Governance, Risk, Compliance
context and strategy

navigating an uncertain world

(updated: 2022-04-22)

What and Why

- Governance: collection of capabilities driving principled performance
    - Example: requiring code reviews
    - Example: Forced 2 week vacations FDIC
- Compliance: externally imposed standards
    - UL listing for electrical appliances
    - PCI standard for card processing
    - FIPS 140-2 for crypto modules
    - Whether your workers are contractors or employees
- Risk: Market, Credit, Operational
    - Great introduction in the free and open source book *Financial Analytics Using R*

Defining Operational Risk

RISK = Loss Event Frequency x Loss Magnitude

- A measurable event
- No such thing as "a risk". Probability of losses associated with scenarios over a period of time.
- a **loss event** is a **threat** acting on an **asset** causing an **effect**
- Effects are CIA
  - Confidentiality (data breach)
  - Integrity (fraud)
  - Availability (theft, DOS, outage)
- Effects have a magnitude, or cost

KINDLY OPS

What are losses?

FAIR six forms of loss

- Primary or direct losses
  - Productivity (business interruption)
  - Replacement (capital assets)
  - Response (crisis management, forensic investigation)
- Secondary or indirect losses
  - Fines & Judgements
  - Reputation
  - Competitive Advantage

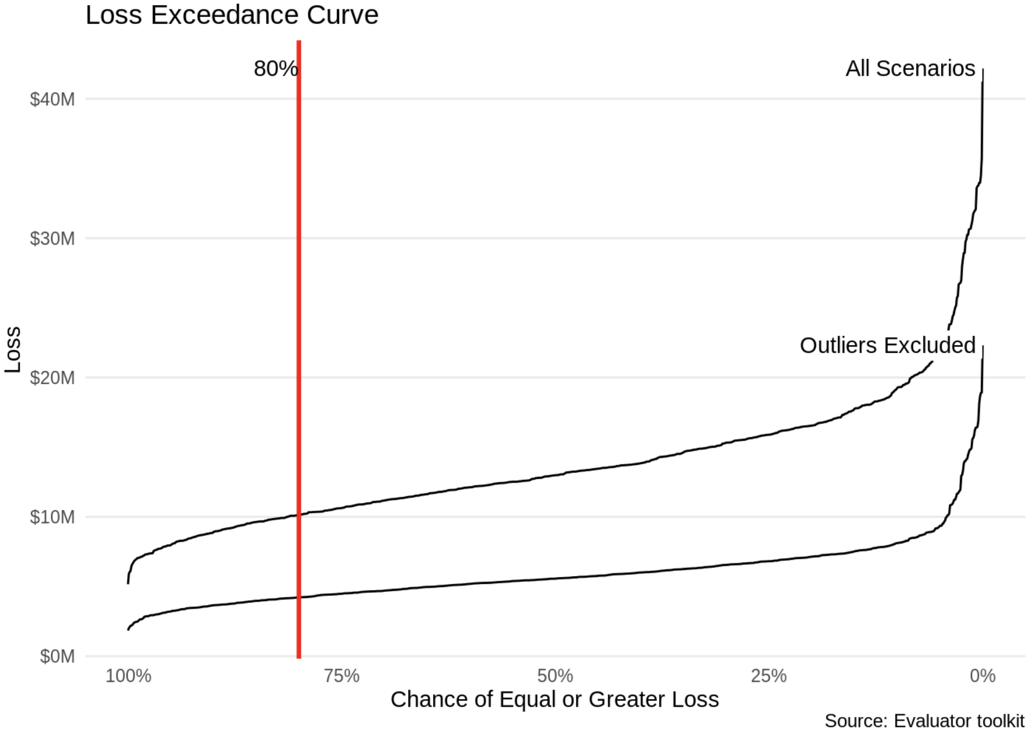
How to express the measurement?

Probability of loss for a scenario

- Probability of loss event
- Probability of magnitude
- Not a single point ordinal number!
- Example from TidyRisk Evaluator

Loss Exceedance Curve

The following loss exceedance curve is a common way to review the expected losses in a year. This figure shows how often total losses *exceed* any particular level during a given year. The 80% line shows that a loss of at least $4,223,248 occurs every four out of five years when outlier scenarios are excluded, or at least $10,142,053 when the outliers are included.



Loss Exceedance Curve

heatmaps - red flag for poor analysis

- cannot add risk scenarios together - how much risk if you add 2 red risks?
- range compression - just barely red vs very red
- doesn't allow for expression of uncertainty
- cannot calculate reduction in risk per dollar spent on security
- Use online tools to get a feel for building a model from range estimates
- Qualitative labels as summaries of ranges is fine

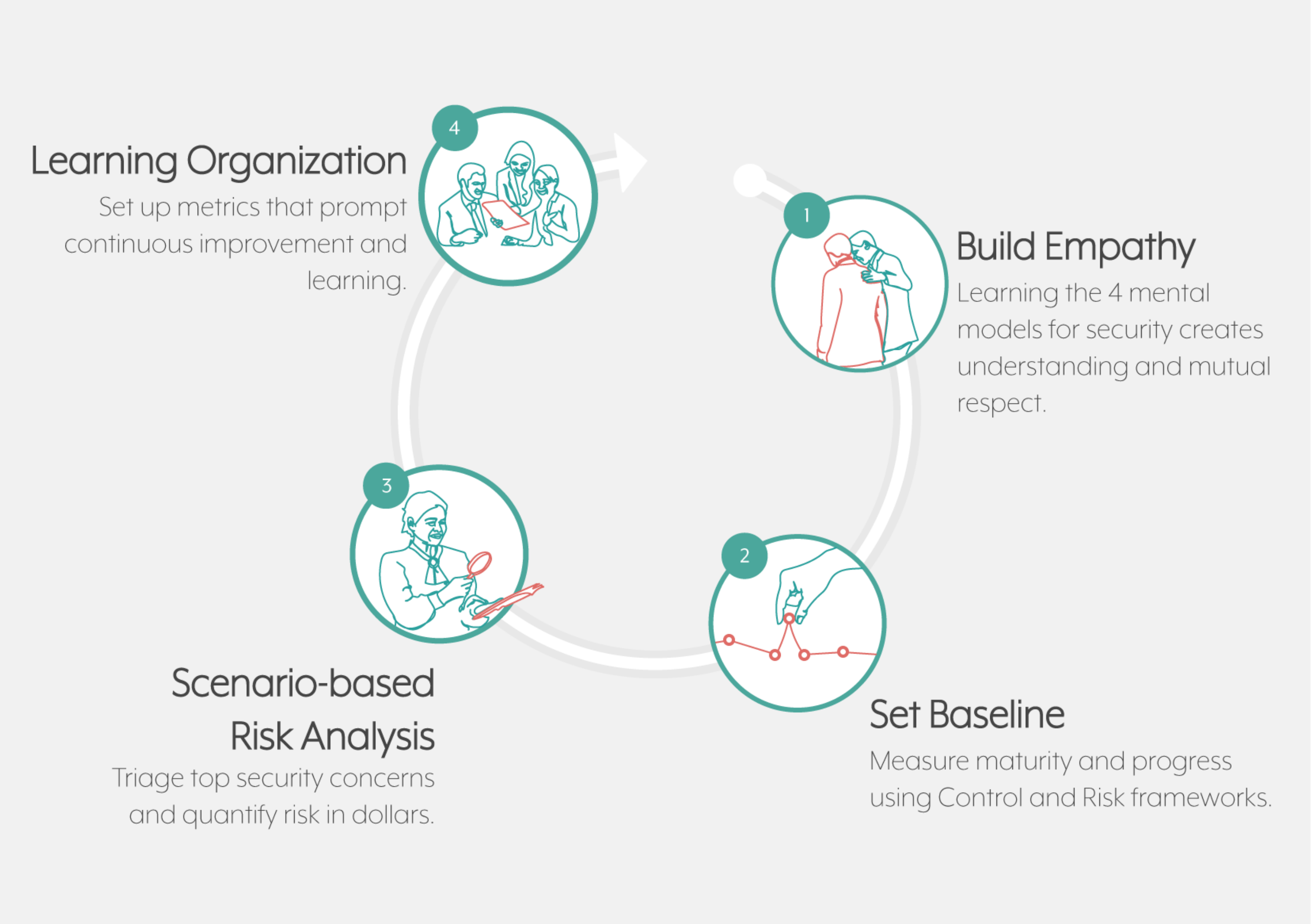
https://www.fairinstitute.org/blog/heat-maps-dont-support-iso-31000
https://www.researchgate.net/publication/266666768_The_Risk_of_Using_Risk_Matrices
https://medium.com/guesstimate-blog

"You can outsource your operations, but you cannot outsource your risk"

US Department of Homeland Security Cyber and Infrastructure Security Agency (CISA) Awareness Briefing on Chinese Cyber Attacks (slides)

STRATEGY

The Kindly Ops approach to GRC



Build Empathy

Learning the 4 mental models for security creates understanding and mutual respect.

Set Baseline

Measure maturity and progress using Control and Risk frameworks.

Scenario-based Risk Analysis

Triage top security concerns and quantify risk in dollars.

Learning Organization

Set up metrics that prompt continuous improvement and learning.

Mental Models and Organizational Learning

- Lance Hayden *People-Centric Security*
    - CC-licensed toolkits
- Security Culture Diagnostic Tool
    - Haven open source SCDS implementation
- Security FORCE metrics
    - Maturity models like CSF give an initial lift, not sustained improvement
    - are these metrics more governance or compliance?

KINDLY OPS

Baseline, top-down

NIST Cyber Security Framework (CSF)

KINDLY
OPS

Baseline - bottom up

CIS Top 20, AWS Foundations Benchmark

KINDLY OPS

baseline - breadth

AWS Well-Architected Framework

Security

Operational Excellence

Reliability

Performance Efficiency

Cost Optimization

FAIR (Factor Analysis Information Risk)

https://www.fairinstitute.org/

ASSESSING CURRENT STATE

- CSF Maturity Model assessment
- CIS Cloud foundations benchmark
- Security Culture Diagnostic

Emerging work

- FAIR Privacy
  - NIST work on quantitative privacy risk for individuals
- NIST further endorsement of FAIR September 2019
  - NIST mapping of FAIR to CSF

Questions?

KINDLY
OPS