SAND2018-4209C

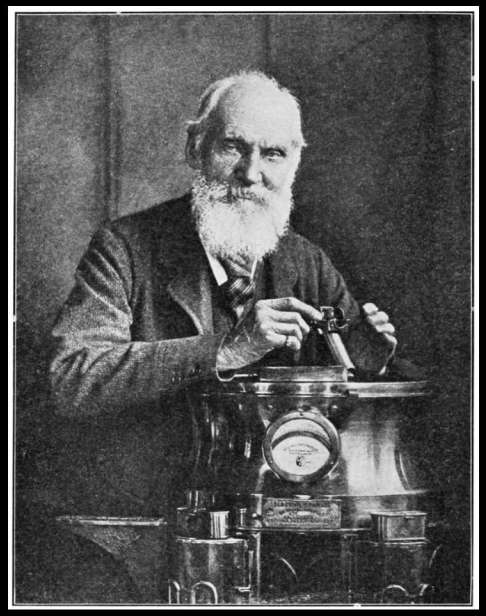
Math Is Hard: Compliance to Continuous Risk Management

Max Blumenthal
Senior Cyber Assurance Architect
Sandia National Laboratories

Christie Gross
Senior Cyber Assurance Architect
Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Lord Kelvin

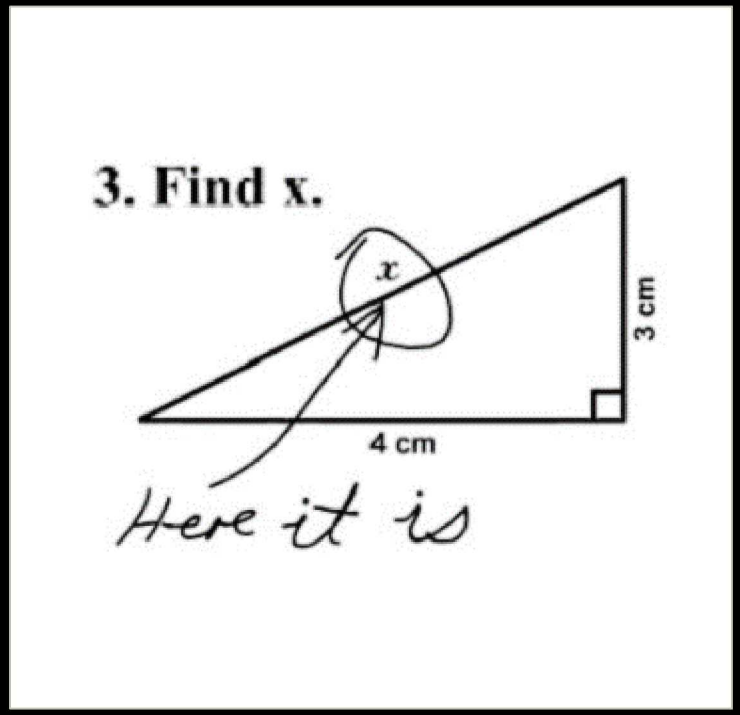


- “When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts advanced to the stage of science.”
- "I can state flatly that heavier than air flying machines are impossible."

Math Is Hard

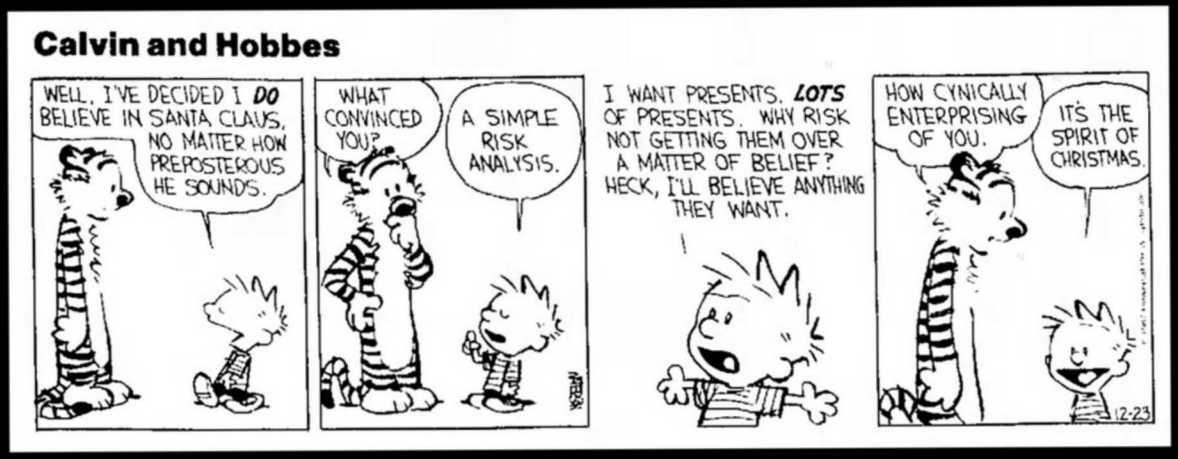
Agenda

- Risk Management Framework
- Continuous Monitoring
- Risk Assessment Methods
  - Qualitative
  - Semi-Quantitative
  - Quantitative
- Advanced Methods
- Quick Start Guide



Goals of Risk Management

- Most frameworks are moving towards a risk-based approach
- Customers increasingly want proven security maturity (competitive edge)
- Reduce waste, prioritize relevant security, and avoid fear mongering
- Make better, more efficient, and cost-effective decisions



Initial Steps to Ensure Buy-in

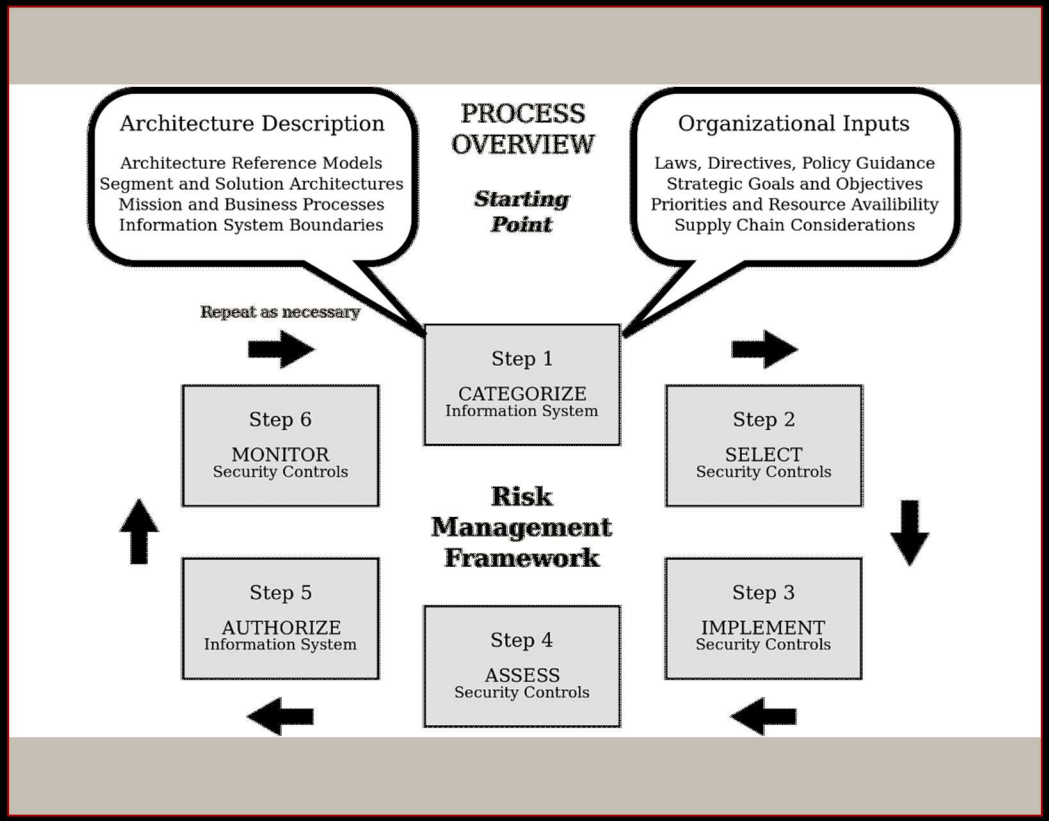
Sandia National Laboratories

- Identify Champions
- Tie to Business Goals/Objectives
- Have industry-relevant use cases ready
- Conduct a proof-of-concept

Selecting a Framework

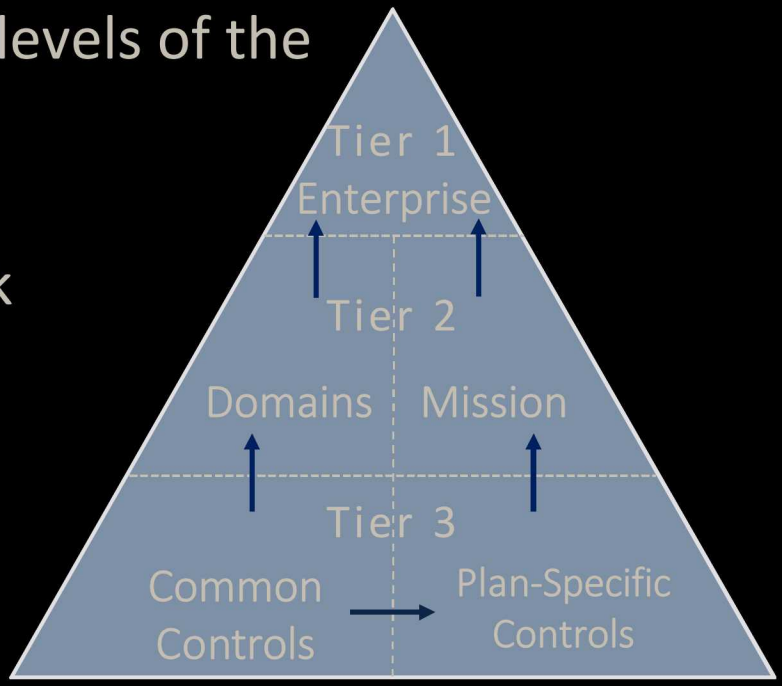
- Example Frameworks
- Need to meet compliance objectives
- For this we will use NIST

NIST Risk Management Framework

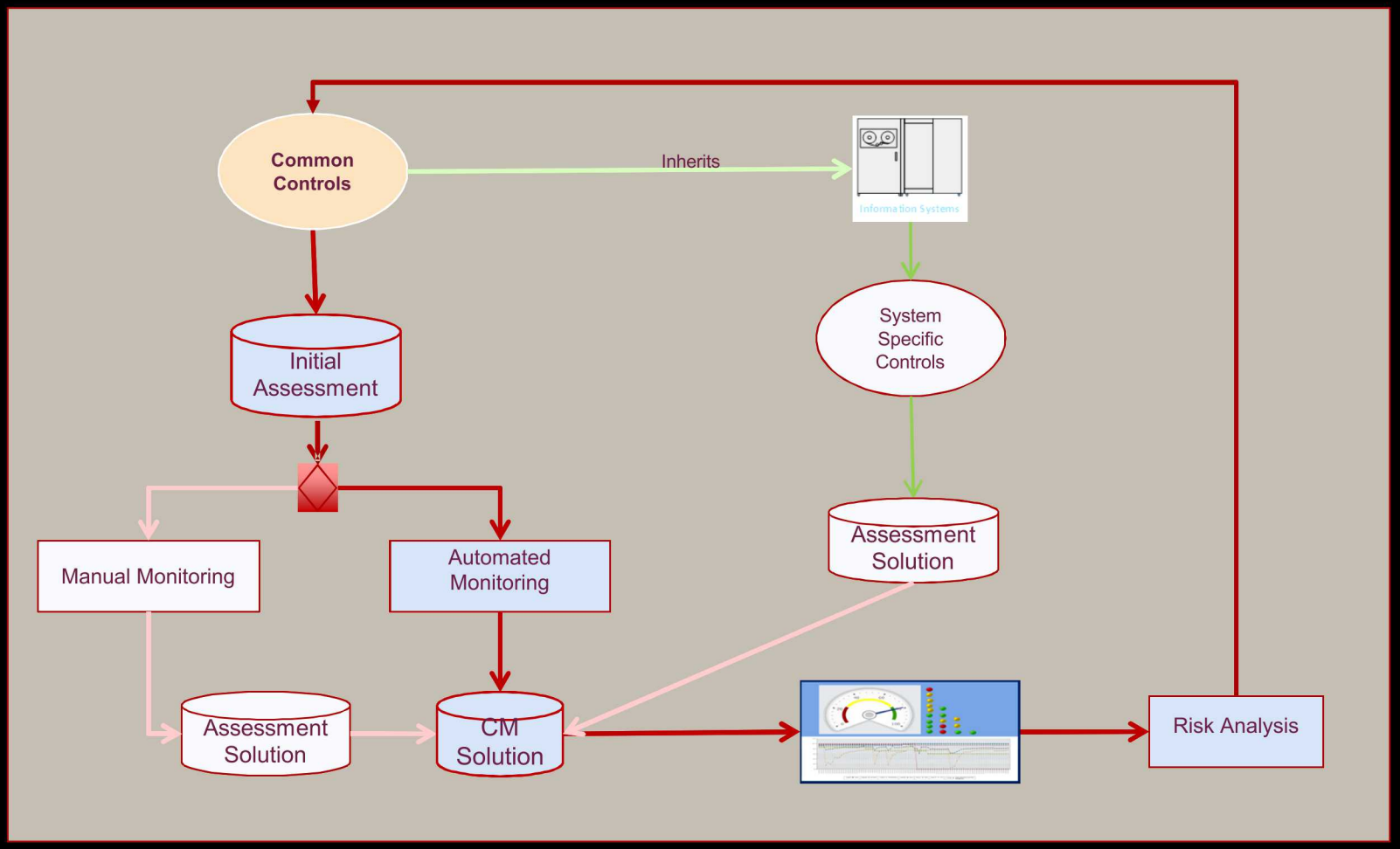


Continuous Monitoring

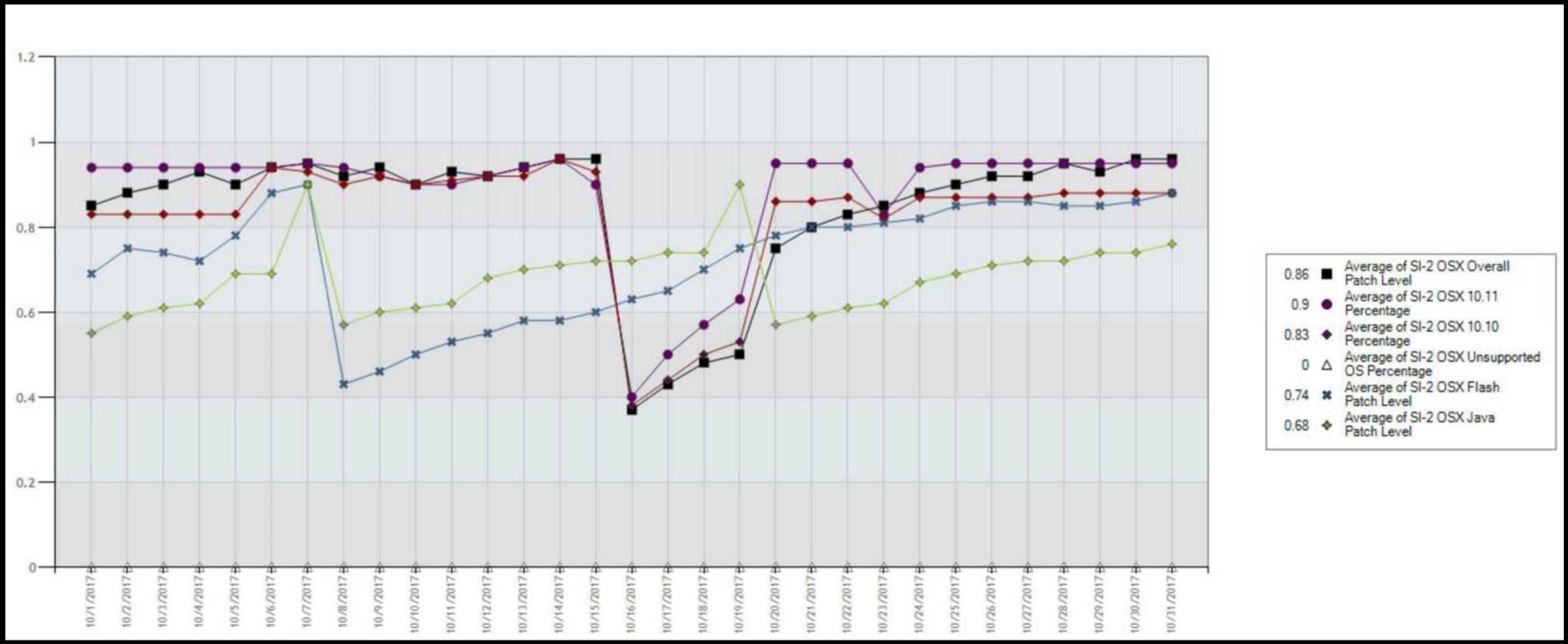
- Identify gaps through the assessment process and ongoing monitoring
- Determine continual effectiveness of controls
  - Automated and manual monitoring methods
- Monitoring frequency determination
- Evaluate security posture at different levels of the enterprise
  - Tier 3, Tier 2, Tier 1
- Feed effectiveness of controls into risk management and analysis



Continuous Monitoring Process



Continuous Monitoring Tier 3



Continuous Monitoring Tier 3

Sandia National Laboratories

Vulnerability and Patch Management Alert Table

Control Number ▲	Control Name	Measure	Criticality	Current State	Alert Level	Weighted	Ideal
CM-3	Configuration Change Control	Time to implement change	High	93.00		279.00	300
MA-2	Controlled Maintenance	Time to Resolve Unscheduled Maintenance	Low	97.00		97.00	100
RA-5	Vulnerability Scanning	% of scan population that is vulnerable	Very High	54.60		218.40	400
SI-2	Patch Management	% patched	High	39.80		119.40	300
Total Vulnerability and Patch Management	Total Vulnerability and Patch Management			64.89		713.80	1,100

Continuous Monitoring Tier 2

Sandia National Laboratories

Domain Alert Table

Domain ▲	Percentage	Alert Level	Weighted	Ideal
Vulnerability and Patch Management	61.22		673.44	1,100
Configuration Management	57.27		1,202.69	2,100
Asset Management	100.00		900	900
Event and Incident Management	94.23		1,036.51	1,100
Domain Total	73.32		3,812.64	5,200

Page 1 of 1 (5 records)

Continuous Monitoring Tier 1

Sandia National Laboratories

Enterprise Alert Table

Enterprise Entity ▲	Percentage	Alert Level	Weighted	Ideal
Mission Total	24.70	🔴	74.1	300
Domain Total	71.40	🟡	3,712.81	5,200
Enterprise Total	68.85	🟡	3,786.91	5,500

Page 1 of 1 (3 records)

Daily Enterprise Total

Enterprise Total

Daily Domain Total

Domain Total

Daily Mission Total

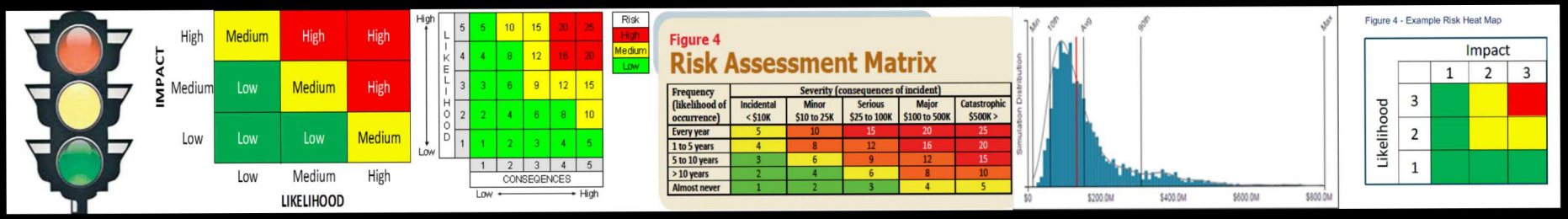
Mission Total

From Monitoring to Risk Quantification

Sandia National Laboratories

- Using Continuous Monitoring data, we can determine our risk exposure
- Once quantified, these risks can be prioritized
- Multiple methods of risk analysis
  - Qualitative, semi-quantitative, quantitative
  - Hybrid approaches can get more buy-in without a major culture shock
- Examples
  - Patching Risk

Evolution of Risk Analysis



IMPACT	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

LIKELIHOOD

LIKELIHOOD	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

CONSEQUENCES

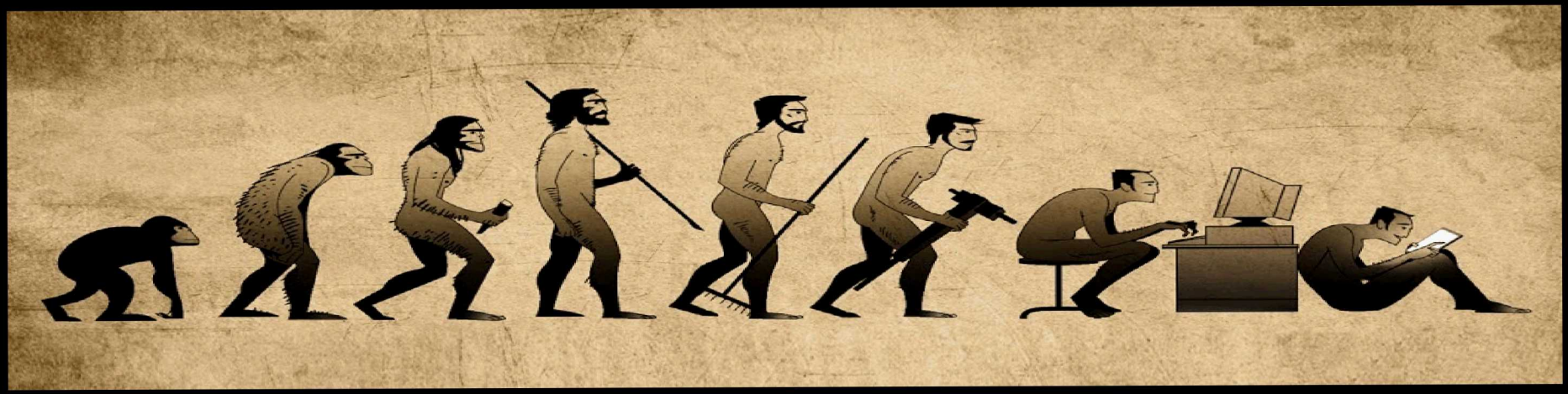
Risk: High, Medium, Low

Figure 4
Risk Assessment Matrix

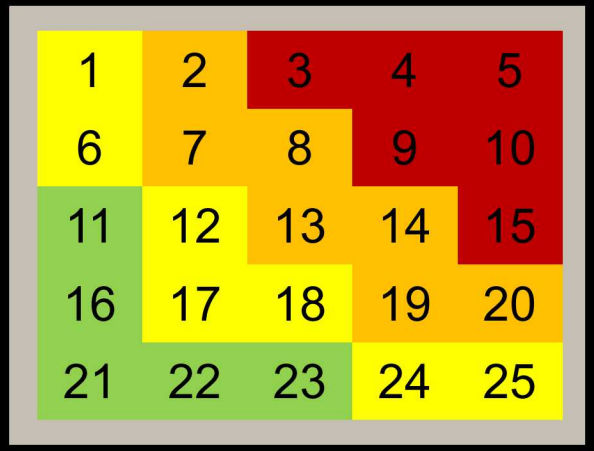
Frequency (likelihood of occurrence)	Severity (consequences of incident)				
	Incidental < $10K	Minor $10 to 25K	Serious $25 to 100K	Major $100 to 500K	Catastrophic $500K >
Every year	5	10	15	20	25
1 to 5 years	4	8	12	16	20
5 to 10 years	3	6	9	12	15
> 10 years	2	4	6	8	10
Almost never	1	2	3	4	5

Figure 4 - Example Risk Heat Map

Likelihood \ Impact	1	2	3
3			
2			
1			



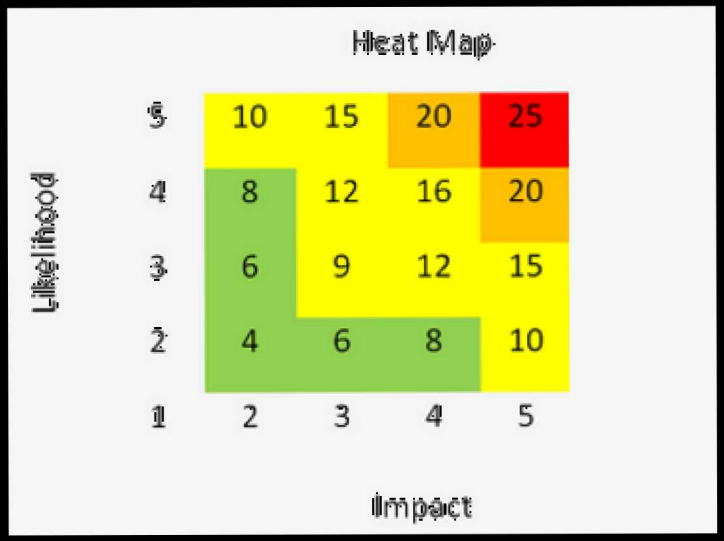
Risk Matrices: What Not to Do



Risk Matrix Goals

- Easily understood
- Defensible
- Actionable

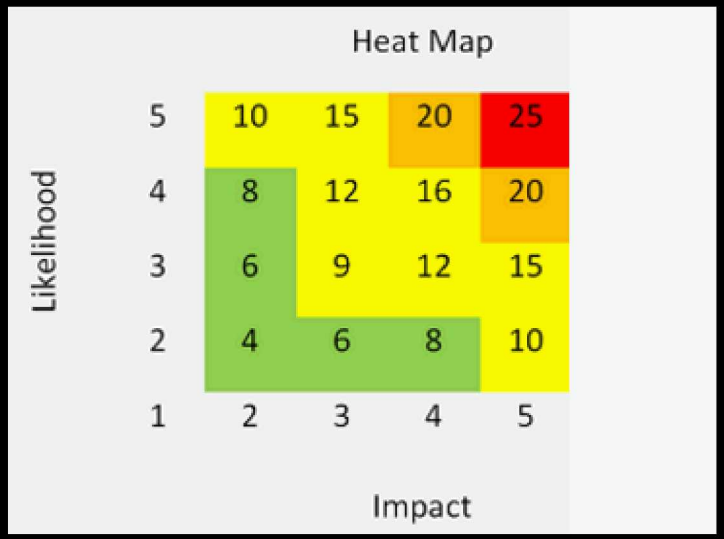
Mathematically-Sound Risk Matrix



Qualitative Risk

- No Definition for Each Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Subjective, but Simple

Mathematically-Sound Risk Matrix



Common Questions

- What does a 12 mean?
- What's the difference between an impact of 3 and an impact of 4?
- Do we prioritize likelihood or impact?

Semi-Quantitative Risk Matrix

$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00	$ 1,000,000,000.00
$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00
$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00
$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00
$ 0.10	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00

Semi-Quantitative Risk

- Definition for Each Risk Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection

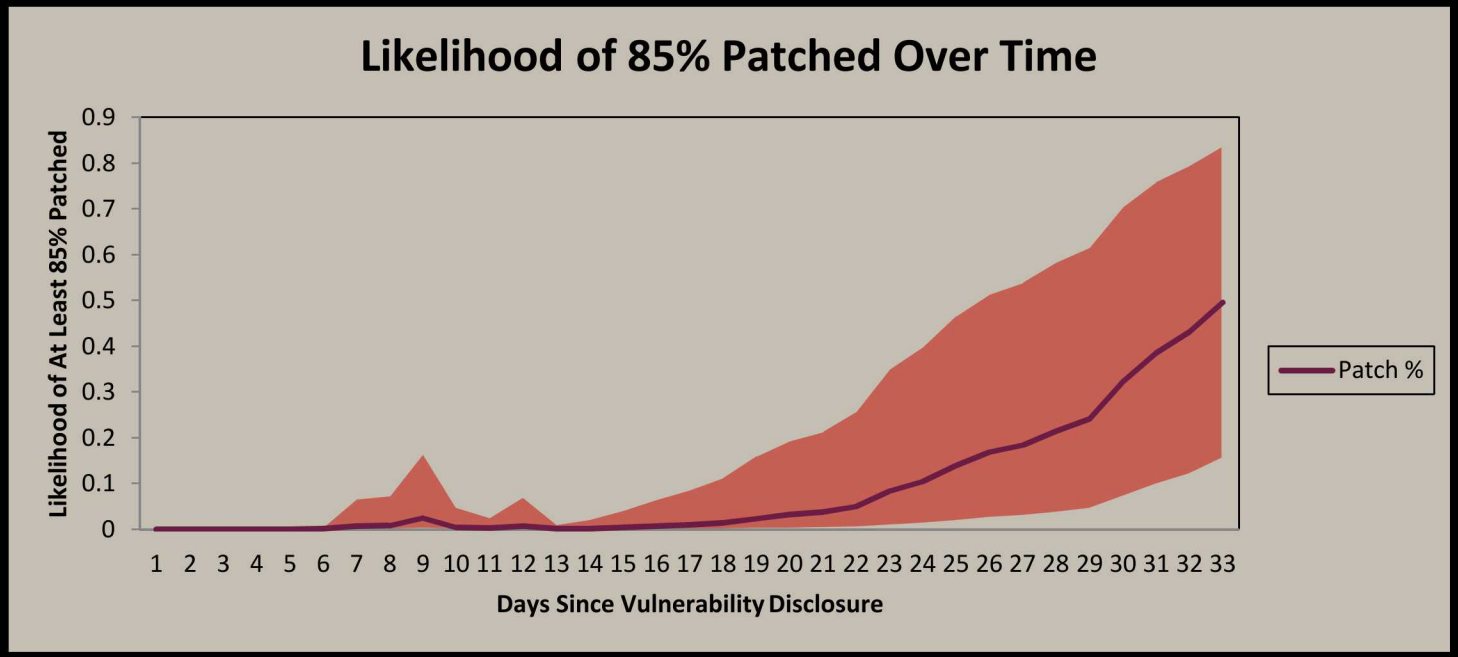
Semi-Quantitative Risk Matrix

$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00	$ 1,000,000,000.00
$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00
$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00
$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00
$ 0.10	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00

Common Questions

- How did you select values?
- What if I'm unsure about the likelihood or impact score?
- Do we prioritize by expected loss?

Patching Use Case



Quantitative Risk Method

Risk	LEF	TEF	Vulnerability	Tcap	RS	LM	Productivity Loss	Other Loss
$ 15,328.00	2.5	25	0.1	0.85	0.8	6131.2	$ 6,131.20	0

Sample	Risk		Average	$ 558,725.46
1	$ 15,328.00		standard	$ 1,565,137.07

	Productivity Loss	Other Loss	Avail Loss	Confidentiality Loss	Tcap	RS	TEF
Low	$ 2,295.54	Availability	$ 1,000.00	$ 2,745,500.00	85%	75%	15
Most Likely	$ 4,213.37	$ -	$ 9,600.00	$ 9,754,005.00	95%	80%	25
High	$ 6,131.20	Confidentiality	$ 10,000.00	$ 16,314,050.00	100%	85%	40

Quantitative Risk

- Incorporates Continuous Monitoring and Threat Information
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection
- Utilizes simulation to build a range of risk, given inherent uncertainties

Quantitative Risk Method

Risk	LEF	TEF	Vulnerability	Tcap	RS	LM	Productivity Loss	Other Loss
$ 15,328.00	2.5	25	0.1	0.85	0.8	6131.2	$ 6,131.20	0

Sample	Risk		Average	$ 558,725.46
1	$ 15,328.00		standard	$ 1,565,137.07

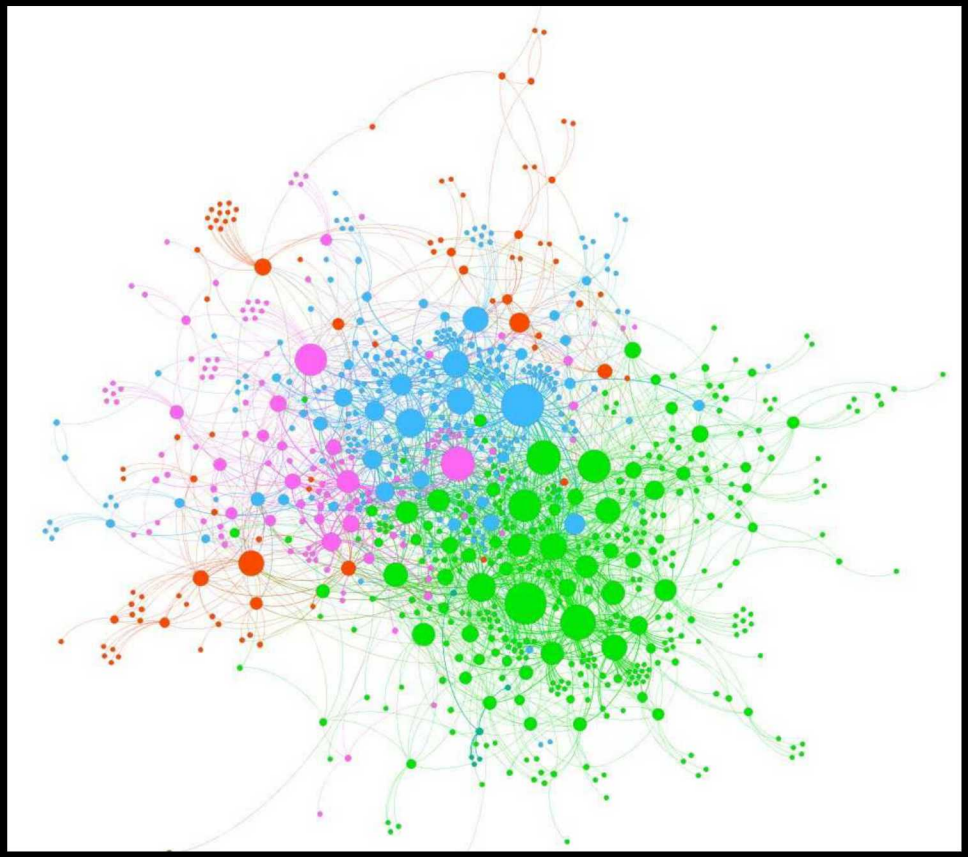
	Productivity Loss	Other Loss	Avail Loss	Confidentiality Loss	Tcap	RS	TEF
Low	$ 2,295.54	Availability	$ 1,000.00	$ 2,745,500.00	85%	75%	15
Most Likely	$ 4,213.37	$ -	$ 9,600.00	$ 9,754,005.00	95%	80%	25
High	$ 6,131.20	Confidentiality	$ 10,000.00	$ 16,314,050.00	100%	85%	40

Common Questions

- Why is there so much uncertainty?
- This seems overly complicated. Why would we not do something simple?
- Does this mean we have a “yellow” risk?
- That number seems off. How can I trust any of this?

Control Mapping for Gap Analysis

Sandia National Laboratories



Quick-start Guide to Risk Management

Sandia National Laboratories

- Take initial steps to foster buy-in with applicable use-cases and proof-of-concepts
- During implementation, map applicable policies to identify areas of focus and potential gaps
- Use manual and automated monitoring of individual policies to measure ongoing effectiveness at a granular level
- Create reports at multiple tiers to identify effectiveness at different levels of the enterprise
- Feed continuous monitoring data into risk analysis solutions
- Utilize quantitative risk to prioritize weaknesses and determine appropriate mitigations

Sandia National Laboratories

Questions