MEETING DOD CONTRACTOR REQUIREMENTS: CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Darrin Thompson, DirectEmployers Association

Sean Hassett, Kompleye

Pat Garcia, Kompleye

DirectEmployers Association

KOMPLEYE

Assurance and Compliance

HISTORY OF DOD SECURITY REQUIREMENTS

EO 13556
NARA
CUI Agent

Nov 2010

Federal Contract Information - FCI

FARS 52.204-21 → EFFECTIVE

Jun 2016

Controlled Unclassified Information - CUI

DFARS 252.202-7012 → ISSUED (NIST SP 800-171 Rev. 1, Oct 2016) → DEADLINE 2017

DFARS 252.202-7019
DFARS 252.202-7020 → ISSUED (NIST SP 800-171 Rev. 2, Jun 2019) → EFFECTIVE (NIST SP 800-171 Rev. 2, Nov 2020)

NARA
NIST
DOD

DFARS 252.202-7021 → CYBERSECURITY MATURITY MODEL CERTIFICATION

STARTED Mar 2019 → V1 Jan 2020 → V1.02 Mar 2020

CMMC replaces a system which contractors self-attest they have met cybersecurity requirements – a model found not credible.

CONTRACTOR REQUIREMENTS: (DFARS) 7019, 7020, 7021

The DFARS 252.204-7019 clause NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

In order to be considered for award, if the Contractor is required to implement NIST SP 800-171, the entity must have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation)

DFARS 252.204.7020 NIST SP 800-171 DOD ASSESSMENT TYPES

Basic Assessment (Self-assessment) of their NIST 800-171 scoring and POAMs submitted to the DOD Supplier Performance Risk System (SPRS). Deadline Nov 30, 2020

The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology. Enforcement capabilities performed by the DIBCAC.

DFARS 252.204-7021 clause requires DoD contractors to maintain the appropriate CMMC level with respect to each contract, while also ensuring any subcontractors are compliant to the same CMMC level.

Level 1: FCI – 17 requirements, 1 maturity level

Level 3: CUI – 130 requirements, 3 maturity levels

NIST SP 800-171 Assessment Methodology Guidance

NIST SP 800-171 Assessment Methodology Version 1.2.1 6.24.2020

Office of Acquistion and Sustainment

Source: https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf

For more information and assistance completing the NIST SP 800-171

Contact Kompleye:

+1 (571)-830-5140.

info@Kompleye.com

CMMC TIMELINE / EXPECTATIONS

CMMC is being implemented through a phased rollout: "Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation."

https://www.acq.osd.mil/cmmc/faq.html

Priority Action (DFARS 252.202-7019)	Recommended Action 1	Recommended Action 2
Meet DFARS Requirements for NIST SP 800-171 Assessment. November 2020 – Deadline (Overdue) If not already performed submit a record of NIST 800-171 Secure Score and associated deliverables within the Supplier Performance Risk System (SPRS).	Perform a scoping exercise to identify level of CMMC certification expected to be required. "Identify and Follow the Data" "Isolate in-scope systems as much as possible (Enclaves)" Perform a CMMC readiness assessment against anticipated expected level of certification.	Discuss with your applicable business partners, vendors, subcontractors their CMMC readiness.

CMMC - MAIN CHALLENGE

METHODOLOGY AND PRACTICE

WHY WE CHOSE THE AGILE APPROACH

- INCREASE OF CONTROL EXPECTATION
- DEEPER UNDERSTANDING OF AUDIT REQUIREMENTS REQUIRED
- GREATER ALIGNMENT OF POLICY TO PROCEDURE REQUIRED

CMMC READINESS - "DEFINE YOUR EPIC"

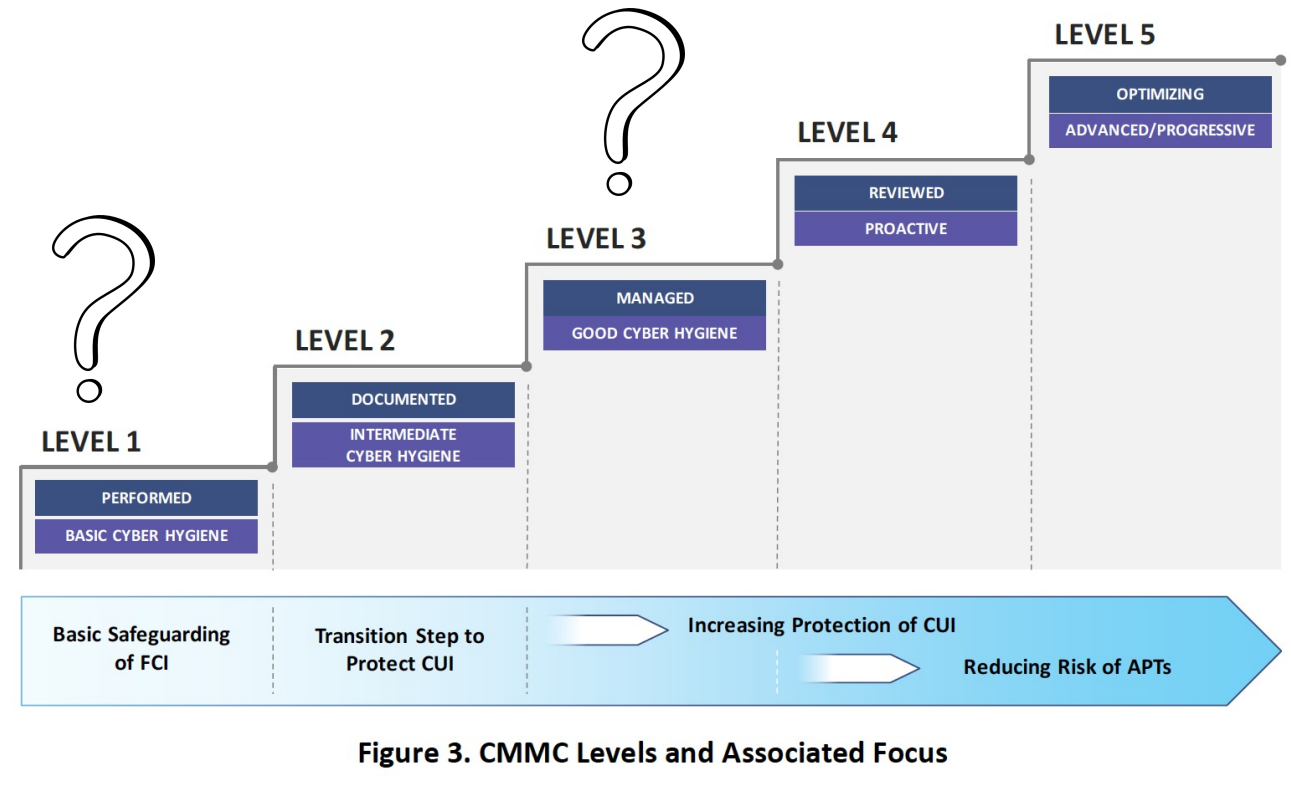


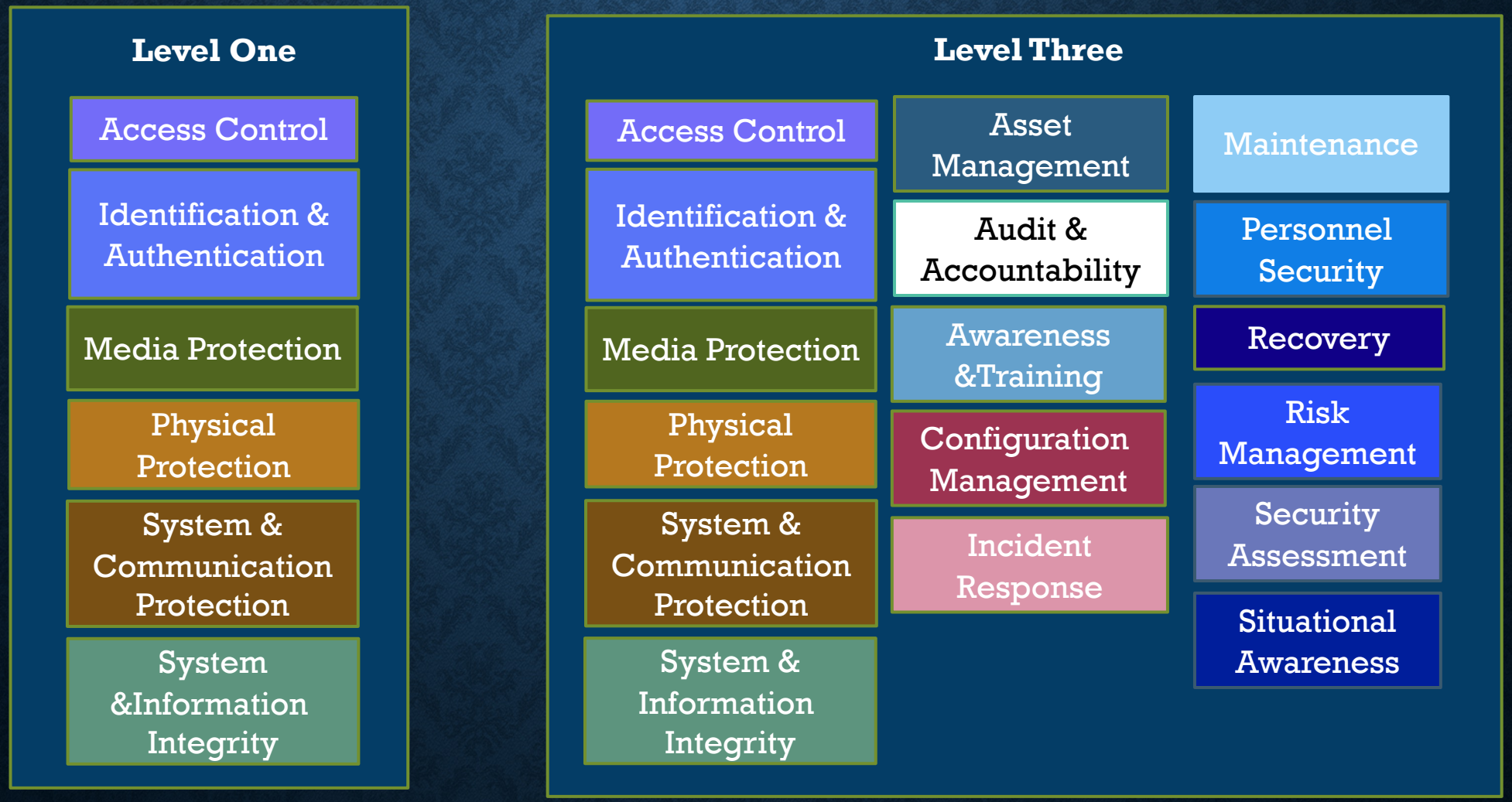
Figure 3. CMMC Levels and Associated Focus

- **Level 1: Federal Contract Information** - is information that is not marked as public or for public release and is subject to minimum cybersecurity requirements. Federal Contract Information does not include information provided by the government to the public or simple transactional information, such as that required to process payments.

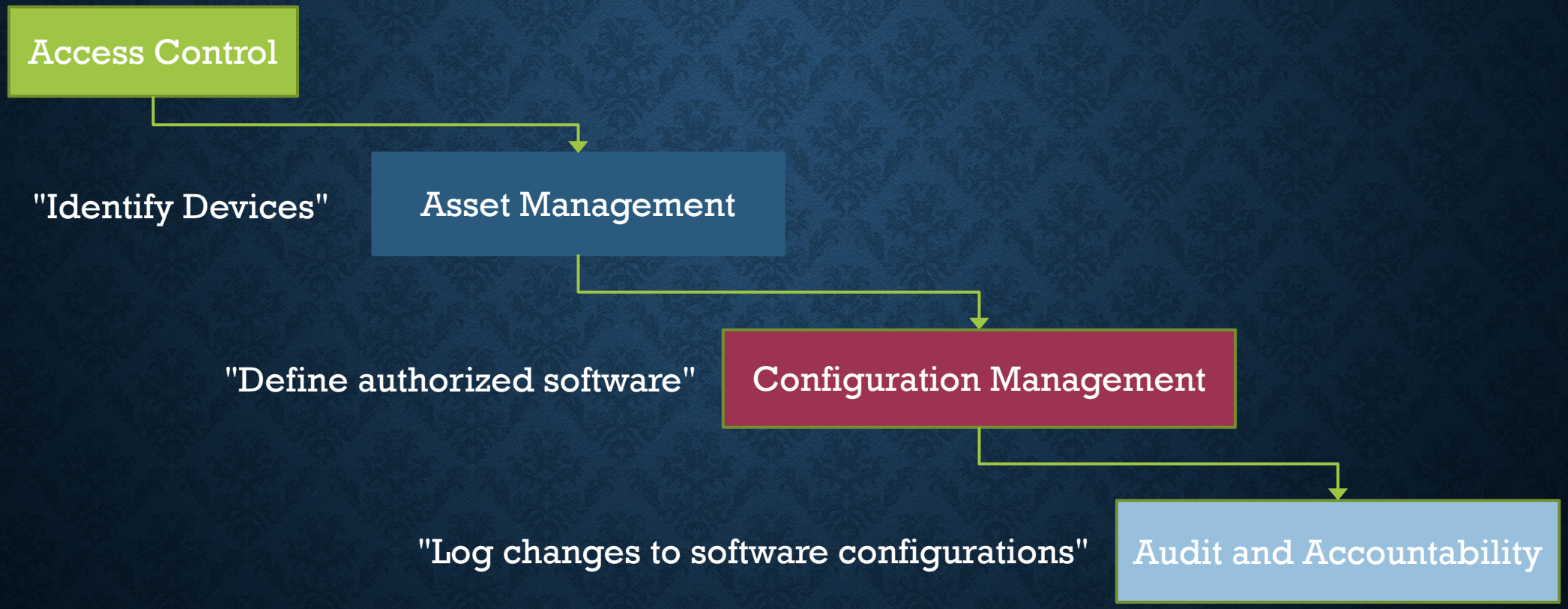
- **Level 3: Controlled Unclassified Information** - is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified. The registry of applicable Controlled Unclassified Information can be found within the National Archives
  - https://www.archives.gov/cui/registry/category-list

CMMC_ModelMain_V1.02

CMMC READINESS - "IDENTIFY YOUR STORIES"



CMMC READINESS - "OVERLAPPING STORIES"



Planning your sprints allows for CMMC to be implemented as an agile process while minimizing the iterations of work required to perform the initial implementation.

METHODOLOGY IN PRACTICE

BY DOMAIN

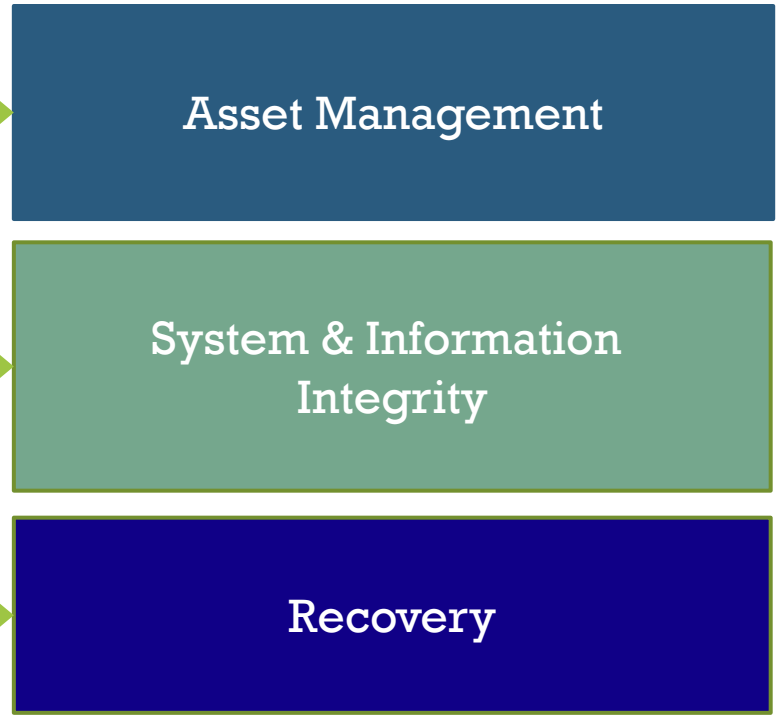
Media Protection

Control: MP.1.118 - Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse."

"Where is your information stored"

"Who can read it"

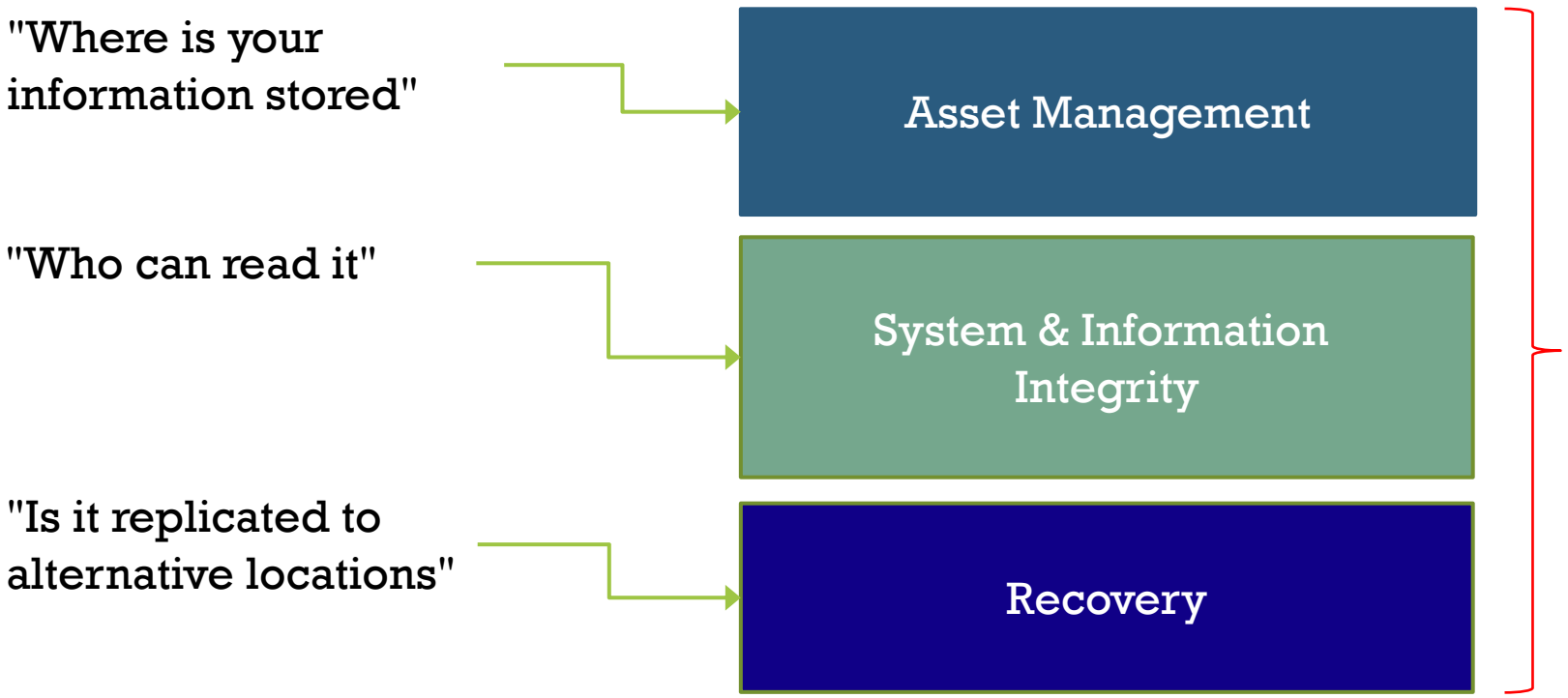
"Is it replicated to alternative locations"



Indirect Challange: Asset Management and Recovery are not required in a level one assessment compared to a level three assessment

Media Protection

Control: MP.1.118 - Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse."



Direct Challenge: Media stored by third party cloud providers cannot be deleted by the organization via traditional methods.

Example: Media Protection Story

Requirement Number	Requirement	Expected Action
MP.1.118	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Cryptoshredding Related Story: System and Information Integrity
MP.2.999	Establish a policy that includes Media Protection.	Develop Media Protection Policy
MP.2.998	Document the CMMC practices to implement the Media Protection policy.	Develop procedure documents to support media protection activities
…. (Continues for remaining 10 practices)	….	…

BY RELATED TASKS

Example: Mixed Domain Story

Requirement Number	Requirement	Expected Action
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	• Write down list of expected user accounts for each system.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	• Review each system and compare user list to documented list of expected users.

BY IMPLEMENTATION

Example: Implement SSO

Task Number	Supports Requirement	Expected Action
T1 – Implementation Scoping	IA.1.076 AC.1.001	• Write down list of expected user accounts for each system • Review each system and compare user list to documented list of expected users • Reconcile delta between expected and actual users • Review limitations and needs based on account types (system vs user)

TOP THREE LESSONS LEARNED

1	2	3
Expected Time Commitment 6 – 12 months. (PDCA) ▪ Information Gathering ▪ Documentation Preparation ▪ System Architecture Reviews ▪ Impact Assessments ▪ Change Control	Be open to change. (Continuous Improvement) ▪ Gain of a better understanding of what your people know ▪ Gain of a better understanding of what your tools can do ▪ Gain of understanding of what your vendors can and cannot do to reduce the scope of compliance	Be included of all required resources. (Synergies) ▪ Executive Sponsors ▪ Business Process Owners ▪ Technology Implementers ▪ Documentation Specialists ▪ Project Managers

INTEGRATION OF LESSONS LEARNED

1	2	3
Read ahead (PDCA) ▪ Look ahead of what your current focused efforts are to prepare for what you anticipate them to be.	Value change. (Continuous Improvement) ▪ Taking a different approach to a process enhances the organizations ability to achieve its objectives.	Create feedback loop (Synergies) ▪ Confirm that implementation team sees value in actions they are performing ▪ Confirm with participating stakeholders that the benchmark of progress made is accurate

Q&A – TOP FIVE

Q1. How soon between now and 2025 will my organization be expected to meet CMMC.	**A1.** As contracts are being renewed the DIB will inform organizations that certification is required. Certification is required at the time of award.
Q2. If we already have other certifications such as PCI, SOC, ISO how much additional work will be required to achieve CMMC certification.	**A2.** Additional efforts to achieve CMMC certification will be based on the initial controls design to meet the specific requirement and the effectiveness of the control to meet the indented capability level.
Q3. How much of the CMMC requirements will be covered by a successful NIST 800-171 implementation.	**A3.** Successfully implementing the NIST 800-171 controls will cover the majority of the CMMC requirements. For a level three certification there would be a remaining 21 controls unique to the CMMC requiring additional implementation.
Q4. Other than an Agile Methodology what other methodologies are organizations using to implement CMMC.	**A4.** High level frameworks such as TOGAF, CMMI, COBIT can guide organization in their designs of enterprise controls and governance processes. Having mature enterprise controls and governance will synergies technology, process, and people to reduce the project friction during CMMC implementation.
Q5. What is the criteria to maintain CMMC certification.	**A5.** CMMC certificate will be valid for 3 years provided that two surveillance audits will be performed on years 2 and 3.

FOR MORE INFORMATION

PATRICIO GARCIA
CEO
KOMPLEYE

SEAN HASSETT
HEAD OF FEDERAL PRACTICE
KOMPLEYE

DARRIN THOMPSON
DIRECTOR,
ENGINEERING
DIRECTEMPLOYERS

HAVE ADDITONAL QUESTIONS OR SUPPORT NEEDS? CONTACT INFO@KOMPLEYE.COM