WERNER

The Institute of Internal Auditors
Detroit Chapter

The Institute of Internal Auditors
Detroit Chapter
Presents

Quantitative Risk Management
Our Journey to Jones FAIR

A Risk Assessment Discussion

Earning CPE Credit

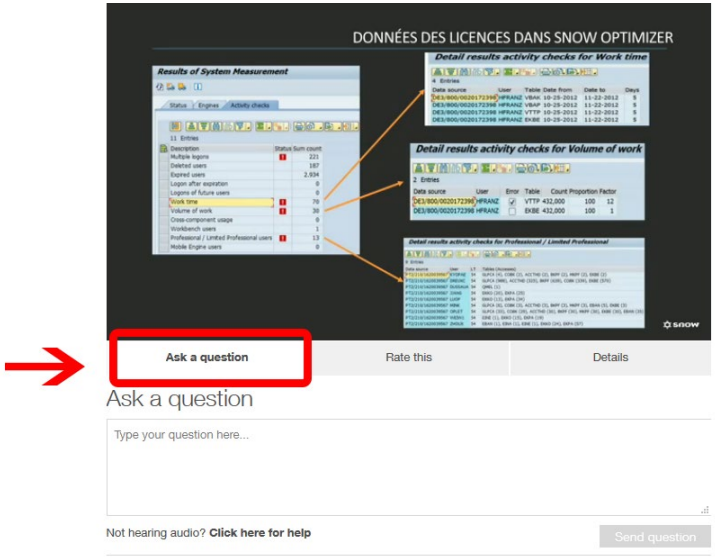
In order to receive CPE credit for this webcast, participants must:

- Attend the webcast on individual computers (one person per computer)
- Answer polling questions asked throughout the webcast
- During polling questions, make sure to submit your answer (You will see the polling results, when your answer is submitted).
- CPE certificates will be sent to the e-mail address on your BrightTALK account within two weeks of this webinar.

If You Have Questions…

If you have questions during the webcast:

- **If necessary, exit Full Screen View by pressing the Esc key**
- **Submit questions through the *Ask a question button***



Please tell us your member status

A) Member Detroit Chapter

B) Member - Central Region District 2 (Fort Wayne, Toledo, Michiana, W. Mich., Lansing)

C) Member - Other District

D) Non-member

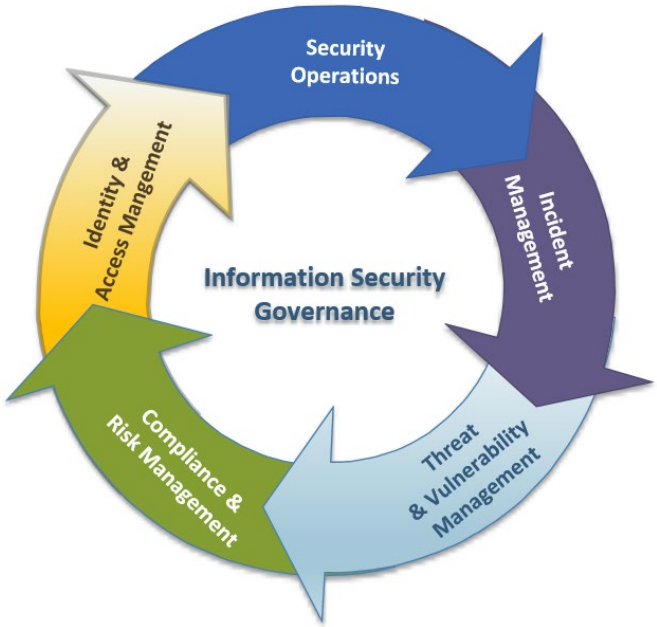
Quantitative Risk Management

Our Journey to Jones FAIR

- Why Jones FAIR?
- Why discussions about risk are often confusing
- Challenges we've found
- Real-world examples

David Elfering
Vice President - Information Security
Werner Enterprises
delfering@werner.com

Information Security Pillars



Werner's Information Security Pillars

- **Governance:** Binds all the program components
- **Threat & Vulnerability Management**: Protect and harden systems and applications
- **Security Operations**: Monitor, detect, respond
- **Incident Management**: Respond to attacks mitigate damage
- **Identity & Access Management**: Control access to key systems and data to protect Werner
- **Risk & Compliance Management**: IT risk and compliance assessments, ranked via quantitative methods. Ensure IT Vendor risk is assessed and managed.

Maturity measures capability & repeatability

- **You cannot manage what you cannot measure**
- **Processes must be repeatable**
- **Measurement provides ability to tune and manage risk**

Security Risk Management

risk

/risk/

noun

1. a situation involving exposure to danger.
   "flouting the law was too much of a risk"

verb

1. expose (someone or something valued) to danger, harm, or loss.
   "he risked his life to save his dog"
   synonyms: endanger, imperil, jeopardize, hazard, gamble, gamble with, chance;

Quantified Risk Management

Measuring the probable frequency and size of future loss

Information Security Risk Strategy

1. Identify
2. **Analyze ← FAIR**
3. Evaluate
4. Treat
5. Monitor

They Will Not Tell You That They Want You to Help Them Calculate IT Risk

They need to know:

Definition:	What is the nature of the risk?
Probability:	What is the likelihood of the negative event occurring?
Timing:	When would the negative event occur?
Impacts:	Should the event occur, what is the potential damage?
Estimates:	How much will it cost to mitigate the risk?

Polling Question

My organization has a strategy for risk that drives meaningful decisions and outcomes.

A) Yes
B) No
C) Uncertain

Polling Question

Information Security Risk Strategy has 5 phases: Identity, Analyze, Evaluate, Treat and Monitor. Which phase does FAIR participate in?

a) Identity
b) Analyze
c) Evaluate
d) Treat
e) Monitor

Why Jones FAIR?

Executive Discussions	• **"How much did our risk go up?"** • **Actionable information for executive risk decisions** • **Meaningful risk discussions**
Repeatable, Measurable, Risk Management	• **If I hear "best practice" one more time…** • **Tired of arbitrary risk assessments** • **Can't improve what you cannot measure** • **Sustained improvement measurement**
Risk Management Not Financially Oriented	• **NIST RMF** • **Gartner Value Adjusted Risk** • **Octave**

Goal: Information Security financial risk portfolio

- Can you be fiduciary without relating risk in dollars?
- A for profit company makes decisions based on monetary impact

Challenges in Transitioning

InfoSec Team	• **"I don't see how this is relevant to me"**
	• **"Well… you are a numbers guy …"**
	• **Learning difference between accuracy & precision**
	• **Rampant addition to qualitative risk**
	• **Learning structured, analytic risk approach**
	  • **Asset, threat, effect**
	  • **Structuring risk into scenarios**
	  • **Scoped data gathering**

Executive Education	• **Risk is a quantity, not a thing** • **We are forecasting not predicting** • **Only two things in life are certain**

Budget	• **License structure is complex**
	• **Added costs you need to account for**
	  • **Educating your team ($10k)**
	  • **Implementation consulting ($17k)**
	  • **FAIR oriented risk register workshop ($10k)**

Summary: Learning to systematically measure & manage risk easier said than done

- InfoSec may be viewed as a technology area, not a risk management resource
- Expect resistance to change
- Executive buy-in takes time and communication
- Don't over buy on licensing; start small; walk then run

Conclusions - Recommendations

Start Small	• Train multiple analysts in advance
	  • Fundamentals training from Risk Lens is quite good
	  • Enroll multiple people in Advanced Analyst course
	• Enroll in free, FairU online resource

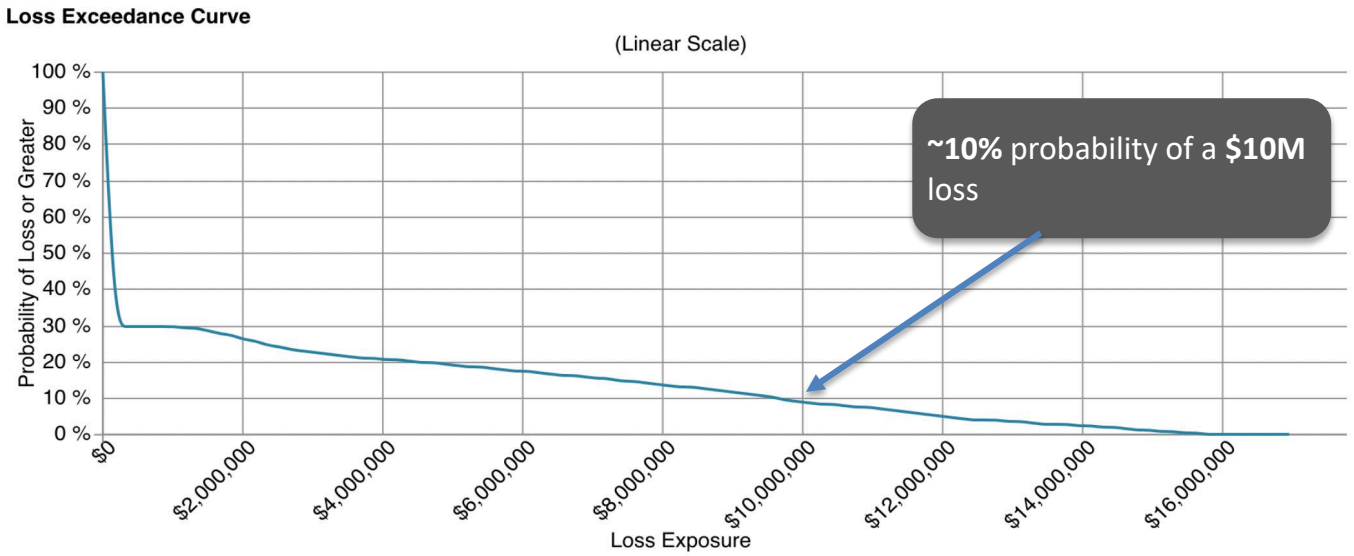
Expect a Learning Curve	• Understanding FAIR doesn't translate to doing quantitative assessments • Leverage education as an opportunity to reach consistent definitions of risk terminology • Framing risk via scenarios and FAIR approach is new ground for most analysts • Risk Lens is straight forward, but takes time to get comfortable in
Unexpected Benefits	• Strong adoption of FAIR by Internal Audit • Aligning audit to business impact & value • FAIR fundamentals lead to better risk discussions
Conclusion	• FAIR answers risk questions that RMF, COBIT, CSF don't • Boards & Executives want the information that quantitative methods can provide • Risk Lens requires firm FAIR understanding to use effectively

Polling Question

FAIR answers risk questions that RMF, COBIT, CSF don’t. True or False

Real World Example

Annualized Loss Exposure – Frequency x Magnitude



10th Percentile	Most Likely	90th Percentile
$0	**$0**	$9.6M
Min $0	Average $2.2M	Max $16.8M

Per event metrics

#

.3 Frequency

Estimated loss events per year

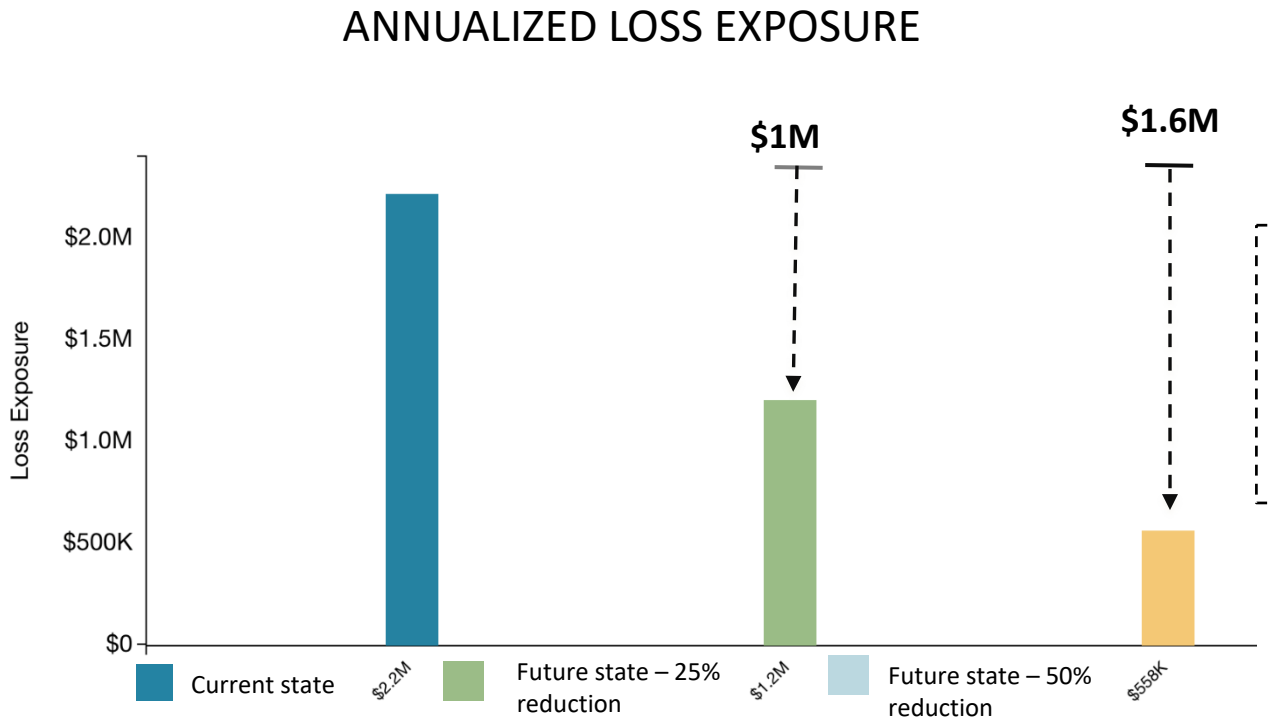
Average (1 in a ~3 year event)

$

Primary Loss: average $3K

Secondary Loss: average $2.2M

Reduction in Loss Exposure



Risk Appetite:
Meaningful risk discussion. What kind of risk profile to executives want?

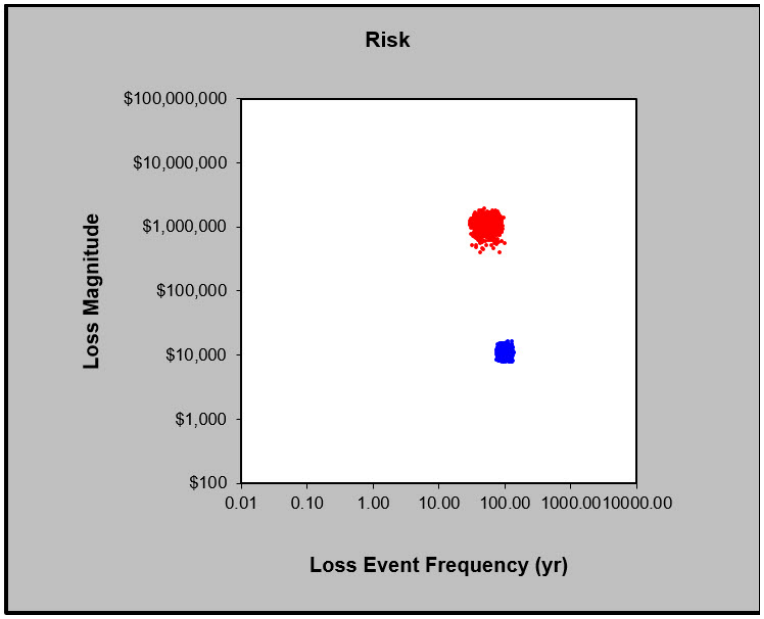
Drive meaningful risk discussions

- **What are the executives willing to tolerate?**
- **How much will it cost to reduce the risk?**
- **When do we transfer risk via options such as insurance?**

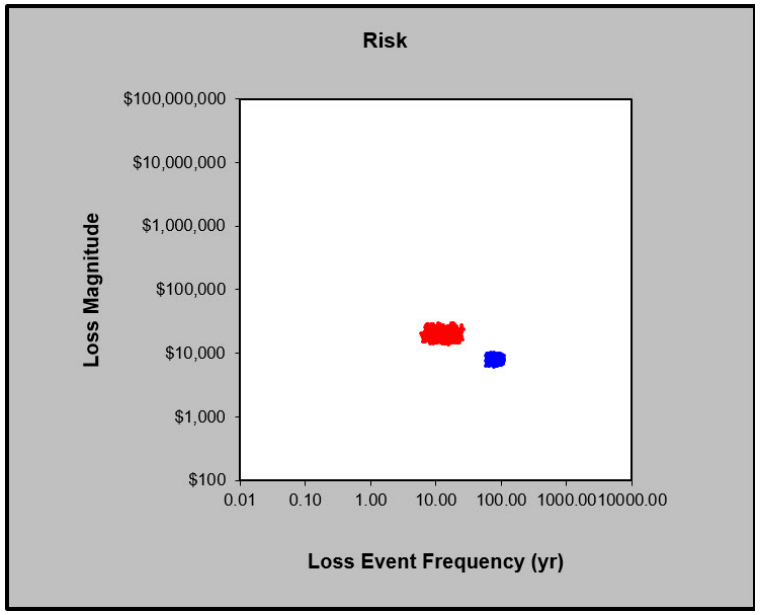
FAIR – First Attempt

Old School FAIR Analysis Circa 2016

How one control can reduce exposure



Office 365 logins without MFA



Office 365 logins MFA

Blue: Primary Loss
Red: Secondary Loss

Loss Tables

- Loss Tables: Where the magic happens
  - Must have loss tables to run forecasts
  - PII (confidentiality) is the easy part
  - Availability requires some work
    - Can you break availability financial loss down by business area?

Personally Identifiable Information (Confidentiality Losses)

Fines & Judgments | Reputation | Response | Lost Customers | Credit Monitoring

Range	Minimum	Most Likely	Maximum	Confidence
1	$0	$0	$0	Low
10	$0	$0	$0	Low
100	$0	$0	$10,000	Medium
1,000	$0	$5,000	$15,000	Medium
10,000	$10,000	$25,000	$150,000	Medium
100,000	$50,000	$100,000	$850,000	Medium
1,000,000	$250,000	$500,000	$1,500,000	Medium
10,000,000	$250,000	$1,000,000	$2,000,000	Medium

Availability Losses

Revenue | Fines & Judgments | Reputation | Response | Guidance

Range	Minimum	Most Likely	Maximum	Confidence
1hr	$0	$0	$0	Low
2hr	$0	$0	$0	Low
4hr	$0	$0	$0	Low
8hr	$0	$0	$0	Low

Polling Question

Forecasts can be run without the loss tables – True or False.

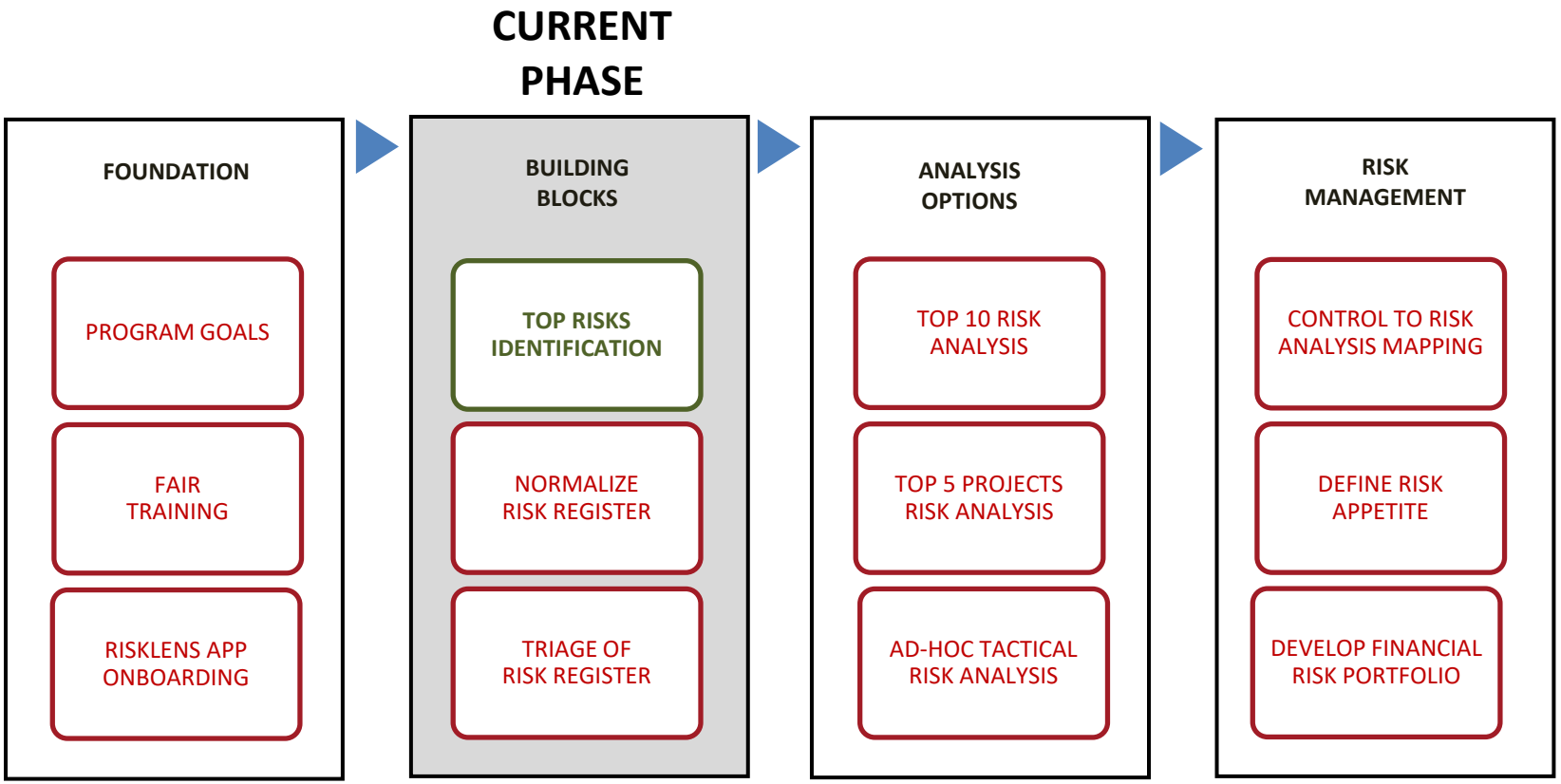
Appendix

- Things we will talk about if time permits

RISK MANAGEMENT ROADMAP

Taking a systematic approach to FAIR implementation

- Not a plug & play move to quantitative risk management
- Keeping the end goal in mind can get lost



Jones FAIR Risk Model

The fundamentals that make FAIR work

- **Loss**: How often and how large?