RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Visualize This! Meaningful Metrics for Managing Risk

SESSION ID: GRC-F02

Moderator: John Johnson
Global Security Strategist
John Deere

Panelists: Alex Hutton
Director of Operations Risk & Governance
A Financial Organization

Jack Jones
President
CXOWARE Inc.

David Mortman
Chief Security Architect and Distinguished Engineer
Dell Enstratius

Caroline Wong
Security Initiatives Director
Cigital

Agenda

- What do you mean by meaningful metrics?
  - Build your own metric – audience participation!
- Metrics Categorization
- Leveraging Frameworks and Models
- What decisions do your metrics focus on supporting? Examples.
- Every organization has loss events. What loss metrics do you capture and how do you leverage them?
- Painting a picture with meaningful metrics

Vocabulary

- Measurement vs. Metric – what's the difference?
  - I had 2 eggs for breakfast this morning
  - It's 46 degrees in Sterling, VA
  - This workshop is 105 minutes long

- A **measurement** is the value of a specific characteristic of a given entity
- A **metric** is the aggregation of one or more measurements to create a piece of business intelligence.
  - What is the question the metric answers?
  - What is the decision the metric supports?
  - What is the environmental context?

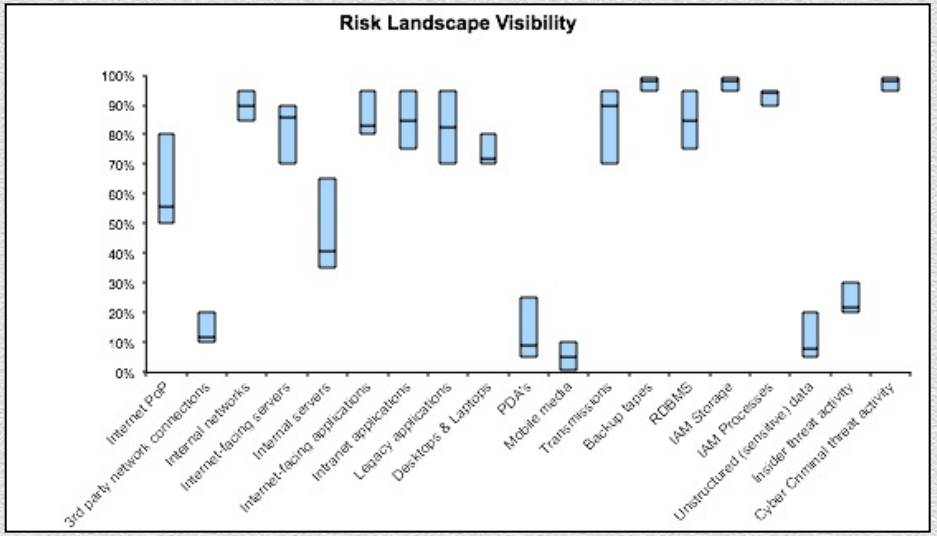
Real Life Metrics

- What metrics are you using to answer questions and make decisions about software security?
  - What question, what decision
  - Who's asking, who's answering
  - What's the goal
  - What environmental context

Build Your Own Metric

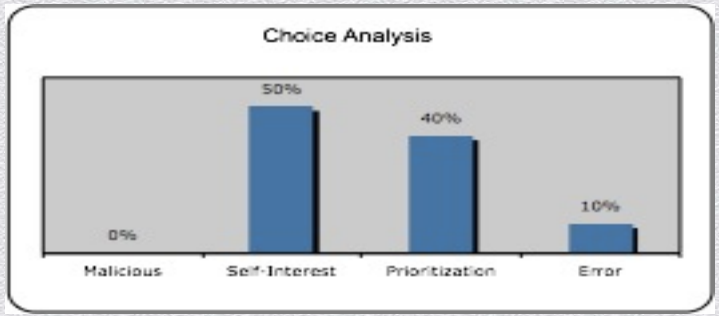
Example

- Risk Landscape Visibility –helps us understand how well informed (or not) our risk decisions are. The values represent data and estimates regarding four elements (asset population, threat conditions, value/liability at risk, and control conditions). This helps us to focus on specific areas of poor visibility, thus improving our ability to make well-informed risk decisions.



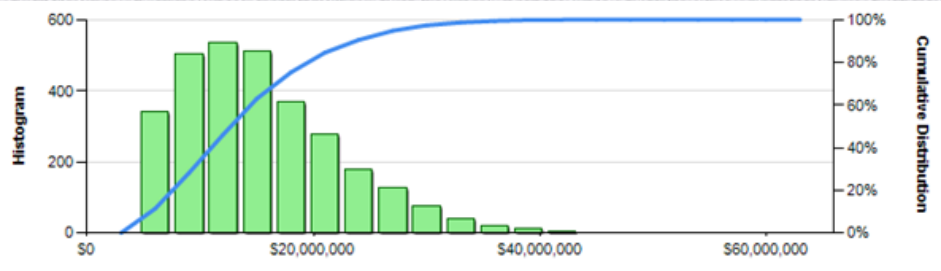
Example

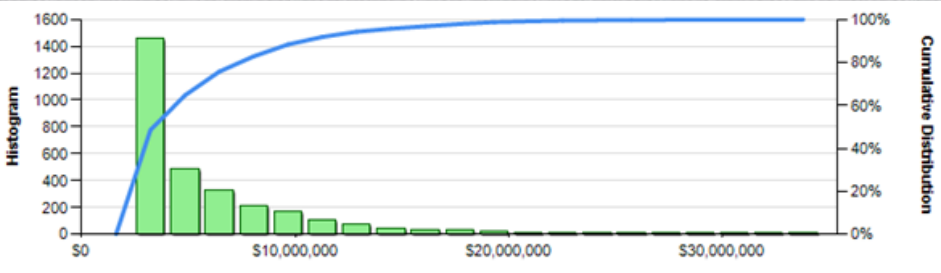
- Root Cause Analysis — which helps us understand why undesirable conditions exist (e.g., non-compliance with policy). This enables us to focus on our efforts to systemically improve.



Example

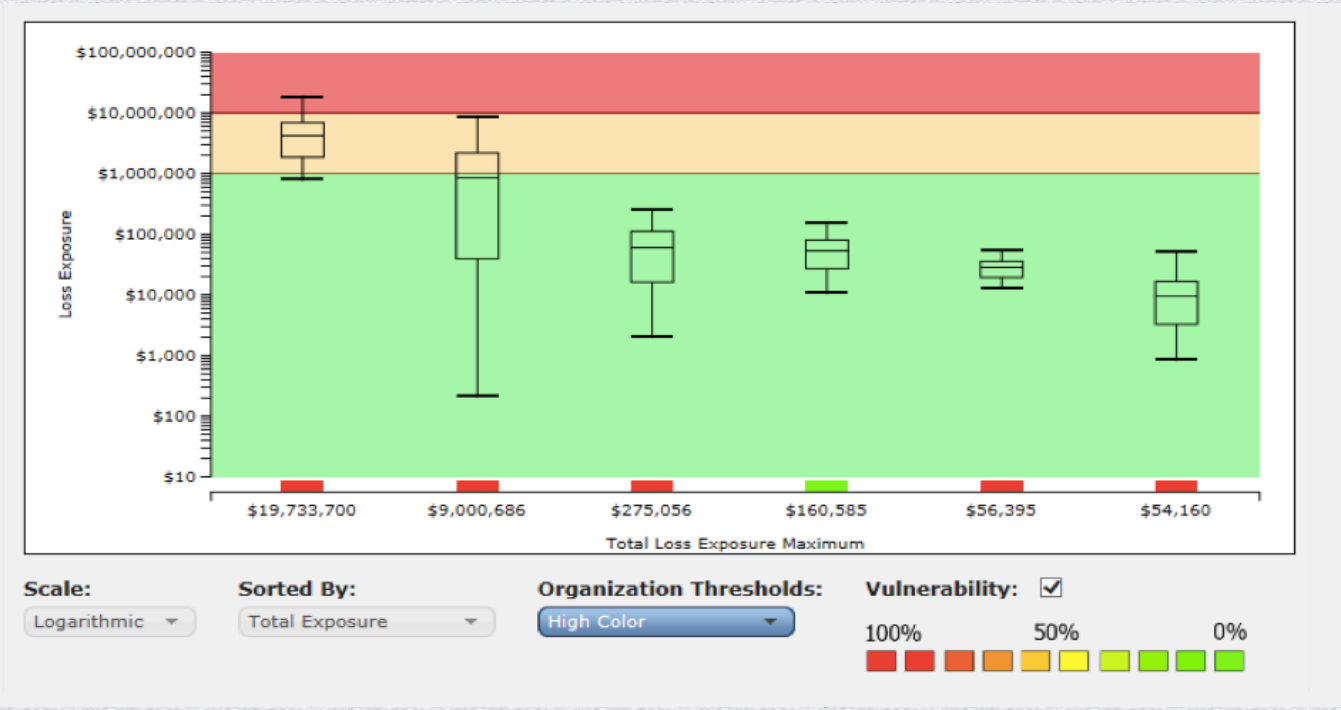
- Loss Exposure Comparison – allows us to compare a current level of loss exposure against a proposed future level assuming the application of new controls. Forms the benefit component of a cost-benefit analysis





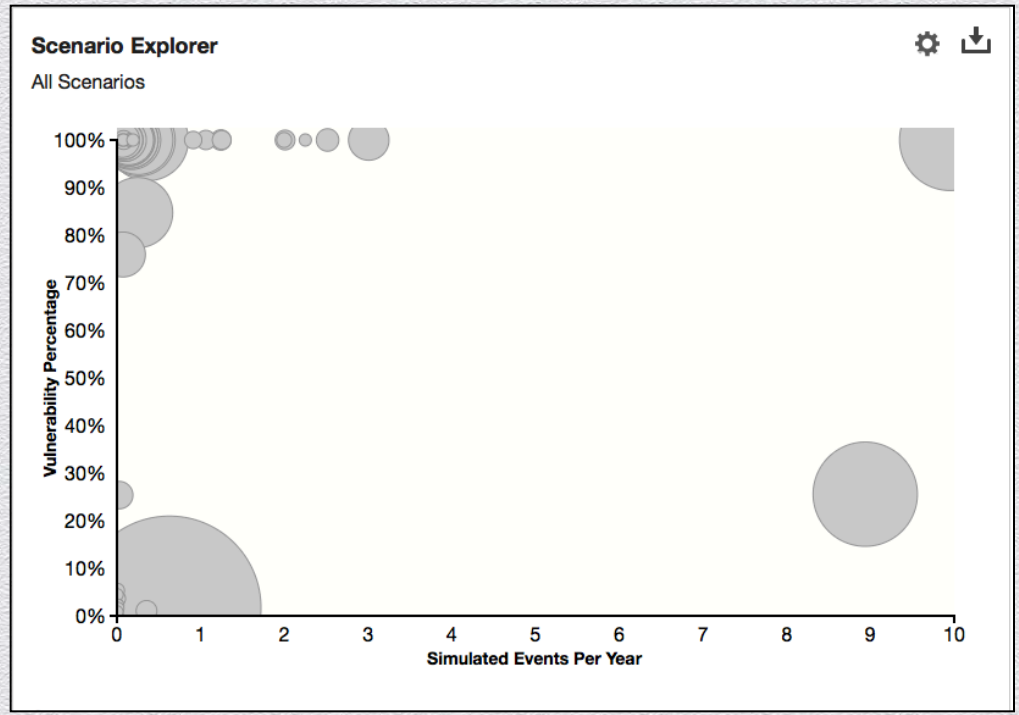
Example

- Risk Scenario Prioritization – allows us to compare the level of loss exposure from multiple scenarios, which improves our ability to prioritize effectively



Example

- Large Scale Scenario Prioritization – allows us to compare the level of loss exposure from many scenarios, which improves our ability to prioritize effectively



Definition of “Risk”?

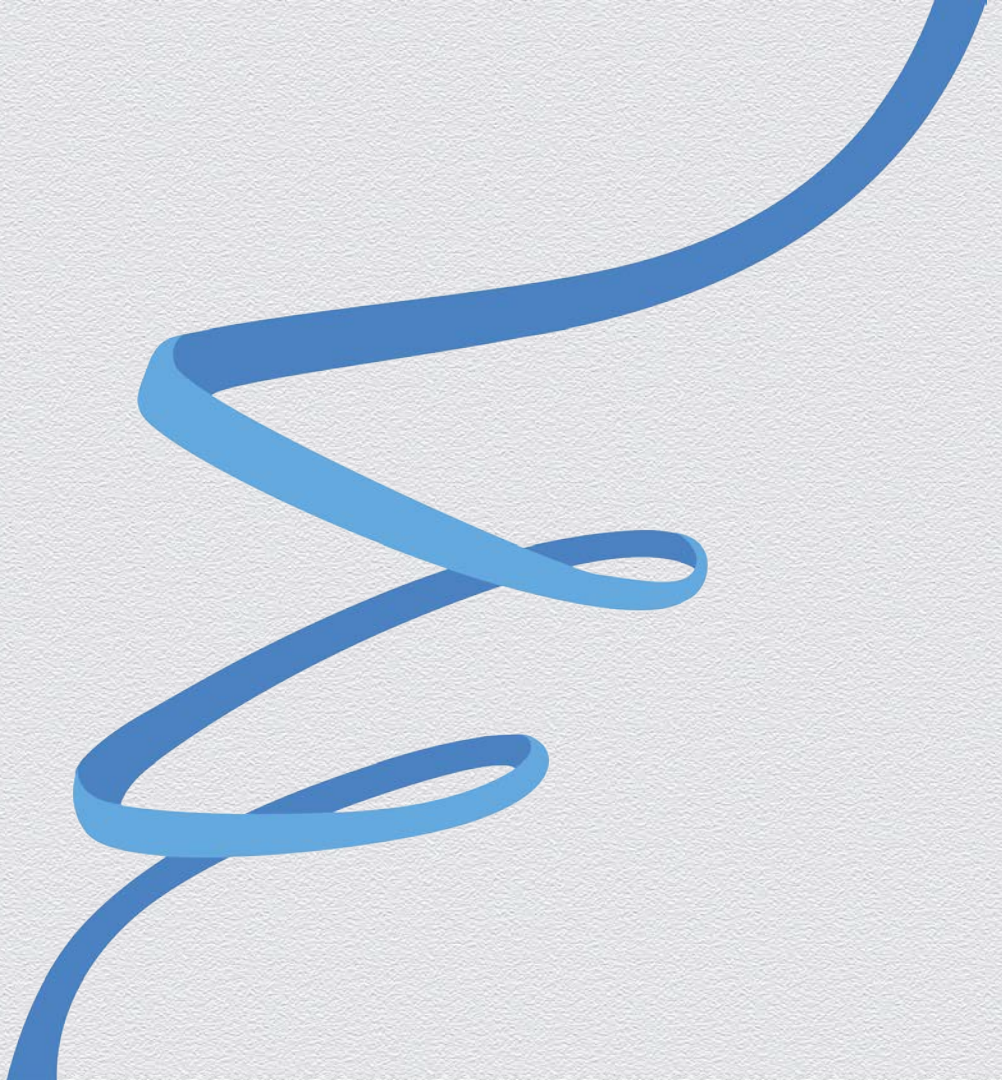
- The probability of a loss event occurring and the probable magnitude of loss that results

Take Aways

- Developing metrics and applying models that are meaningful in the context of your organization
- Breaking down metrics by category
- Choosing frameworks and models
- Delivering the right metrics for your audience, so they can make informed decisions about business risk management
- Applying useful examples to help you quantify risk at your organization and present it concisely to your management

Good metrics and practices → Good Governance → Risk Reduction

Appendix



My Fitness Pal

- I ask questions and make decisions about my health every day
  - What should I eat for breakfast?
  - How much? How often?
  - What kind of exercise should I do?
  - For what length of time? How often?
- I can change my behavior by setting goals and measuring progress
  - SMART goals
  - Specific, measurable, actionable, reasonable, time-based

Software Security Metrics

BUSINESS QUESTION	METRIC – BUSINESS INTEL	COMMENTS
What's the impact on production defects of a 10% increase in software security spending for static analysis?	**Trend in SSI cost vs. Trend in production software security defects**	Comparing the two trendlines is more useful than looking at either in isolation
Which security technology stacks and components harbor the greatest amount of defects?	**Discoveries of vulnerability x / App component type**	Understanding the prevalence of a vuln for a specific app component type is more useful than counting discovery instances without the environmental context
How long does it take the organization to successfully respond to process variances?	**Average days to remediate variance / Variance type**	Understanding the time it takes to address variances by variance type is more useful than without the environmental context
How much extra work is caused by the need to triage results (remove false positives, etc) from testing tools?	**Static analysis false positives / Tool / Defect type / Tech stack / Analysis rule**	Any of the counts alone are less useful than when viewed together for more complete business context
What is the impact of training on software security defects found in various types of testing?	**Web app Java code from developers with 8 hours of instruction has 20% fewer defects found by static analysis than code from untrained developers**	Look at desired outcomes of training rather than

A Software Security Framework

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Manage-ment

Four domains

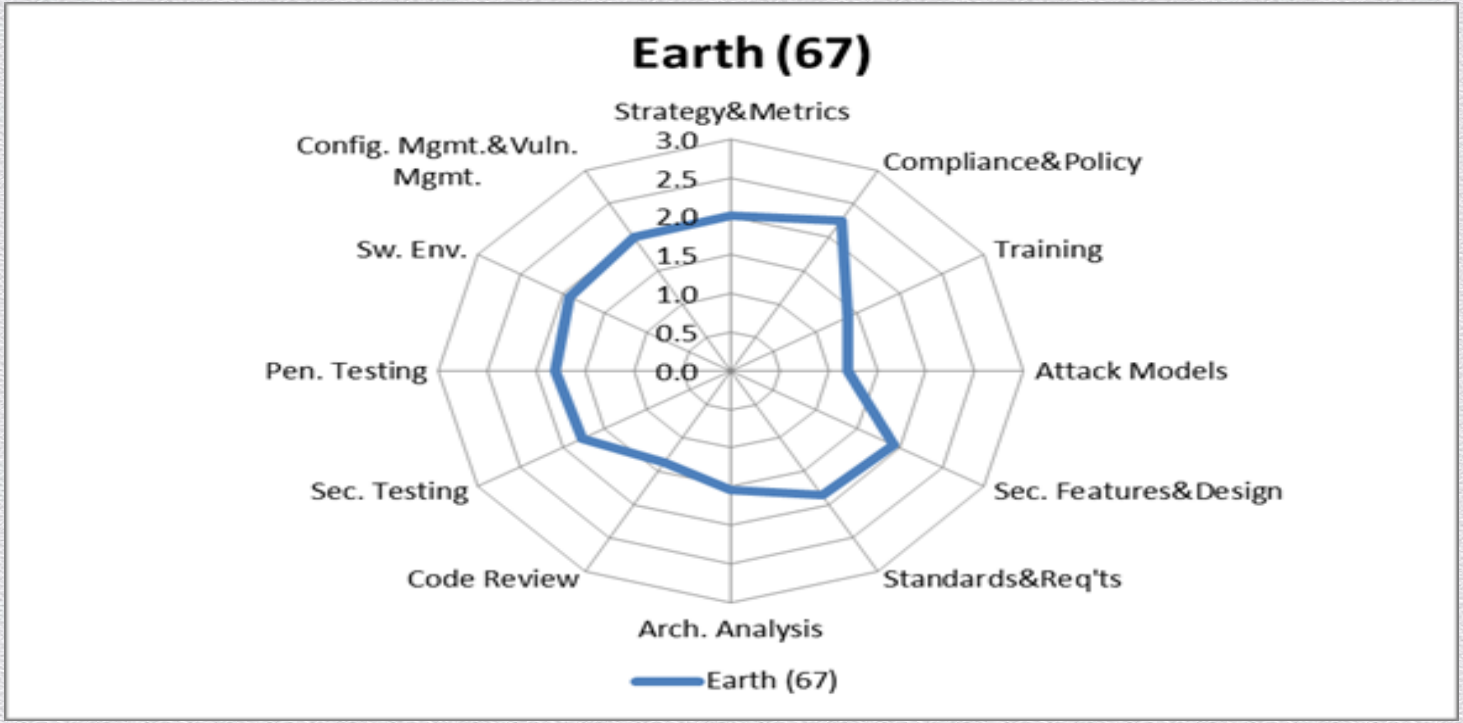
Twelve practices

See informIT article on BSIMM website http://bsimm.com

BSIMM Scorecard

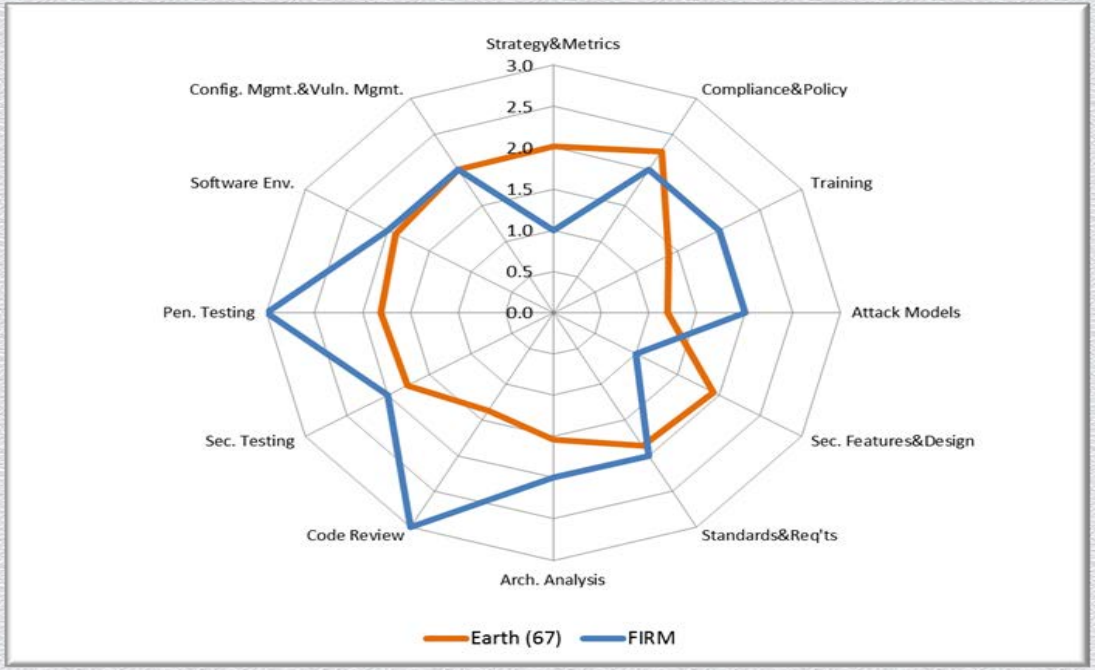
Governance		Intelligence		SSDL Touchpoints		Deployment	
Activity	Observed	Activity	Observed	Activity	Observed	Activity	Observed
[SM1.1]	44	[AM1.1]	21	[AA1.1]	56	[PT1.1]	62
[SM1.2]	34	[AM1.2]	43	[AA1.2]	35	[PT1.2]	51
[SM1.3]	34	[AM1.3]	30	[AA1.3]	24	[PT1.3]	43
[SM1.4]	57	[AM1.4]	12	[AA1.4]	42	[PT2.2]	24
[SM1.6]	36	[AM1.5]	42	[AA2.1]	10	[PT2.3]	27
[SM2.1]	26	[AM1.6]	16	[AA2.2]	8	[PT3.1]	13
[SM2.2]	31	[AM2.1]	7	[AA2.3]	20	[PT3.2]	8
[SM2.3]	27	[AM2.2]	11	[AA3.1]	11		
[SM2.5]	20	[AM3.1]	4	[AA3.2]	4		
[SM3.1]	16	[AM3.2]	6				
[SM3.2]	6						
[CP1.1]	43	[SFD1.1]	54	[CR1.1]	24	[SE1.1]	34
[CP1.2]	52	[SFD1.2]	53	[CR1.2]	34	[SE1.2]	61
[CP1.3]	45	[SFD2.1]	26	[CR1.4]	50	[SE2.2]	31
[CP2.1]	24	[SFD2.2]	29	[CR1.5]	23	[SE2.4]	25
[CP2.2]	28	[SFD2.3]	9	[CR1.6]	25	[SE3.2]	10
[CP2.3]	29	[SFD3.1]	13	[CR2.2]	10	[SE3.3]	9
[CP2.4]	25	[SFD3.2]	9	[CR2.5]	15		
[CP2.5]	35			[CR3.1]	18		
[CP3.1]	14			[CR3.2]	4		
[CP3.2]	11			[CR3.3]	6		
[CP3.3]	8			[CR3.4]	1		

Earth (67)


Earth (67)
Strategy&Metrics
Compliance&Policy
Training
Attack Models
Sec. Features&Design
Standards&Req'ts
Arch. Analysis
Code Review
Sec. Testing
Pen. Testing
Sw. Env.
Config. Mgmt.&Vuln. Mgmt.
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Earth (67)

BSIMM as a Measuring Stick

- Compare a firm with peers using the high water mark view
- Compare business units
- Chart an SSI over time



BSIMM Scorecard with FAKE Firm Data

BSIMM-V Scorecard for: FIRM — Raw Score: 37

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM	Activity	BSIMM-V Firms	FIRM
[SM1.1]	44	1	[AM1.1]	21	1	[AA1.1]	56	1	[PT1.1]	62	1
[SM1.2]	34		[AM1.2]	43		[AA1.2]	35	1	[PT1.2]	51	1
[SM1.3]	34	1	[AM1.3]	30		[AA1.3]	24	1	[PT1.3]	43	
[SM1.4]	57	1	[AM1.4]	12	1	[AA1.4]	42		[PT2.2]	24	1
[SM1.6]	36		[AM1.5]	42	1	[AA2.1]	10		[PT2.3]	27	
[SM2.1]	26		[AM1.6]	16		[AA2.2]	8	1	[PT3.1]	13	1
[SM2.2]	31		[AM2.1]	7		[AA2.3]	20		[PT3.2]	8	
[SM2.3]	27		[AM2.2]	11	1	[AA3.1]	11				
[SM2.5]	20		[AM3.1]	4		[AA3.2]	4				
[SM3.1]	16		[AM3.2]	6							
[SM3.2]	6										
[CP1.1]	42	1	[SFD1.1]	54		[CR1.1]	24		[SE1.1]	34	
[CP1.2]	52		[SFD1.2]	53	1	[CR1.2]	34	1	[SE1.2]	61	1
[CP1.3]	45	1	[SFD2.1]	26		[CR1.4]	50	1	[SE2.2]	31	1
[CP2.1]	24		[SFD2.2]	29		[CR1.5]	23		[SE2.4]	25	
[CP2.2]	28		[SFD3.1]	9		[CR1.6]	25	1	[SE3.2]	10	
[CP2.3]	28		[SFD3.2]	13		[CR2.2]	10		[SE3.3]	9	
[CP2.4]	25		[SFD3.3]	9		[CR2.5]	15				
[CP2.5]	35	1				[CR2.6]	18				
[CP3.1]	14					[CR3.2]	4	1			
[CP3.2]	11					[CR3.3]	6				
[CP3.3]	8					[CR3.4]	1				
[T1.1]	50	1	[SR1.1]	48	1	[ST1.1]	51	1	[CMVM1.1]	59	1
[T1.5]	29		[SR1.2]	43		[ST1.3]	55	1	[CMVM1.2]	59	
[T1.6]	23	1	[SR1.3]	45	1	[ST2.1]	27	1	[CMVM2.1]	50	1
[T1.7]	33		[SR1.4]	27	1	[ST2.4]	13		[CMVM2.2]	44	
[T2.5]	9		[SR2.2]	23		[ST3.1]	11		[CMVM2.3]	30	
[T2.6]	13	1	[SR2.3]	19		[ST3.2]	8		[CMVM3.1]	6	
[T2.7]	9		[SR2.4]	19		[ST3.3]	6		[CMVM3.2]	6	
[T3.1]	4		[SR2.5]	22	1	[ST3.4]	5		[CMVM3.3]	2	
[T3.2]	4		[SR3.1]	8		[ST3.5]	7				
[T3.3]	8		[SR3.2]	12							
[T3.4]	9										
[T3.5]	5										

Legend:
- Activity: 111 BSIMM-V activities, shown in 4 domains and 12 practices
- BSIMM Firms: count of firms (out of 67) observed performing each activity
- the most common activity within a practice
- a common activity not observed in this assessment
- a common activity observed in this assessment
- a practice where firm's high-water mark score is below the BSIMM-V average

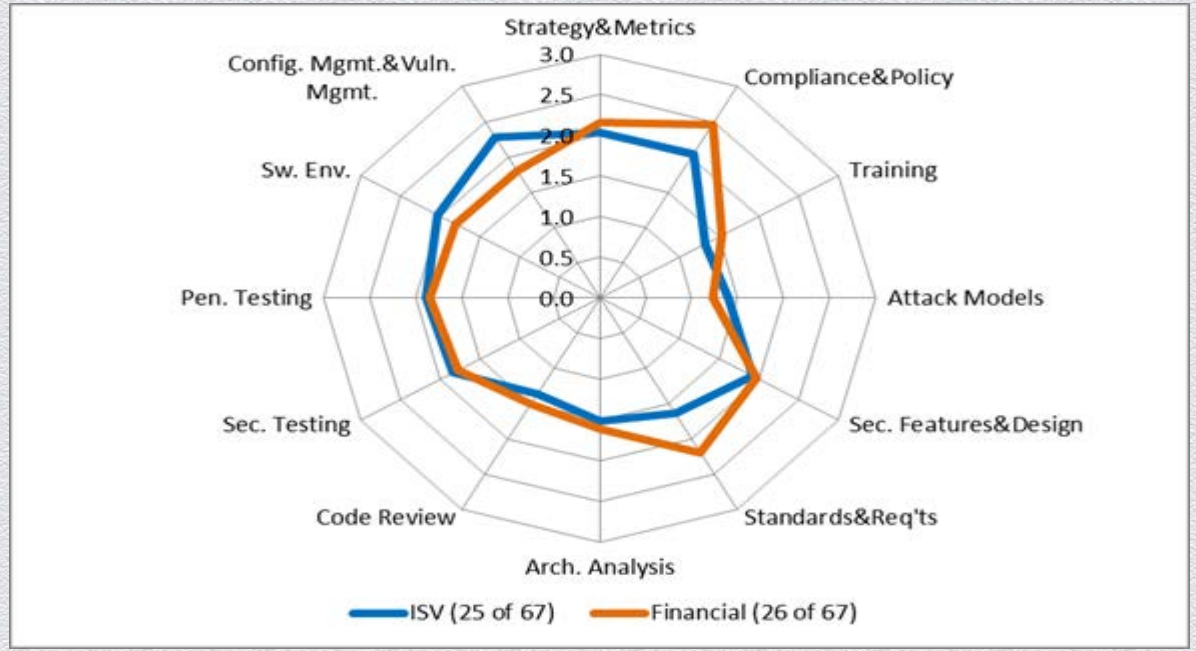
Top 12 activities

purple = good?

red = bad?

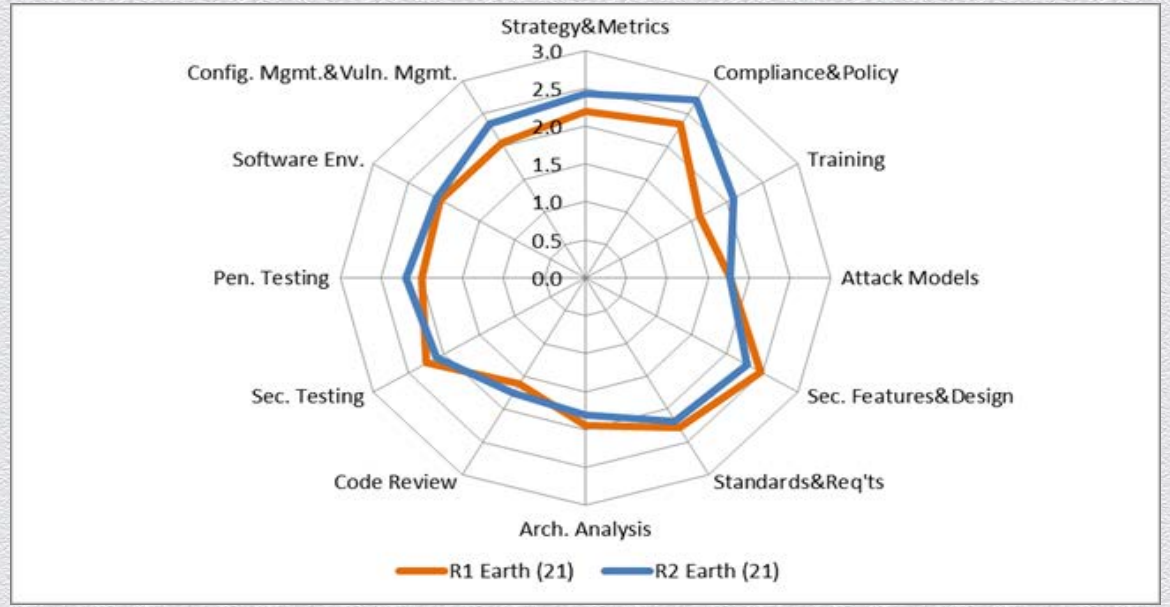
"Blue shift" practices to emphasize

Each of us is a Special Snowflake (NOT)



ISV (25) results are similar to financial services (26)

BSIMM Longitudinal: Improvement over Time



21 firms measured twice (an average of 24 months apart)

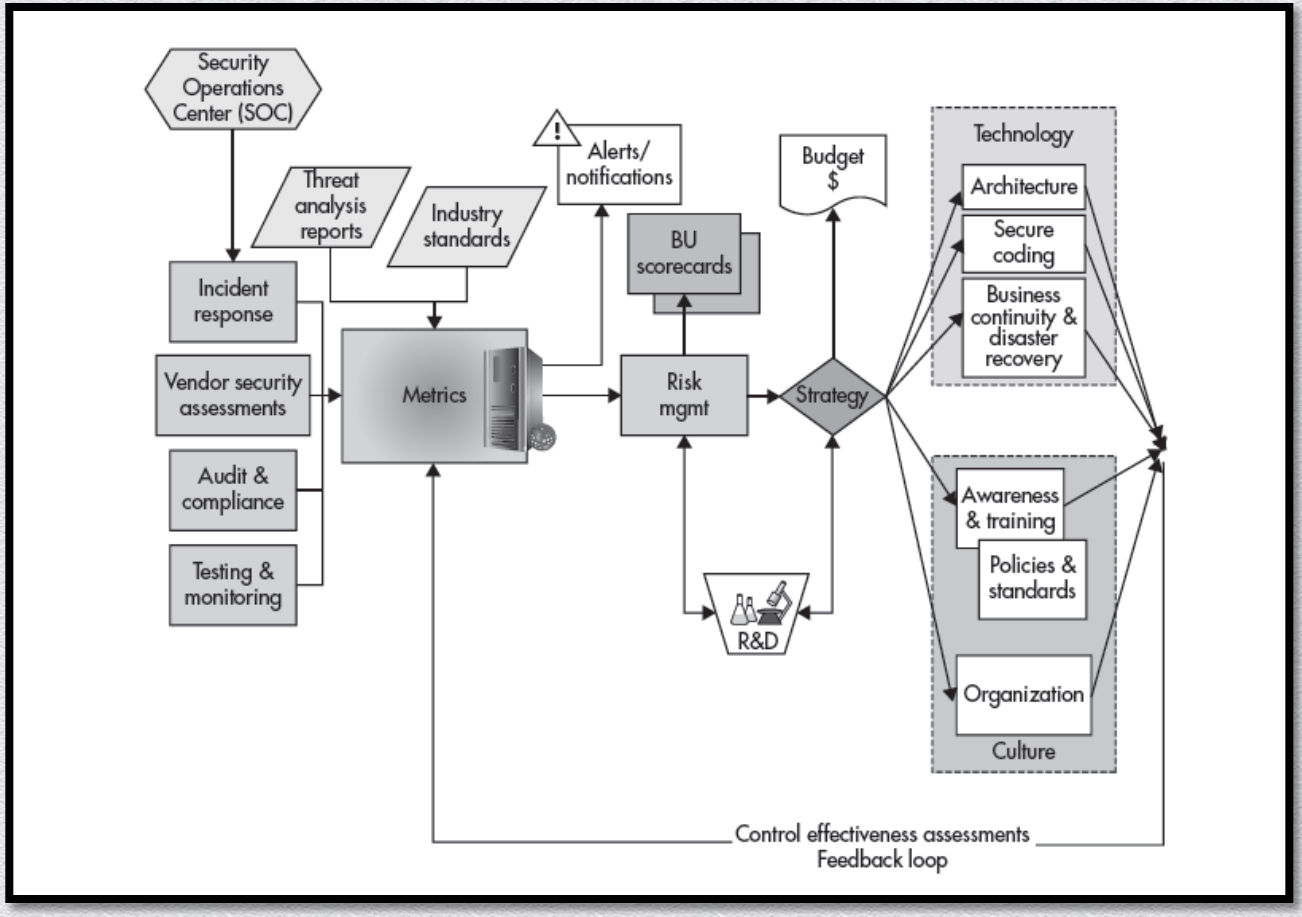
Show how firms improve

An average of 16% activity increase

BSIMM by the Numbers

	BSIMM1	BSIMM2	BSIMM3	BSIMM4	BSIMM-V
Firms	9	30	42	51	67
Measurements	9	49	81	95	161
2nd Measurements	0	0	11	13	21
3rd Measurements	0	0	0	1	4
SSG Members	370	635	786	974	976
Satellite Members	710	1150	1750	2039	1954
Developers	67,950	141,175	185,316	218,286	272,358
Applications	3970	28,243	41,157	58,739	69,039
Avg SSG Age	5.32	4.49	4.32	4.13	4.28
SSG Avg of Avgs	1.13 / 100	1.02 / 100	1.99 / 100	1.95 / 100	1.4 / 100
Financials	4	12	17	19	26
ISVs	4	7	15	19	25
High Tech	2	7	10	13	14

The Predictive Security Model



Top Ten Risks