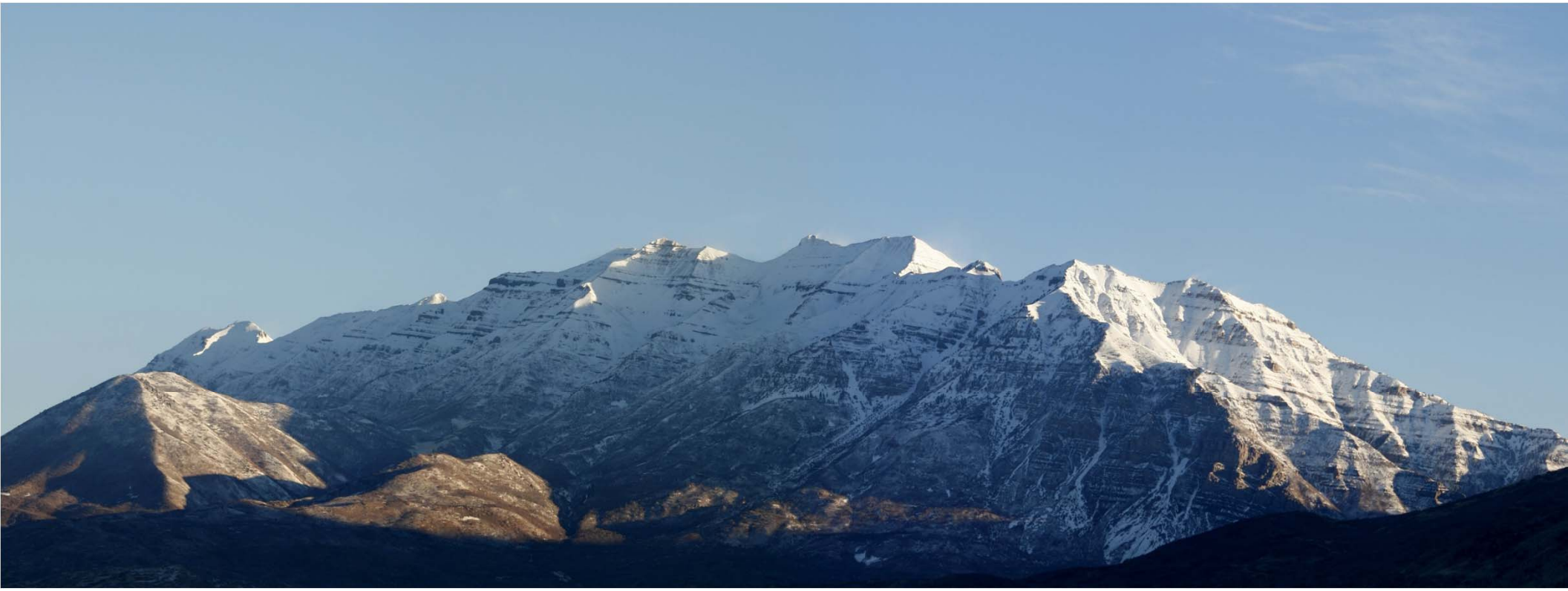
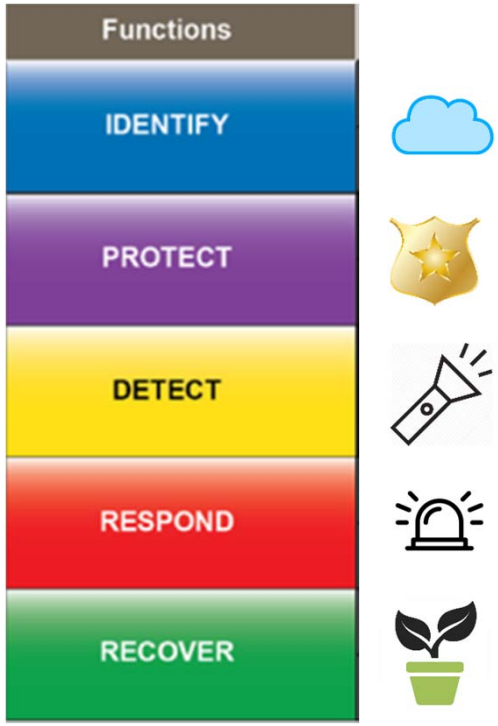
What Is Your Security Profile?



Establishing an Enterprise Security Profile from Quantitative Measurements

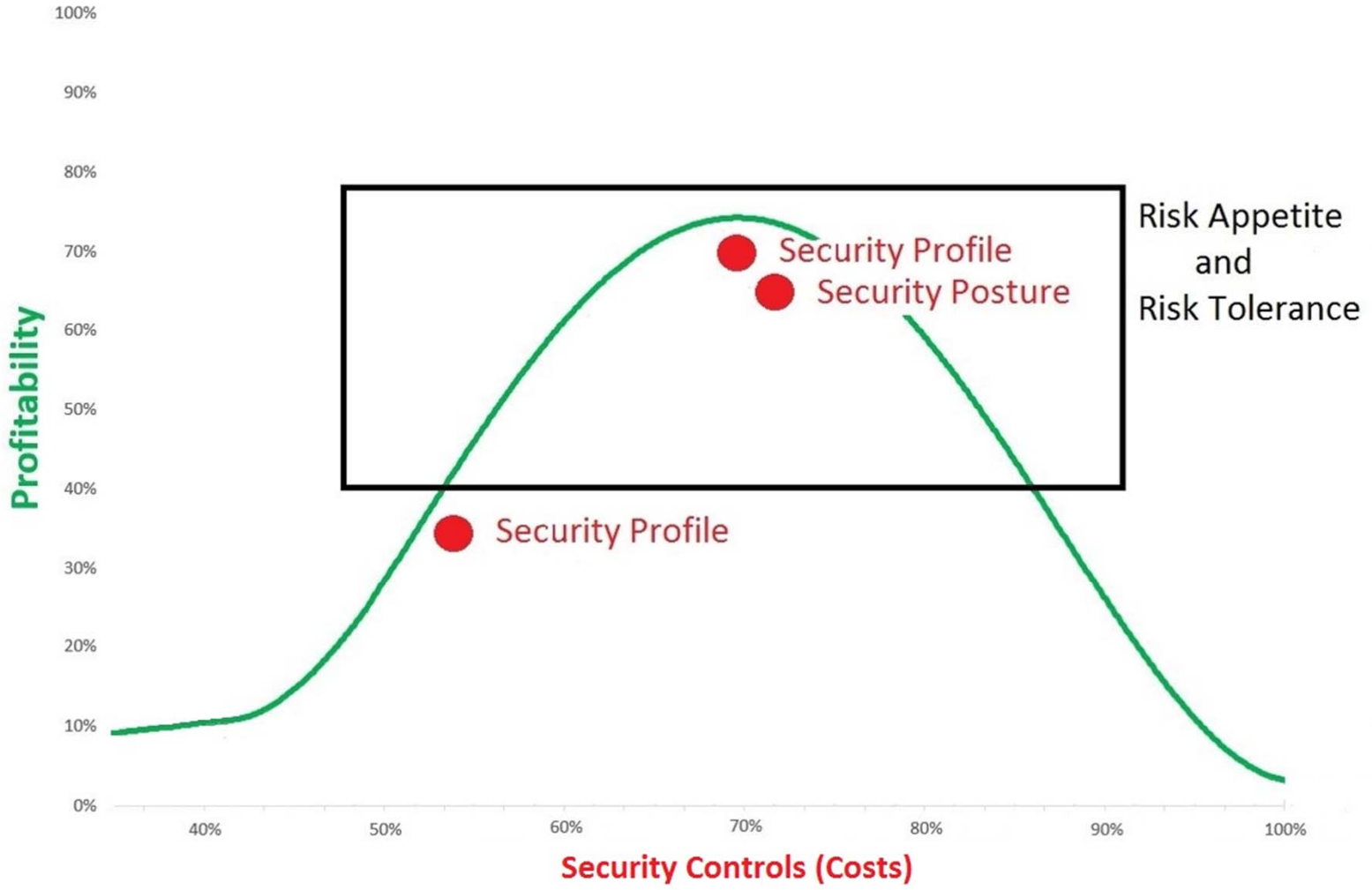
Enterprise Security Profile Model

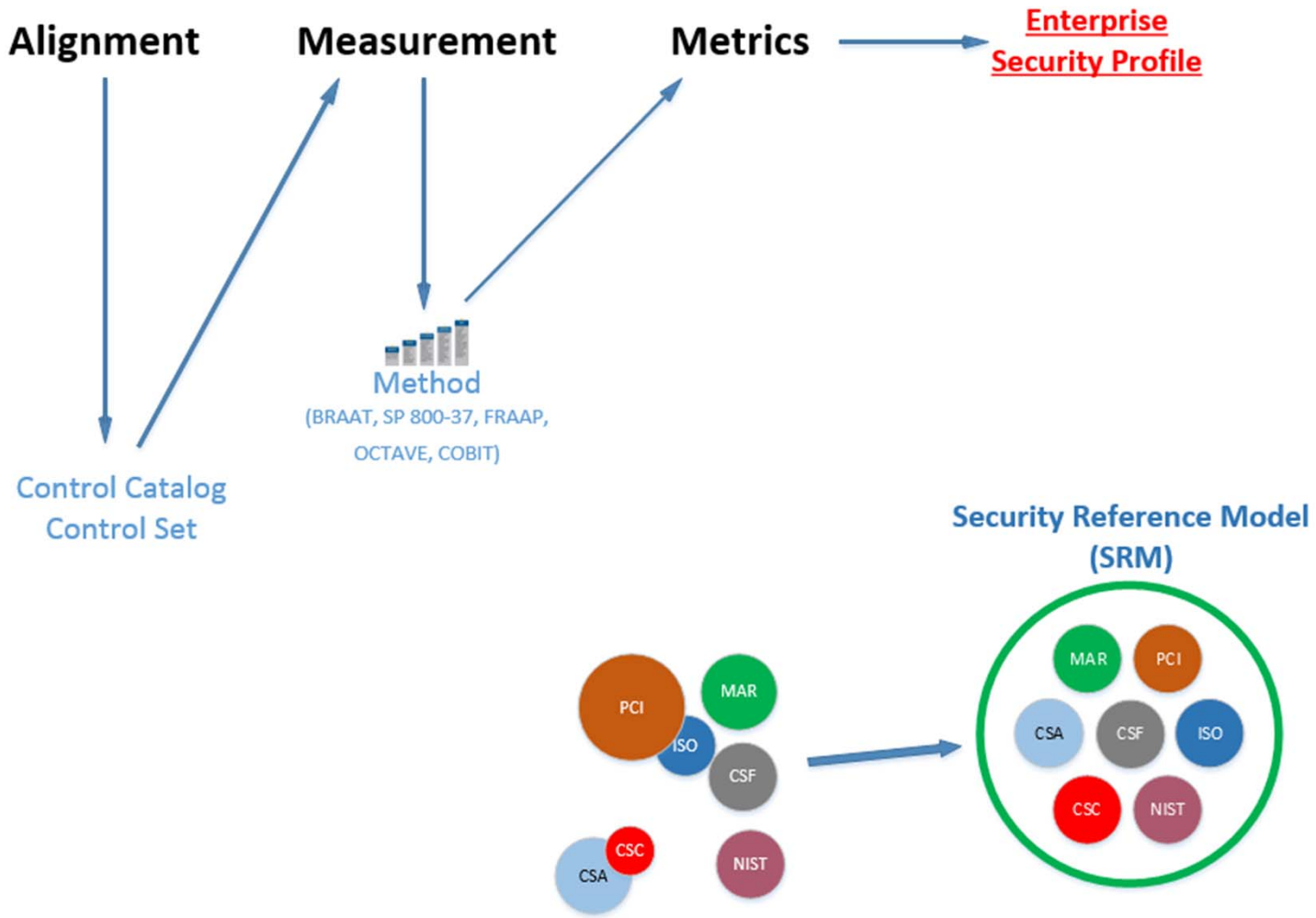
1. Alignment
2. Measurement
3. Metrics



Utilizing the
NIST Cybersecurity Framework
as a
Maturity Model

Risk Management for Security Controls

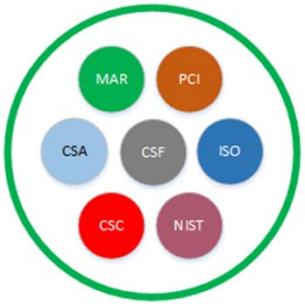



Alignment
Measurement
Metrics
Enterprise Security Profile
Method
(BRAAT, SP 800-37, FRAAP, OCTAVE, COBIT)
Control Catalog
Control Set
Security Reference Model (SRM)
PCI
MAR
ISO
CSF
CSC
CSA
NIST
MAR
PCI
CSA
CSF
ISO
CSC
NIST

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

		Organization (one)
PR.AC-4 (2.1-4.2)	Assessments	
SCID	Control Set	to
2.0-0.0	CSF Protect	Control Catalog (many)
2.1-0.0	Access Control	
2.1-4.0	Separation of duties	
2.1-4.2	PCI DSS v.3.2, 6.4.2	
2.1-4.2	ISO 27001, A.6.1.2	
2.1-4.2	NIST 800-53, AC-5	



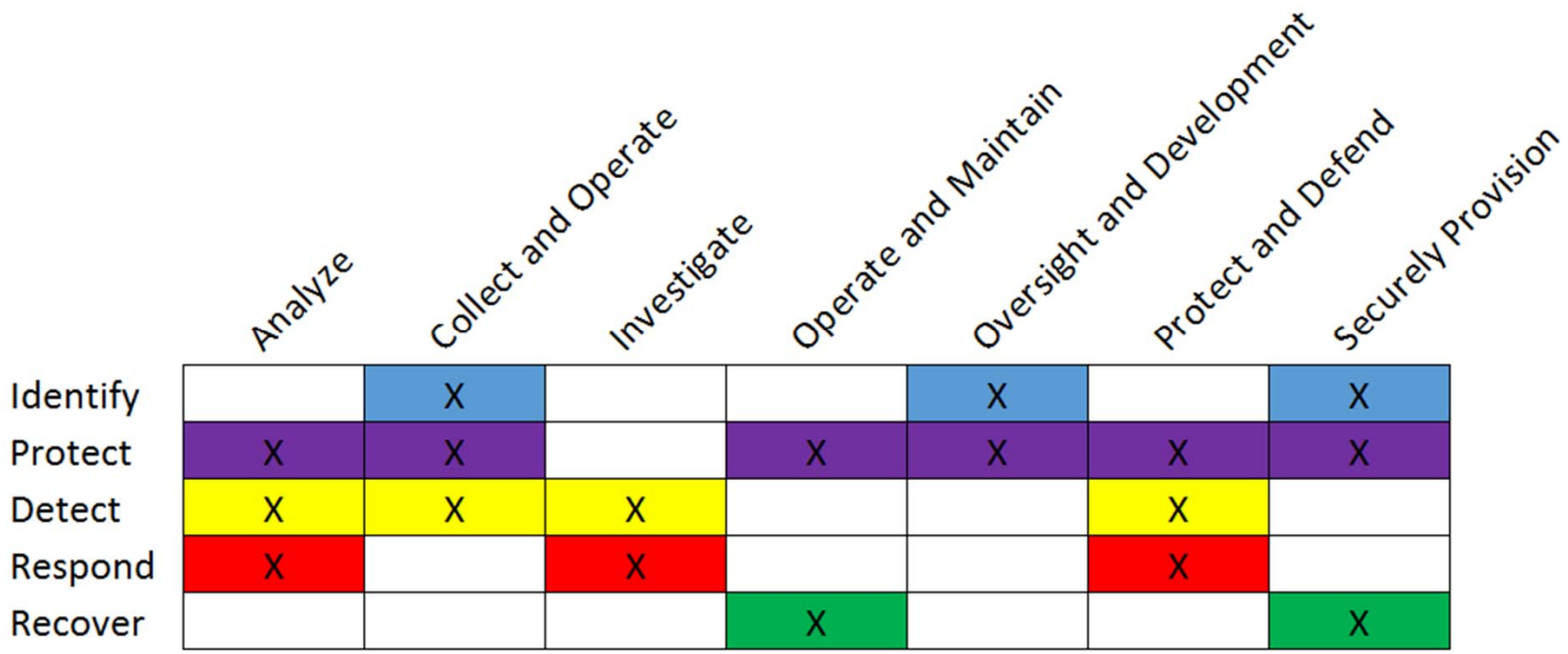
Executive Summary

Security Profile

64.7%

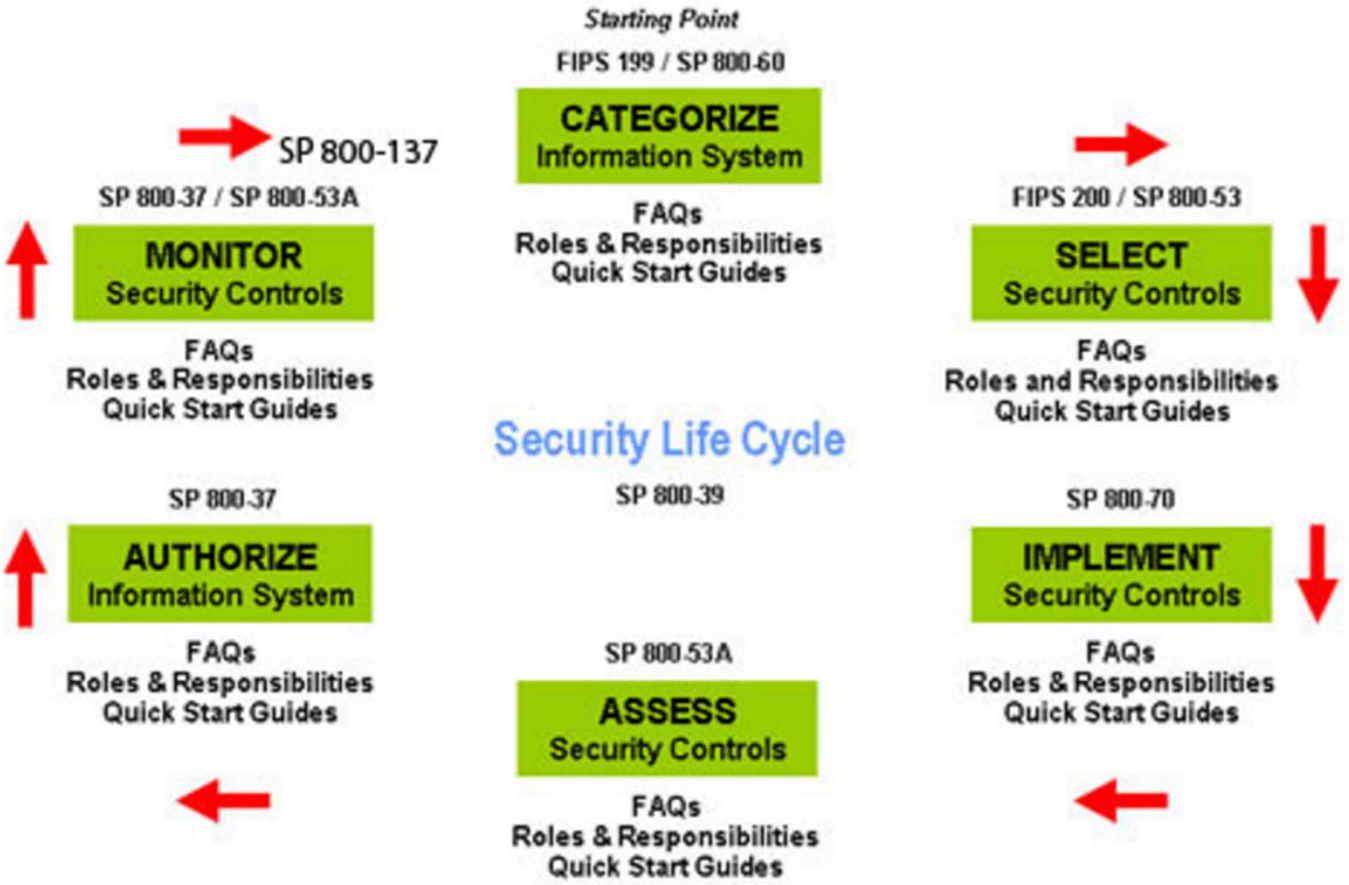
Function Scores	Control Catalog Score	Function	Category	Category Name	SCID #	Control Set Score 0	1	2	3	4	5	6	7	8	9	10	11	12
62%	62%	IDENTIFY	ID.AM	Asset Management	1.1-x.x		65%	62%	65%	70%	51%	57%						
	61%		ID.BE	Business Environment	1.2-x.x		56%	52%	57%	65%	62%							
	60%		ID.GV	Governance	1.3-x.x		62%	57%	67%	59%								
	64%		ID.RA	Risk Assessment	1.4-x.x		64%	77%	79%	63%	54%	37%						
	62%		ID.RM	Risk Management Strategy	1.5-x.x		51%	74%	72%									
69%	71%	PROTECT	PR.AC	Access Control	2.1-x.x		74%	70%	65%	69%	73%							
	67%		PR.AT	Awareness and Training	2.2-x.x		66%	69%	70%	66%	64%							
	68%		PR.DS	Data Security	2.3-x.x		80%	66%	70%	66%	65%	63%	56%					
	64%		PR.IP	Information Protection Processes and Procedures	2.4-x.x		63%	66%	65%	66%	70%	61%	62%	65%	62%	52%	63%	62%
	71%		PR.MA	Maintenance	2.5-x.x		72%	71%										
	73%		PR.PT	Protective Technology	2.6-x.x		78%	55%	73%	73%								
66%	64%	DETECT	DE.AE	Anomalies and Events	3.1-x.x		65%	67%	65%	57%	66%							
	66%		DE.CM	Security Continuous Monitoring	3.2-x.x		66%	79%	63%	59%	63%	62%	69%	67%				
	66%		DE.DP	Detection Processes	3.3-x.x		70%	65%	63%	68%	62%							
66%	66%	RESPOND	RS.AN	Analysis	4.1-x.x		66%	70%	62%	62%								
	63%		RS.CO	Communications	4.2-x.x		60%	60%	68%	74%	49%							
	60%		RS.IM	Improvements	4.3-x.x		53%	63%										
	65%		RS.MI	Mitigation	4.4-x.x		63%	63%	66%									
	73%		RS.RP	Response Planning	4.5-x.x		73%											
59%	54%	RECOVER	RC.CO	Communications	5.2-x.x		44%	44%	74%									
	63%		RC.IM	Improvements	5.3-x.x		72%	44%										
	60%		RC.RP	Recovery Planning	5.5-x.x		60%											

NIST Cybersecurity Framework Alignment to the Cybersecurity Workforce Framework



What is BRAAT?

- Bridging Risk Assessment and Analysis Totals (BRAAT)
  - A method to bring the operational security risk measurements of a configuration item (CI) to the perspective of management
  - Risk assessment and analysis with the fundamental elements
    - Uses FIPS 199/200 with the NIST RMF to measure each CI
    - Assessment shows if it is on or off
    - Analysis determines its risk in relation to the business operations
  - Beginning step at level 1 of a capability maturity model
    - It is the method in the Enterprise Security Profile Model
  - Receives input from other sources of risk management measurements
  - 3D block diagram showing the interactive layers of technology



http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/

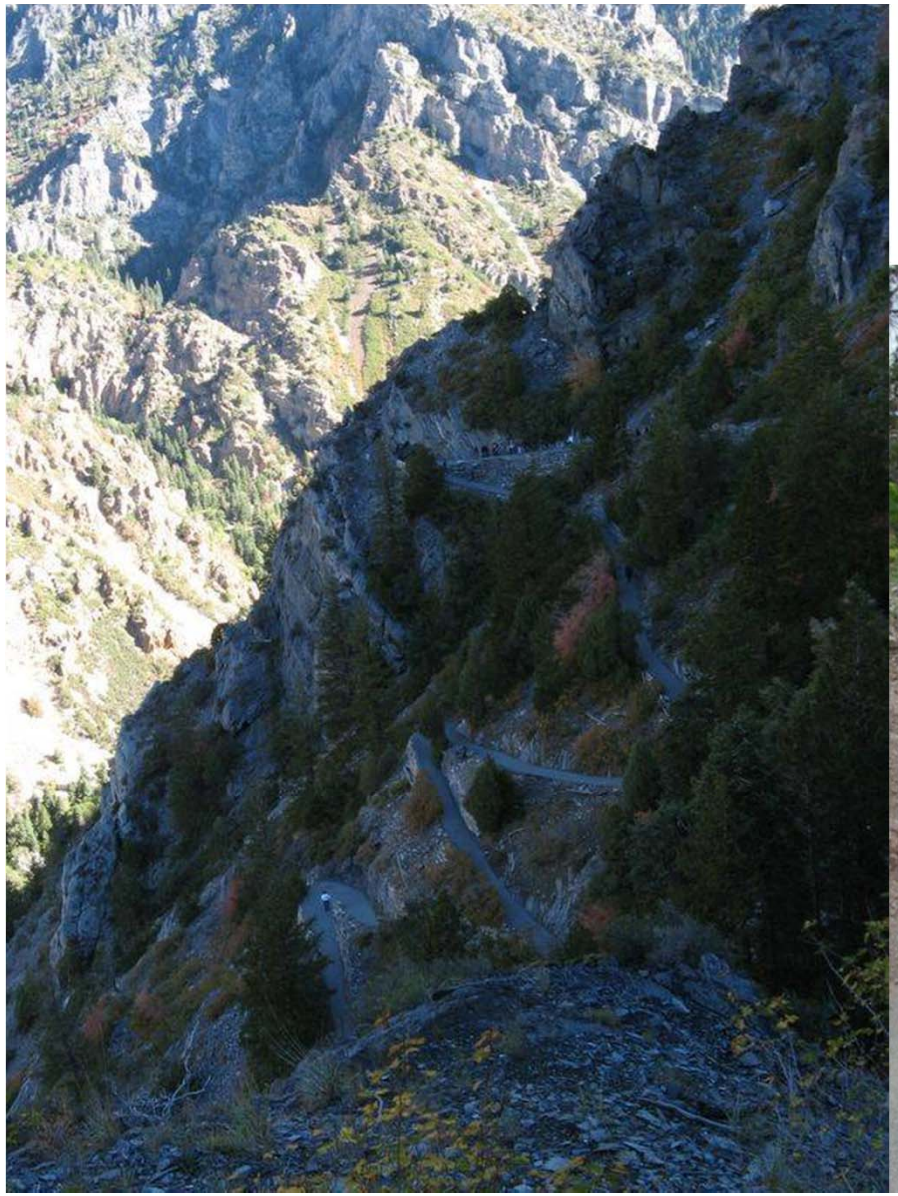
Features, Advantages and Benefits

- Input
  - Security Architecture
    - Supplier SIG
  - Compliance & Governance
  - Internal Controls
  - Control set definitions
  - External Auditors
  - Risk Management Framework
  - Operating companies

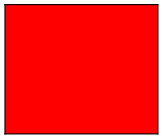
ESPM

- Output
  - Quantitative Metrics
  - Risk ranking
    - At risk vendors (RFP)
    - At risk suppliers
  - Quick auditing request results
  - Security policy with controls
  - Operational control list
    - SME checklist of controls
  - Allocation of resources to risks
  - Environmental perspective

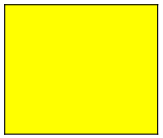
Perspective and control









Kent Pankratz, MSISA, CISSP

Kent strives to improve the alignment, measurement and metrics that are used by managers and administrators with an Enterprise Security Profile Model to maintain an advantage against adversaries that threaten an organization's valuable information.

He has a diverse employment history which includes implementing security solutions as a consultant, support engineer and security analyst across many industries for the last 20 years. His work includes implementing complex security systems, such as identity management and security information and event management.

Kent completed his Masters of Science of Information Security and Assurance (MSISA) at Norwich University in 2015 and is listed as an active Certified Information Systems Security Professional (CISSP) since 2012.

Contact Information

- Kent.Pankratz@amfam.com
- kent@veritysecurity.com
- 608-515-8849

Resources

- http://www.veritysecurity.com/resources
- https://www.linkedin.com/in/kentpankratz