Evolution of OIG FISMA Metrics

Information Security and Privacy Advisory Board
October Meeting

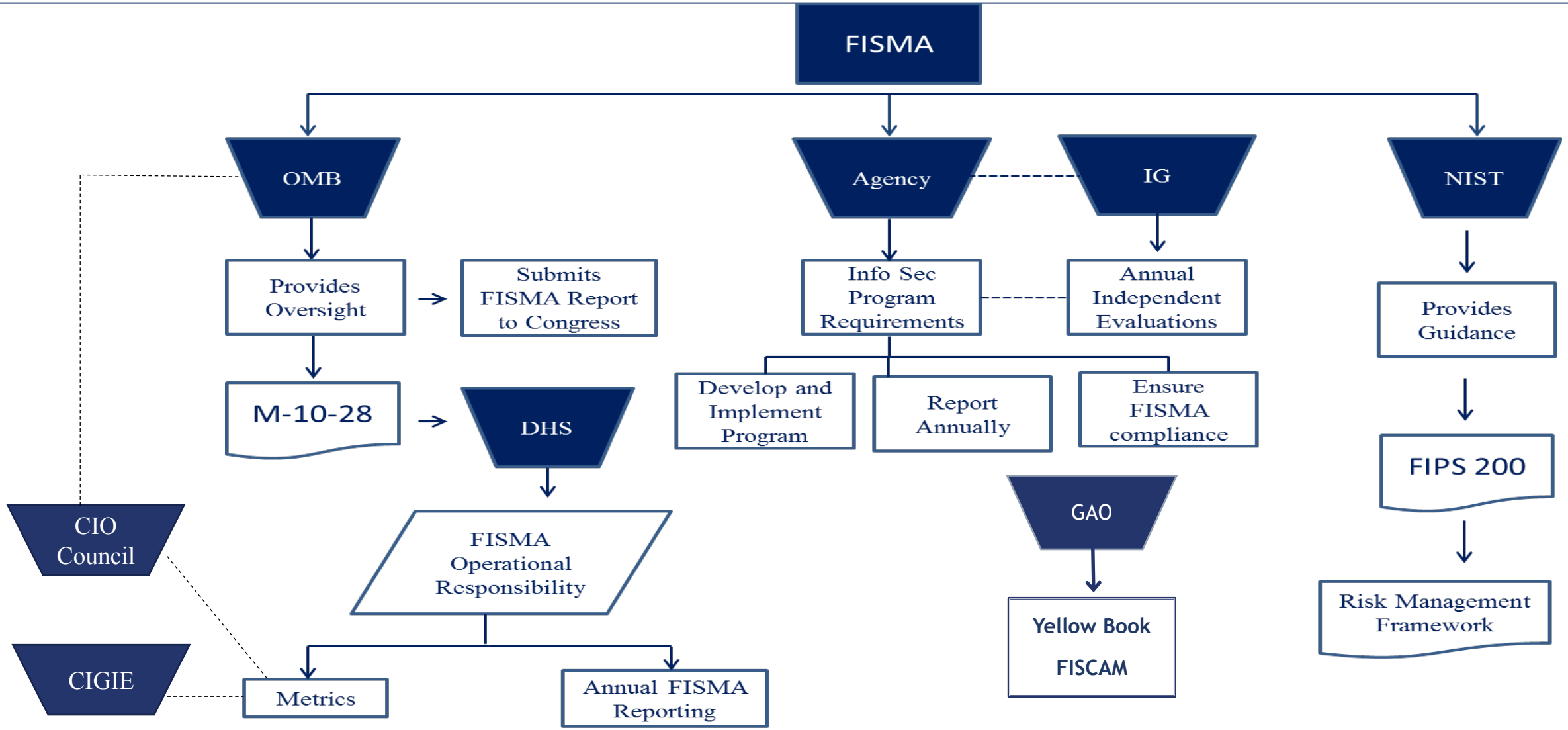
Peter Sheridan
Khalid Hasan

October 27, 2017

Agenda

- Inspector General (IG) FISMA metrics background
- Maturity model approach to independent evaluations of agency information security programs
- IG FISMA metrics and the NIST Cybersecurity Framework
- Future direction of FISMA metrics
- Next steps

Key FISMA Responsibilities



FISMA of 2002 vs. FISMA of 2014

FISMA of 2002

- Perform an annual independent evaluation of information security program and practices
  - Testing effectiveness of policies and procedures for subset of systems
  - An assessment of **compliance** with FISMA and related policies, procedures, standards, and guidelines

FISMA of 2014

- Perform an annual independent evaluation of information security program and practices
  - Testing effectiveness of policies and procedures for subset of systems
  - An assessment of **the effectiveness** of the information security policies, procedures, and practices of the agency

Security Control Effectiveness

Security control *effectiveness* addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies

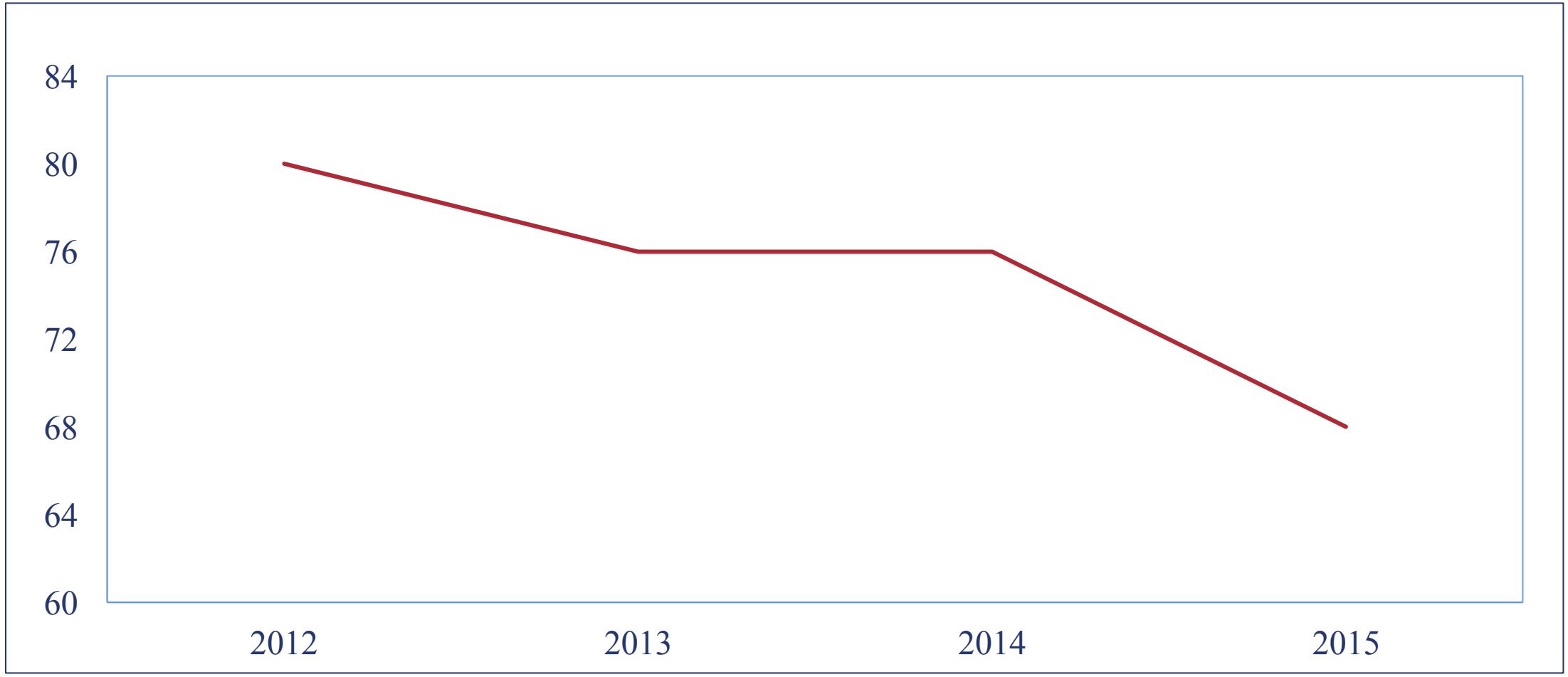
Source: NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

Previous Years' FISMA Reporting Approach

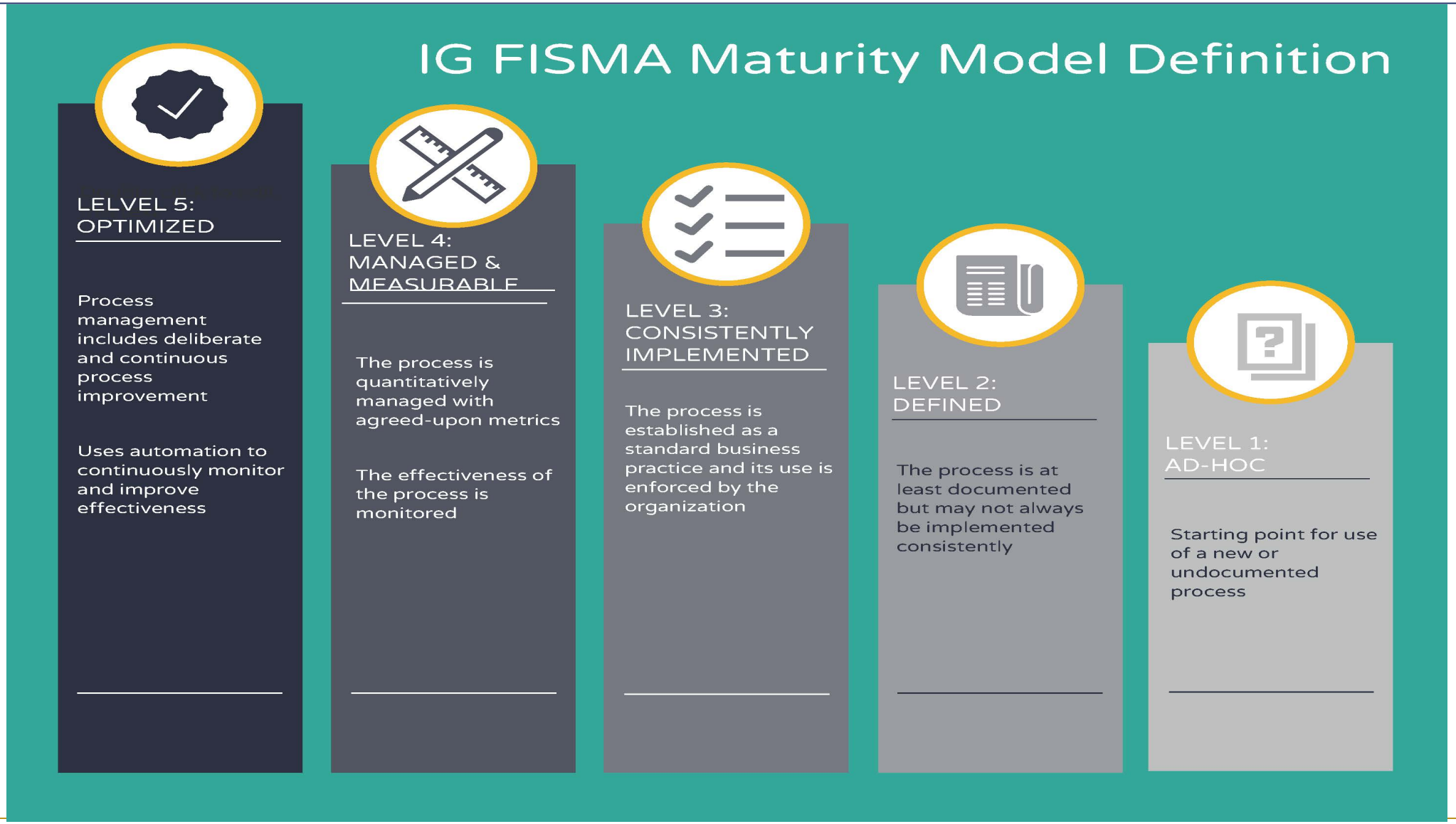
- FISMA reporting guidance for IGs has generally included compliance-based measures across various domains that IGs must respond to with a "Yes" or "No"
  - Information security continuous monitoring
  - Configuration management
  - Identity and access management
  - Incident response and reporting
  - Risk management
  - Security training
  - Plan of action and milestones
  - Contingency planning
  - Contractor systems

Cyber Security Program Area[a]	Program in place		Program not in place	
	No.	%	No.	%
Configuration management	16	70%	7	30%
Identity and access management	17	74%	6	26%
Incident response and reporting	19	83%	4	17%
Risk management	13	57%	10	43%
Security training	19	83%	4	17%
POA&M	18	78%	5	22%
Remote access management	21	91%	2	9%
Contingency planning	18	78%	5	22%
Contractor systems	16	70%	7	30%

Government-wide FISMA Compliance "Scorecard" (2012 – 2015)

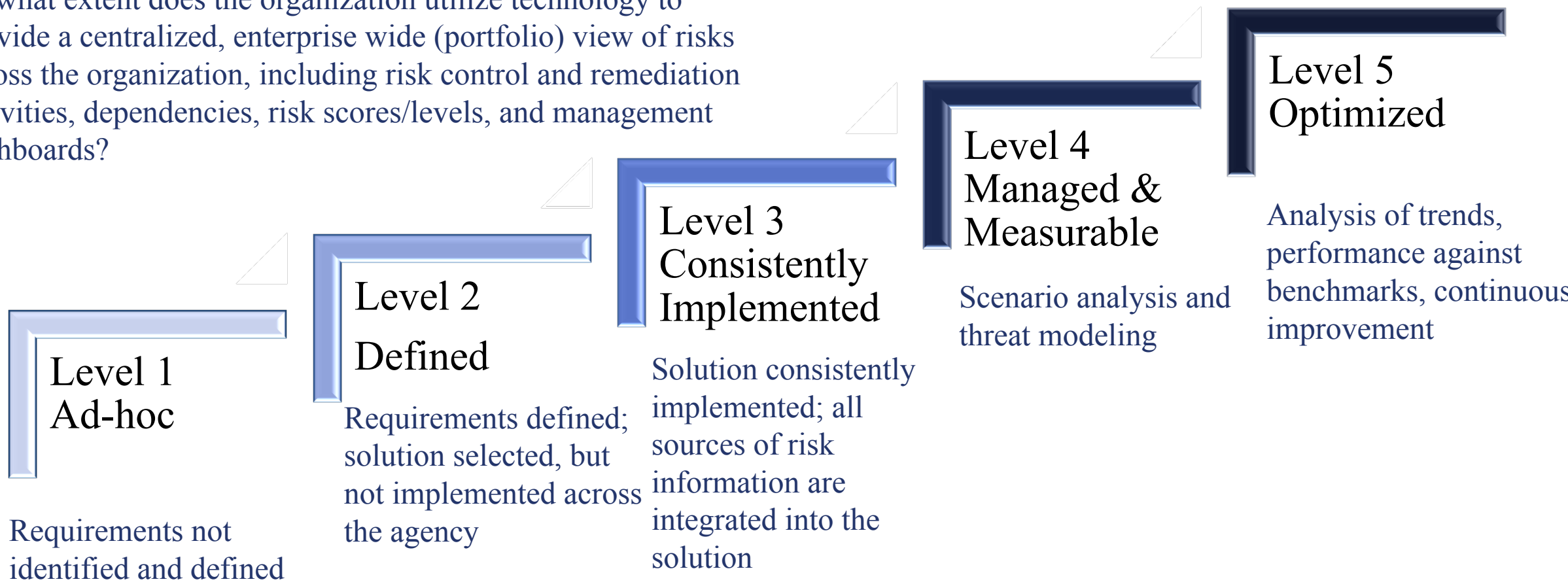


FISMA Evaluation Maturity Model



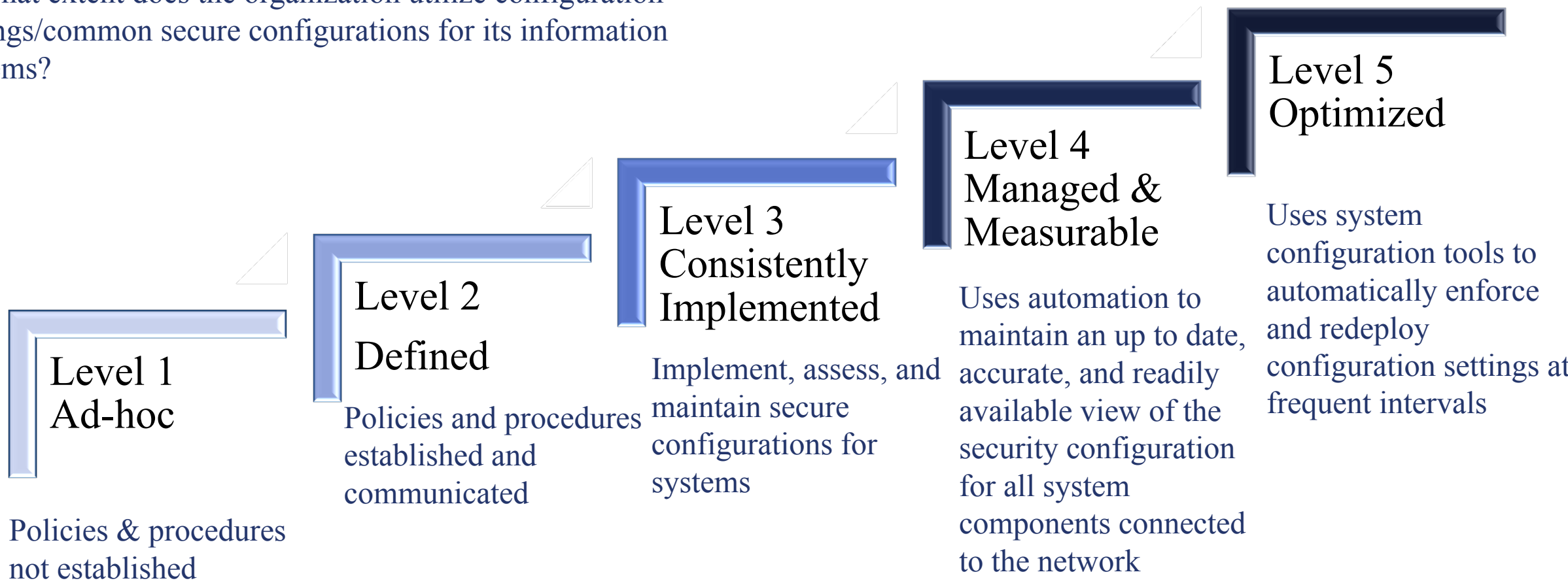
Example Maturity Indicator for Risk Management

To what extent does the organization utilize technology to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?



Example Maturity Indicator for Configuration Management

To what extent does the organization utilize configuration settings/common secure configurations for its information systems?



Scoring Methodology

FY 2017 FISMA IG Metrics scoring methodology will seek to provide a balanced assessment of agency information security capabilities

- Agency IGs will assess capabilities on a spectrum of potential maturity levels
- Overall maturity for each NIST Function will be recommended based on the most frequently occurring level (mode)
  - Goal is to provide a representative maturity level, but IGs can substitute a different score if they choose
- Overall agency maturity will be determined by the IG
  - This allows IGs to customize their assessments based on agency circumstances

2015 ISCM Evaluation Results

Agency Progress Against ISCM CAP Goals

Automated Software Asset Inventory	89%
Capability to Detect & Block Unauthorized Software	68%
Secure Configuration Management	92%
Vulnerability Management	52%

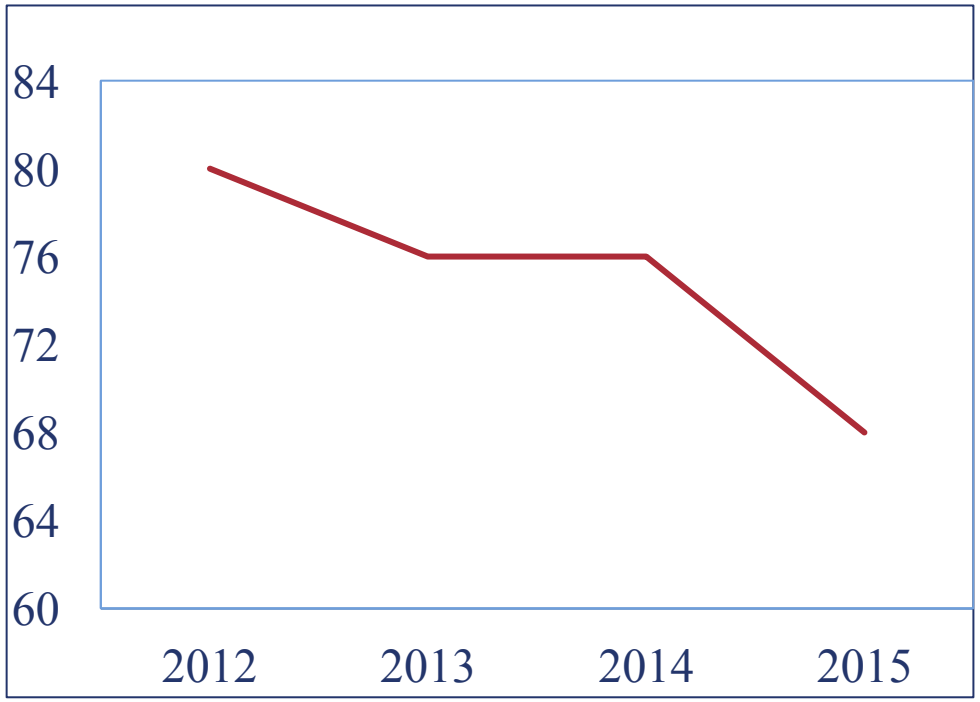
OIG ISCM Maturity Evaluations

Maturity Level	No. of Agencies	%
Ad Hoc	15	63%
Defined	6	25%
Consistently Implemented	2	8%
Managed and Measurable	0	0%
Optimized	0	0%
Not Scored	1	4%

Source: OMB FY 2016 FISMA Report to Congress

What Results are we Seeing?

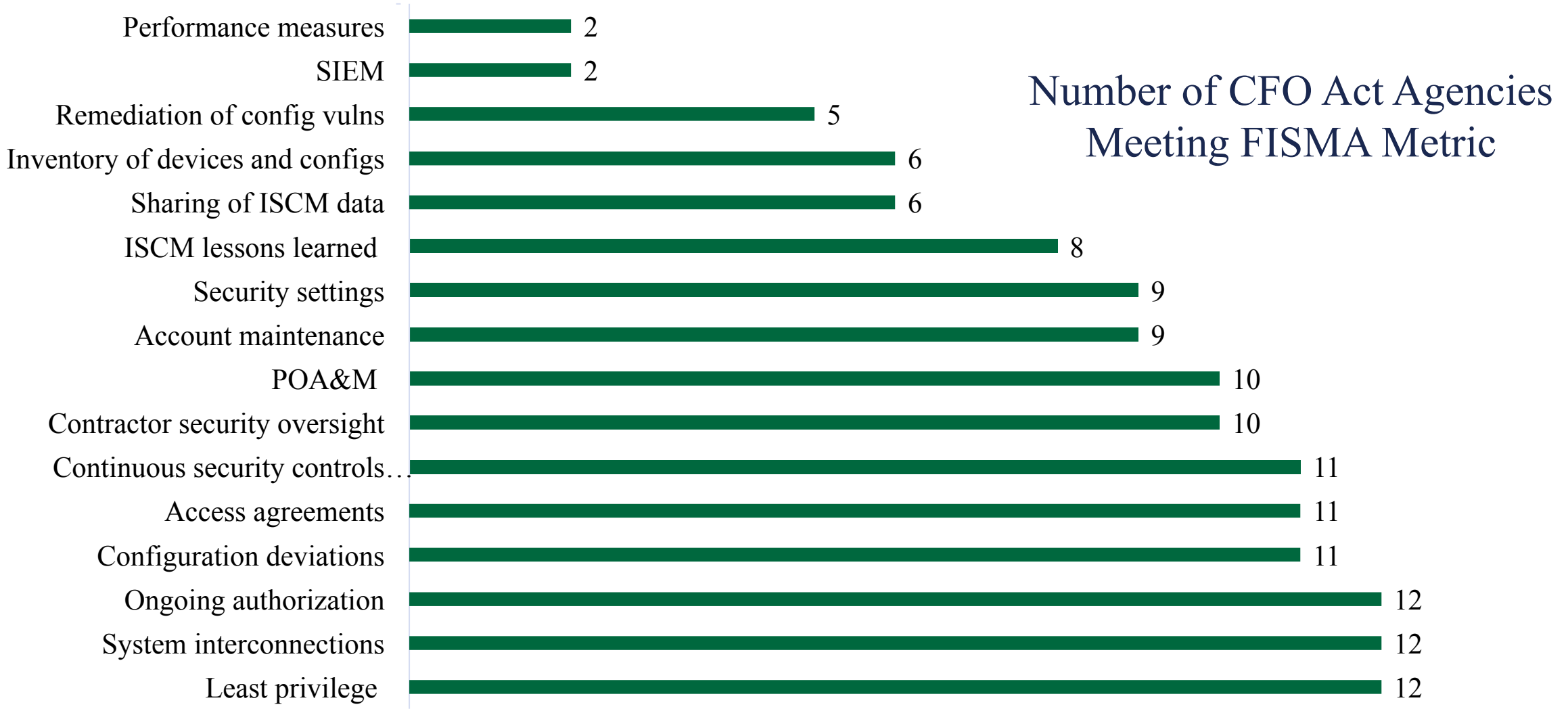
Previous Government-wide Compliance-based Scorecard



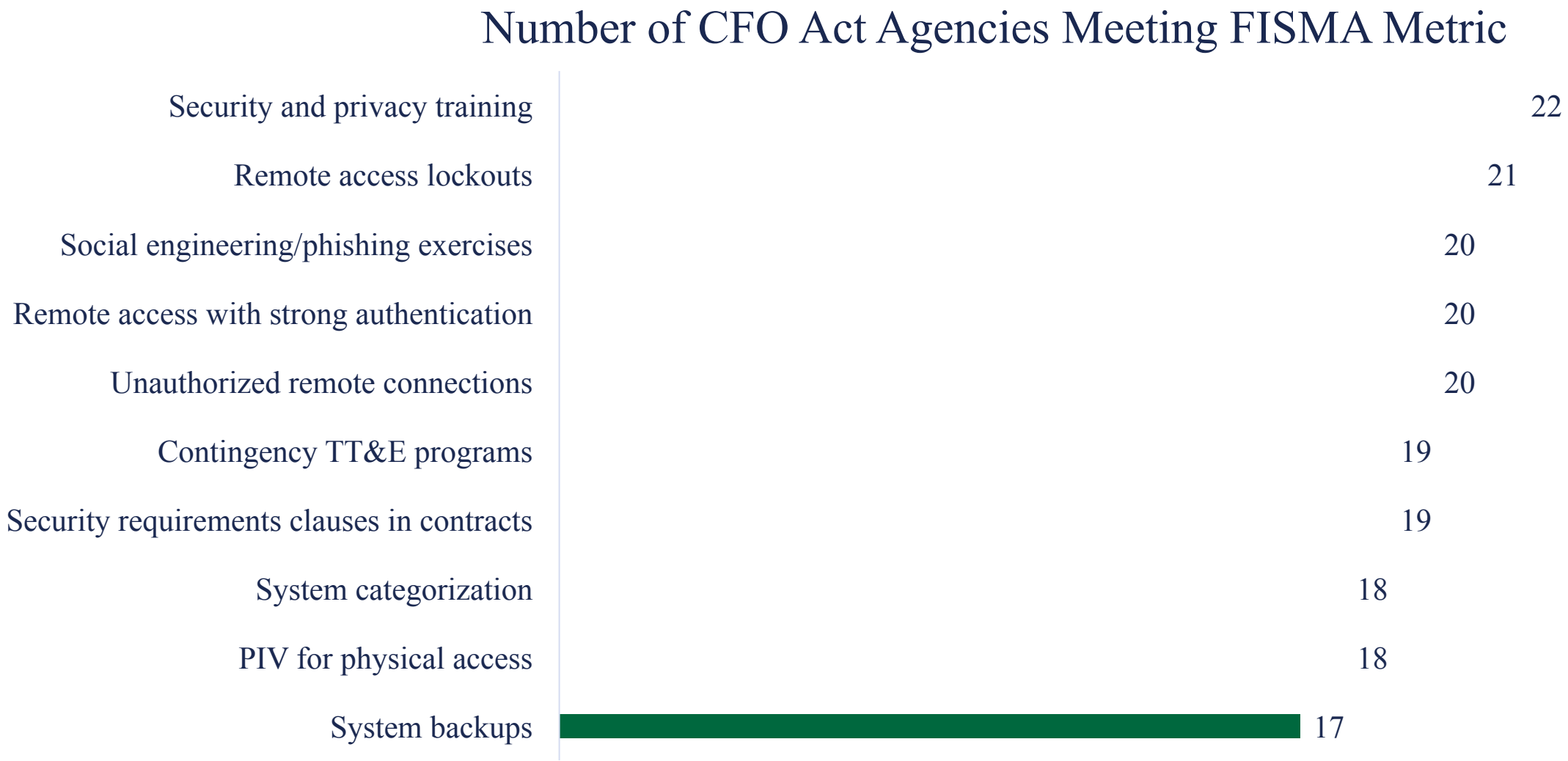
New Government-wide Maturity-based Scorecard

Cybersecurity Framework Area	Average Rating
Identify	Level 2: Defined
Protect	Level 3: Consistently Implemented
Detect	Level 2: Defined
Respond	Level 2: Defined
Recover	Level 3: Consistently Implemented
Overall	**Level 2: Defined**

Common Areas of Weaknesses in FY 2016



Common Areas of Strength in FY 2016



Impact of maturity model approach at our OIG

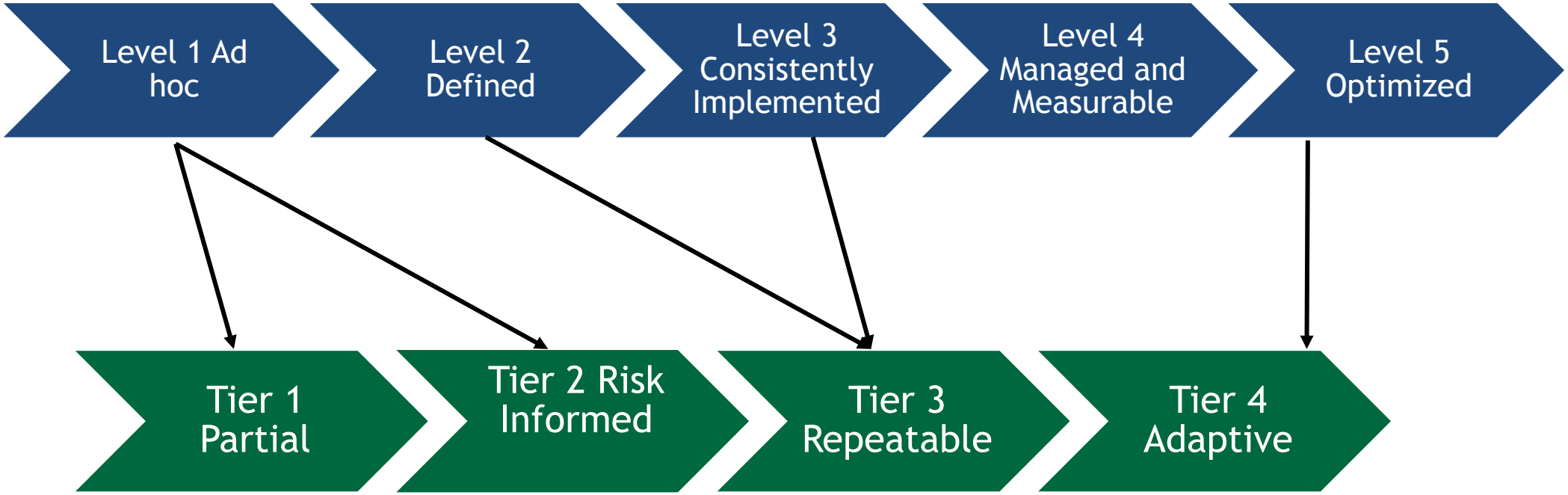
- Improved working relationship with CIO and led to greater understanding of what is needed to mature the organization's infosec program
- Helped the organization define how it plans to implement the components of an effective infosec program
- Improved communication of the status of the agency's info sec program amongst stakeholders

NIST CSF and Relation to FISMA Metrics

CSF Function Area	CSF Categories/Attributes	FISMA Metric Areas
Identify	Asset management, business environment, governance, risk management	Identify – risk management
Protect	Access control, training, data security, config mgmt, change control, remote access, sdlc	Protect – configuration mgmt; I&A, training
Detect	Continuous monitoring, incident detection,	Detect – ISCM Respond – incident response
Respond	Response planning, communications, analysis, mitigation	Respond – incident response
Recover	Recovery planning, improvements, communications	Recover - contingency planning

IG Maturity Levels vs. CSF Implementation Tiers

IG FISMA Maturity Levels



CSF Implementation Tiers

CSF Core Areas Not in IG Metrics

- **Identify**
  - ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
- **Protect**
  - PR.AC-2: Physical access to assets is managed and protected
  - PR.DS-1: Data-at-rest is protected
  - PR.DS-2: Data-in-transit is protected
  - PR.DS-4: Adequate capacity to ensure availability is maintained
  - PR.DS-7: The development and testing environment(s) are separate from the production environment
  - PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
  - PR.IP-6: Data is destroyed according to policy

CSF Core Areas Not in IG Metrics (cont.)

- **Protect**
  - PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
  - PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
  - PR.PT-2: Removable media is protected and its use restricted according to policy
  - PR.PT-4: Communications and control networks are protected
- **Detect**
  - DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
  - DE.CM-5: Unauthorized mobile code is detected

CSF Core Areas Not in IG Metrics (cont.)

- **Recover**
  - RC.CO-1: Public relations are managed
  - RC.CO-2: Reputation after an event is repaired

Supply Chain Metrics in 2017 IG FISMA Metrics

CSF v1.1	2017 IG FISMA Metrics
ID.SC-1: cyber supply chain risk management processes are identified established, assessed, and managed	5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk
ID.SC-2: identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process	
ID.SC-3: suppliers and partners are required by contract to implement appropriate measures	11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services
ID.SC-4: suppliers and partners are monitored	
ID.SC-5: response and recovery planning and testing are conducted with critical suppliers/providers	58. The organization coordinates information system contingency plan testing with organizational elements responsible for related plans. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.

Other CSF v1.1 Metric Changes

- **Risk assessment metrics (identify)**
  - Cyber threat intelligence and vulnerability information is received from information sharing forums and sources
- **Access control metrics (protect)**
  - Issuing, managing, verifying, revoking and auditing identities and credentials for authorized devices, users, and processes
  - Identity proofing and assertions
- **Data Security (protect)**
  - Added metric on integrity checking mechanisms
- **Protective technology (protect)**
  - New metric on configuring systems to provide only essential capabilities and operating systems in predefined states to achieve availability

Impact to Future IG FISMA Metrics

- Anticipate additional metrics related to
  - Cybersecurity supply chain risk assessment process
  - Coordination of response planning and testing with critical suppliers/providers
  - Protection of data at rest and in transit
  - Data destruction
  - Cyber threat intelligence (e.g. deep/dark web exposure)

- Incorporate the concept of a "profile" to tailor the scoring of IG metrics to agencies' risk environment
  - A "profile" aligns cybersecurity activities with business requirements, risk tolerances, and resources
  - Defines specific practices to address the framework core

Sample Profile for Manufacturing Company

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
		ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1

		Maintain Personnel Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	Subcategories				
PR	Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3
		PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4	PR.AC-4
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5
	Awareness and Training	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1	PR.AT-1
		PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2	PR.AT-2
		PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3	PR.AT-3
		PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4	PR.AT-4
		PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5	PR.AT-5
	Data Security	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1	PR.DS-1
		PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2	PR.DS-2
		PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3	PR.DS-3
		PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4	PR.DS-4
		PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5	PR.DS-5
		PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6	PR.DS-6
		PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7	PR.DS-7
		PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1	PR.IP-1

Source: Draft NIST Cybersecurity Framework Manufacturing Profile, available at http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

Potential Next Steps

- Develop an “evaluation guide” to include suggested test steps/indicators for IG use
- Incorporate a more robust scoring methodology with weighting applied to attributes that are of greater risk or concern to stakeholders
- Evaluate options to tailor maturity attributes based on organizational missions/resources/risks

Questions?