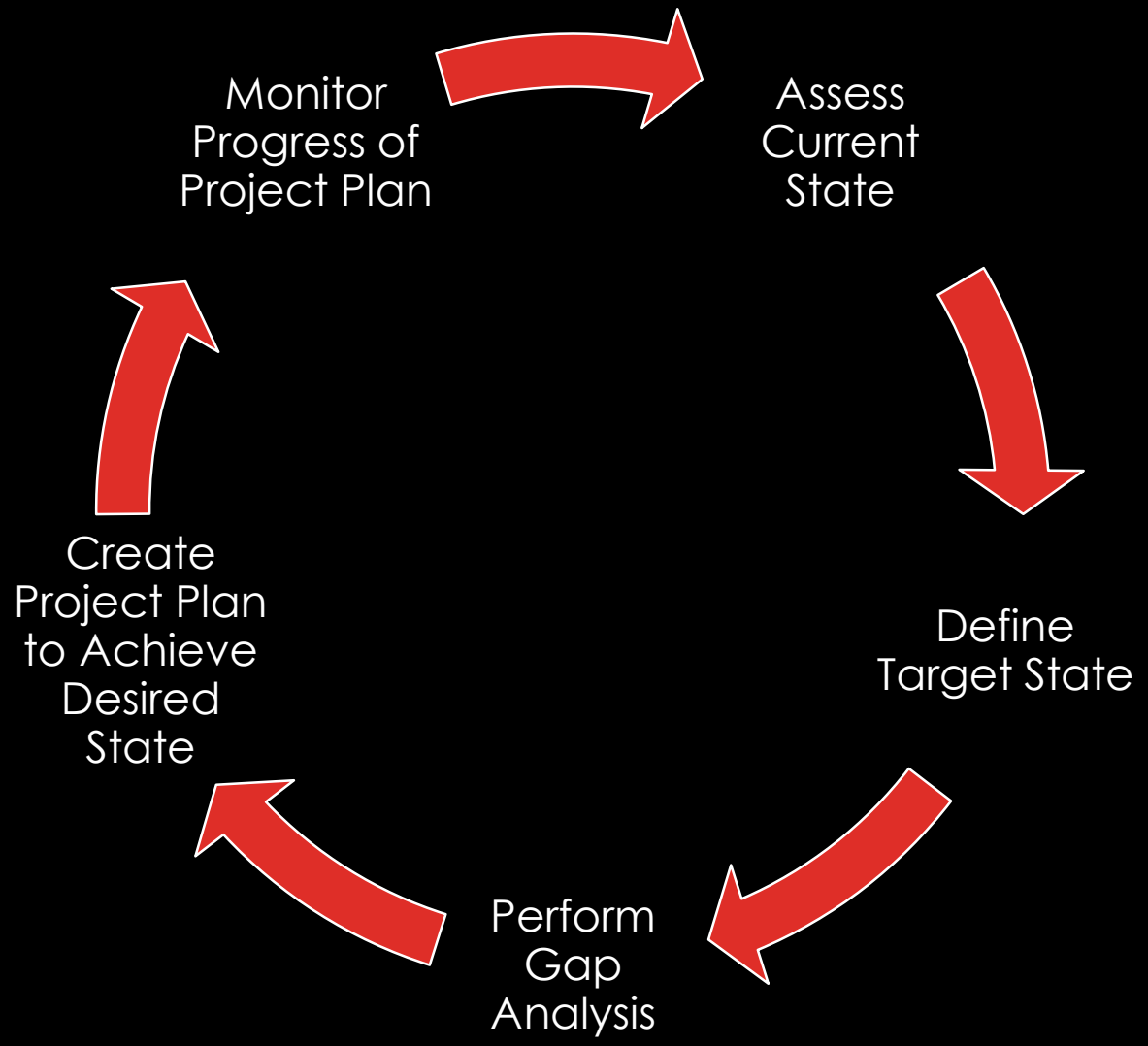
NIST CYBERSECURITY FRAMEWORK

JD Rogers – CISO American Financial Group

LEGAL DISCLAIMER

The following presentation is for information and discussion purposes only. Any views or opinions expressed are the speakers'; shall not be construed as legal advice; and do not necessarily reflect any corporate position, opinion or view of American Financial Group, Inc., or its affiliates, or a corporate endorsement, position or preference with respect to any contractual terms and provision or any related issues. If you have any questions or issues of a specific nature, you should consult appropriate legal or regulatory counsel to review the specific circumstances involved.

NIST OVERVIEW



NIST OVERVIEW

- Identify
  - Find out what you have and what's important
- Protect
  - Build controls to protect and mitigate risks
- Detect
  - Watch for bad things to happen
- Respond
  - Re-act and deal with bad things happening
- Recover
  - Put things back to a good state after issues occur

NIST OVERVIEW

- Tiers
  - 1 - Partial
  - 2 – Risk Informed
  - 3 - Repeatable
  - 4 - Adaptive

NIST OVERVIEW

Identify	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established
	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	ID.GV-1: Organizational information security policy is established
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

PHASE 1

NIST Implementation Tier	Maturity Level	Maturity Definition	Easy-to-Understand Maturity
1	0	Non-Existent	Never Heard of It
	1	Initial	Heard of it. Pilot. Proof of Concept
2	2	Repeatable	A process is in place but not formalized
	3	Defined	A process is in place and is formalized
3	4	Managed	Ad hoc reporting, self audits/Management Monitored
4	5	Optimized	Automated/Reviewed and improved

PHASE 1

- Governance
  - Buy in from BoD, Exec, Management
  - 3rd Party
  - Metrics
  - Acquisitions and Divestitures
- Information Technology
  - Business
  - Leadership
  - Data management
  - Personnel

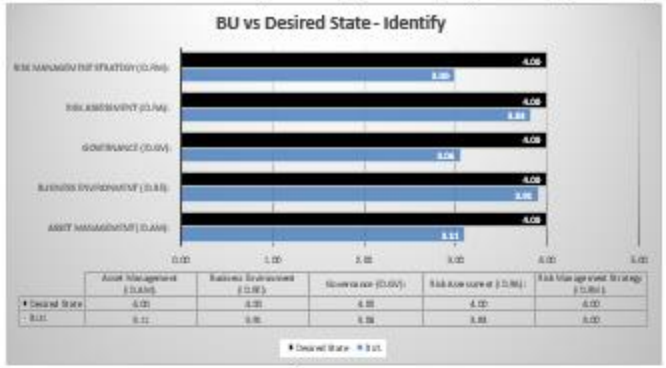
PHASE 1

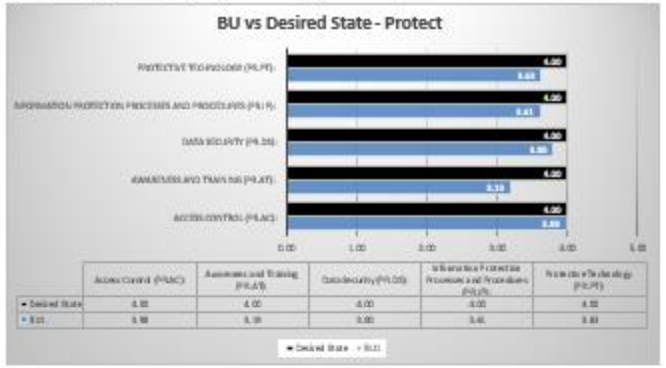
Identify	ID.BE-1: The organization's role in the supply chain is identified and communicated	Out of Scope	
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Out of Scope	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Priorities for each BU's mission, objectives, and activities are established at the enterprise level, documented, and communicated across the company.	
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Specific functions around technology, which are critical to the success of the BU, have been defined and plans are in place to understand any dependencies of those functions and ensure they are maintained adequately.	
	ID.BE-5: Resilience requirements to support delivery of critical services are established	Requirements to maintain support of critical services are documented. Key stakeholders are identified, and adequate resources (people, funding, & tools) are provided to support the process.	
	ID.GV-1: Organizational information security policy is established	There is an enterprise-wide security policy, which all employees are responsible for reading and signing off on annually. Education includes a mechanism to measure understanding of the policy.	
	ID.GV-2: Information security roles &	Business Unit Management aligns their security priorities with the EISG roadmap and prioritizes resources to meet agreed upon deadlines.	

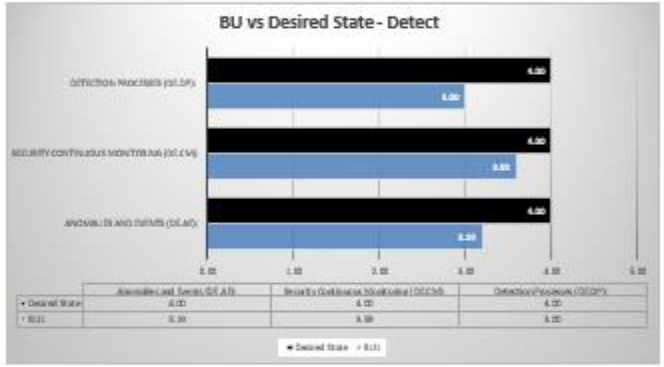
PHASE 1 - INTERVIEWS

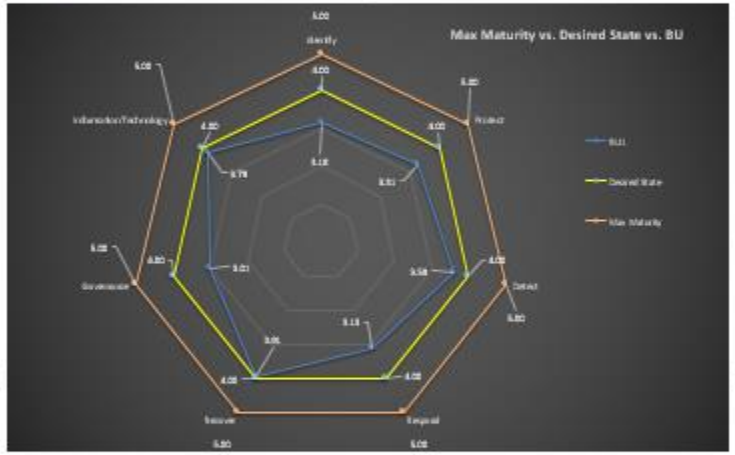
Function	Category	BU4	BU2	BU3	BU4	BU5	BU6	BU7	BU8	Average for Company
Identify	Asset Management (ID.AM):	3.53	4.00	3.33	3.67	3.08	2.70	2.48	2.48	3.16
	Business Environment (ID.BE):	3.00	2.33	4.67	2.67	2.47	2.40	2.03	2.03	2.70
	Governance (ID.GV):	3.46	3.38	3.45	2.69	2.50	2.34	2.67	2.67	2.90
	Risk Assessment (ID.RA):	3.47	3.20	2.40	3.60	2.60	2.28	2.48	2.48	2.81
	Risk Management Strategy **(ID.RM):**	3.00	4.33	2.33	4.00	3.47	2.97	2.77	2.77	3.20
Protect	Access Control (PR.AC):	3.40	3.25	3.00	3.50	2.63	2.23	2.40	2.40	2.85
	Awareness and Training (PR.AT):	2.80	3.80	2.20	4.00	3.40	2.94	2.78	2.78	3.09
	Data Security (PR.DS):	3.47	3.00	3.43	3.29	3.79	3.07	2.27	2.84	3.15
	Information Protection Processes and Procedures (PR.IP):	3.41	3.50	2.83	2.95	2.46	2.20	2.47	2.47	2.78
	Maintenance (PR.MA):	3.41	3.36	2.91	3.09	2.59	2.36	2.27	2.27	2.78
	Protective Technology (PR.PT):	3.50	2.67	2.67	3.00	2.33	2.33	2.67	2.67	2.73
Detect	Anomalies and Events (DE.AE):	3.94	4.00	3.40	3.00	2.90	2.66	2.42	2.42	3.09
	Security Continuous Monitoring (DE.CM):	3.23	2.88	2.38	3.25	2.94	2.64	2.29	2.79	2.80
	Detection Processes (DE.DP):	3.40	2.80	4.40	3.00	3.00	2.94	2.28	2.48	3.04
Respond	Response Planning (RS.RP):	4.00	4.00	4.00	5.00	4.00	5.00	3.00	3.00	4.00
	Communications (RS.CO):	3.80	3.80	4.20	3.80	3.50	3.48	3.46	3.06	3.64
	Analysis (RS.AN):	4.60	3.40	3.40	2.80	2.20	2.44	4.98	4.98	3.60
	Mitigation (RS.MI):	4.00	4.00	3.67	3.00	2.83	2.50	2.47	2.47	3.12
	Improvements (RS.IM):	3.00	2.50	2.50	2.50	3.00	2.50	3.00	3.00	2.75
Recover	Recovery Planning (RC.RP):	3.00	5.00	2.00	5.00	4.00	5.00	2.00	2.00	3.50
	Improvements (RC.IM):	3.50	3.00	4.50	2.50	4.50	4.80	4.85	4.85	4.06
	Communications (RC.CO):	3.67	3.33	3.67	3.33	3.67	4.00	3.00	3.33	3.50
Governance	Board of Directors (GV.BD):	2.47	3.00	4.67	4.00	3.75	3.35	4.25	4.25	3.72
	Executive Management (GV.EM):	3.00	3.00	4.00	3.00	2.00	2.73	2.47	2.47	2.83
	Management (GV.MG):	2.00	2.75	3.00	2.25	2.75	3.30	3.60	3.60	2.91
	Third Parties (GV.TP):	4.00	2.50	3.50	0.50	0.25	4.00	4.00	4.00	2.84
	Acqu / Divest (GV.AD):	4.00	3.00	3.00	2.00	3.00	3.30	2.47	2.47	2.90
	System Onboarding (GV.SO):	4.38	2.65	4.92	2.23	2.65	2.71	2.58	2.58	3.09
	Metrics (GV.MC):	3.33	2.33	2.33	0.67	4.33	4.23	4.43	4.43	3.26
Information Technology	Business (IT.BU):	4.00	4.00	4.00	3.00	3.00	2.70	2.40	2.40	3.19
	Leadership Team (IT.LT):	2.00	4.00	0.67	2.33	2.47	2.33	2.50	2.50	2.35
	Development (IT.DV):	2.67	2.22	2.00	4.56	2.00	2.47	2.44	2.44	2.60
	Personnel (IT.PR):	3.00	2.20	2.20	4.00	4.60	4.48	4.36	4.36	3.65
	Data Management (IT.DM):	2.20	2.20	2.80	2.60	2.90	3.08	3.26	3.26	2.79

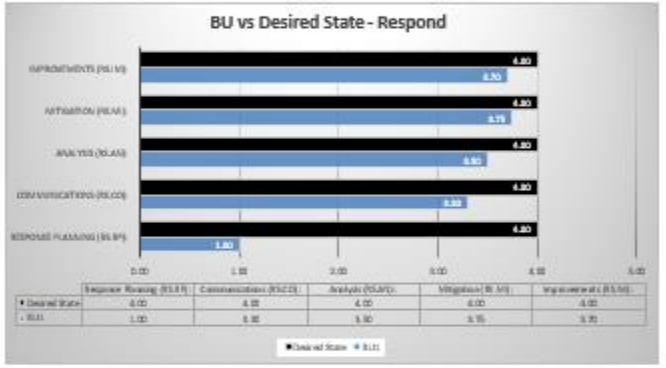
PHASE 1

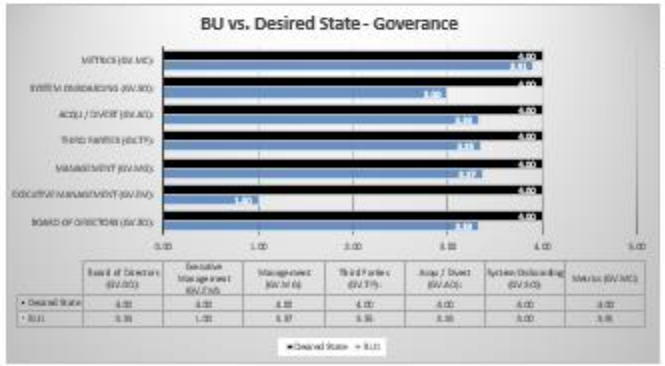

BU vs Desired State - Identify

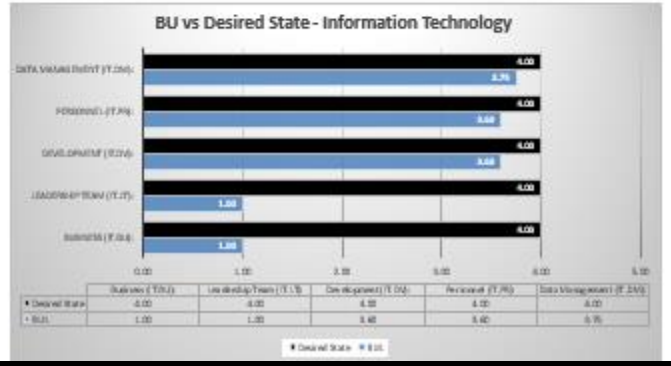

BU vs Desired State - Protect

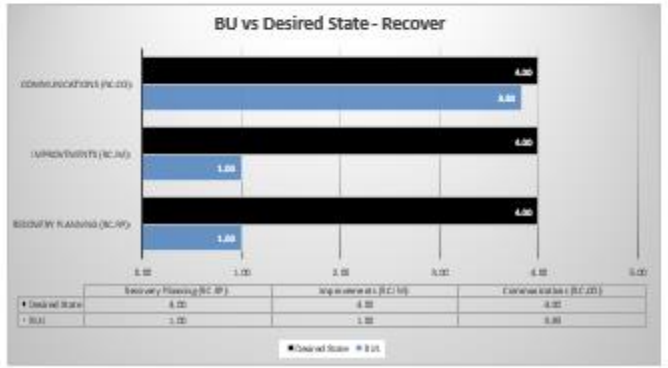

BU vs Desired State - Detect


Max Maturity vs. Desired State vs. BU


BU vs Desired State - Respond

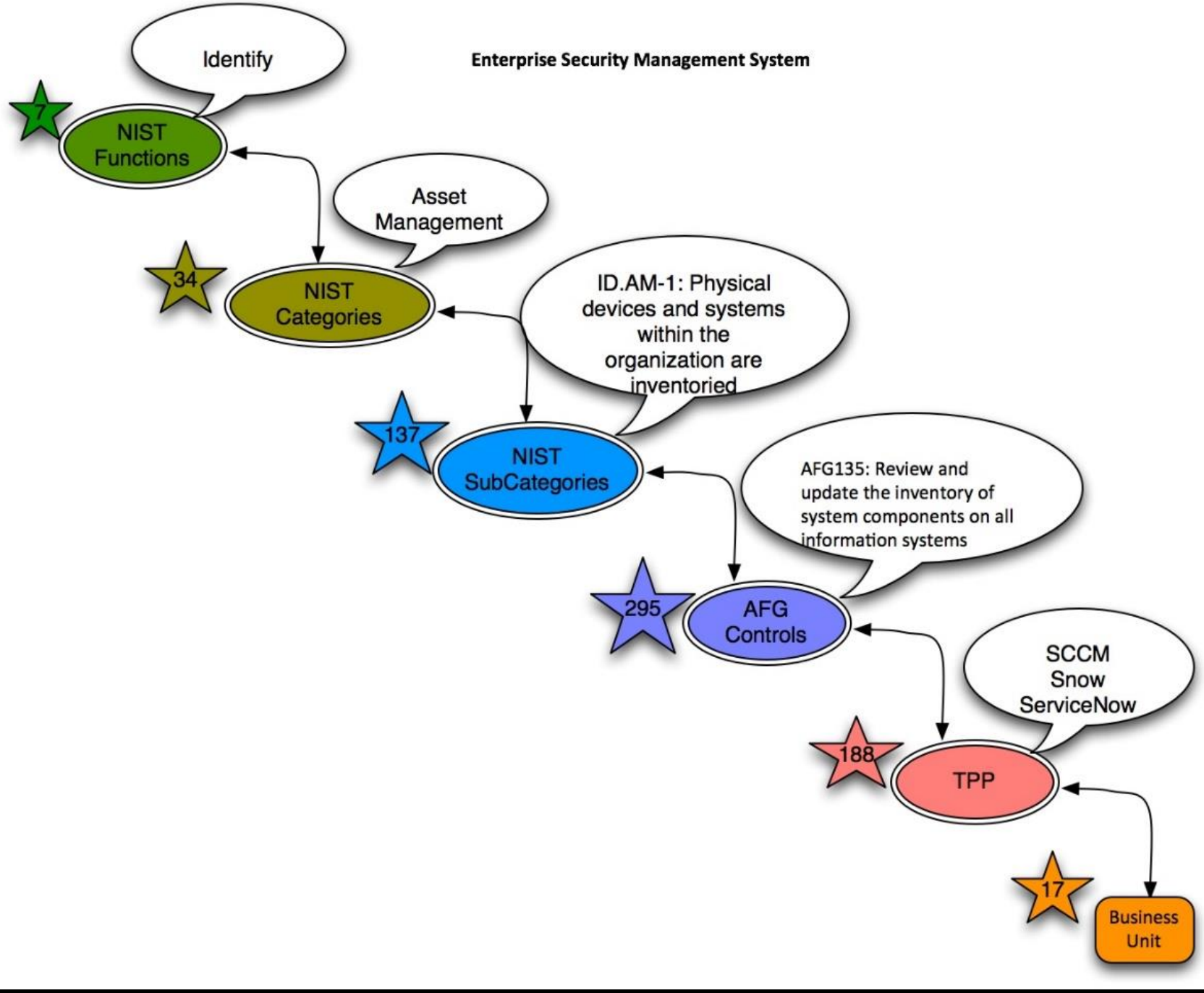

BU vs. Desired State - Goverance


BU vs Desired State - Information Technology


BU vs Desired State - Recover

PHASE 1

- 6 to 8 month process
- Internal Audit
- Security
- BU IT
- Not very repeatable
- Trust but verify
- The data generated more questions

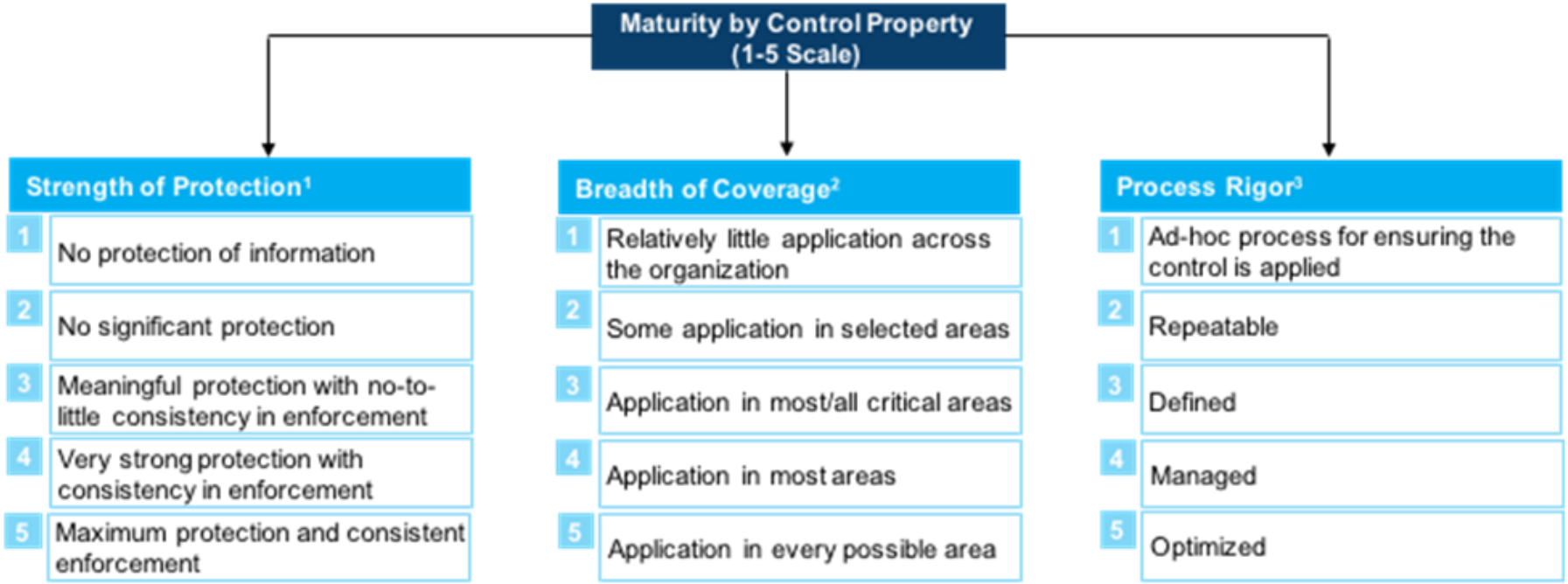


PHASE 2

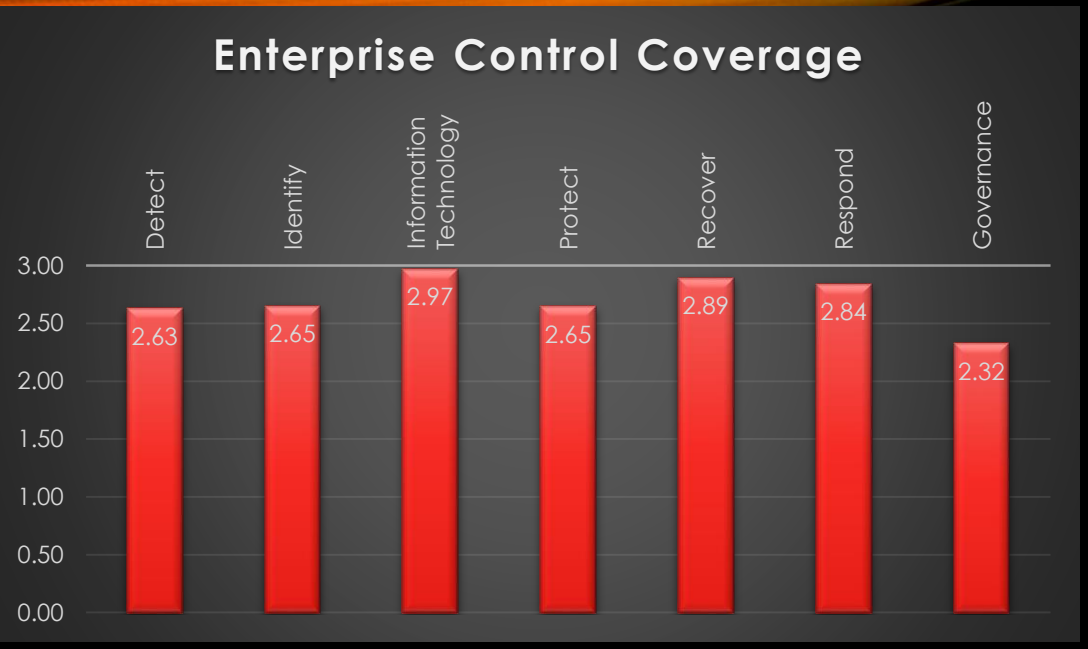
- TPP
  - Technology
  - People
  - Process

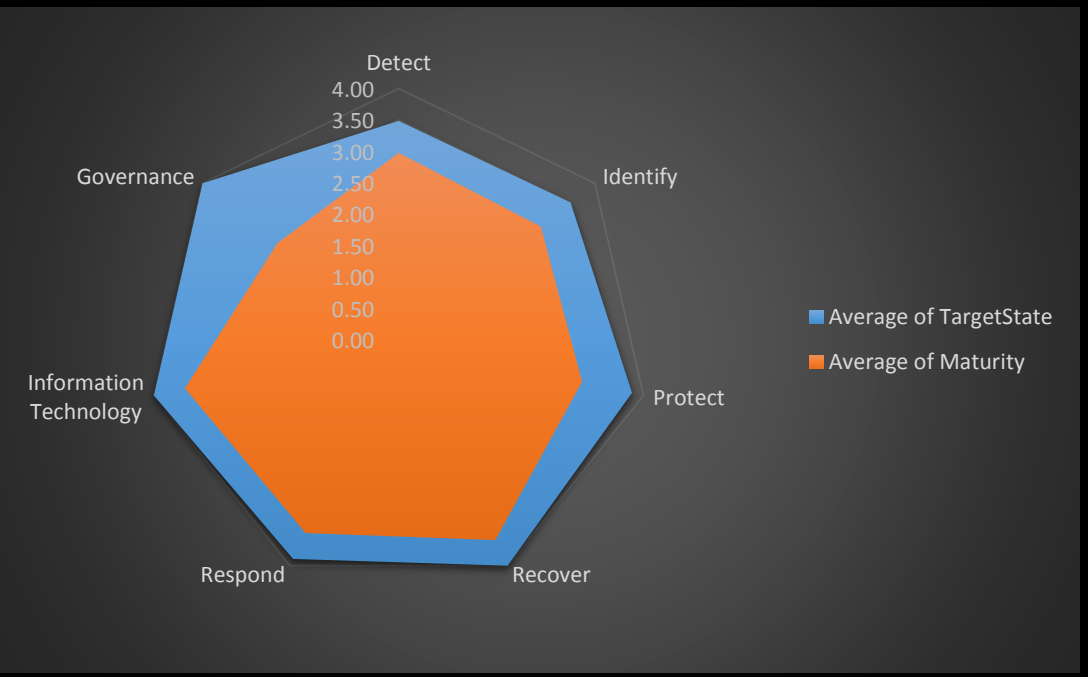
- Maturity
- Control Coverage

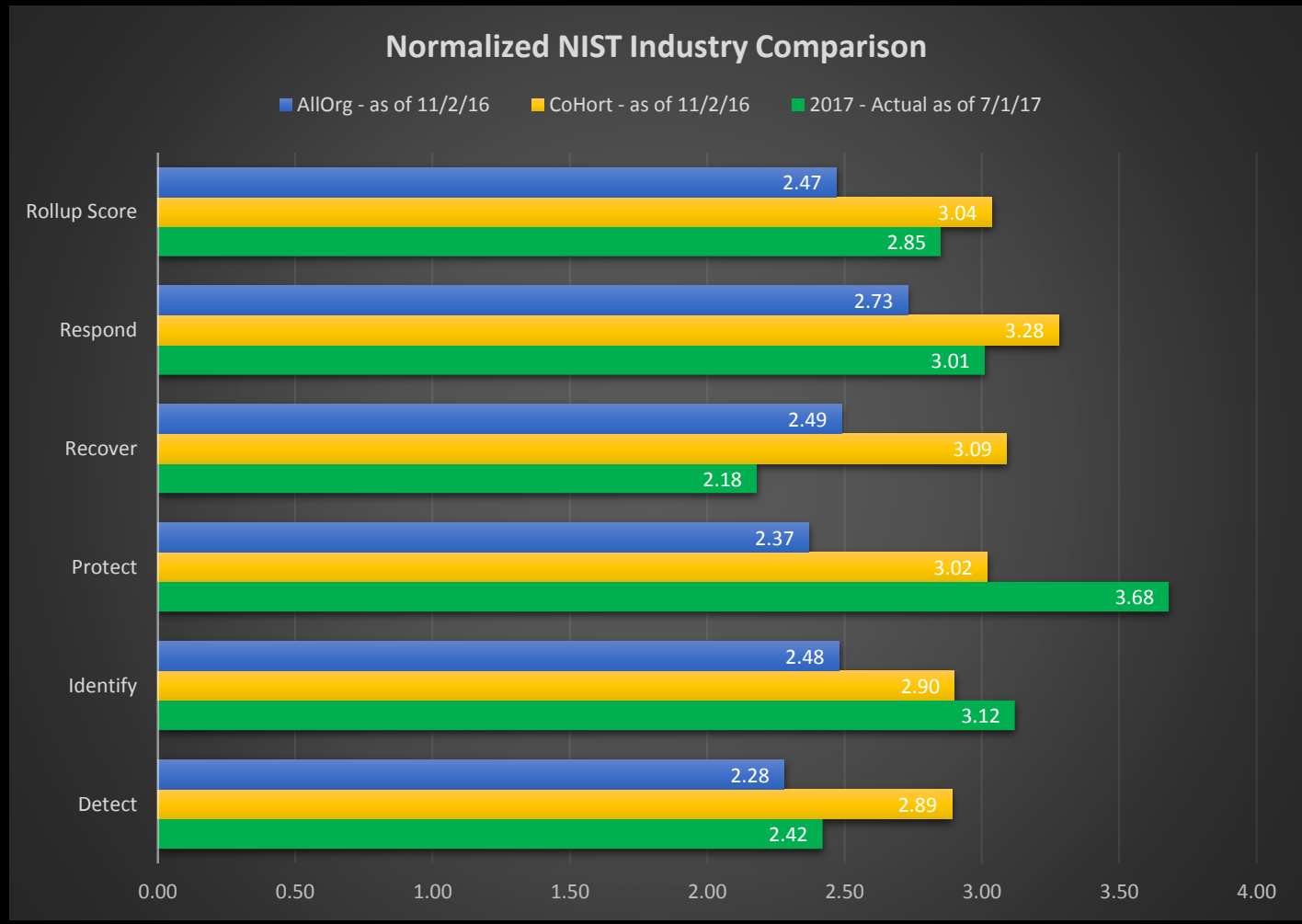
AFG PHASE 2


Maturity by Control Property (1-5 Scale)
Strength of Protection[1]
1 No protection of information
2 No significant protection
3 Meaningful protection with no-to-little consistency in enforcement
4 Very strong protection with consistency in enforcement
5 Maximum protection and consistent enforcement
Breadth of Coverage[2]
1 Relatively little application across the organization
2 Some application in selected areas
3 Application in most/all critical areas
4 Application in most areas
5 Application in every possible area
Process Rigor[3]
1 Ad-hoc process for ensuring the control is applied
2 Repeatable
3 Defined
4 Managed
5 Optimized

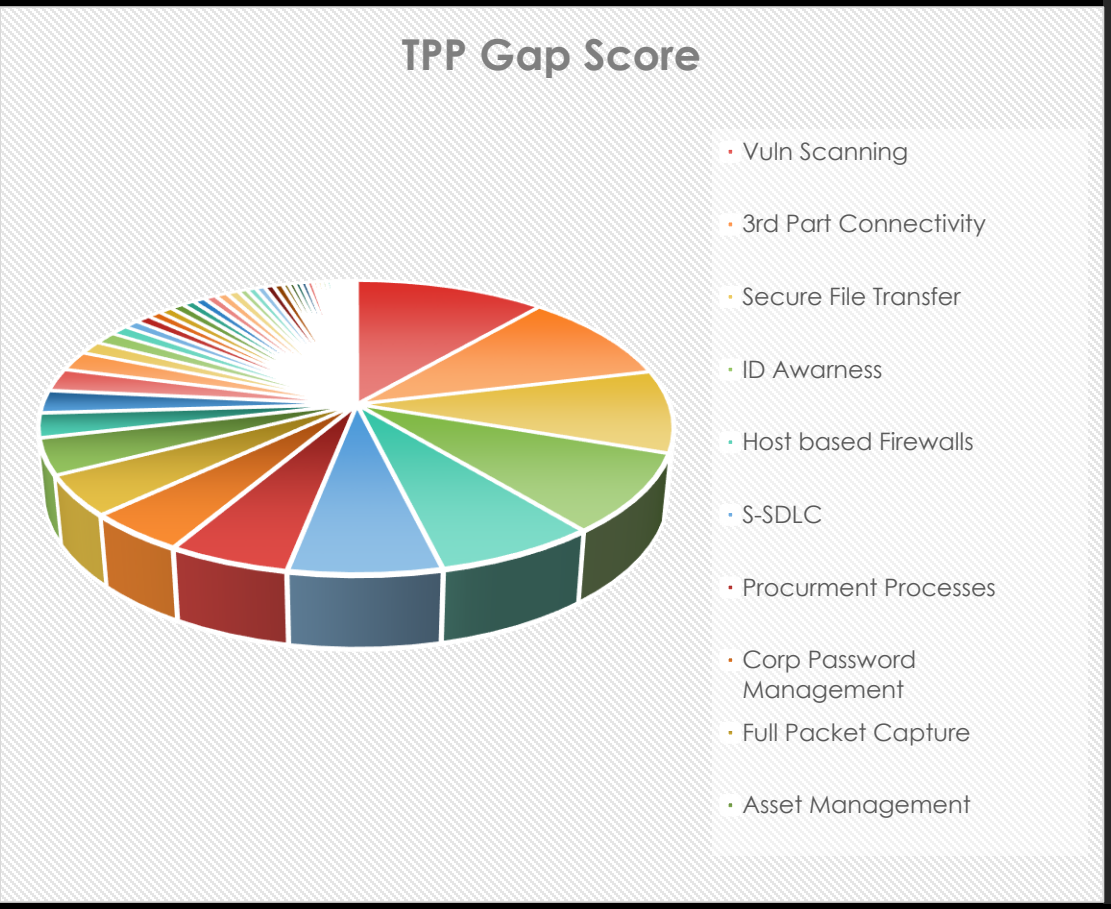
PHASE 2

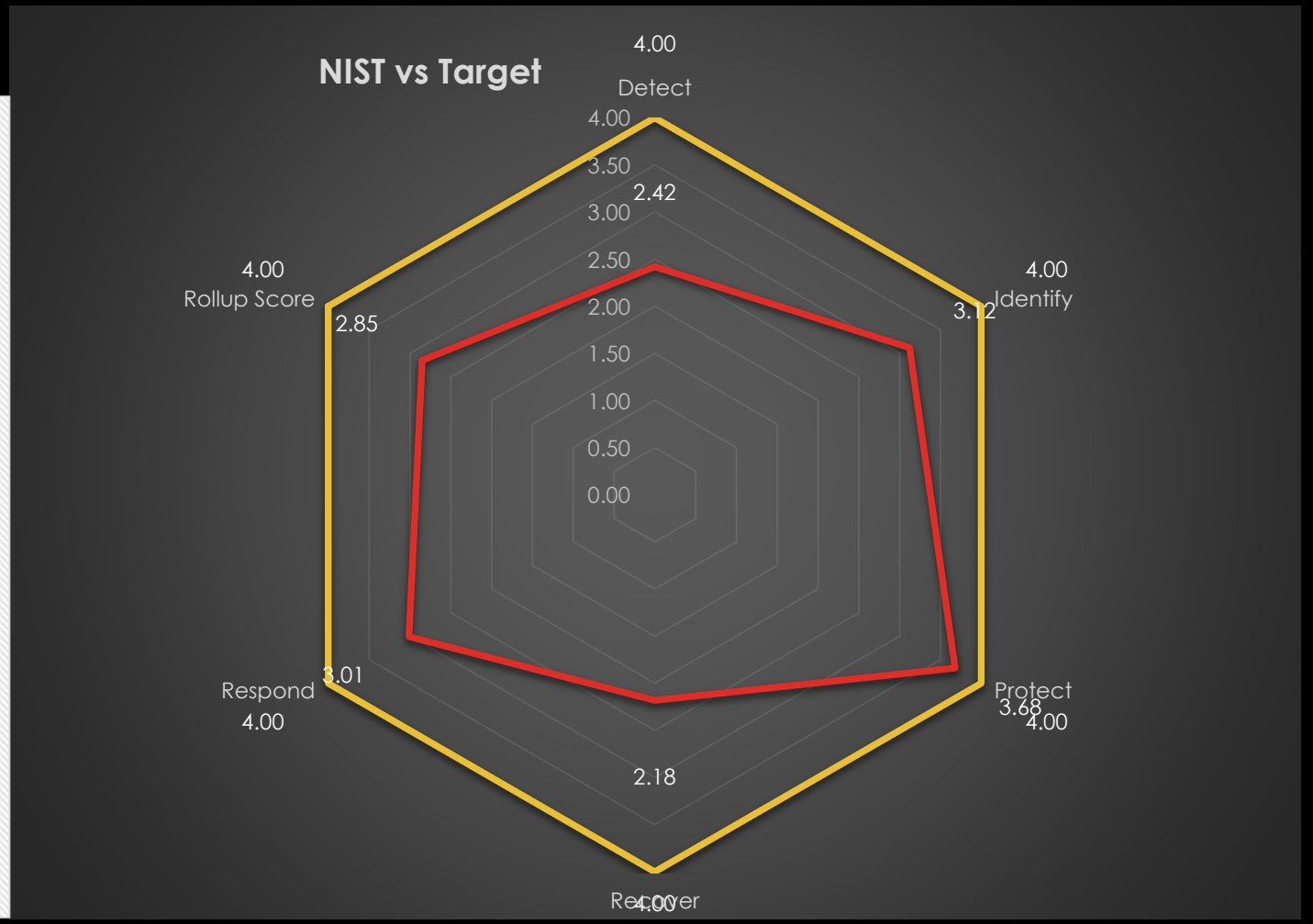

Enterprise Control Coverage
Detect
Identify
Information Technology
Protect
Recover
Respond
Governance
3.00
2.50
2.00
1.50
1.00
0.50
0.00
2.63
2.65
2.97
2.65
2.89
2.84
2.32


Detect
Identify
Protect
Recover
Respond
Information Technology
Governance
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
Average of TargetState
Average of Maturity

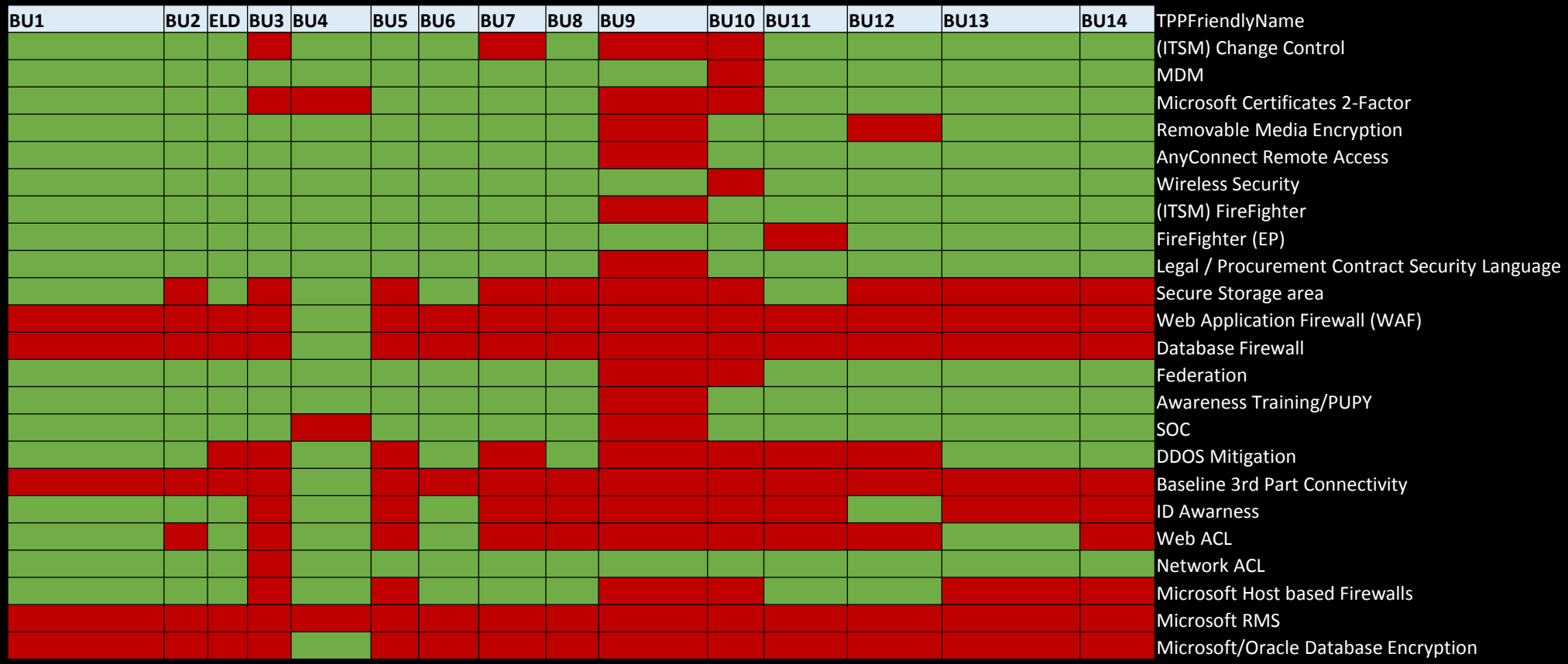

Normalized NIST Industry Comparison
AllOrg - as of 11/2/16
CoHort - as of 11/2/16
2017 - Actual as of 7/1/17
Rollup Score
2.47
3.04
2.85
Respond
2.73
3.28
3.01
Recover
2.49
3.09
2.18
Protect
2.37
3.02
3.68
Identify
2.48
2.90
3.12
Detect
2.28
2.89
2.42
0.00
0.50
1.00
1.50
2.00
2.50
3.00
3.50
4.00

PHASE 2

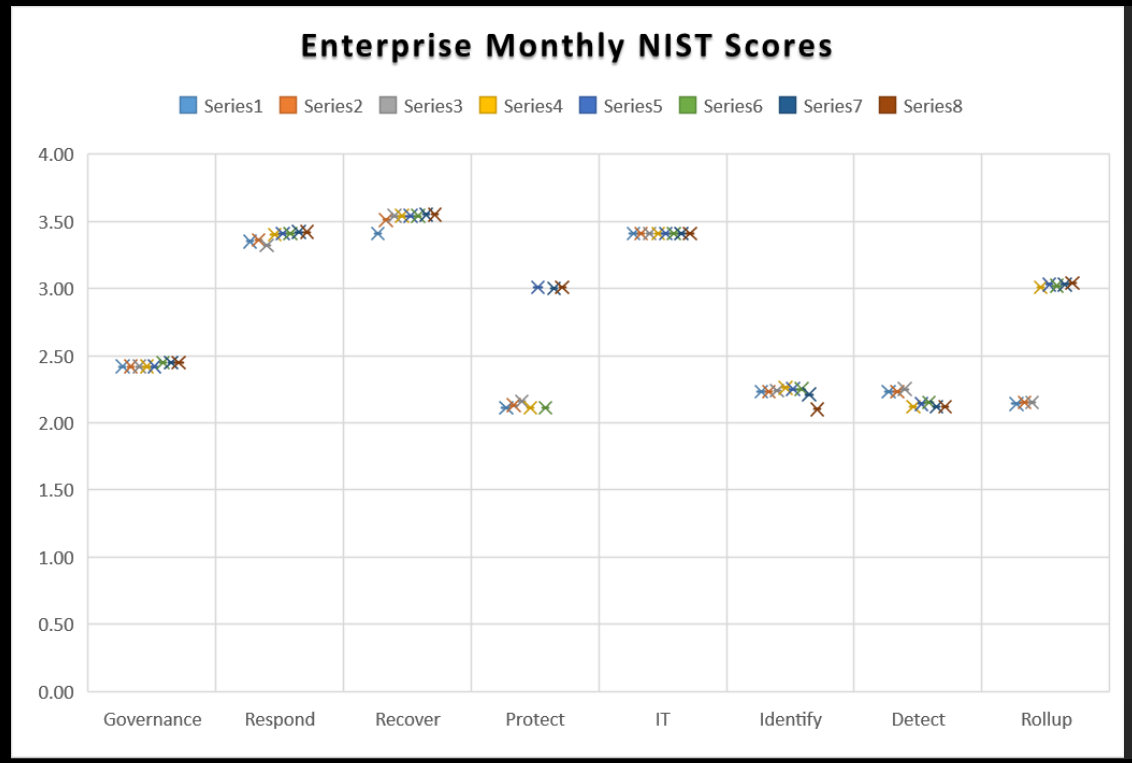

TPP Gap Score
Vuln Scanning
3rd Part Connectivity
Secure File Transfer
ID Awarness
Host based Firewalls
S-SDLC
Procurment Processes
Corp Password Management
Full Packet Capture
Asset Management

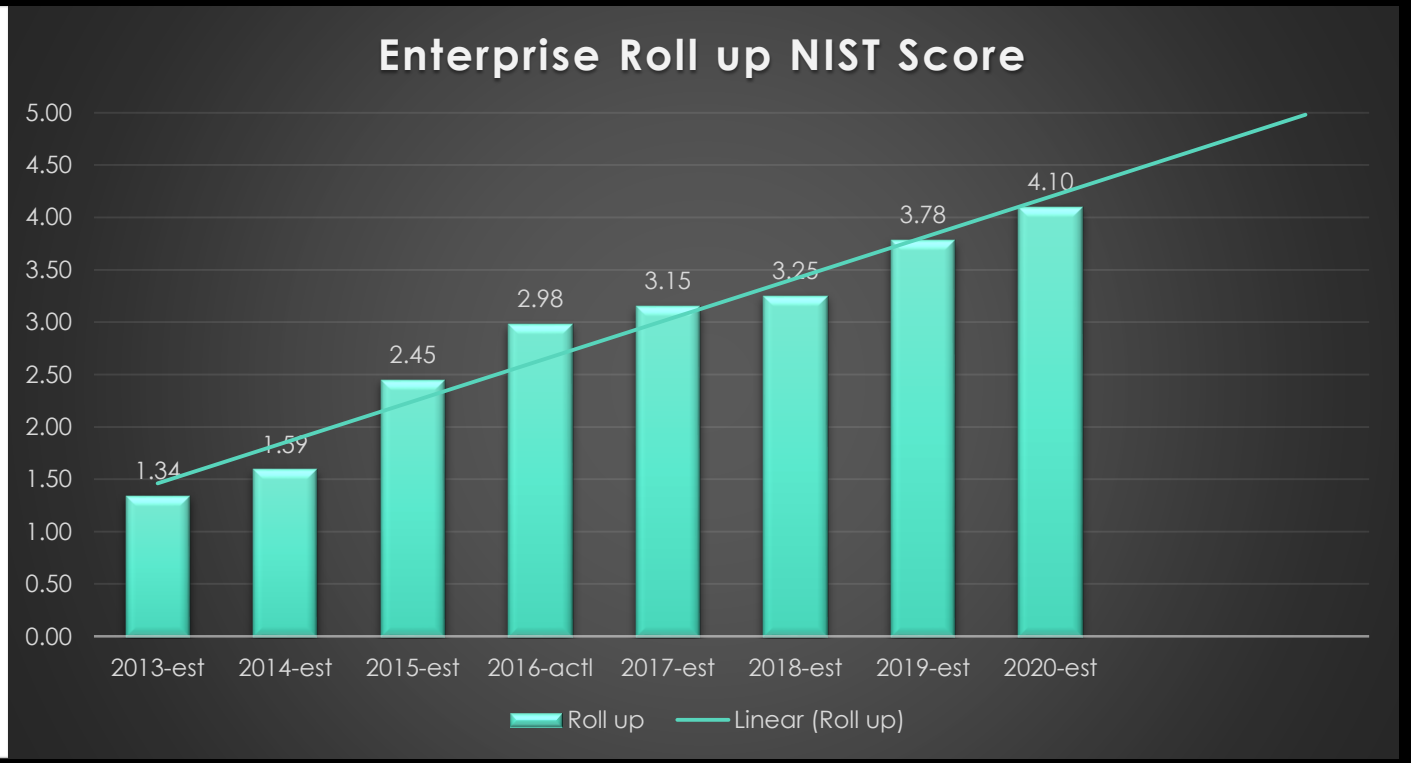

NIST vs Target
4.00
Detect
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
2.42
4.00
Identify
3.12
4.00
Protect
3.68
4.00
2.18
Recover
4.00
3.01
Respond
4.00
2.85
4.00
Rollup Score

PHASE 2


BU1
BU2
ELD
BU3
BU4
BU5
BU6
BU7
BU8
BU9
BU10
BU11
BU12
BU13
BU14
TPPFriendlyName
(ITSM) Change Control
MDM
Microsoft Certificates 2-Factor
Removable Media Encryption
AnyConnect Remote Access
Wireless Security
(ITSM) FireFighter
FireFighter (EP)
Legal / Procurement Contract Security Language
Secure Storage area
Web Application Firewall (WAF)
Database Firewall
Federation
Awareness Training/PUPY
SOC
DDOS Mitigation
Baseline 3rd Part Connectivity
ID Awarness
Web ACL
Network ACL
Microsoft Host based Firewalls
Microsoft RMS
Microsoft/Oracle Database Encryption

PHASE 2


Enterprise Monthly NIST Scores
Series1
Series2
Series3
Series4
Series5
Series6
Series7
Series8
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
Governance
Respond
Recover
Protect
IT
Identify
Detect
Rollup


Enterprise Roll up NIST Score
5.00
4.50
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
1.34
1.59
2.45
2.98
3.15
3.25
3.78
4.10
2013-est
2014-est
2015-est
2016-actl
2017-est
2018-est
2019-est
2020-est
Roll up
Linear (Roll up)

PHASE 3

- TPP Cost
- Risk register mapping
- Project mapping
- Auditability

QUESTIONS?

- JD Rogers
- jrogers3@gaig.com