width	Magnitude Display Mode
$	000s	10	50	Total Risk

Sums Primary and Secondary Risk across all potential events

Standard Measures

- Averages
- Probability of a loss within a time period
- Magnitude of a single loss given a probability of occurrence
- Loss thresholds, risk appetite
- Probability distribution of likely outcomes

Cyber Risk as an Operational Risk: Open FAIR^{TM} Risk Taxonomy and Analysis Standards



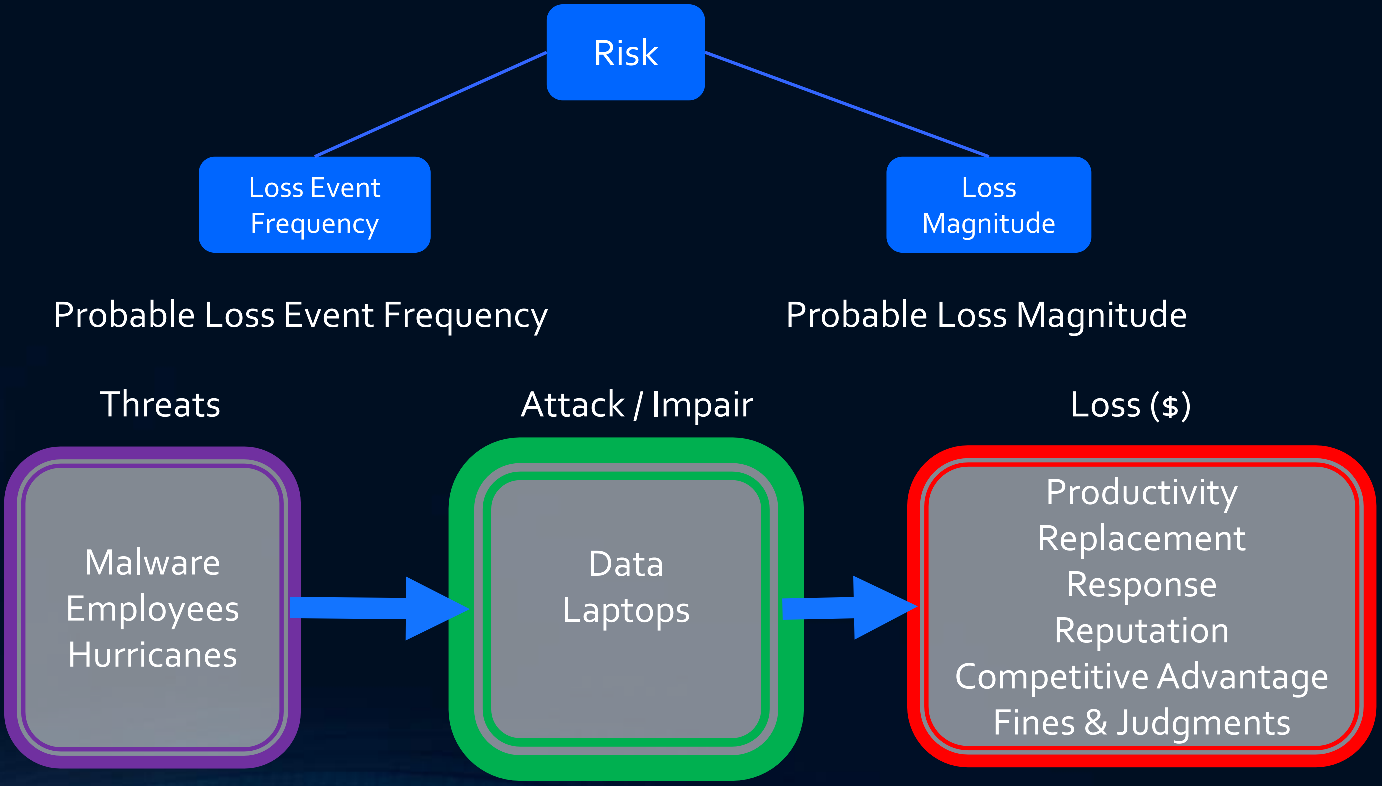
Effective Management

Well Informed Decisions

Effective Comparisons

Meaningful Measurements

Accurate Risk Model



Risk

Loss Event Frequency

Loss Magnitude

Probable Loss Event Frequency

Probable Loss Magnitude

Threats

Malware
Employees
Hurricanes

Attack / Impair

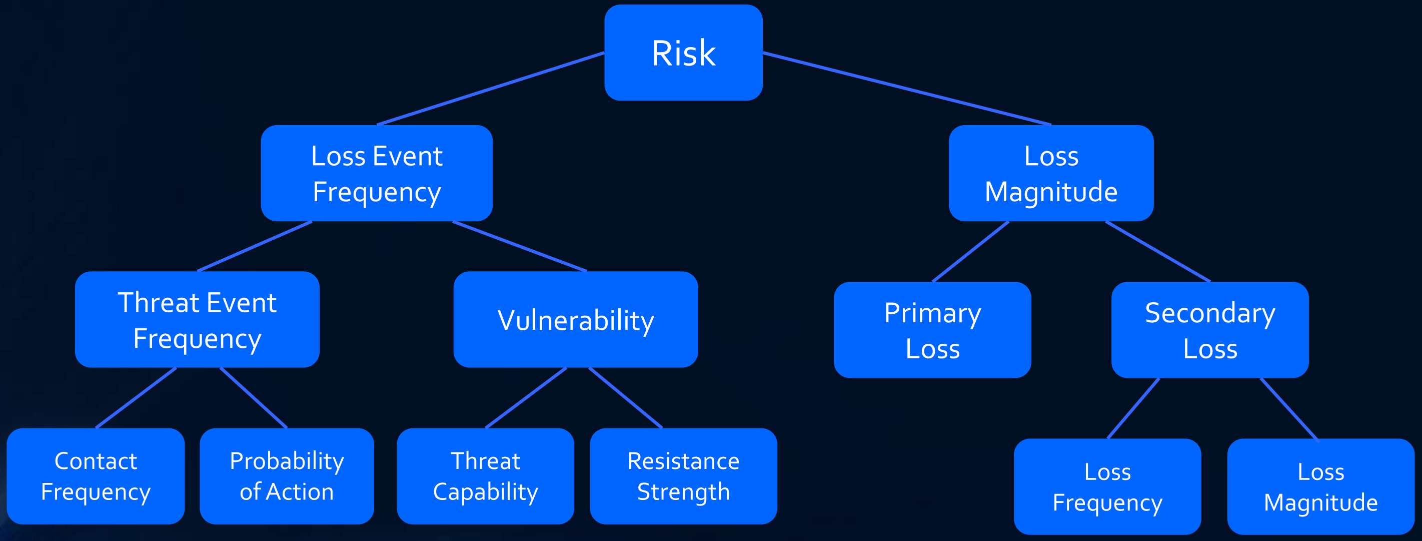
Data
Laptops

Loss ($)

Productivity
Replacement
Response
Reputation
Competitive Advantage
Fines & Judgments

Modelling Risk

- Work within the Open FAIR^{TM} Taxonomy
  - Using calibrated estimates (Min, Max, Most Likely) for the risk factors
  - Most analyses stop here



Probable Loss Event Frequency

Probable Loss Magnitude

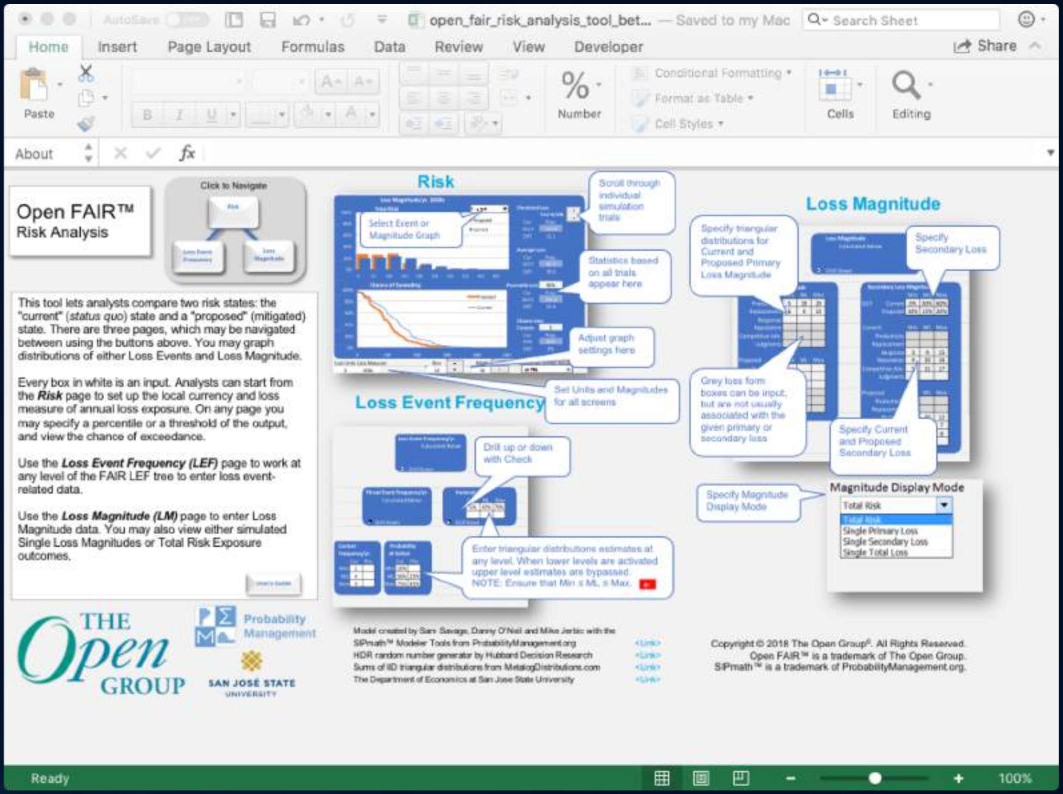
Open FAIR$^{\text{TM}}$: Standardizes Cyber Risk

- Measured as any other risk: In dollars. Total risk now may be aggregated and managed
- Defensible Cyber Risk Analyses
  - Capital requirements
  - Risk-based compliance
  - Disclosure
  - Preventive, Detective, Corrective Control Business Case

- Initial Assessment
- Insurance / Transfer
- Project Business Case Support and Prioritization
- The Analytic Engine for “Risk Based” Compliance or decision making

Open FAIR Risk Analysis Tool Using SIPMATH Distributions

SAN JOSÉ STATE
UNIVERSITY
DEPARTMENT OF ECONOMICS



Open FAIR™
Risk Analysis

This tool lets analysts compare two risk states: the "current" (*status quo*) state and a "proposed" (mitigated) state. There are three pages, which may be navigated between using the buttons above. You may graph distributions of either Loss Events and Loss Magnitude.

Every box in white is an input. Analysts can start from the ***Risk*** page to set up the local currency and loss measure of annual loss exposure. On any page you may specify a percentile or a threshold of the output, and view the chance of exceedance.

Use the ***Loss Event Frequency (LEF)*** page to work at any level of the FAIR LEF tree to enter loss event-related data.

Use the ***Loss Magnitude (LM)*** page to enter Loss Magnitude data. You may also view either simulated Single Loss Magnitudes or Total Risk Exposure outcomes.

THE Open GROUP
Probability Management
SAN JOSÉ STATE UNIVERSITY

Risk

Select Event or Magnitude Graph

Scroll through individual simulation trials

Statistics based on all trials appear here

Adjust graph settings here

Set Units and Magnitudes for all screens

Loss Event Frequency

Drill up or down with Check

Enter triangular distributions estimates at any level. When lower levels are activated upper level estimates are bypassed. NOTE: Ensure that Min ≤ ML ≤ Max.

Loss Magnitude

Specify triangular distributions for Current and Proposed Primary Loss Magnitude

Specify Secondary Loss

Grey loss form boxes can be input, but are not usually associated with the given primary or secondary loss

Specify Current and Proposed Secondary Loss

Specify Magnitude Display Mode

Magnitude Display Mode

Total Risk ▾
- Total Risk
- Single Primary Loss
- Single Secondary Loss
- Single Total Loss

Model created by Sam Savage, Danny O'Neil and Mike Jerbic with the
SIPmath™ Modeler Tools from ProbabilityManagement.org <Link>
HDR random number generator by Hubbard Decision Research <Link>
Sums of IID triangular distributions from MetalogDistributions.com <Link>
The Department of Economics at San Jose State University <Link>

Copyright © 2018 The Open Group®. All Rights Reserved.
Open FAIR™ is a trademark of The Open Group.
SIPmath™ is a trademark of ProbabilityManagement.org.

Probability
Management

Source: https://publications.opengroup.org/i181

It Works

"FAIR is the future of information security, as that's how we will bridge the gap and talk about risk in a common language."

- CISO Fed Reserve NY

http://www.opengroup.org/certifications/openfair

http://www.fairinstitute.org

SAN JOSÉ STATE
UNIVERSITY

DEPARTMENT OF ECONOMICS

Leading in Developing and Teaching the Open FAIR^{TM} Risk Standard

- Academic Program with the Open Group
  - Norwegian Regional Health Authority Risk Analysis
  - Open FAIR^{TM} Risk Analysis Process Guide
- Open FAIR Risk Analysis Tool Using SIPMATH Distributions
- Twenty one students Open FAIR^{TM} Certified

THE Open GROUP

Probability Management

The Open Group
Open
Certified
Open FAIR

Resources

- Open FAIR Risk Taxonomy and Risk Analysis Standards
  - https://publications.opengroup.org/c13k
  - https://publications.opengroup.org/c13g
- Open FAIR Risk Analysis Tool Using SIPMATH Distributions
  - https://publications.opengroup.org/i181
- The Open FAIR Tool with SIPMATH Distributions: Guide to the Theory of Operation
  - https://publications.opengroup.org/g181
- Open FAIR Risk Analysis Process Guide
  - https://publications.opengroup.org/guides/g180
- Norwegian Regional Health Authority Paper
  - https://publications.opengroup.org/white-papers/healthcare/w176
- Foundational texts
  - *How to Measure Anything* by Douglass Hubbard
  - *Measuring and Managing Information Risk* by Jack Freund and Jack Jones

THE Open GROUP

SAN JOSÉ STATE
UNIVERSITY
DEPARTMENT OF ECONOMICS

Probability
Management

Local Risk Interest Groups Standardizing Risk

PRMIA
Professional Risk Managers' International Association

rma®
THE RISK MANAGEMENT ASSOCIATION

FAIR
INSTITUTE

SAN JOSÉ STATE
UNIVERSITY

DEPARTMENT OF ECONOMICS

Thank You

Mike Jerbic
stephen.jerbic@sjsu.edu