

## 10 Dimensions of Security Performance for Agility & Rapid Learning

SESSION ID: STR-W03A

**Russell C. Thomas**

Security Data Scientist  
Zions Bancorporation

@MrMeritology



# For multi-taskers

- ◆ This presentation: <http://bit.ly/1gsz8yY>
- ◆ Blog posts, slides, resources:  
<http://exploringpossibilityspace.blogspot.com>
- ◆ Tweet: #RSAC @MrMeritology

*Disclaimer: These views and ideas are personal. I do not represent my employer.*

# **RSA**CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

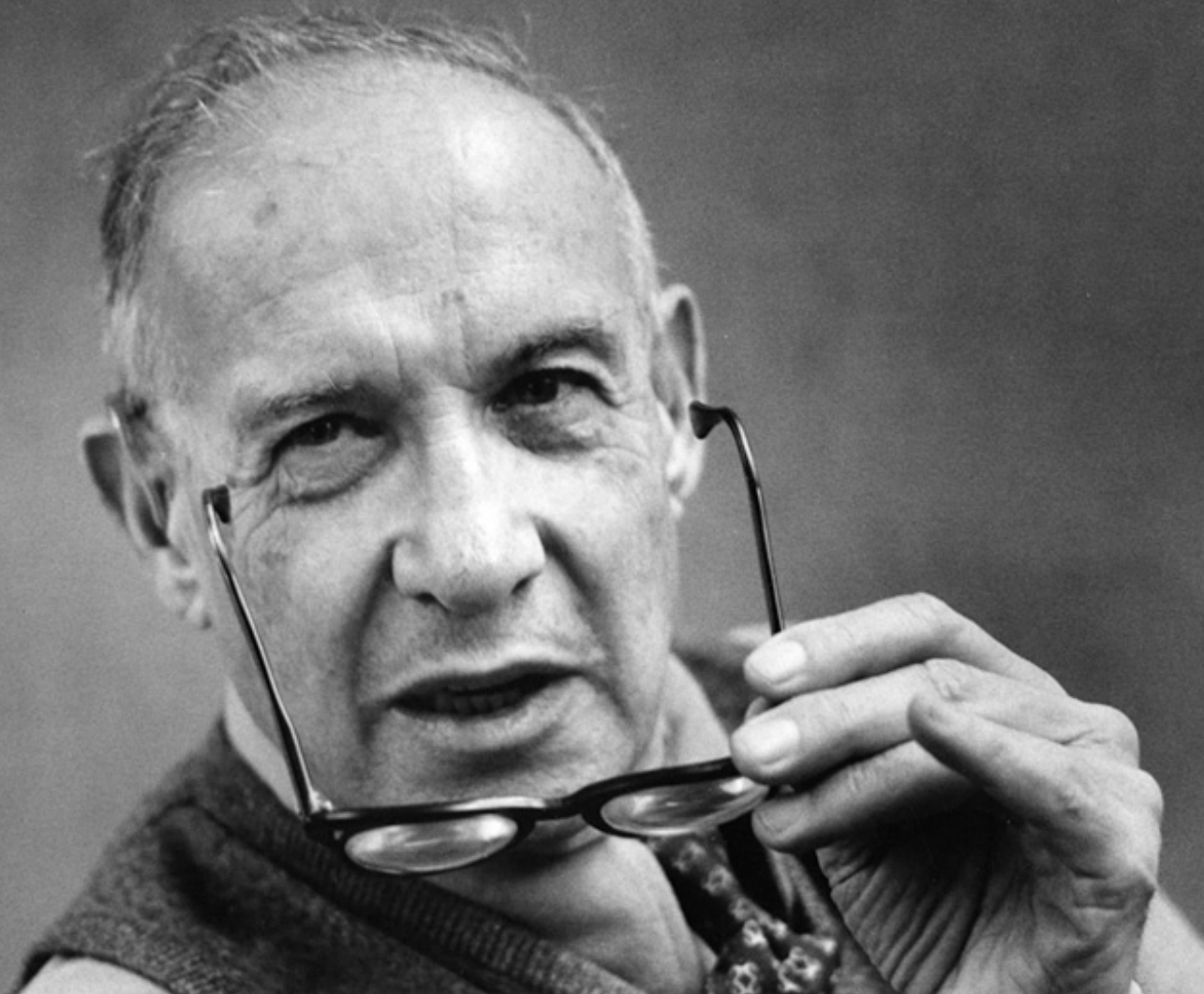


## **Audience Poll**

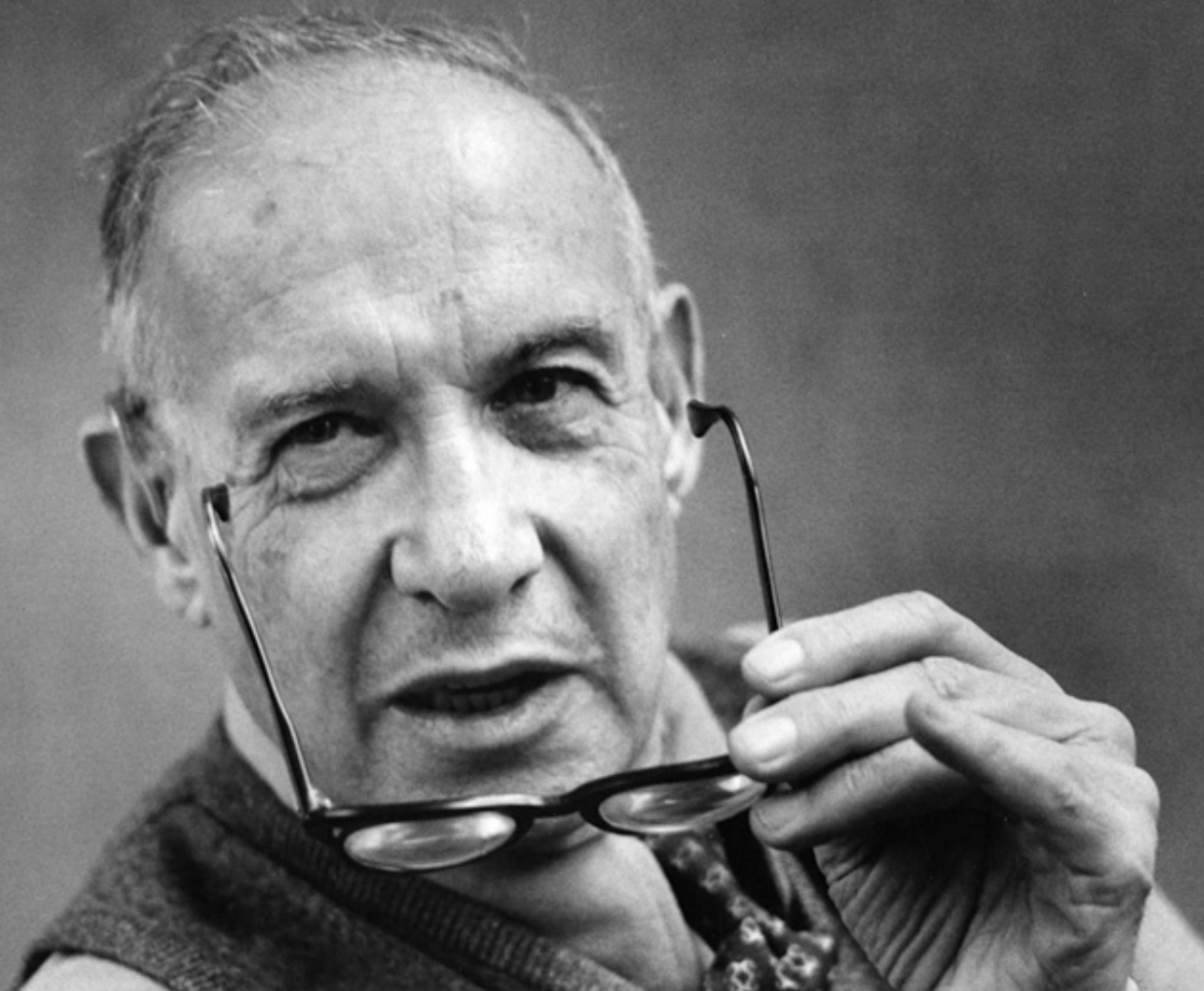
# Outline

- ◆ What is “performance”?
- ◆ Whirlwind tour of the Ten Dimensions framework
- ◆ How to aggregate many metrics into a performance score
- ◆ A short case: learning and agility in action

Who  
is  
this?



# Peter Drucker



 #RSAC

**RSACONFERENCE2014**

# Drucker on Performance

- ◆ Performance happens when effort is guided toward outcomes – i.e. **objectives**
- ◆ Setting good objectives requires **imaginative understanding**
- ◆ When facing **uncertainty**, focus on...
  - ◆ What you can control, do, or decide
  - ◆ How those decisions and actions **shape the future**

# “Cyber\* security performance” is...

- ◆ ...**systematic improvements**...
- ◆ ...in an organization's protection **capabilities** and **dynamic posture**...
- ◆ ...in the face of a rapidly-changing and uncertain **adversarial environment.**”

\* “Cyber security” is confluence of information security, privacy, digital rights, identity, IP protection, and information aspects of National & Homeland security

**RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



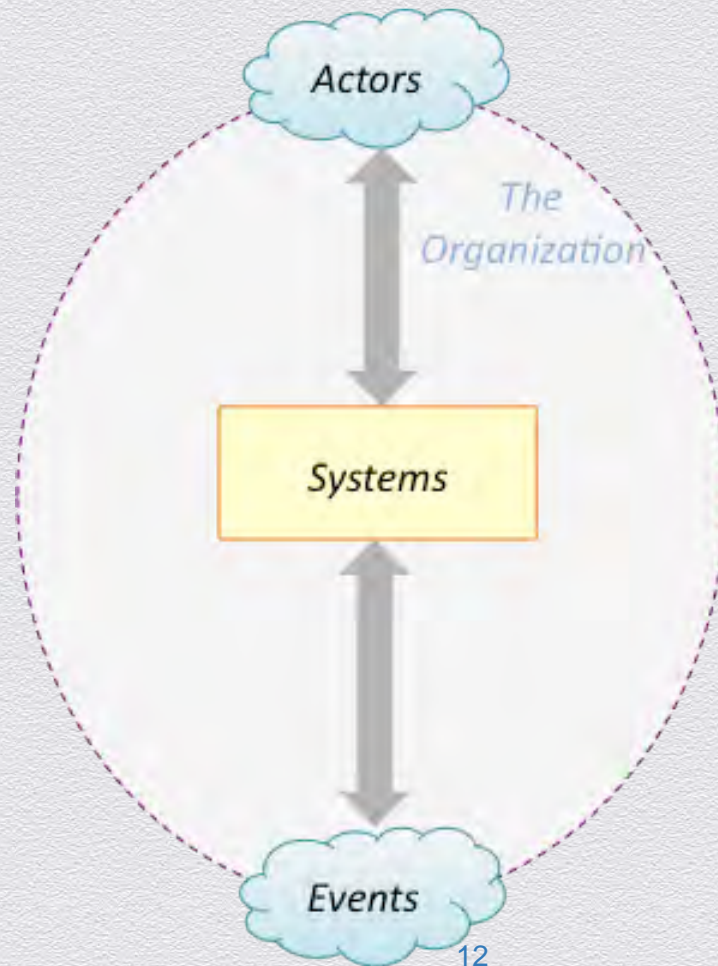
## Ten Dimensions in Three Minutes

# Managerial Value of a Framework

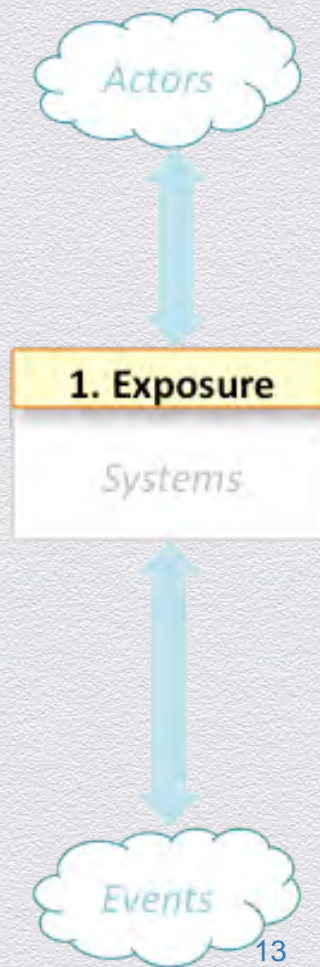
- ◆ To focus your attention on **neglected** areas and relationships
- ◆ Gives you a **roadmap**
  - ◆ You are “here”
  - ◆ Where do we want to be? When?

# Balanced Scorecard Approach

- ◆ Identify all the major **canonical** dimensions of performance
- ◆ Measure and report them separately, but in a way that allows comparisons – e.g. **performance indices**
- ◆ Given **context**, apply managerial judgment to **balance** investment and results

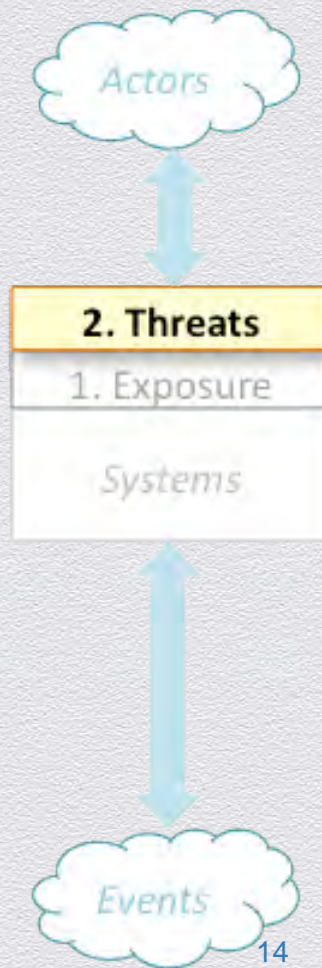


# 1. Optimize Exposure

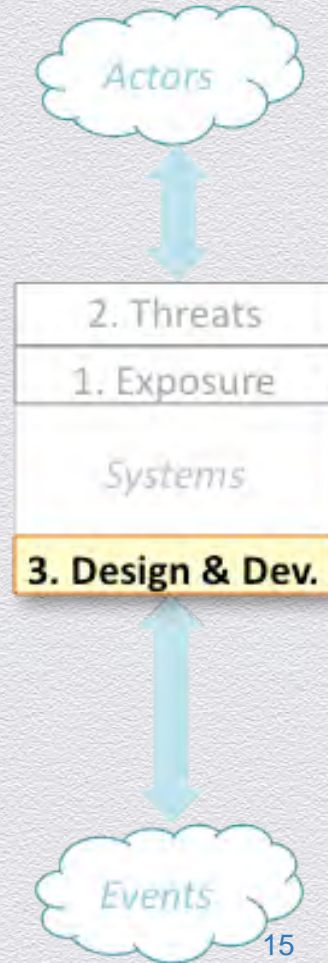


13

## 2. Effective Threat Intelligence

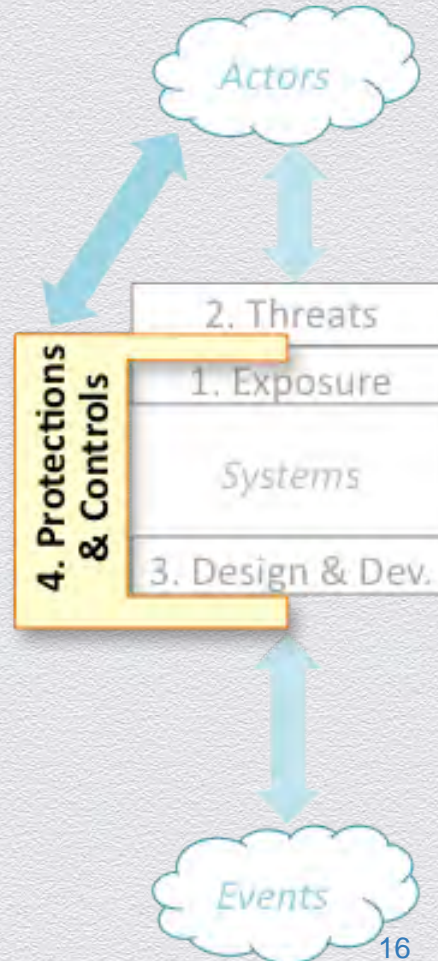


### 3. Effective Design & Development

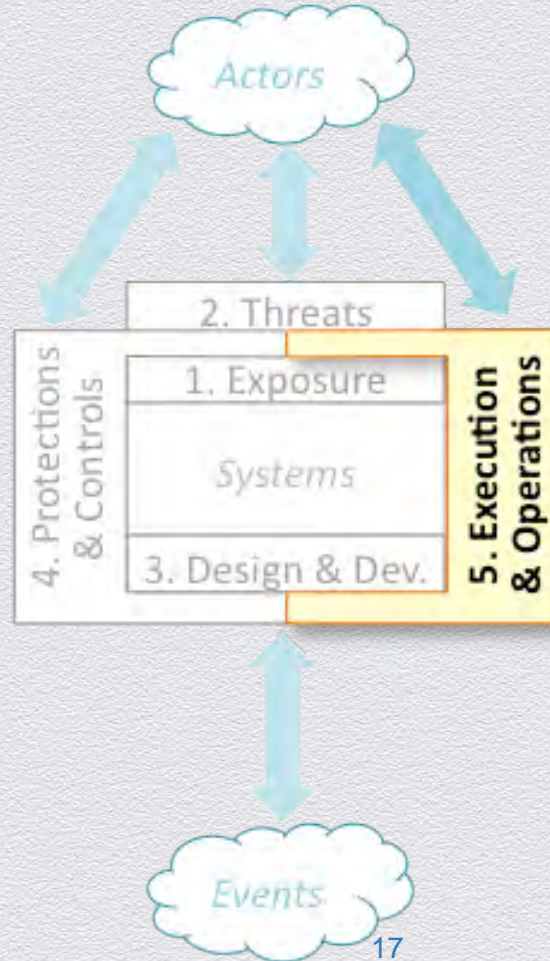


15

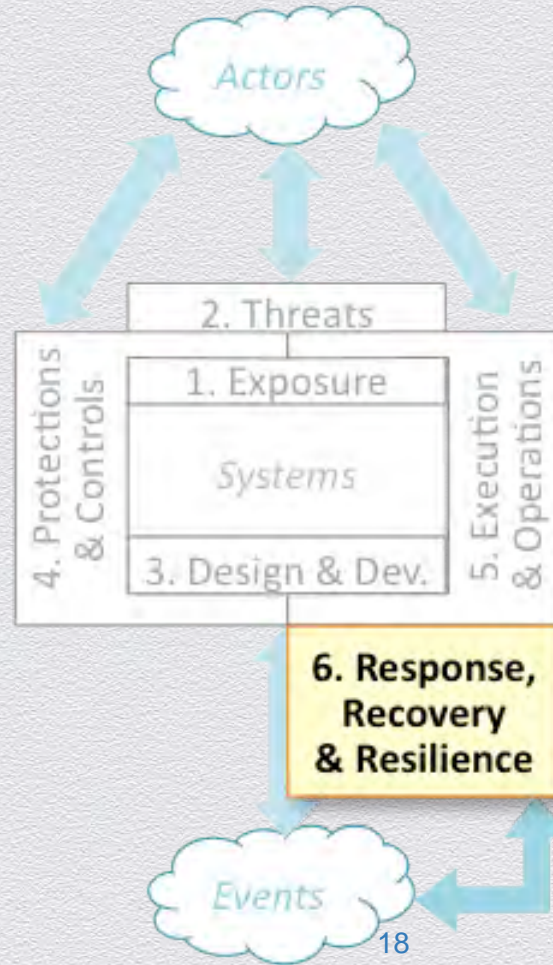
## 4. Quality of Protection & Controls



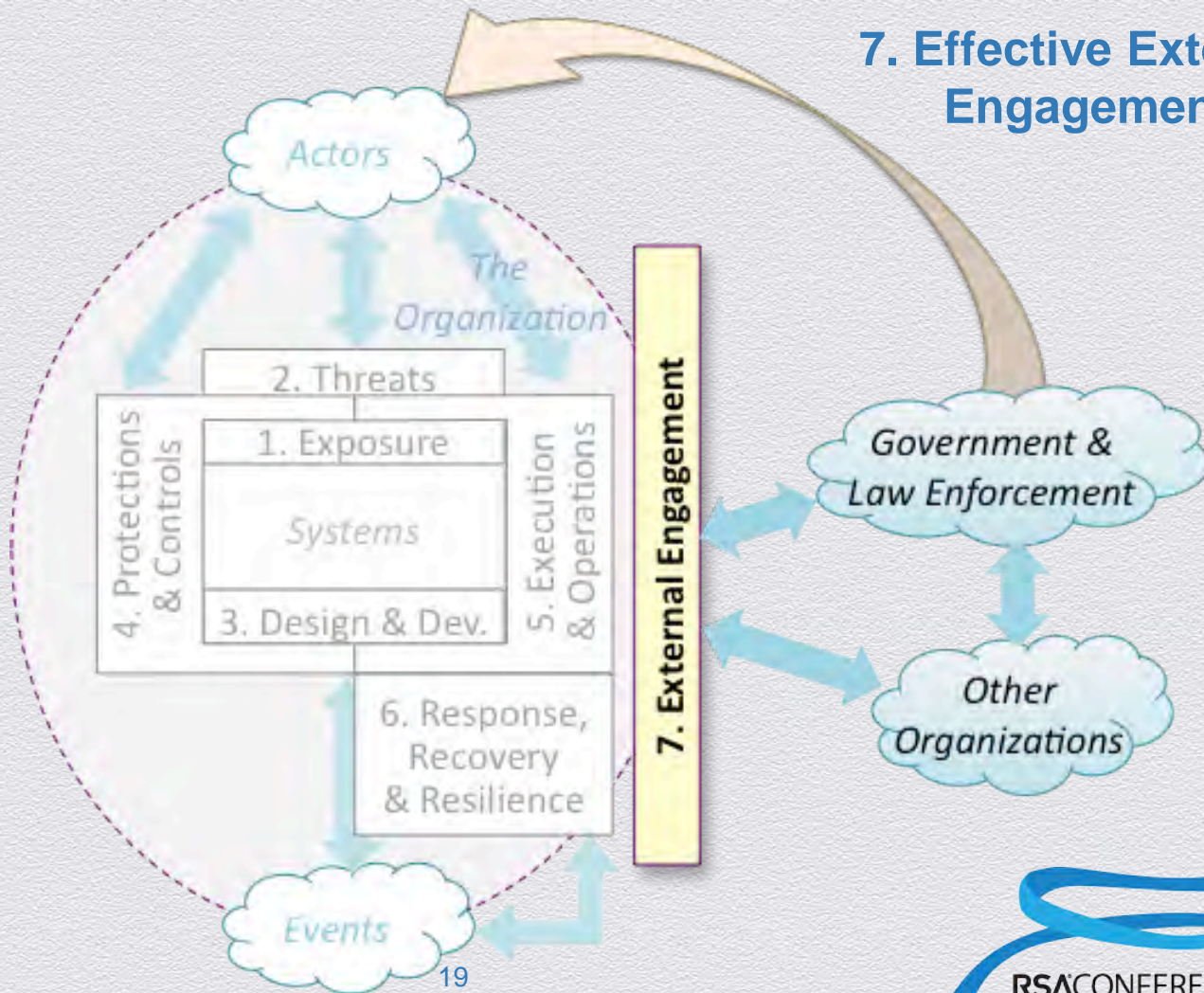
## 5. Effective & Efficient Execution & Operations



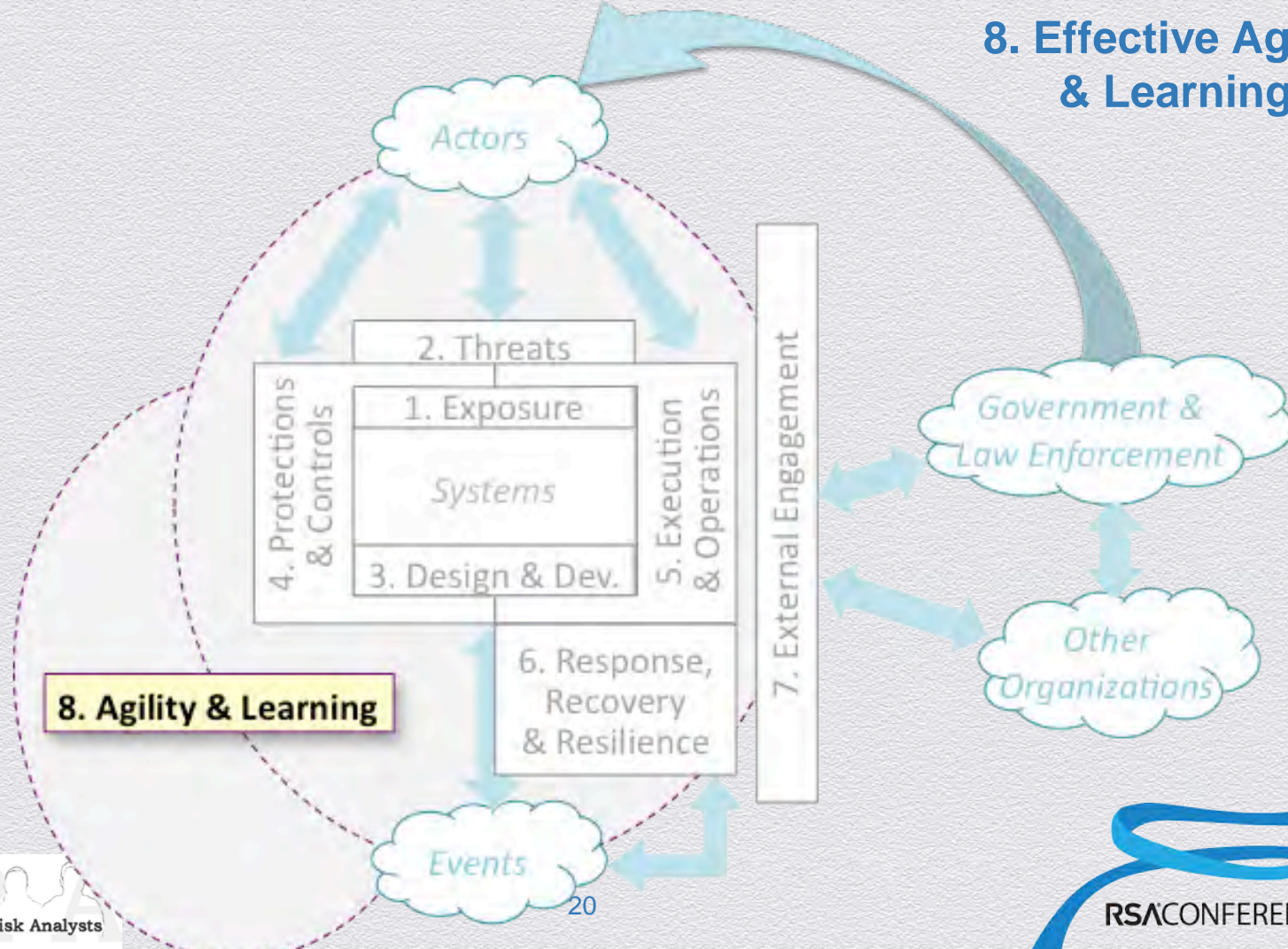
## 6. Effective Response, Recovery, & Resilience



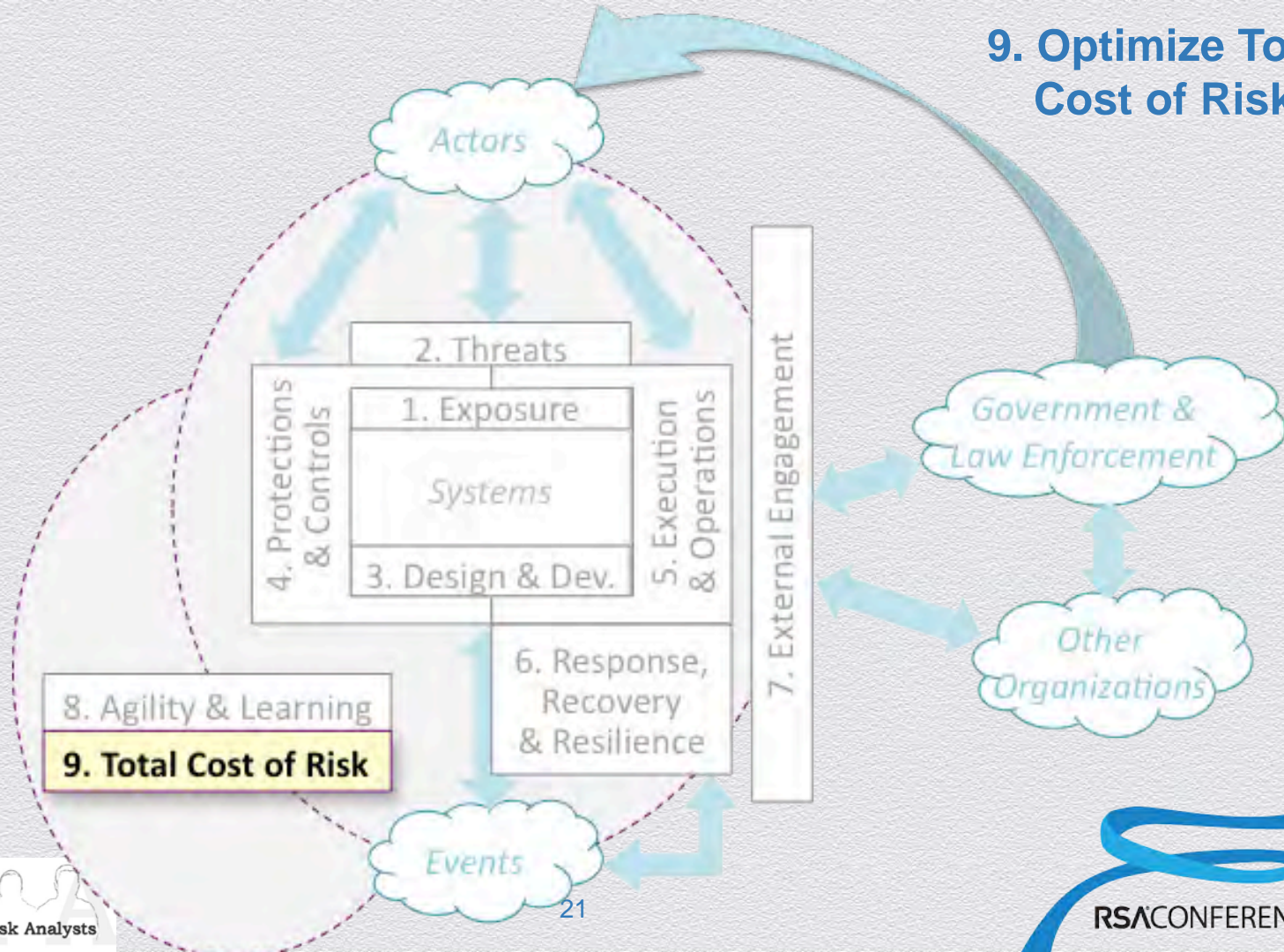
## 7. Effective External Engagement



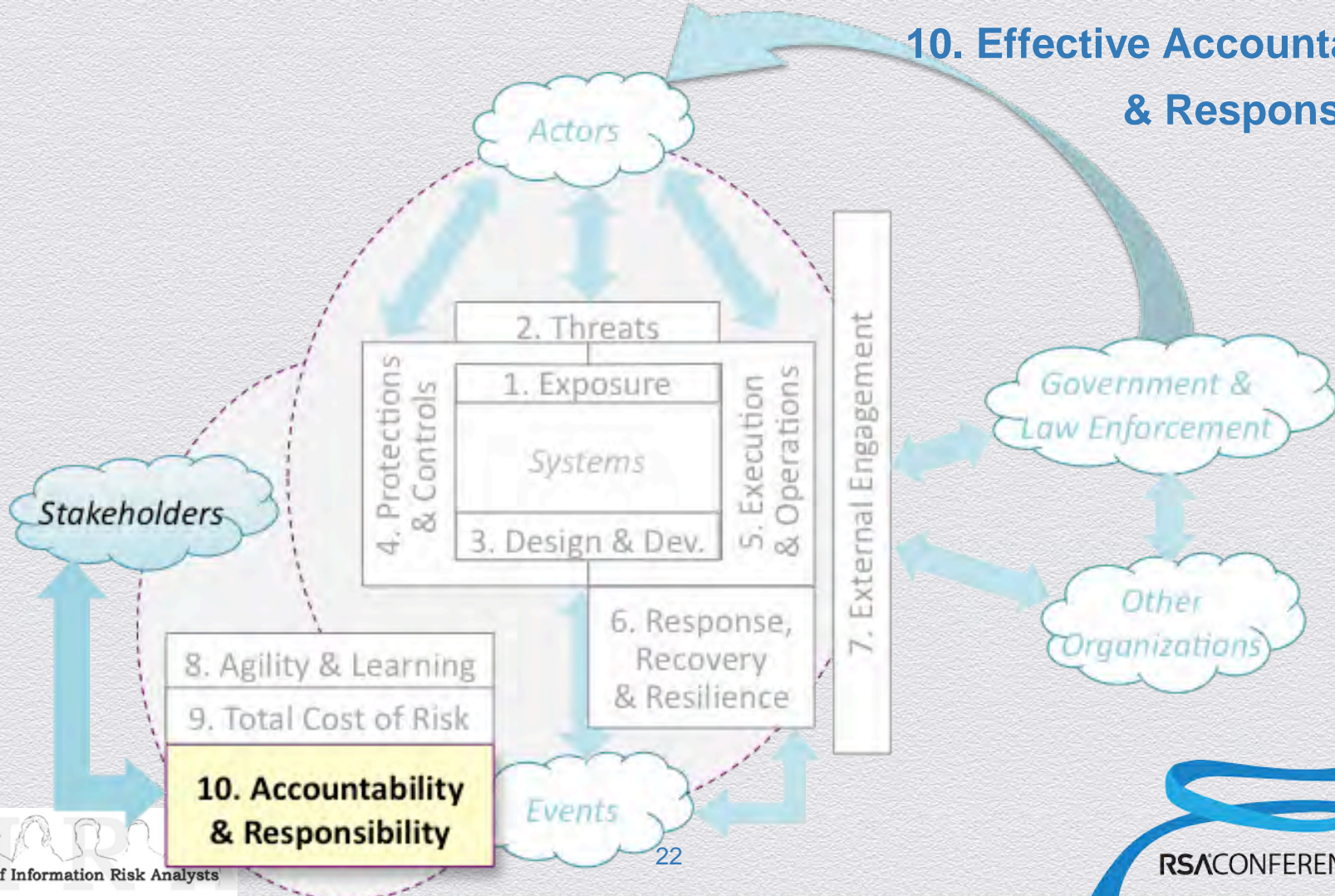
## 8. Effective Agility & Learning

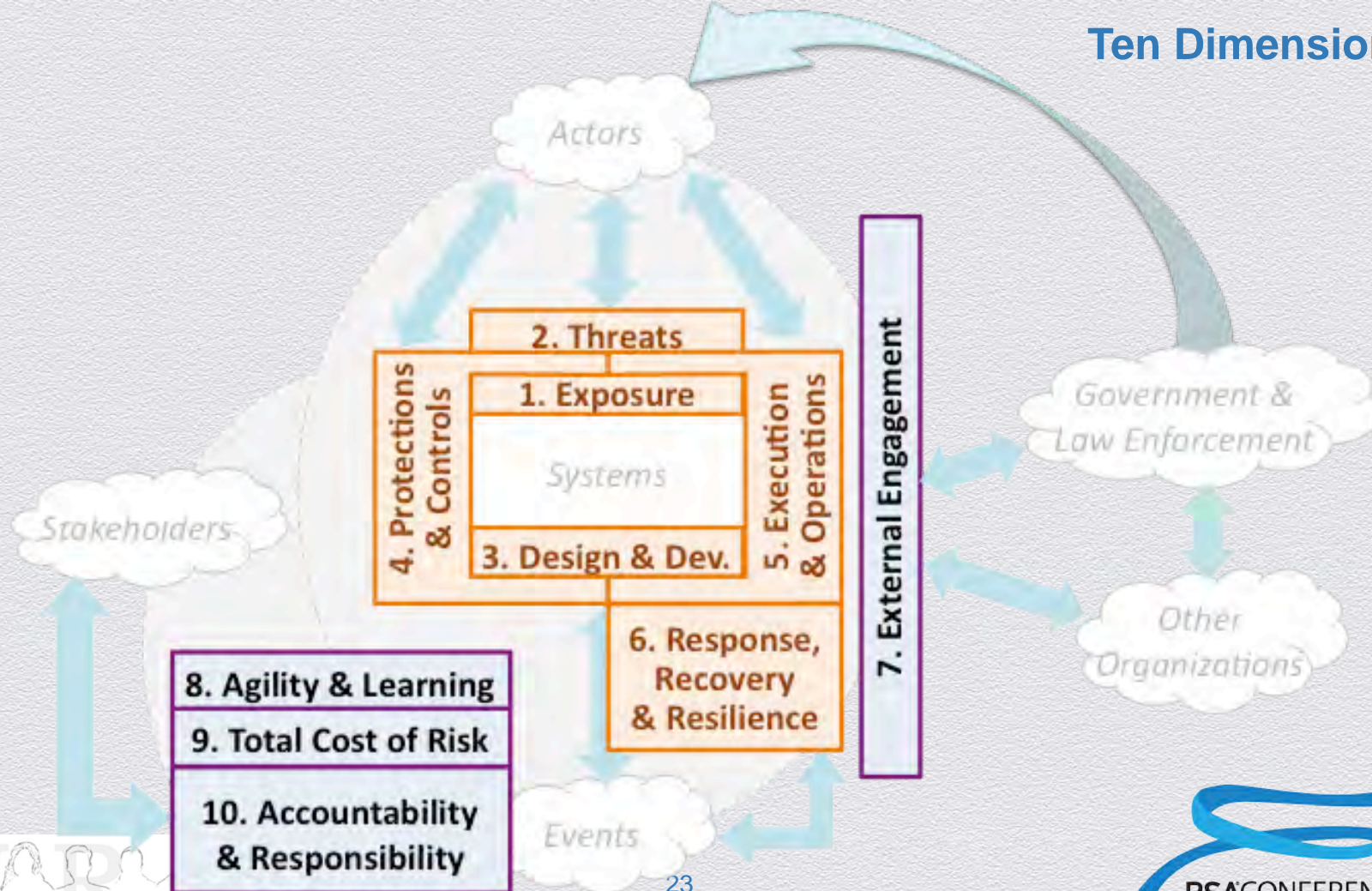


## 9. Optimize Total Cost of Risk



## 10. Effective Accountability & Responsibility

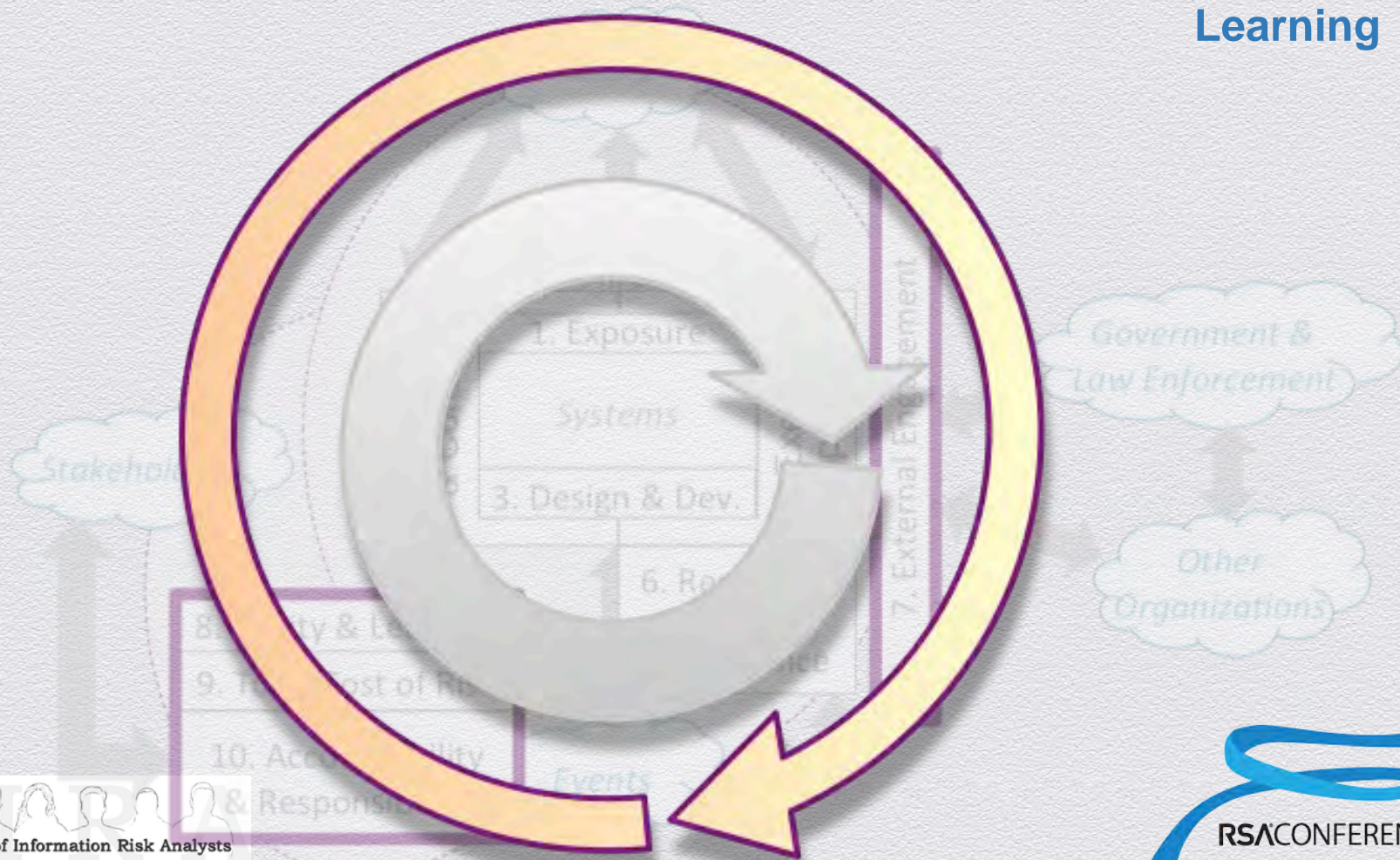




# Single Loop Learning



# Double Loop Learning



## Single Loop Learning



## Double Loop Learning





## **Aggregating metrics into a performance score**

# Usual method: Arithmetic

*A single formula for all score values*

## ◆ Score =

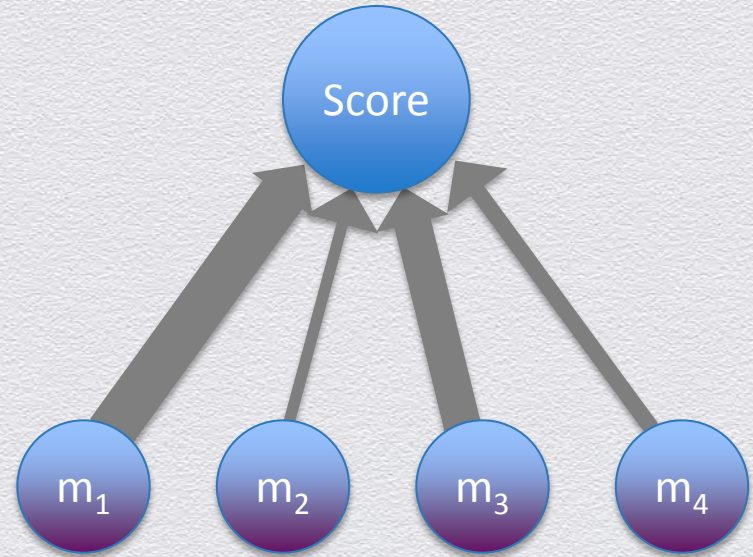
$\text{weight}_1 \times \text{metric}_1 +$

$\text{weight}_2 \times \text{metric}_2 +$

$\text{weight}_3 \times \text{metric}_3 +$

$\text{weight}_4 \times \text{metric}_4 +$

...

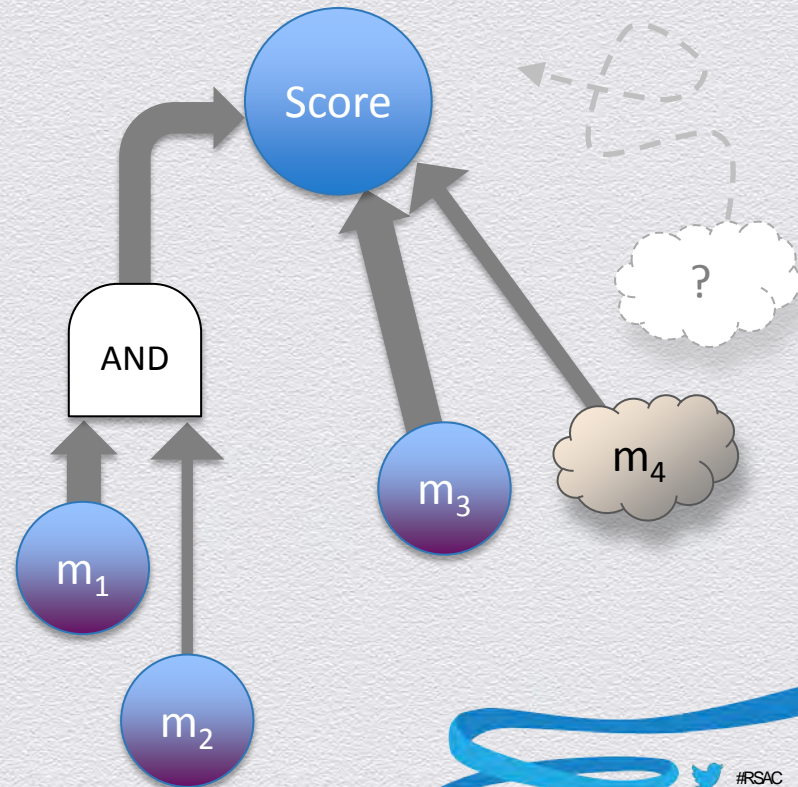


# But what about this?

#	Metrics	Value		Range		
1	Pass audit?	yes		yes or no	<b>Score values</b>	
2	Number of open critical vulns	0		>= 0		<b>1</b>
3	% of servers w/ up-to-date patches	100	%	0 to 100		<b>2</b>
4	% staff with InfoSec certifications	100	%	0 to 100		<b>3</b>
5	avg # years of InfoSec experience	15	yrs.	>= 0		<b>4</b>
						<b>5</b>

# Simple Arithmetic Can't Handle Messiness

- ◆ Non-linearity
- ◆ Contextual relevance & dependence
- ◆ Vagueness
- ◆ Incommensurate
- ◆ Absence
- ◆ Learning that restructures what you know



# New Way: “Thomas Scoring System”

*A different Weight of Evidence formula for EACH score value*

- ◆ Every score has a range of  $N$  values:  $a_1 .. a_n$
- ◆ Number of metrics =  $K$  (which could expand or contract)
- ◆ Individual metric values are EVIDENCE that either support or don't support particular score values
- ◆ Weight of Evidence for the  $i^{\text{th}}$  Score Value,  $a_i$ :

$$W_{a_i} = \sum_{\text{metric} = 1}^K (\text{Logical Condition} \times \text{Relevance} \times \text{Significance})_{\text{metric}}$$

# This is your “Performance Hypothesis”

$$W_{a_i} = \sum_{\text{metric} = 1}^K (\text{Logical Condition} \times \text{Relevance} \times \text{Significance})_{\text{metric}}$$

- ◆ Subject to testing, experiments, critical evaluations, peer comparisons, etc.
- ◆ *Evolution of your “performance hypothesis” is direct evidence of your progress in learning what drives performance!*

# An Example

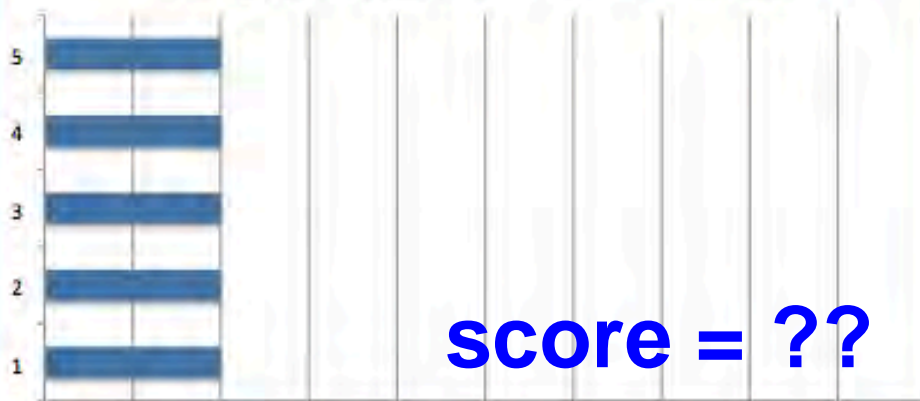
#	Metrics	Value		Range		
1	Pass audit?	yes		yes or no	<b>Score values</b>	
2	Number of open critical vulns	0		>= 0		<b>1</b>
3	% of servers w/ up-to-date patches	100	%	0 to 100		<b>2</b>
4	% staff with InfoSec certifications	100	%	0 to 100		<b>3</b>
5	avg # years of InfoSec experience	15	yrs.	>= 0		<b>4</b>
						<b>5</b>

# No Metrics... No Clarity

#	Metrics	Value	Range	Weight of					
1	Pass audit?		yes or no	Scores values	Evidence				
2	Number of open critical vulns		>= 0	1	0.20	Score with most weight	3		
3	% of servers w/ up-to-date patches	%	0 to 100	2	0.20	Weighted mean score	3.00		
4	% staff with InfoSec certifications	%	0 to 100	3	0.20	Clarity	0.00		←
5	avg # years of InfoSec experience	yrs.	>= 0	4	0.20	Ambiguity	0.00		←
				5	0.20	Most reasonable score	none		←
	Metric weights	even	weights	Sum	1.00				

#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	✓	TRUE
2	(1) audit = 'no'	✓	TRUE
3	(2) critical vulns <= 4	✓	TRUE
4	(2) critical vulns =5 to 10	✓	TRUE
5	(2) critical vulns > 10	✓	TRUE
6	(3) % servers up-to-date > 90%	✓	TRUE
7	(3) % servers up-to-date = 80% to 90%	✓	TRUE
8	(3) % servers up-to-date <= 80%	✓	TRUE
9	(4) % staff w/ InfoSec certs > 90%	✓	TRUE
10	(4) % staff w/ InfoSec certs = 50% to 90%	✓	TRUE
11	(4) % staff w/ InfoSec certs < 50%	✓	TRUE
12	(5) avg # years of InfoSec exp. > 10	✓	TRUE
13	(5) avg # years of InfoSec exp. = 5 to 10	✓	TRUE
14	(5) avg # years of InfoSec exp. <= 5	✓	TRUE

Weight of Evidence for Score Values

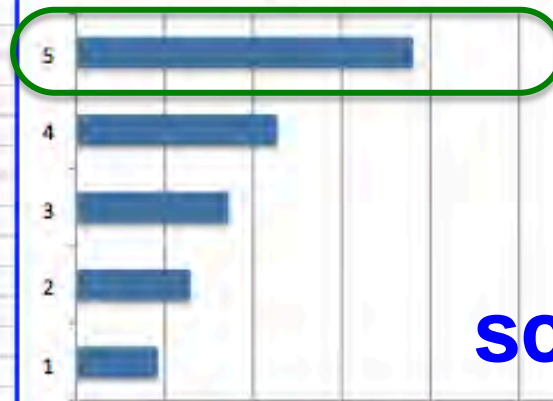


# Best Case... Clearly

#	Metrics	Value	Range	Weight of		
1	Pass audit?	yes	yes or no	Scores values	Evidence	
2	Number of open critical vulns	0	>= 0	1	0.09	Score with most weight 5
3	% of servers w/ up-to-date patches	100	0 to 100	2	0.13	Weighted mean score 3.67
4	% staff with InfoSec certifications	100	0 to 100	3	0.17	Clarity 0.34
5	avg # years of InfoSec experience	15	>= 0	4	0.23	Ambiguity 0.06
				5	0.38	Most reasonable score 4.14
	Metric weights	even	weights	Sum	1.00	

#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	TRUE	FALSE
2	(1) audit = 'no'	FALSE	FALSE
3	(2) critical vulns <= 4	TRUE	FALSE
4	(2) critical vulns =5 to 10	FALSE	FALSE
5	(2) critical vulns > 10	FALSE	FALSE
6	(3) % servers up-to-date > 90%	TRUE	FALSE
7	(3) % servers up-to-date = 80% to 90%	FALSE	FALSE
8	(3) % servers up-to-date <= 80%	FALSE	FALSE
9	(4) % staff w/ InfoSec certs > 90%	TRUE	FALSE
10	(4) % staff w/ InfoSec certs = 50% to 90%	FALSE	FALSE
11	(4) % staff w/ InfoSec certs < 50%	FALSE	FALSE
12	(5) avg # years of InfoSec exp. > 10	TRUE	FALSE
13	(5) avg # years of InfoSec exp. = 5 to 10	FALSE	FALSE
14	(5) avg # years of InfoSec exp. <= 5	FALSE	FALSE

Weight of Evidence for Score Values



score = 4.1

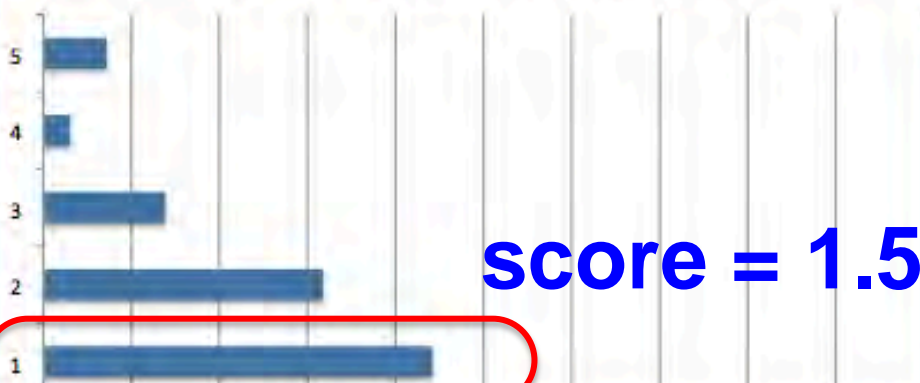
# Worst Case... Clearly

#	Metrics	Value	Range	Weight of	Evidence
1	Pass audit?	no	yes or no		
2	Number of open critical vulns	15	>= 0	1	0.44
3	% of servers w/ up-to-date patches	50	0 to 100	2	0.32
4	% staff with InfoSec certifications	40	0 to 100	3	0.14
5	avg # years of InfoSec experience	3	>= 0	4	0.03
				5	0.07
	Metric weights	user		Sum	1.00

Score with most weight	1
Weighted mean score	1.97
Clarity	0.53
Ambiguity	0.05
Most reasonable score	1.45

#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	FALSE	FALSE
2	(1) audit = 'no'	TRUE	FALSE
3	(2) critical vulns <= 4	FALSE	FALSE
4	(2) critical vulns =5 to 10	FALSE	FALSE
5	(2) critical vulns > 10	TRUE	FALSE
6	(3) % servers up-to-date > 90%	FALSE	FALSE
7	(3) % servers up-to-date = 80% to 90%	FALSE	FALSE
8	(3) % servers up-to-date <= 80%	TRUE	FALSE
9	(4) % staff w/ InfoSec certs > 90%	FALSE	FALSE
10	(4) % staff w/ InfoSec certs = 50% to 90%	FALSE	FALSE
11	(4) % staff w/ InfoSec certs < 50%	TRUE	FALSE
12	(5) avg # years of InfoSec exp. > 10	FALSE	FALSE
13	(5) avg # years of InfoSec exp.= 5 to 10	FALSE	FALSE
14	(5) avg # years of InfoSec exp. <= 5	TRUE	FALSE

Weight of Evidence for Score Values

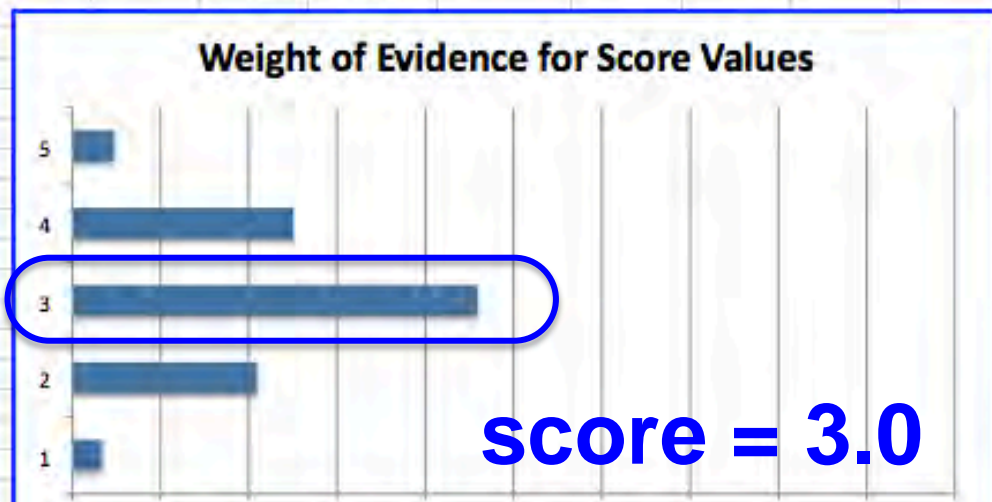


score = 1.5

# Typical Middle Case... Clearly

#	Metrics	Value	Range	Weight of					
1	Pass audit?	yes	yes or no	Scores values	Evidence				
2	Number of open critical vulns	5	>= 0	1	0.03	Score with most weight	3		
3	% of servers w/ up-to-date patches	85	0 to 100	2	0.21	Weighted mean score	3.07		
4	% staff with InfoSec certifications	70	0 to 100	3	0.46	Clarity	0.53		
5	avg # years of InfoSec experience	7	>= 0	4	0.25	Ambiguity	0.05		
				5	0.05	Most reasonable score	3.06		
	Metric weights	even	weights	Sum	1.00				

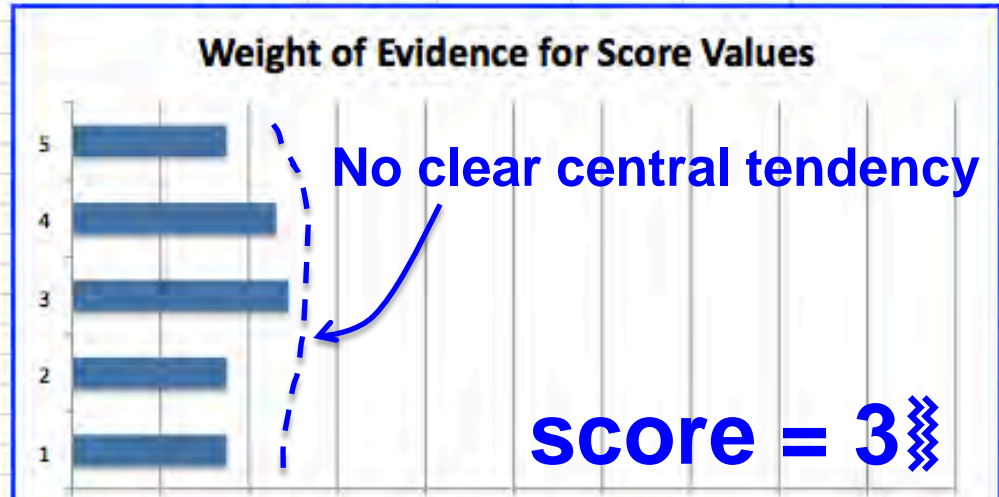
#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	TRUE	FALSE
2	(1) audit = 'no'	FALSE	FALSE
3	(2) critical vulns <= 4	FALSE	FALSE
4	(2) critical vulns = 5 to 10	TRUE	FALSE
5	(2) critical vulns > 10	FALSE	FALSE
6	(3) % servers up-to-date > 90%	FALSE	FALSE
7	(3) % servers up-to-date = 80% to 90%	TRUE	FALSE
8	(3) % servers up-to-date <= 80%	FALSE	FALSE
9	(4) % staff w/ InfoSec certs > 90%	FALSE	FALSE
10	(4) % staff w/ InfoSec certs = 50% to 90%	TRUE	FALSE
11	(4) % staff w/ InfoSec certs < 50%	FALSE	FALSE
12	(5) avg # years of InfoSec exp. > 10	FALSE	FALSE
13	(5) avg # years of InfoSec exp. = 5 to 10	TRUE	FALSE
14	(5) avg # years of InfoSec exp. <= 5	FALSE	FALSE



# Mixed Case... Muddy

#	Metrics	Value	Range	Weight of
1	Pass audit?	no	yes or no	Evidence
2	Number of open critical vulns	0	>= 0	1 0.17 Score with most weight 3
3	% of servers w/ up-to-date patches	85	0 to 100	2 0.17 Weighted mean score 3.06
4	% staff with InfoSec certifications	70	0 to 100	3 0.24 Clarity 0.10
5	avg # years of InfoSec experience	15	>= 0	4 0.23 Ambiguity 0.06
				5 0.17 Most reasonable score 3.08
	Metric weights	even	weights	Sum 1.00

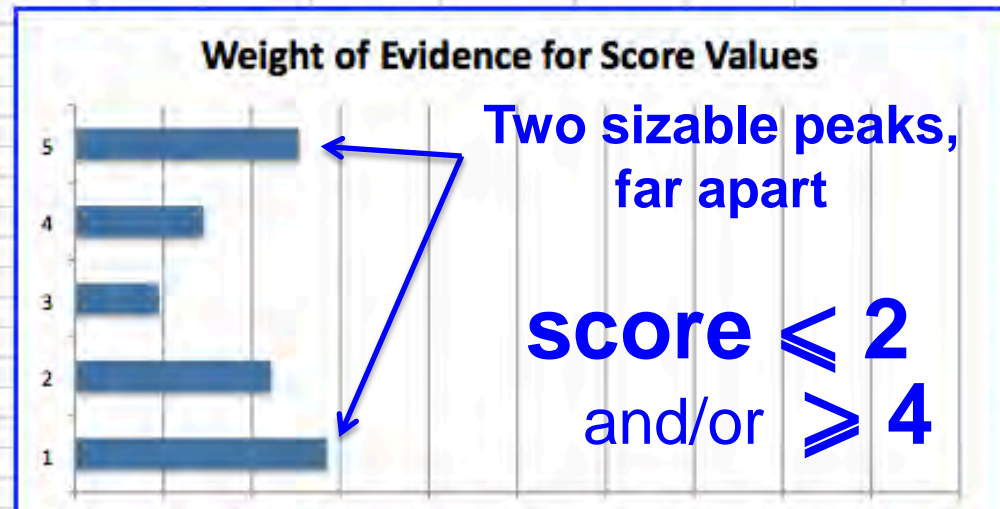
#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	FALSE	FALSE
2	(1) audit = 'no'	TRUE	FALSE
3	(2) critical vulns <= 4	TRUE	FALSE
4	(2) critical vulns = 5 to 10	FALSE	FALSE
5	(2) critical vulns > 10	FALSE	FALSE
6	(3) % servers up-to-date > 90%	FALSE	FALSE
7	(3) % servers up-to-date = 80% to 90%	TRUE	FALSE
8	(3) % servers up-to-date <= 80%	FALSE	FALSE
9	(4) % staff w/ InfoSec certs > 90%	FALSE	FALSE
10	(4) % staff w/ InfoSec certs = 50% to 90%	TRUE	FALSE
11	(4) % staff w/ InfoSec certs < 50%	FALSE	FALSE
12	(5) avg # years of InfoSec exp. > 10	TRUE	FALSE
13	(5) avg # years of InfoSec exp. = 5 to 10	FALSE	FALSE
14	(5) avg # years of InfoSec exp. <= 5	FALSE	FALSE



# Conflicting Case... WTF?

#	Metrics	Value	Range	Weight of					
1	Pass audit?	no	yes or no	Scores values	Evidence				
2	Number of open critical vulns	0	>= 0	1	0.28	Score with most weight	1		
3	% of servers w/ up-to-date patches	100	0 to 100	2	0.22	Weighted mean score	2.86		
4	% staff with InfoSec certifications	0	0 to 100	3	0.09	Clarity	0.24		
5	avg # years of InfoSec experience	15	>= 0	4	0.15	Ambiguity	0.25		
				5	0.25	Most reasonable score	2.55		
	Metric weights	even	weights	Sum	1.00				

#	Metric Conditions	Evidence	Absent
1	(1) audit = 'yes'	FALSE	FALSE
2	(1) audit = 'no'	TRUE	FALSE
3	(2) critical vulns <= 4	TRUE	FALSE
4	(2) critical vulns = 5 to 10	FALSE	FALSE
5	(2) critical vulns > 10	FALSE	FALSE
6	(3) % servers up-to-date > 90%	TRUE	FALSE
7	(3) % servers up-to-date = 80% to 90%	FALSE	FALSE
8	(3) % servers up-to-date <= 80%	FALSE	FALSE
9	(4) % staff w/ InfoSec certs > 90%	FALSE	FALSE
10	(4) % staff w/ InfoSec certs = 50% to 90%	FALSE	FALSE
11	(4) % staff w/ InfoSec certs < 50%	TRUE	FALSE
12	(5) avg # years of InfoSec exp. > 10	TRUE	FALSE
13	(5) avg # years of InfoSec exp. = 5 to 10	FALSE	FALSE
14	(5) avg # years of InfoSec exp. <= 5	FALSE	FALSE



# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



## *Case Study:* “Shadow IT”

For operational efficiency, IT only manages "Approved" servers and services

"Shadow"

Local or contract Sys Admin executes custom patching process

??

Huh? exceptions?

Shadow servers + services "Black hole"

IT executes "official" patching process, governed by IT's operational goals

"Approved"

InfoSec updates "must patch" list per Policy & regs, vuln & threat intel.,

*rinse, repeat*

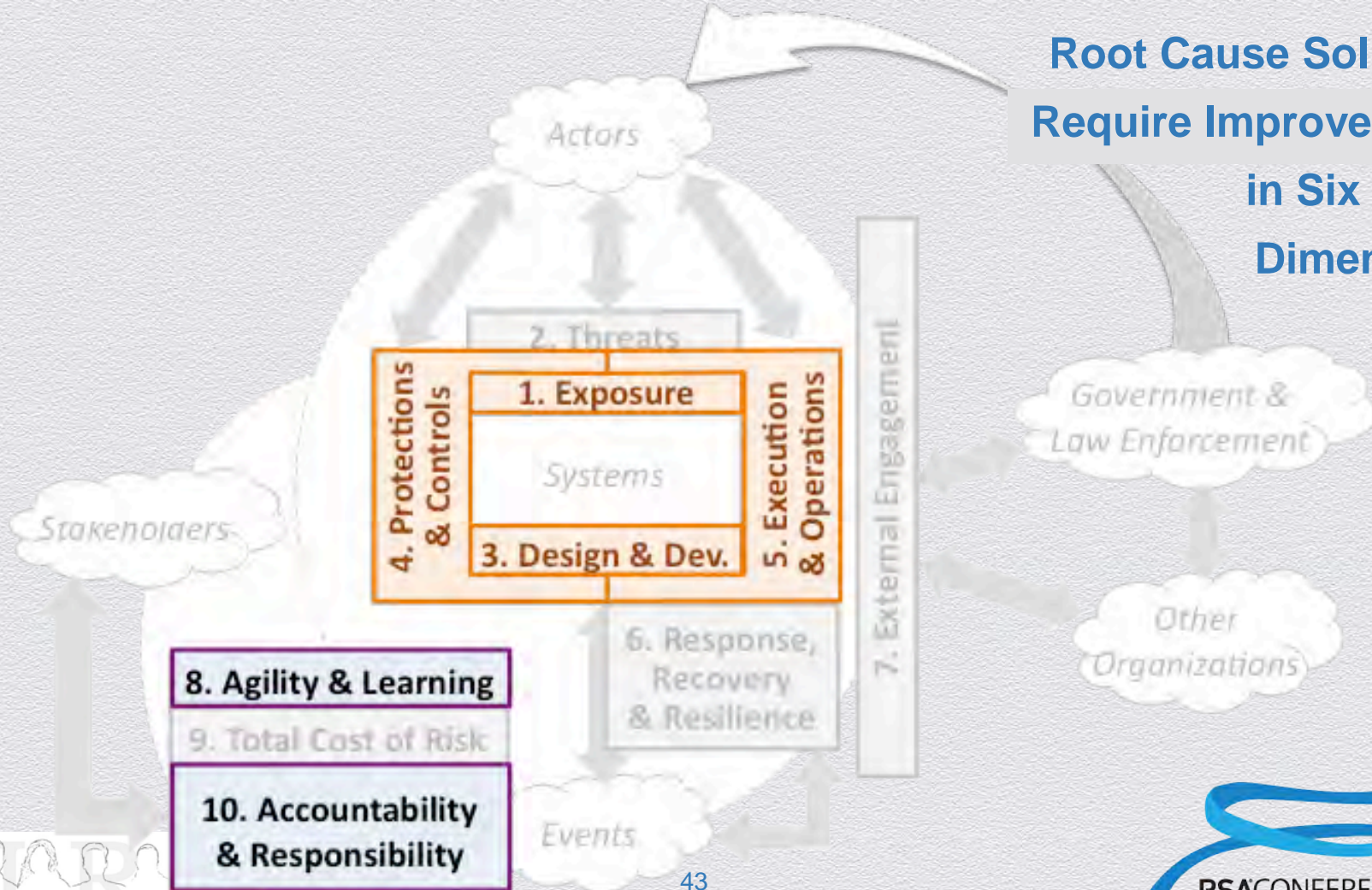
IT requests exceptions to "must patch" list

and exception list

# Root Causes

- ◆ **Misaligned objectives & values** between InfoSec and IT Ops
- ◆ Operational & organizational **disconnect** between InfoSec and “Shadow systems”
- ◆ **Unintended consequences** of IT policies on Line of Business teams
  - ◆ Increases population of “Shadow systems”
- ◆ **Unintended consequences** of repeated cycles of patch exceptions
  - ◆ The more that are approved, the more that are requested

# Root Cause Solutions Require Improvements in Six of Ten Dimensions



# New Objectives and Action Plans

## 1. Optimize Exposure

- ◆ Modify Identity/Authentication services to **automatically** log basic config. information of “Shadow” systems & servers

## 3. Effective Design & Development

- ◆ With IT Ops, design patch decision process to include **alternate remediation** paths

## 4. Quality of Protection & Controls

- ◆ Expand **flexibility** in current controls
- ◆ Add “teeth” to controls on “Shadow” servers

# New Objectives and Action Plans (cont.)

## 5. Efficient/Effective Execution & Operations

- ◆ IT Ops staff trained in 4 alternate remediations

## 8. Effective Agility & Learning

- ◆ Measure “Time to remediation” for systems with critical data
  - ◆ Rather than just “time to patch” and “% servers with current patches”

## 10. Effective Accountability & Responsibility

- ◆ LOB executives given responsibility for risk of their “Shadow” servers and services via “risk surcharge”

# Summary

- ◆ Security Performance is Management by Objectives
- ◆ The Ten Dimensions focus your attention on neglected areas
- ◆ Aggregate metrics into scores using inference, not arithmetic
- ◆ Organization learning and agility is key
  - ◆ Single loop – improving what you do today
  - ◆ Double loop – changing directions, doing different things
- ◆ Start where you are. [Start now.](#)
- ◆ and...

A black and white portrait of Peter Drucker, an older man with thinning hair, wearing a dark sweater over a collared shirt. He is holding a pair of glasses in his right hand, looking directly at the camera with a serious expression.

# Read Peter Drucker!

A blue wavy line graphic that starts from the bottom left and curves towards the right, ending near the Twitter logo and hashtag.

 #RSAC

**RSACONFERENCE2014**

# Contact Information and Resources

**Russell C. Thomas**

[@MrMeritology](#)

Blog: Exploring Possibility Space

[russell.thomas@meritology.com](mailto:russell.thomas@meritology.com)