Why Should I Care?

Cybersecurity Maturity Model Certification (CMMC): DoD / Non-DoD

Cherry Bekaert LLP
Your Guide Forward

Introductions – Cherry Bekaert

Industry Concentrations

- Government
- Government Contractors
- Healthcare & Life Sciences
- Hospitality & Retail
- Industrial Manufacturing
- Not-for-profits
- Private Equity
- Professional Services
- Real Estate & Construction
- Technology

Services inclusive of:

- Advisory
- Assurance
- Tax
- Wealth Management

Introductions – Steve Holliday MBB, CISM

- Present – Director, CIO Advisory Services (Digital Advisory)
- Past:
  - 20+ years manufacturing (GE, Tredegar)
  - 6 years financial services (GE / Genworth)
  - 2 years wholesale distribution (Home Depot / HD Supply)
  - Primarily:
    - Operations Management
    - Continuous Improvement
    - Information Technology
- Duke University (BSME), Illinois State University (MBA)
- Outside Work: Family, Fitness, Fun
- Fun Fact: I've visited 47/50 US States
- steve.holliday@cbh.com

Introductions – You (by way of hands)

- Industry

Manufacturing	Healthcare	Not for Profit	Technology	Transportation
Professional Services	Financial Services	Government	Real Estate / Construction	Other?

- Your Function
  - IT
  - Information Security
  - Risk Management
  - Other?
- Your Role (with Information Security)
  - Decision Maker
  - Doer / SME
  - No direct responsibilities
- Any Government Contractors (ie – CMMC may apply?)
- Have you heard of CMMC before this presentation?
- Anyone familiar with NIST 800-171?

Background - CMMC

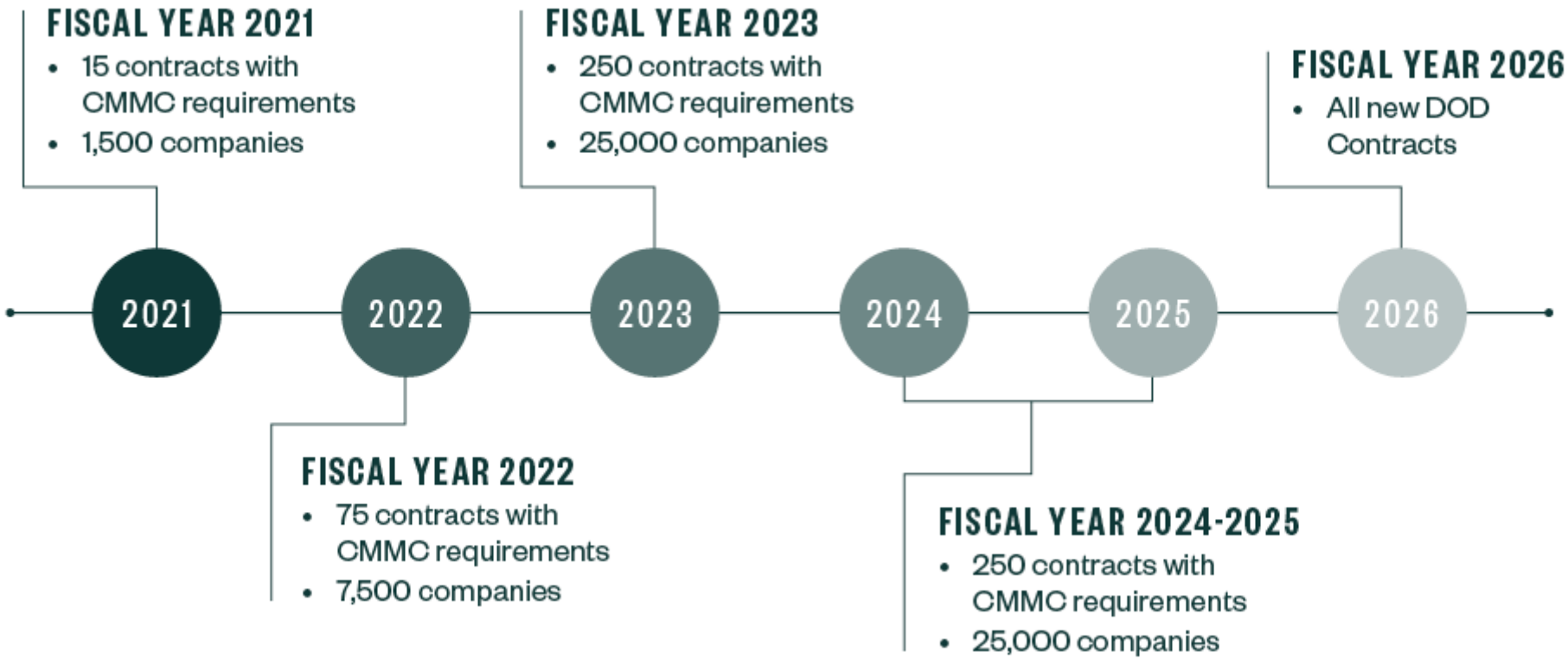
Cyber Maturity Model Certification

- **A training, certification, and third party assessment program of cybersecurity** in the United States government Defense Industrial Base (DIB) aimed at measuring the maturity of an organization's cybersecurity processes (process institutionalization) toward demonstrating compliance with the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI*).

*Think of CUI – As You Organization’s Highly Confidential Information

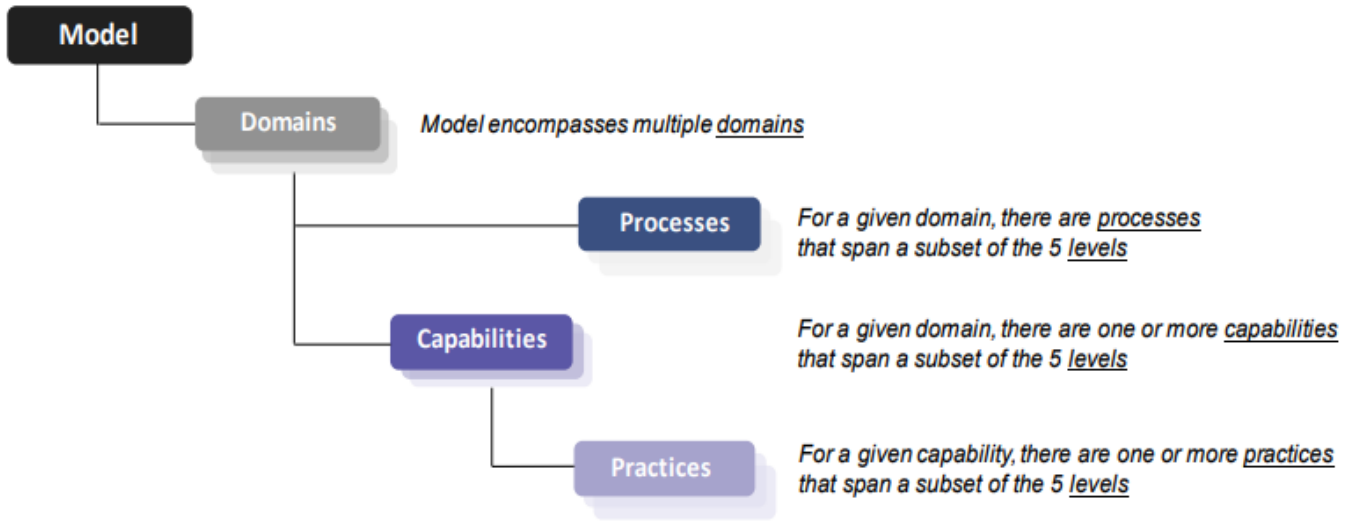
Background - CMMC

Deployment / Expansion



Background - CMMC

Basic Structure



Model v1.0 encompasses the following:

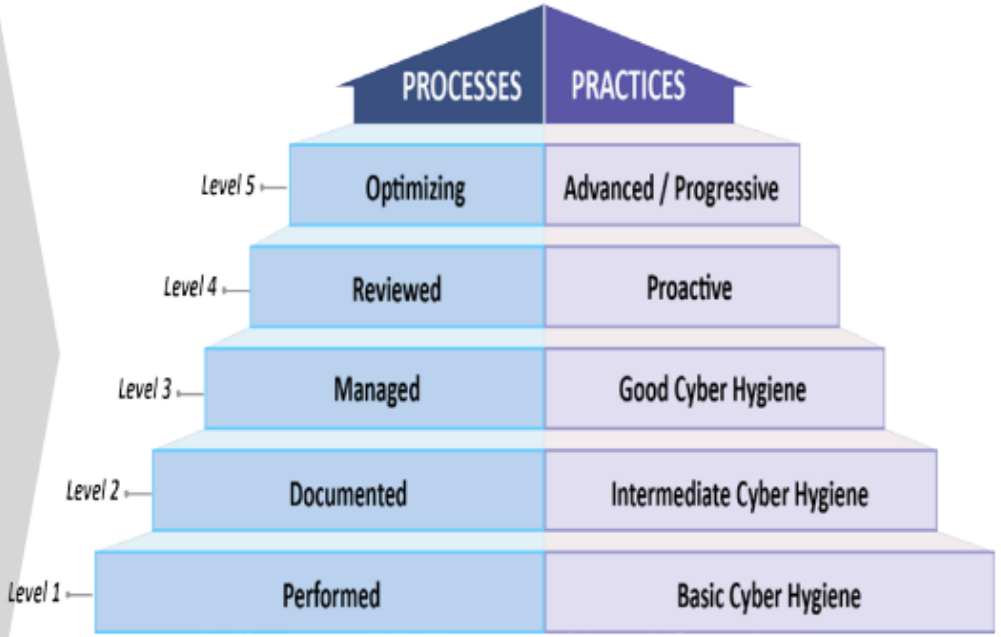
- 17 capability domains
- 43 capabilities
- 5 processes across five levels to measure process maturity
- 171 practices across five levels to measure technical capabilities

https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

17 Domains, Cybersecurity Maturity through Processes and Practices

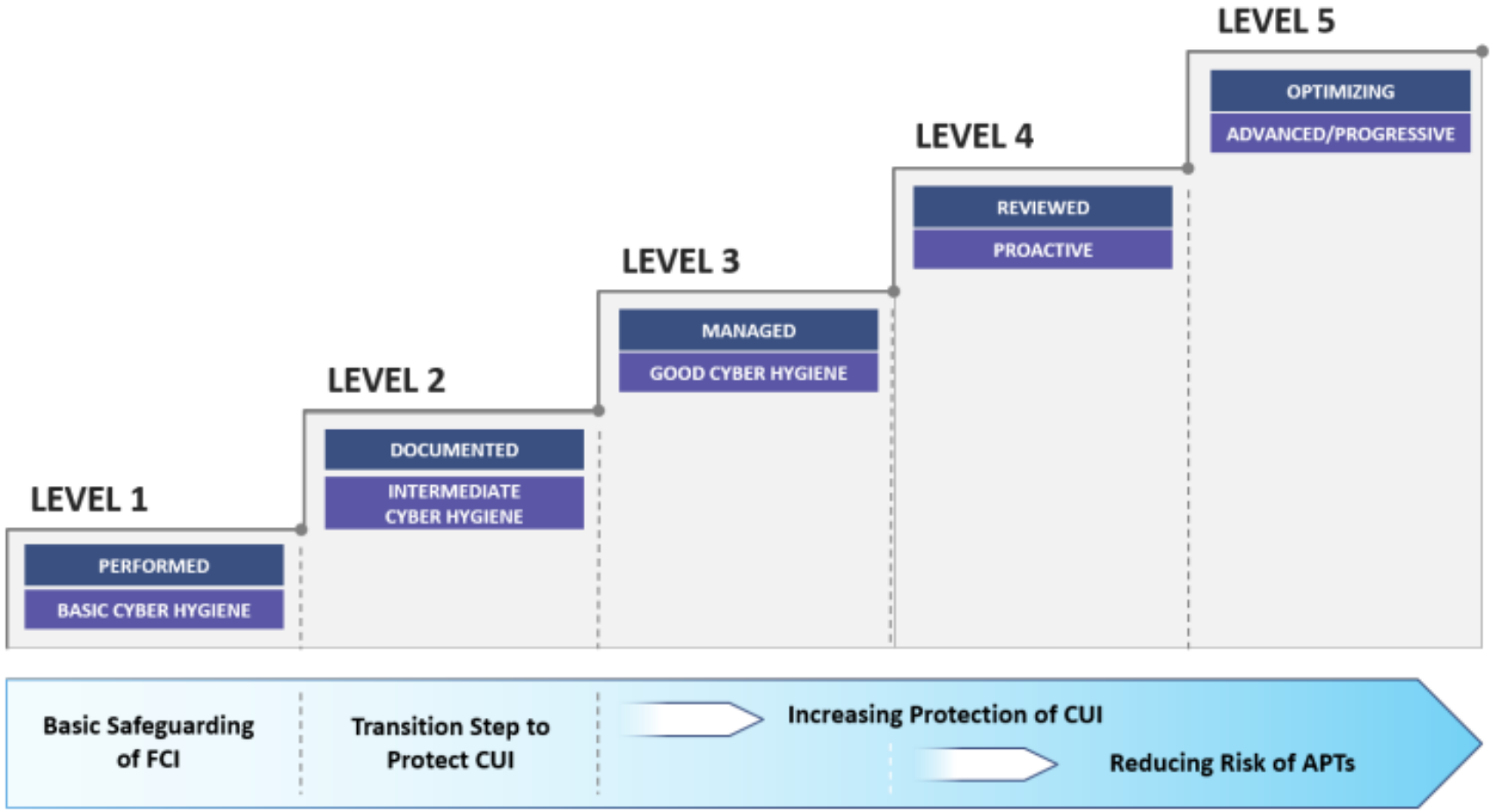
Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	



https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

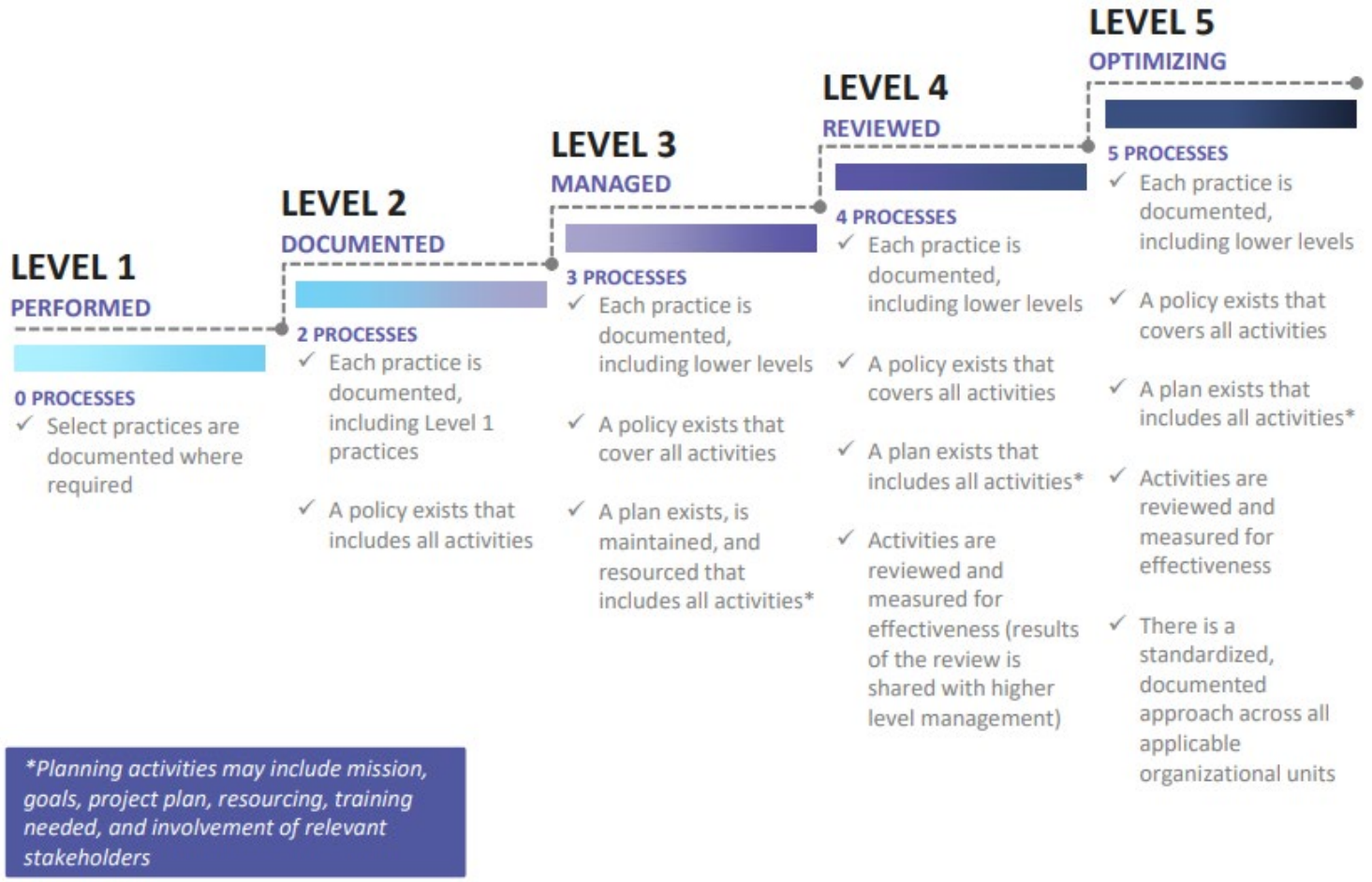
Focus / Outputs by Level



https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

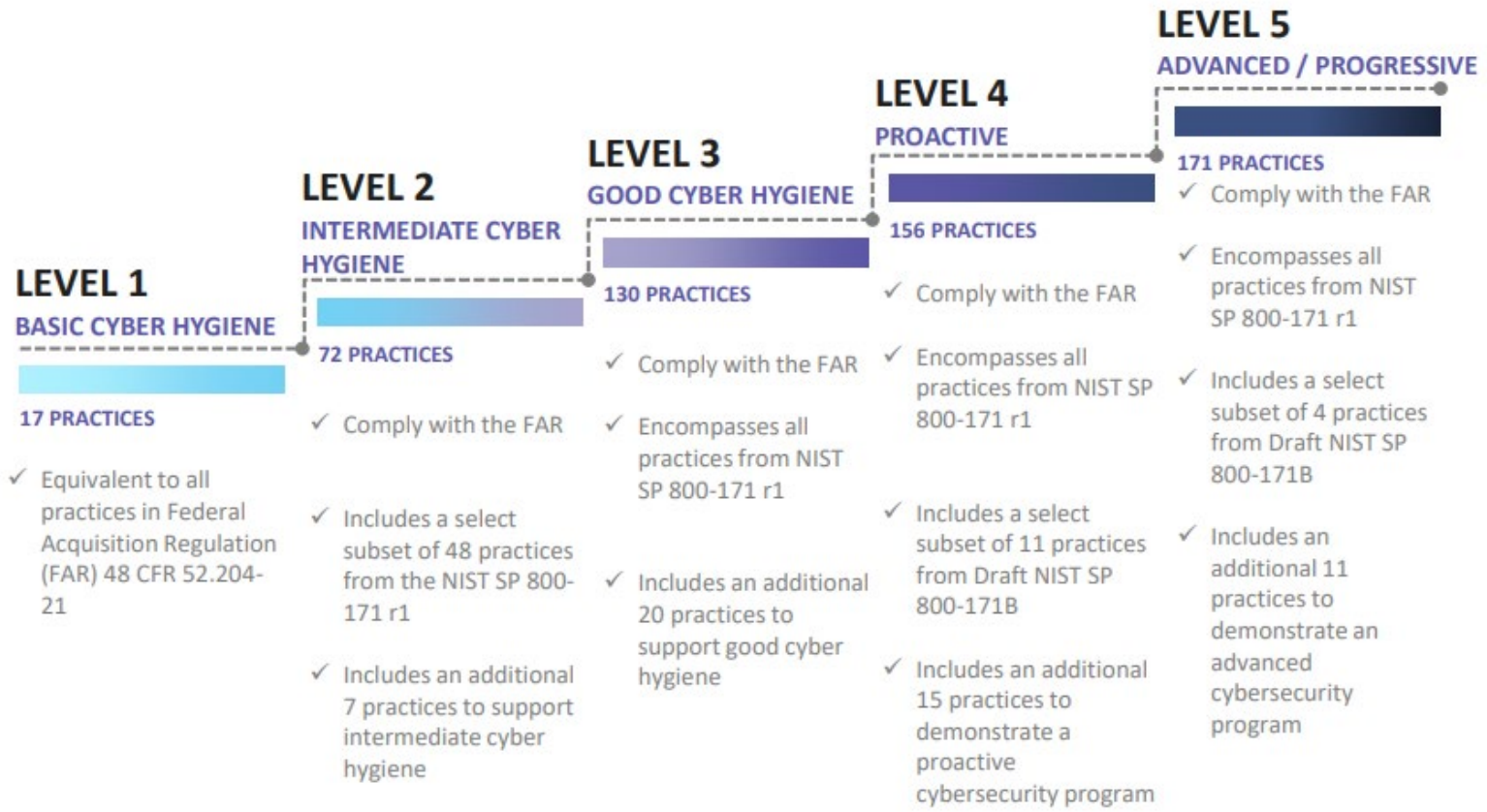
Processes by Level



https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

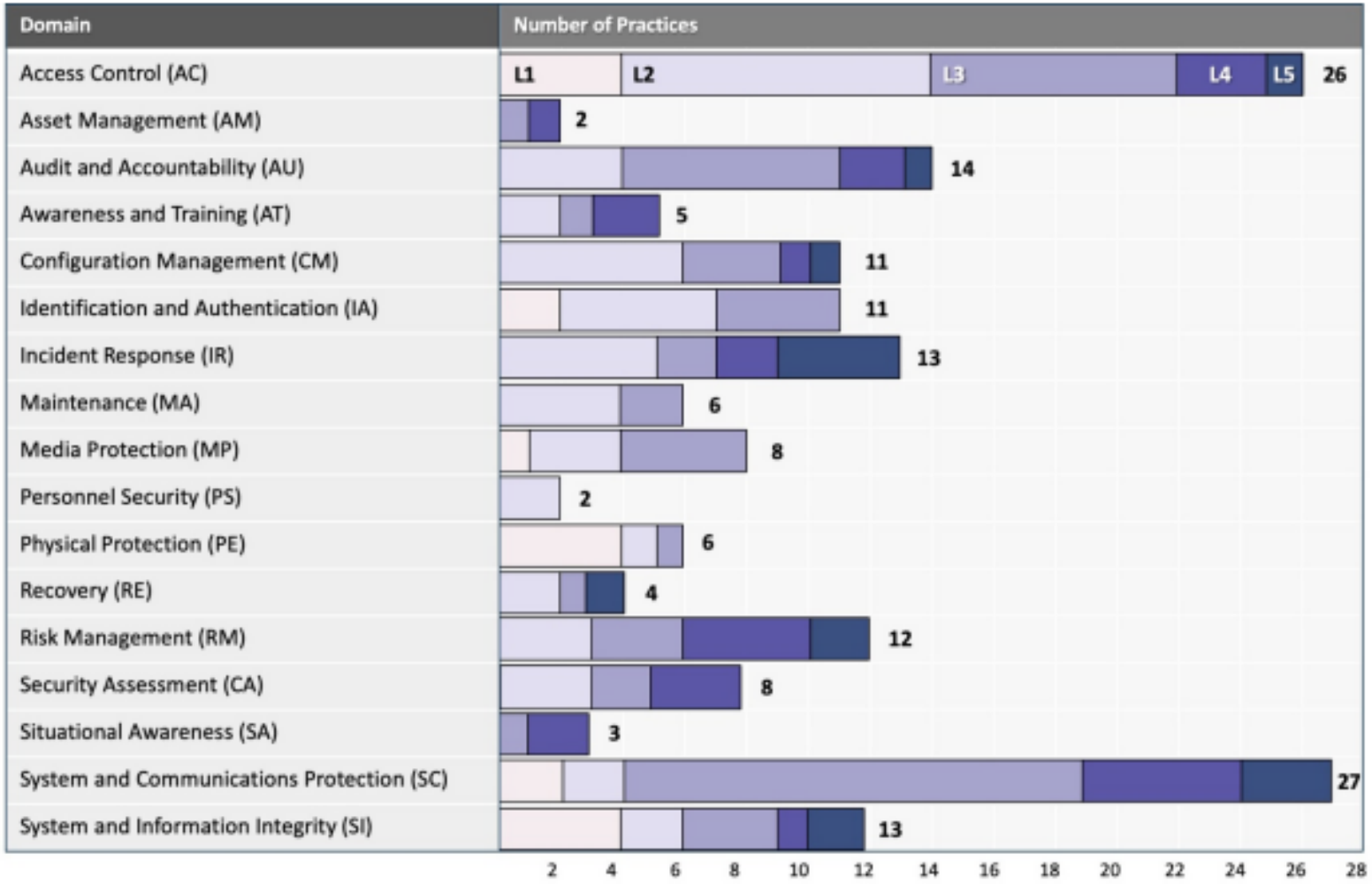
Practices by Level



https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

- Practices by Domain, by Level (maturity)
- Thoughts on “most basic”?
- Which jump out as most extensive?



https://www.cmmcaudit.org/cmmc-version-1-0-released-analysis-for-dod-contractors/

Background - CMMC

Example: Media Protection (MP) L1 – L5

- XX.#.@@@ where:
  - XX is the domain
  - # is the maturity level
  - 1@@ is the practice
  - 9@@ is the process
- (MP) Media Protection
  - 8 Practices
    - 1 x L1
    - 3 x L2
    - 4 x L3
  - 5 Processes
    - 2 x L2
    - 1 x L3
    - 1 x L4
    - 1 x L5

Reference	Requirement
MP.1.118	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
MP.2.119	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
MP.2.120	Limit access to CUI on system media to authorized users.
MP.2.121	Control the use of removable media on system components.
MP.2.998	Document the CMMC practices to implement the Media Protection policy.
MP.2.999	Establish a policy that includes Media Protection.
MP.3.122	Mark media with necessary CUI markings and distribution limitations.
MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.
MP.3.124	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
MP.3.997	Establish, maintain, and resource a plan that includes Media Protection.
MP.4.996	Review and measure Media Protection activities for effectiveness.
MP.5.995	Standardize and optimize a documented approach for Media Protection across all applicable organizational units.

Discussion – Use of CMMC

- Where is your organization in its cyber security journey?

- Does your organization use a security maturity model?
  - Which one?
  - If not, do you see any possibilities for application of CMMC?
  - If not – what are your plans to advance?
  - If so, how do you see this helping you?
- How does your organization gage progress in its continuous improvement cyber security journey?

Wrap Up

- CMMC – Recap
  - Timeline
  - Who
  - What

- Value to organizations
  1) Implementing a framework like CMMC requires consideration of the information at risk, what puts that information at risk, and what steps can be taken to help safeguard that information
  2) Whether you've chosen a framework or not, it is helpful to have a plan and see your journey over time
  3) A framework is like a map, it helps to measure progress in your journey
  4) No matter where your organization is along it's journey, it can ALWAYS improve

Questions?

Appendix

Capabilities by Domain

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance

Capabilities by Domain (cont'd)

Domain	Capability
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections