RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

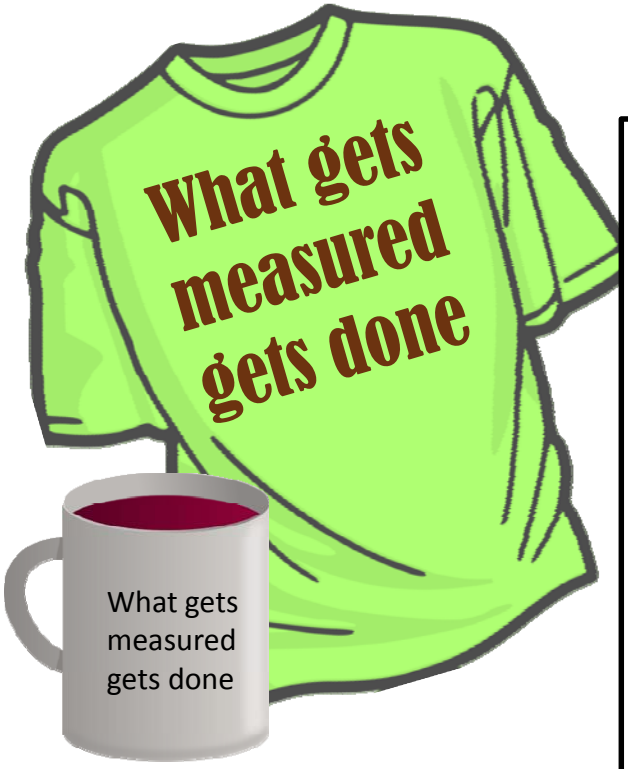
SESSION ID: GRC-R03F

Effectively Measuring Cybersecurity Improvement: A CSF Use Case

Greg Witte
Sr. Cybersecurity Engineer
G2, Inc.
@TheNetworkGuy

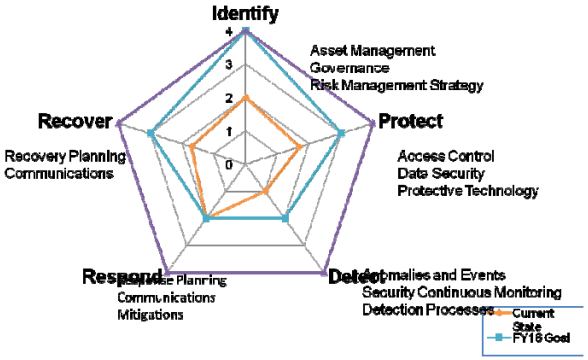
Tom Conkle
Cybersecurity Engineer
G2, Inc.
@TomConkle

Measuring the status of your cybersecurity program helps manage security goals



Cybersecurity Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)			
PROTECT (PR)			
DETECT (DE)			
RESPOND (RS)			
RECOVER (RC)			



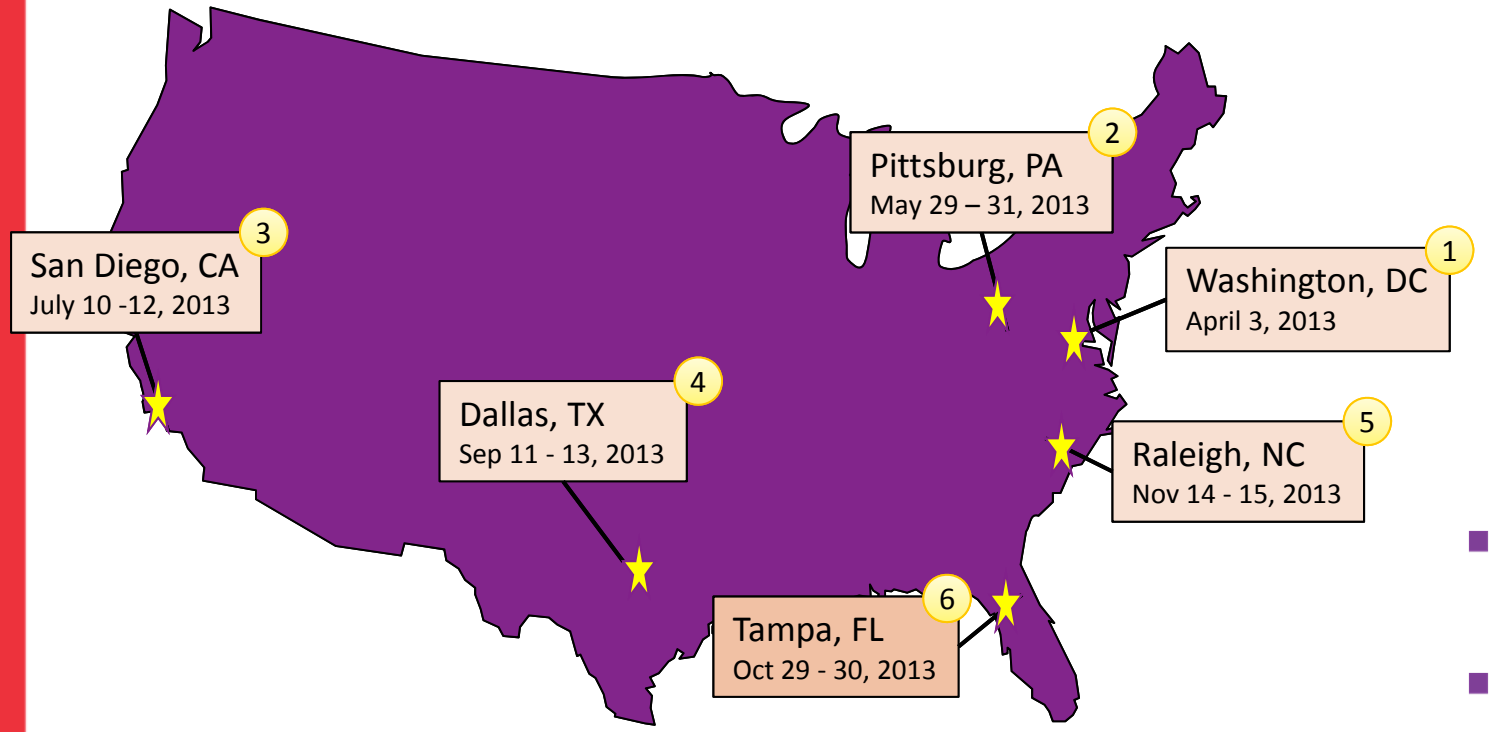
Agenda

- Cybersecurity Framework refresher
- Measuring your security program
- Now what you do with the metric

Executive Order 13636 asked for the creation of a Cybersecurity Framework for all sectors

- Executive Order Requirements
  - Be flexible
  - Be non-prescriptive
  - Leverage existing approaches, standards, practices
  - Be globally applicable
  - Focus on risk management vs. rote compliance
- Framework for Improving Critical Infrastructure Cybersecurity
  - Referred to as “The Framework”
  - Issued by NIST on February 12, 2014.

The Framework was developed in partnership among industry, academia and government



- NIST Conducted 5 workshops
- Released 3 RFIs

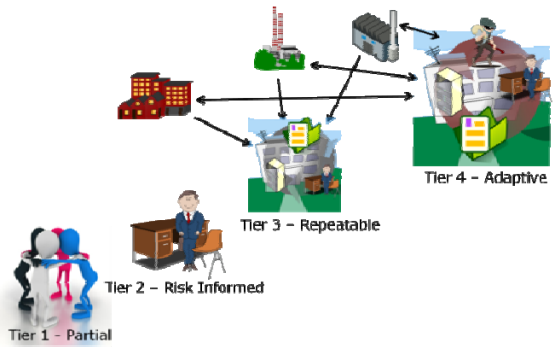
The Framework establishes three primary components

ILLUSTRATIVE

Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	COBIT 5 APO01.03, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	COBIT 5 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1 NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	CCS CSC 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-3: Physical access to assets is managed and protected	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3, 4.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 3.9, SR 6.2 (0), SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	CCS CSC 8 COBIT 5 DSS01.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	COBIT 5 BAI07.08 ISA 62443-2-1:4.4.3.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4

Implementation Tiers



Framework Profiles

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire	H				

The Framework Core establishes a common language

- Consists of 5 Functions
  - Identify, Protect, Detect, Respond, Recover
- Describes a set of cybersecurity activities, desired outcomes
- Includes references to industry proven standards
- Three levels (Function, Categories, and Subcategories) of fidelity

Framework Core

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

The subcategories describe expected outcomes

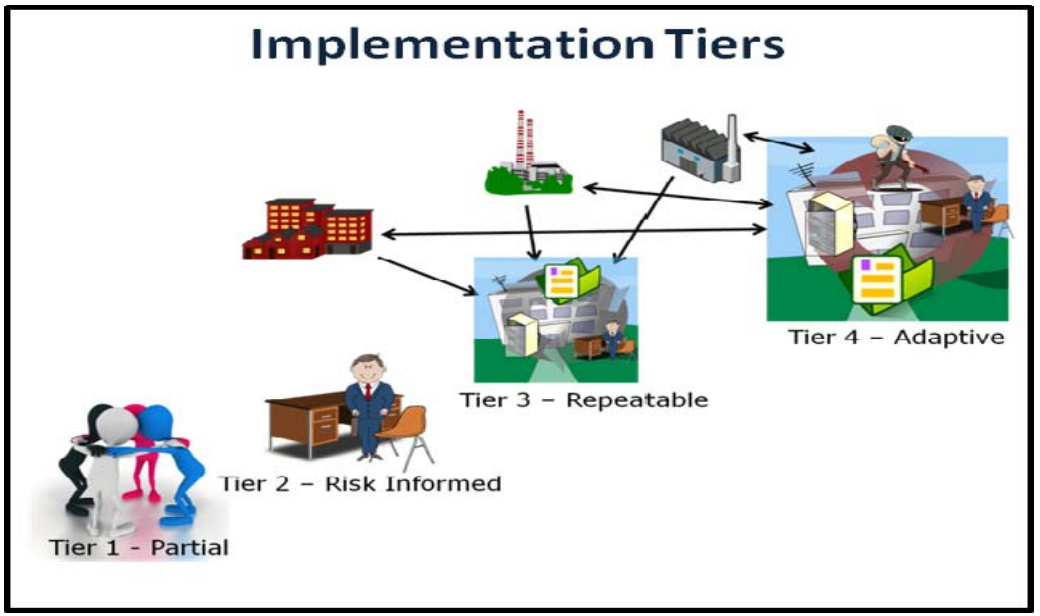
EXAMPLE

Framework Core

	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9

Organizations select a Implementation Tier based on their risk threshold

- Three attributes of Tiers:
  - Risk Management Process
  - Integrated Risk Management Program
  - External Participation



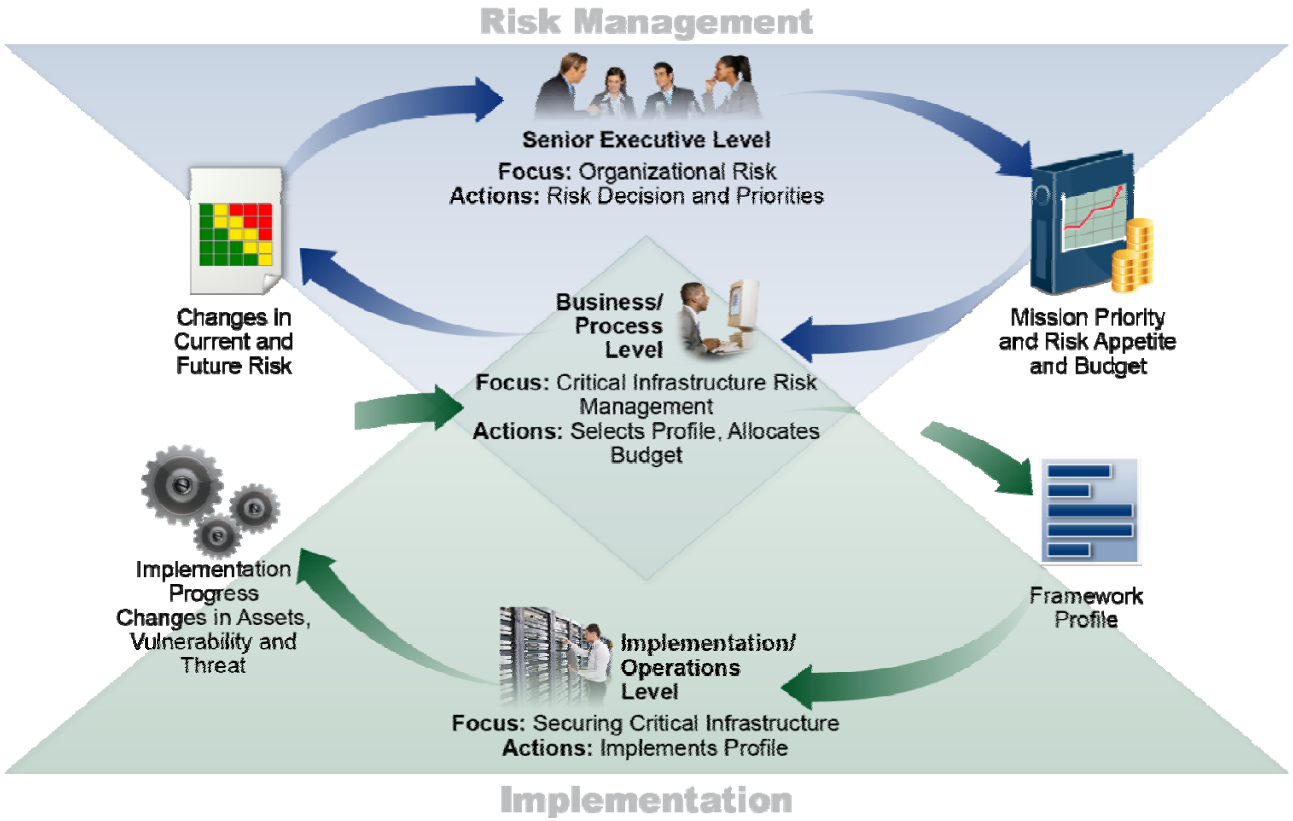
Tier 4 may not always be the goal

Profiles help organizations capture their cybersecurity program

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management: data, personnel, de… and facilities th… organization to a… purposes are identi… consistent with th… importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are	M				
		systems are catalog…					
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and …	H				

CURRENT PROFILE EXAMPLE

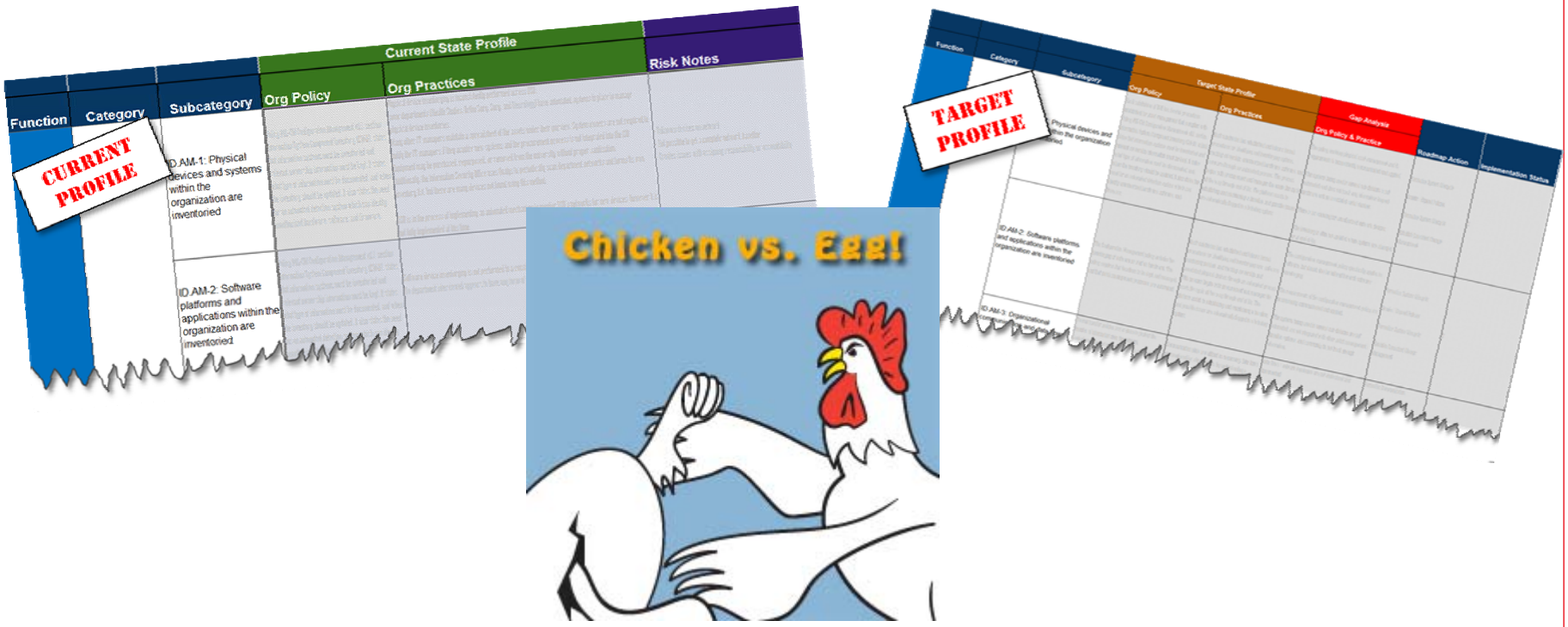
The Framework establishes a common language for cybersecurity



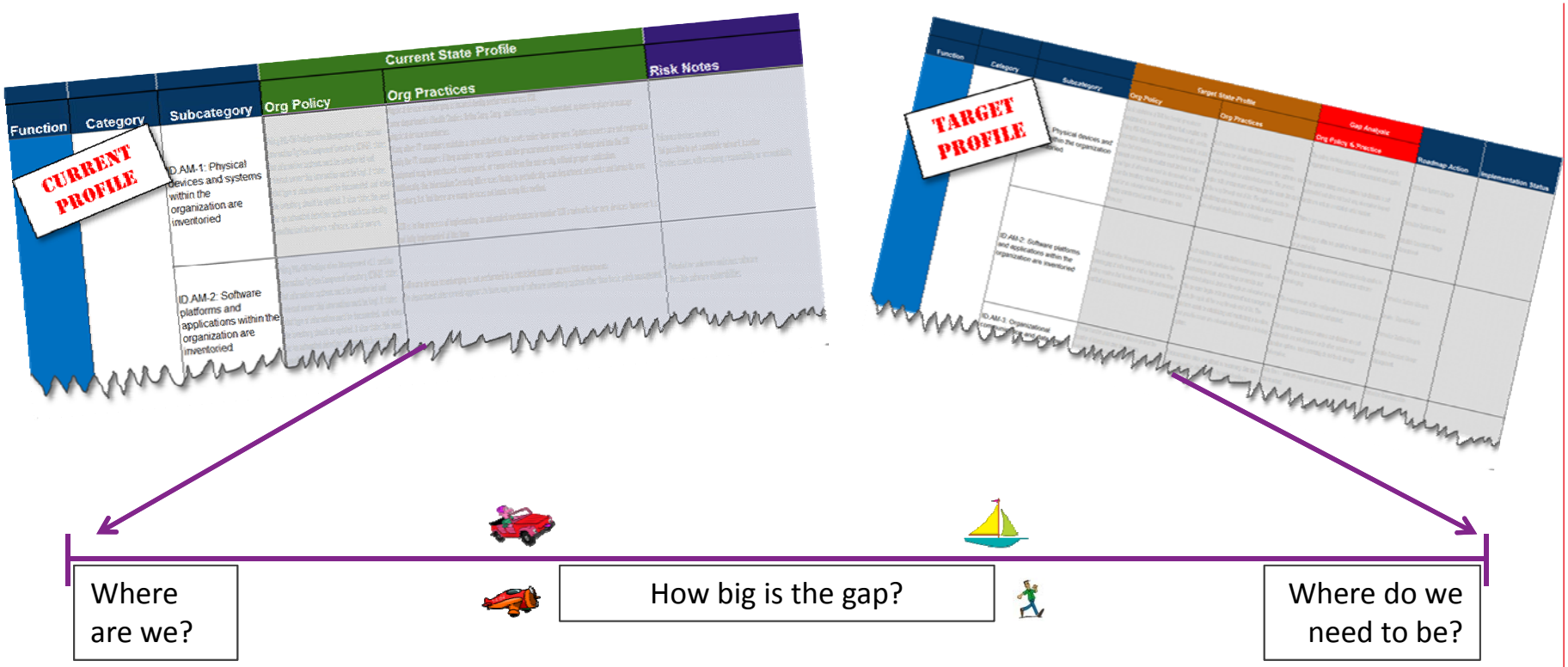
The Framework identifies seven steps for developing/improving a cybersecurity program

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan (Build a Roadmap)

Where you start is less important than the accuracy of the information recorded

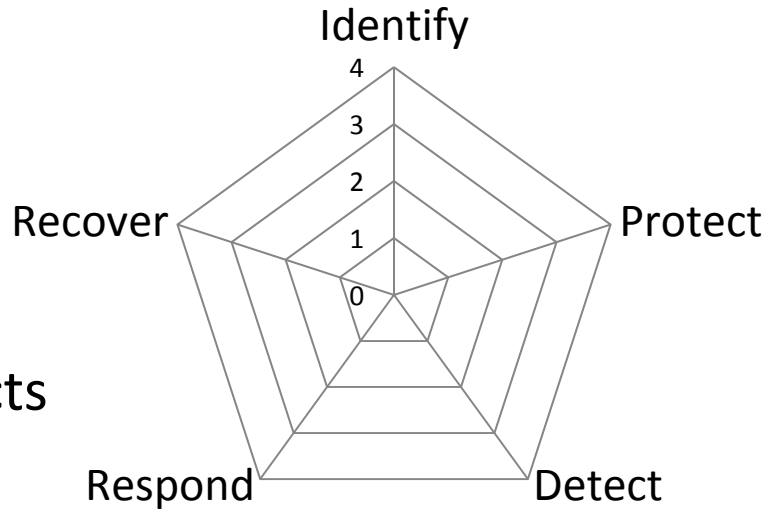


Artifacts generated from implementing the Framework aide is establishing metrics

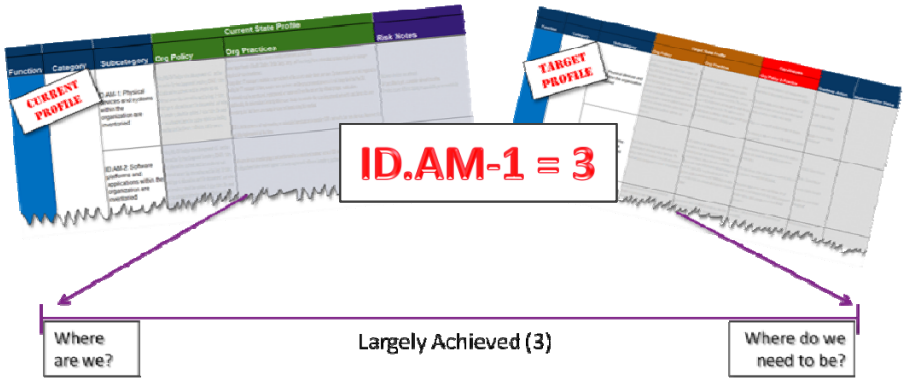


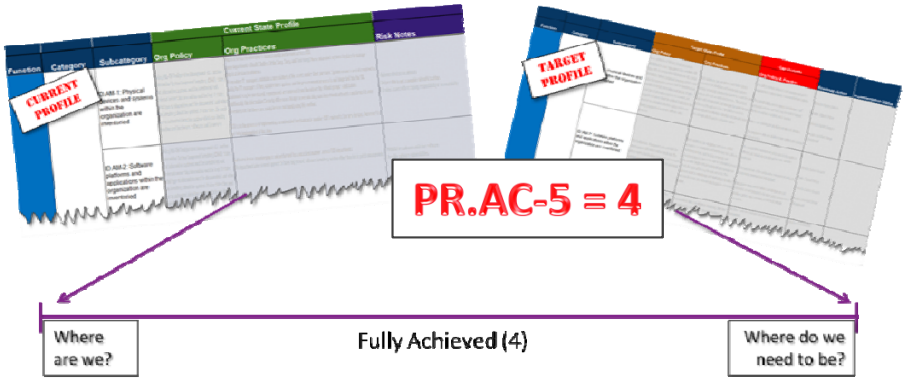
ISO 15504 establishes a standard that can be leveraged to measure the gap

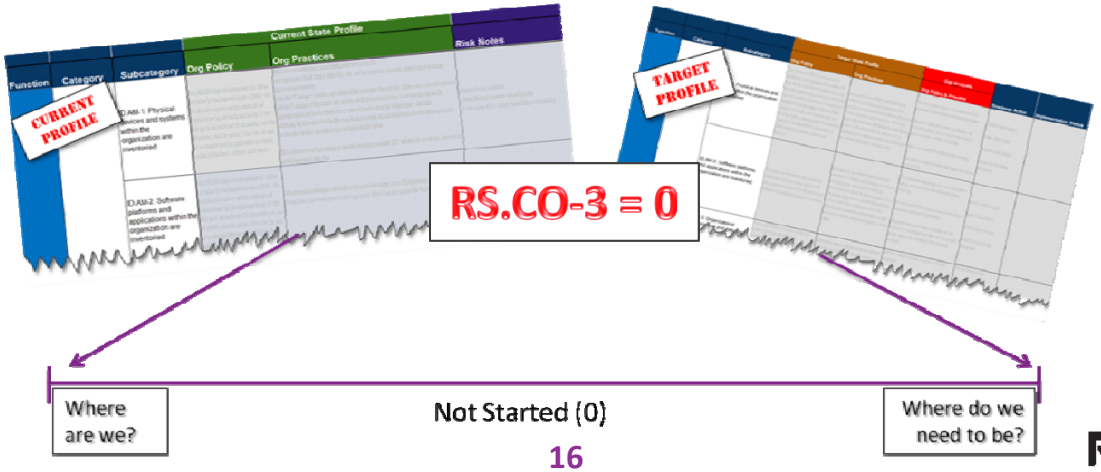
- ISO 15504 Achievement Status
  - Not achieved (1% - 15%)
  - Partially achieved (>15% - 50%)
  - Largely achieved (>50%- 85%)
  - Fully achieved (>85% - 100%)
- A fifth (5) level was added for projects that were not started
- A scale from 0 – 4 was aligned to the ratings



ISO 15504 achievement rating can be applied to the gaps

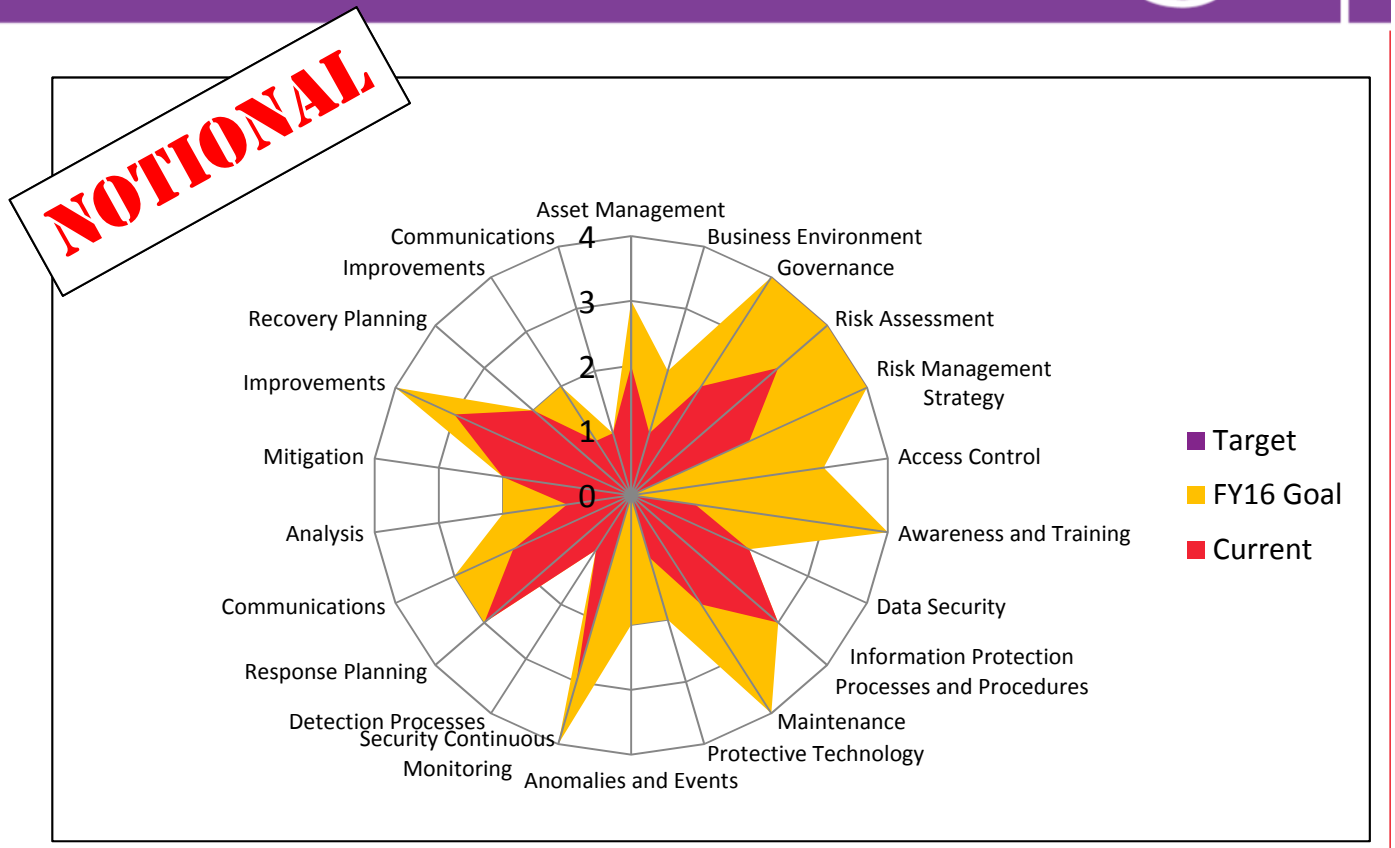






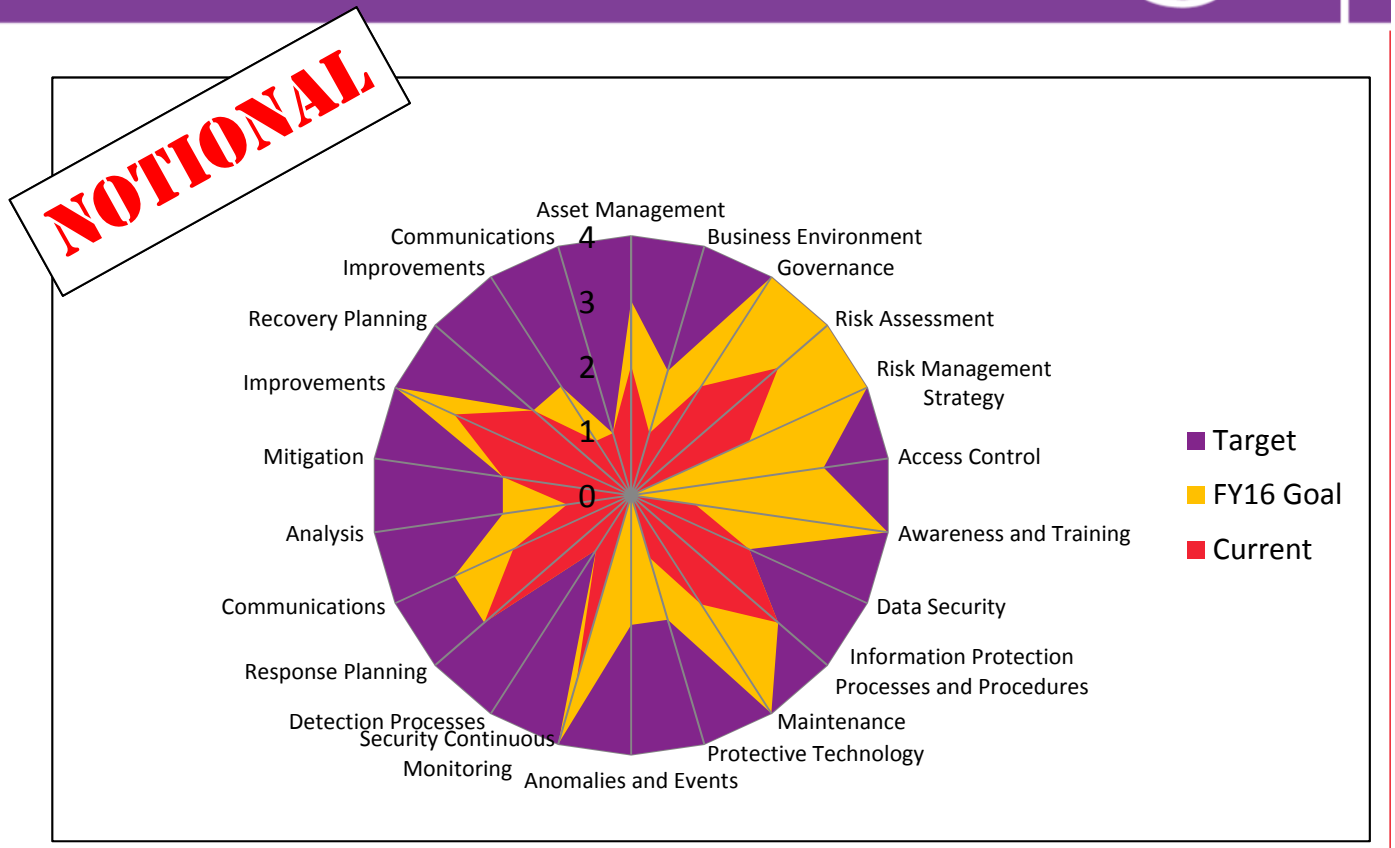
The gaps can be summarized at the Function or Category level

#	Rating
0	Not Started
1	Not Achieved
2	Partially Achieved
3	Largely Achieved
4	Fully Achieved

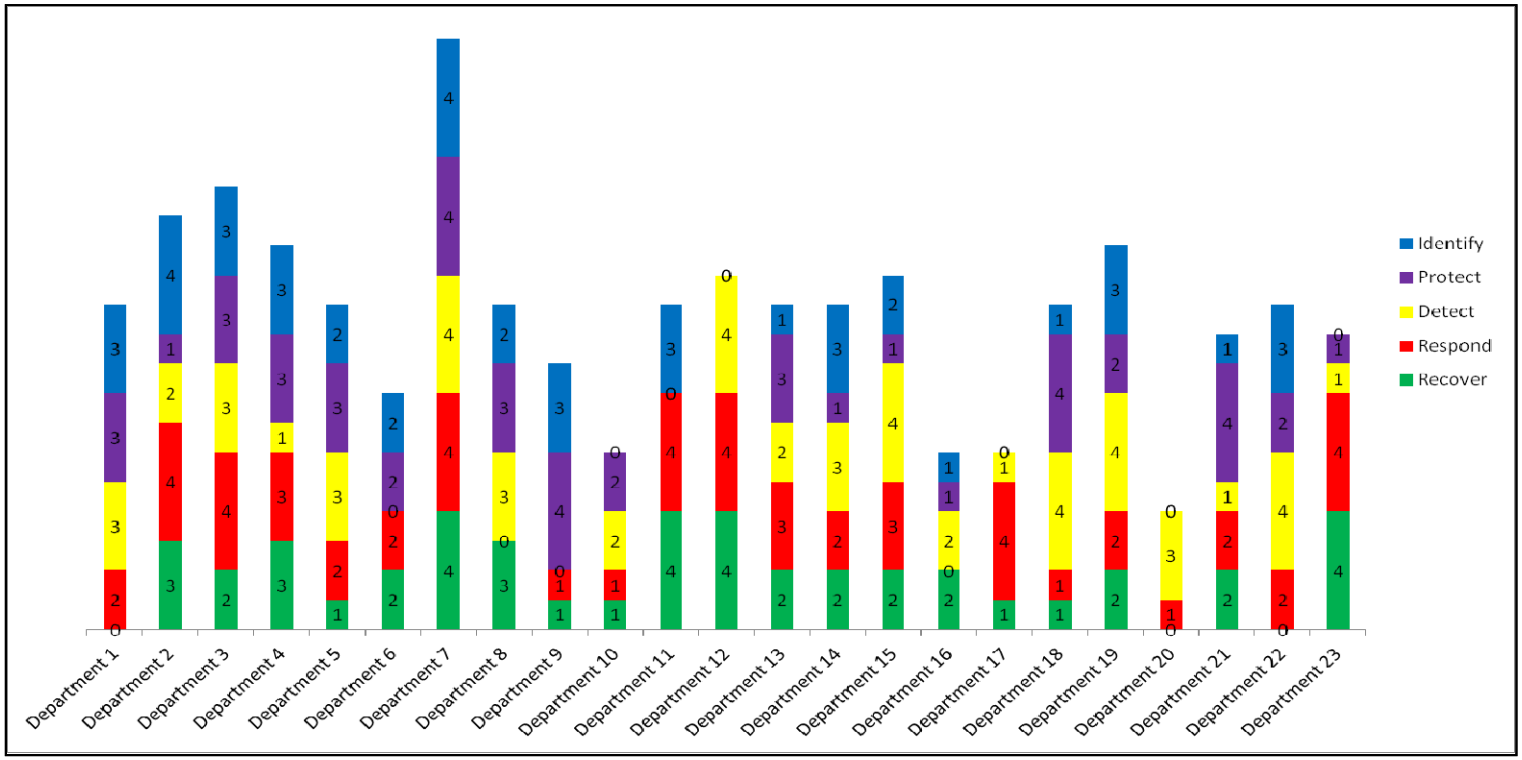


Progress can be measured as the Target State Profile objectives are obtained

#	Rating
0	Not Started
1	Not Achieved
2	Partially Achieved
3	Largely Achieved
4	Fully Achieved

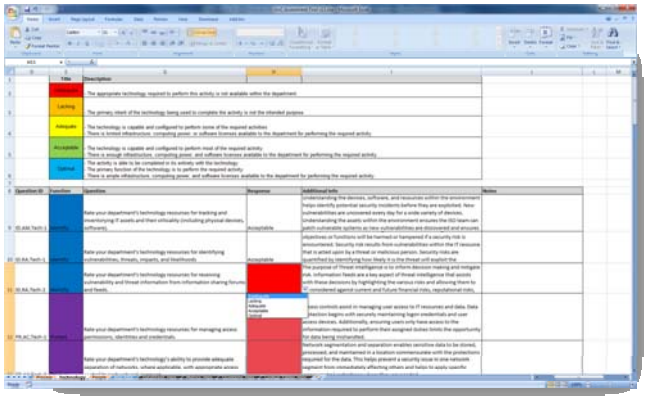


The status of departments security program can be measured using the standard



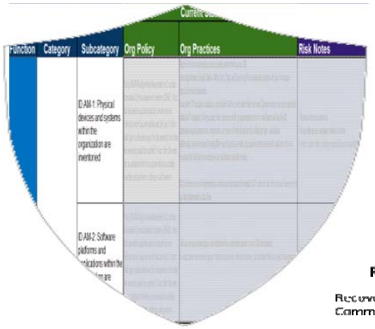
Internal assessment provide monitor continuous improvement

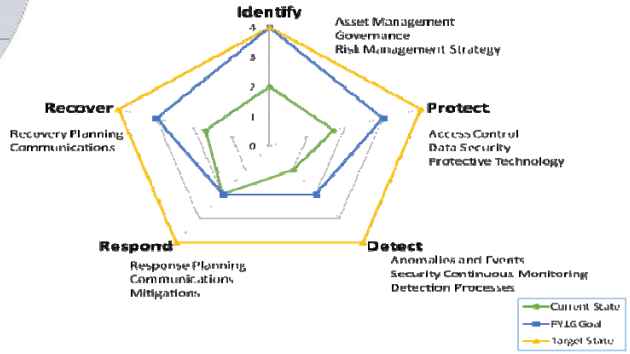
- Developed a survey for all departments to complete
- The survey monitored departments progress towards achieving the outcomes described in the Target State Profile
- Each option represented progress towards their gap closing activity

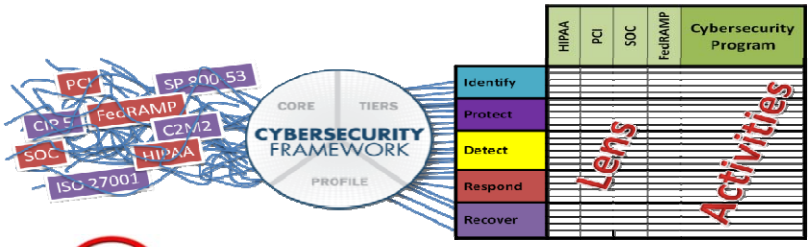


There are several benefits for using the Cybersecurity Framework

- Common Language
- Collaboration Opportunities
- Easily Maintain Compliance
- Ability to Demonstrate Due Care
- Secure Supply Chain
- Measuring Cybersecurity Status
- Cost Efficiency







Rote Compliance ≠ Secure

There are several resources available to help you use the Framework

- Government Programs
  - Department of Homeland Security's C3 Voluntary Program
  - NIST Industry Resources
- Internet Resource Centers
  - Cybersecurity Framework (CForum)

You can apply the Framework to track improvements in your security program

- Next week you should:
  - Determine how the Framework can be used in your organization to measure improvements to the security program
- In the first three months following this presentation you should:
  - Begin having discussions within your organization on your Current state
  - Apply the Cybersecurity Framework to develop/improve a risk-based cybersecurity program for your organization
- Within six months you should:
  - Be able to continually monitor your progress towards achieving Target state outcomes

Q&A

We are available if you have additional questions

Greg Witte
Senior Security Engineer
Greg.Witte @G2-inc.com
(301) 346-2385

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@G2-inc.com
(443) 292-6679

Where are we?

Not Started (0)

Where do we need to be?