Enterprise Security Profile Model (ESPM)

- Presented by Kent Pankratz, MSISA, CISSP

  kent@veritysecurity.com, 608-515-8849

- January 5, 2018

VERITY SECURITY

VERITY SECURITY

Presentation Summary

- Review the Enterprise Security Profile Model (ESPM)
  - Purpose
  - Functions
  - Capabilities
- Illustrate how the ESPM incorporates the NIST Cybersecurity Framework
- Answer questions and/or provide a demonstration
  - Review the ESPM Mappings to the Framework

VERITY SECURITY

CISO Concerns

2015. Deloitte. https://www.prnewswire.com/news-releases/deloitte-reveals-top-challenges-facing-new-chief-information-security-officers-300127504.html

VERITY SECURITY

The Purpose of the ESPM

What is the Security Profile?

Facilitate communications

Generate support and trust

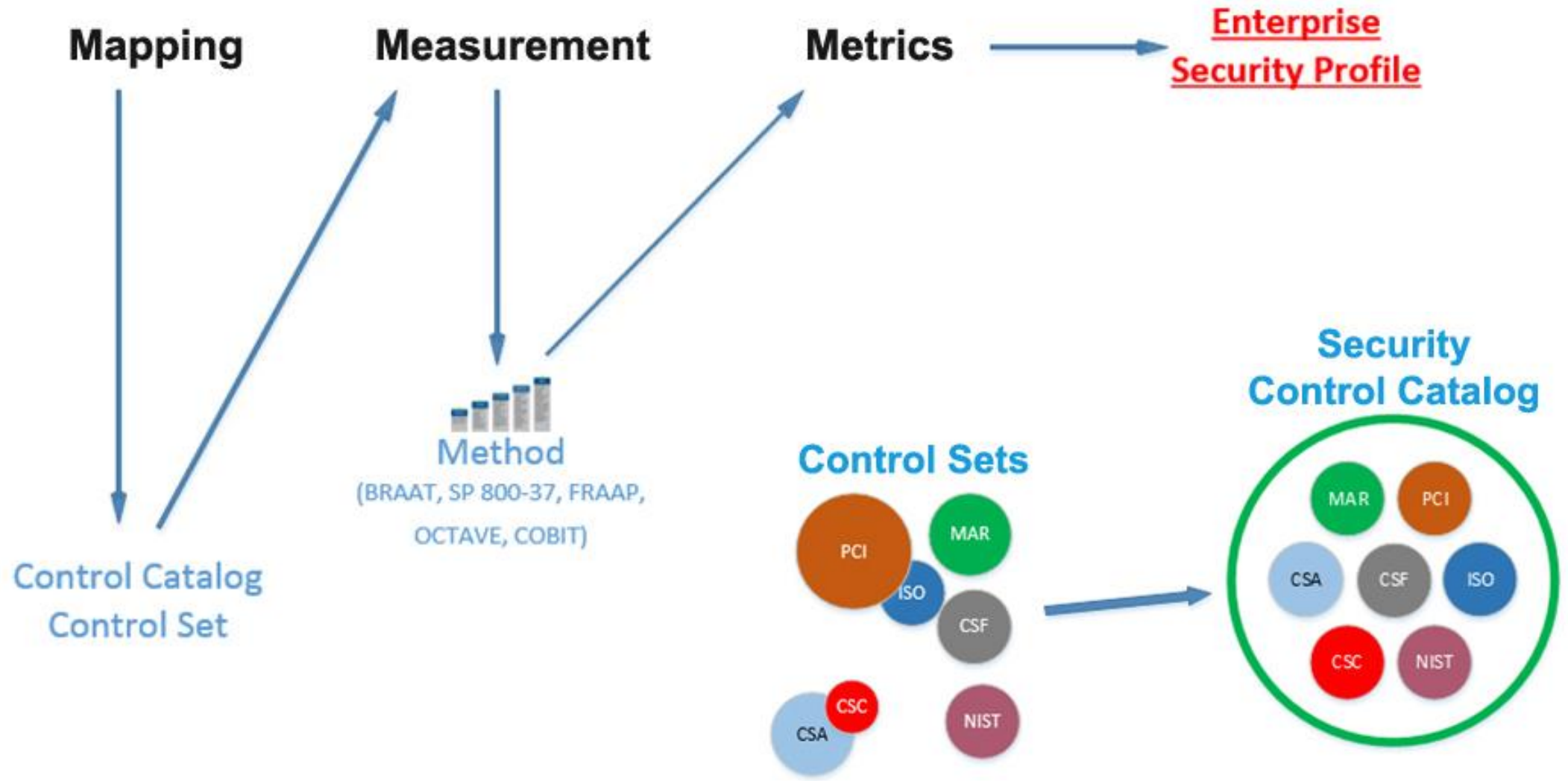
Create a wholistic governance strategy

Merge compliance with risk analysis

Establish a security risk management lifecycle

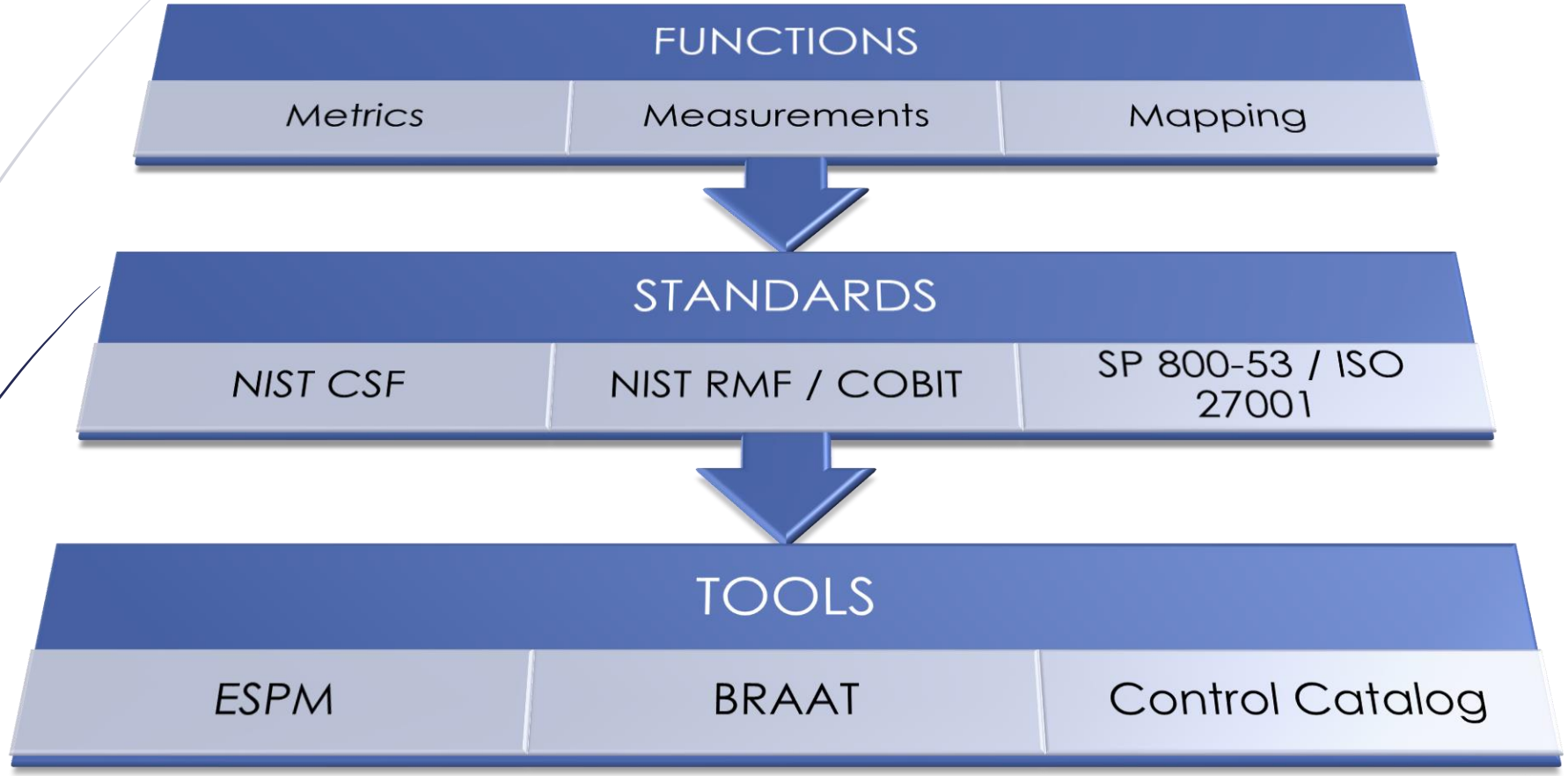
VERITY SECURITY

ESPM Functions



VERITY SECURITY

Correlations



VERITY SECURITY

Executive Summary

Security Profile

35.6%

Function Scores

Function	Function Score
IDENTIFY	33.5%
PROTECT	34%
DETECT	40%
RESPOND	43%
RECOVER	26%

Control Catalog

Control Catalog Score	Function	Category	Category Name	STN	0	1	2	3	4	5	6	7	8	9	10	11	12
Control Set Score				39.4%													
39%	IDENTIFY	ID.AM	Asset Management	1.1-x.x		50%	58%	33%	34%	26%	34%						
24%		ID.BE	Business Environment	1.2-x.x		23%	28%	30%	23%	22%							
34%		ID.GV	Governance	1.3-x.x		19%	44%	58%	50%								
23%		ID.RA	Risk Assessment	1.4-x.x		12%	43%	28%	31%	47%	49%						
40%		ID.RM	Risk Management Strategy	1.5-x.x		42%	58%	30%									
41%		ID.SC	Supply Chain Risk Management	1.6-x.x		50%	39%	31%	38%	82%							
32%	PROTECT	PR.AC	Access Control	2.1-x.x		25%	30%	45%	35%	31%	50%						
43%		PR.AT	Awareness and Training	2.2-x.x		41%	44%	37%	48%	45%							
35%		PR.DS	Data Security	2.3-x.x		43%	38%	31%	31%	39%	25%	41%	55%				
33%		PR.IP	Information Protection Processes and Procedures	2.4-x.x		24%	32%	46%	40%	27%	46%	30%	51%	42%	24%	31%	57%
28%		PR.MA	Maintenance	2.5-x.x		28%	28%										
33%		PR.PT	Protective Technology	2.6-x.x		23%	42%	36%	34%	54%							
36%	DETECT	DE.AE	Anomalies and Events	3.1-x.x		40%	28%	43%	32%	35%							
40%		DE.CM	Security Continuous Monitoring	3.2-x.x		41%	35%	36%	39%	27%	35%	37%	59%				
46%		DE.DP	Detection Processes	3.3-x.x		51%	52%	51%	37%	35%							
46%	RESPOND	RS.AN	Analysis	4.1-x.x		44%	44%	87%	43%								
40%		RS.CO	Communications	4.2-x.x		41%	25%	48%	54%	61%							
56%		RS.IM	Improvements	4.3-x.x		58%	55%										
47%		RS.MI	Mitigation	4.4-x.x		45%	45%	49%									
25%		RS.RP	Response Planning	4.5-x.x		25%											
46%	RECOVER	RC.CO	Communications	5.2-x.x		47%	48%	42%									
29%		RC.IM	Improvements	5.3-x.x		27%	34%										
3%		RC.RP	Recovery Planning	5.5-x.x		3%											

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Access Control	Least Privilege and Separation of Duties	(2.1-4.x)
	Awareness and Training		(2.2-x.x)
	Data Security		(2.3-x.x)
	Information Protection Processes and Procedures		(2.4-x.x)
	Maintenance		(2.5-x.x)
	Protective Technology		(2.6-x.x)
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure

VERITY SECURITY

Security Taxonomy Number (STN)

PR (2.0-0.0)	Executive Review	Organization (one)
PR.AC (2.1-0.0)	Management Review	
PR.AC-4 (2.1-4.0)	Unit Requirements	
PR.AC-4 (2.1-4.2)	Assessments	
STN	Communication	to
2.0-0.0	CSF Protect	Control Catalog (many)
2.1-0.0	Access Control	
2.1-4.0	Separation of duties	
2.1-4.1	PCI DSS v.3.2, 6.4.2	
2.1-4.2	ISO 27001, A.6.1.2	
2.1-4.3	NIST 800-53, AC-5	

VERITY SECURITY

Intermission

- The Enterprise Security Profile Model (ESPM)
  - Identifies the current security performance of an organization
  - Utilizes the mapping of controls, measures them, and provides metrics for decisions
  - Facilitates communication and trust that the security controls are performing
- The NIST Cybersecurity Framework is central to the ESPM
  - The mapping of controls is a one-to-one correlation to the descriptions of the controls

Next:

- Answer questions and/or provide a demonstration