Cybersecurity Maturity Model Certification (CMMC)

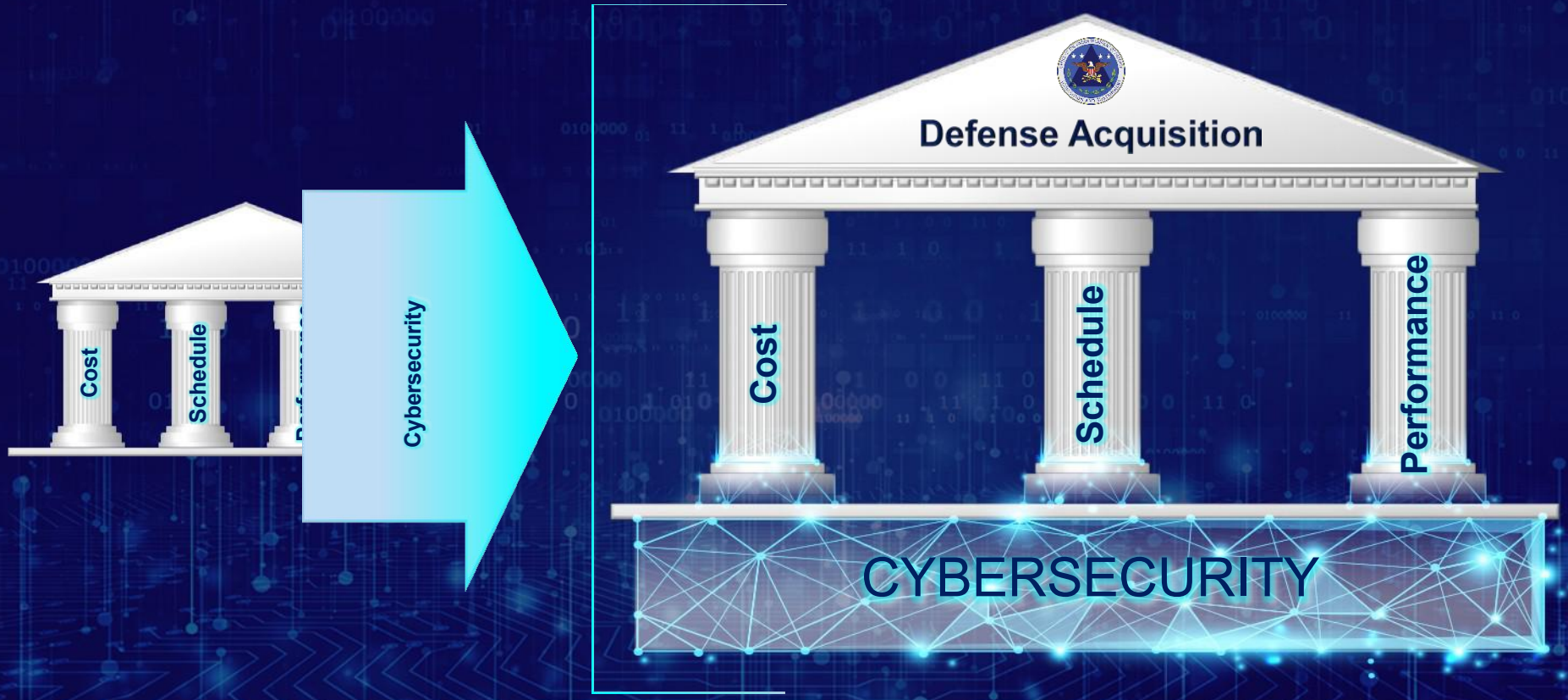
CMMC Model v1.0

31 January 2020

Original: 米国国防総省（Department of Defence: DoD）
https://www.acq.osd.mil/cmmc/index.html
→黄は某氏超訳（どかせばオリジナル英文）

安全な基盤がなければ
すべての機能はリスクに晒される

費用、期間、性能は
セキュアな環境があってこそ機能する



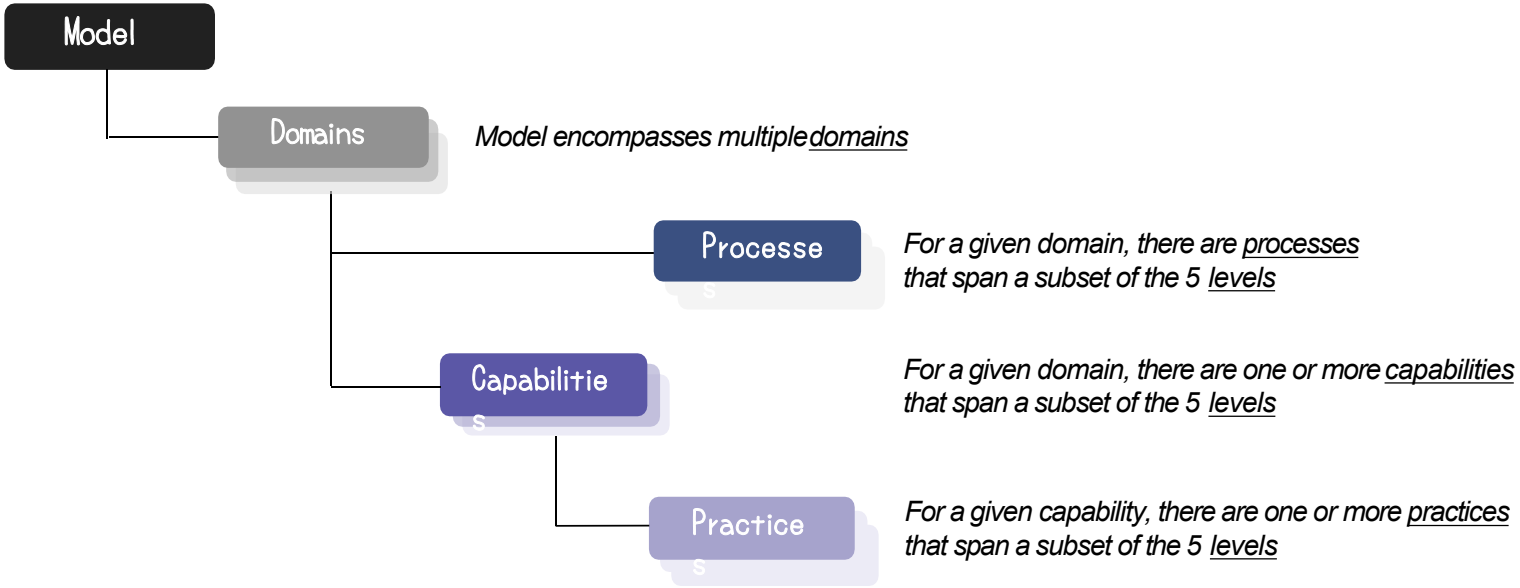
CMMC Model v1.0 Overview

- CMMCは将来のDoDのための、統一されたサイバーセキュリティ標準である
- CMMCモデルv1.0には下記項目が含まれる
  - 17の機能領域(ドメイン)、43の機能
  - 5つのプロセス:プロセスの成熟度測定(5段階)
  - 171のプラクティス:技術的能力測定(5段階)

CMMC Model v1.0: Number of Practices and Processes Introduced at each Level

CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1

CMMC Model Framework



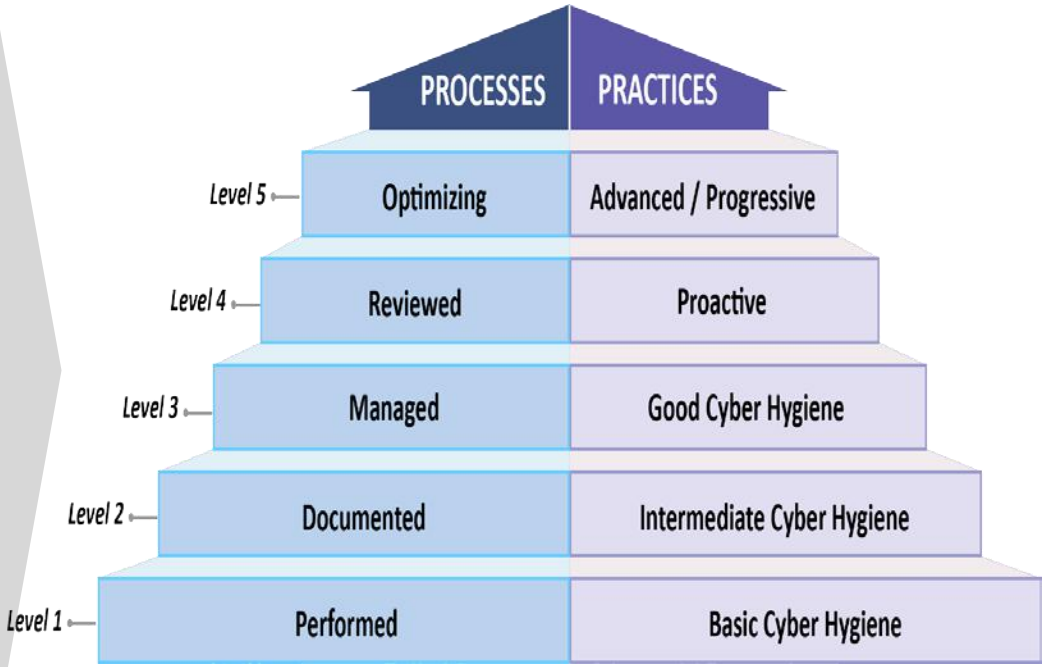
- ・CMMCモデルフレームワークは、プロセスとサイバーセキュリティのベストプラクティスを一連の領域に組み込む
  - プロセスの成熟度またはプロセスの制度化は、(セキュリティ)活動が組織の運用に組み込まれているまたは浸透している範囲を特徴付ける。活動が深く浸透しているほど、次のようになる。
    - 組織は、ストレス(圧力)時を含め、活動を継続して実行する。
    - 結果は、一貫性があり、再現性があり、高品質である。
  - プラクティスは、ドメインの各レベルで実行される活動である。

CMMC Model Structure

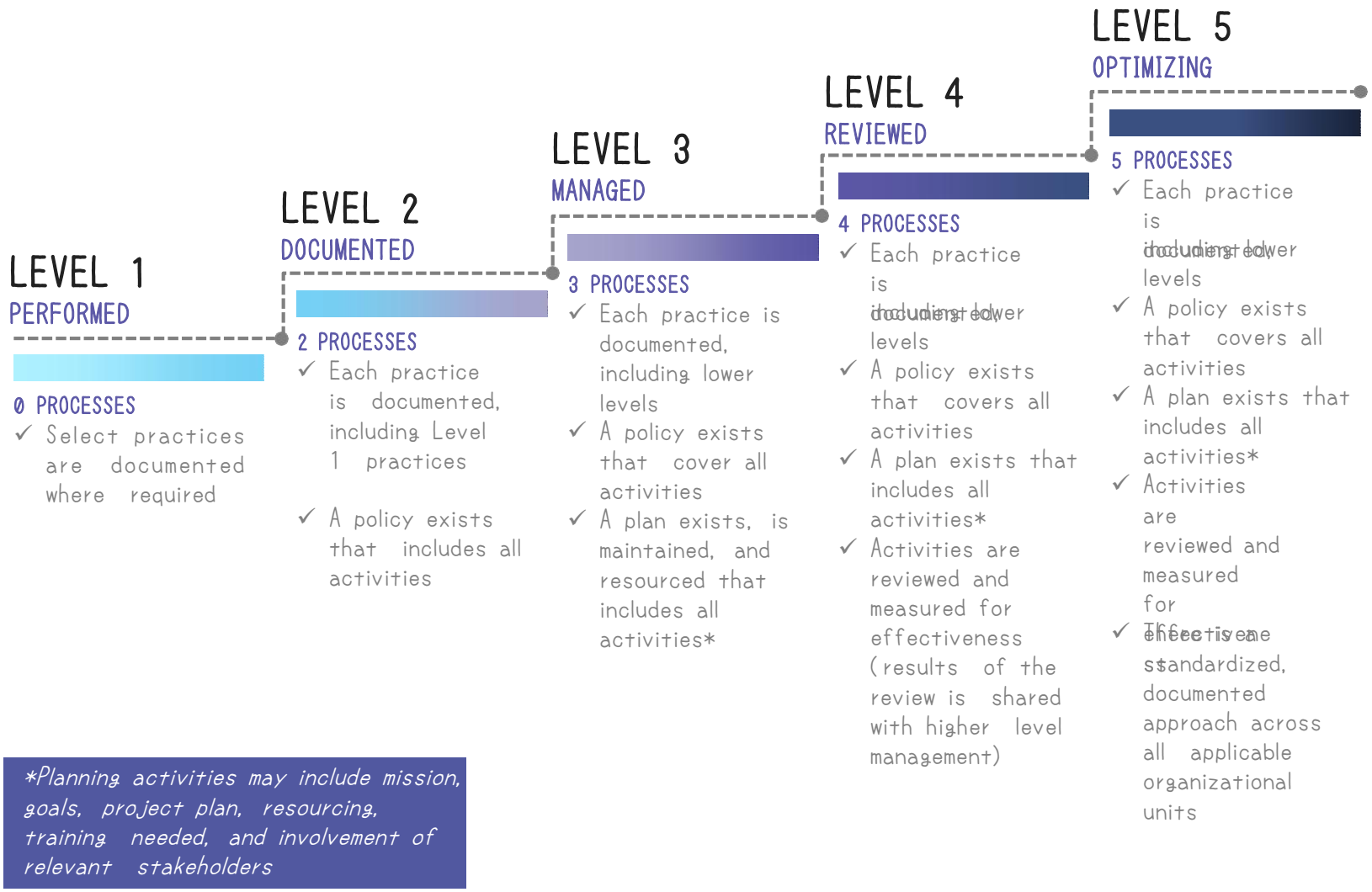
17の機能ドメイン（V1.0）

アクセス制御（AC）	問題対応（IR）	リスク管理（RM）
資産管理（AM）	メンテナンス（MA）	セキュリティ評価（CA）
トレーニングと気付き（AT）	媒体保護（MP）	状況認識（SA）
監査と説明責任（AU）	人事セキュリティ（PS）	システムと通信の保護（SC）
構成管理（CM）	物理防御（PE）	システムと情報の整合性（SI）
認証と認可（IA）	復旧（RE）	

CMMC Model with 5 levels measures cybersecurity maturity

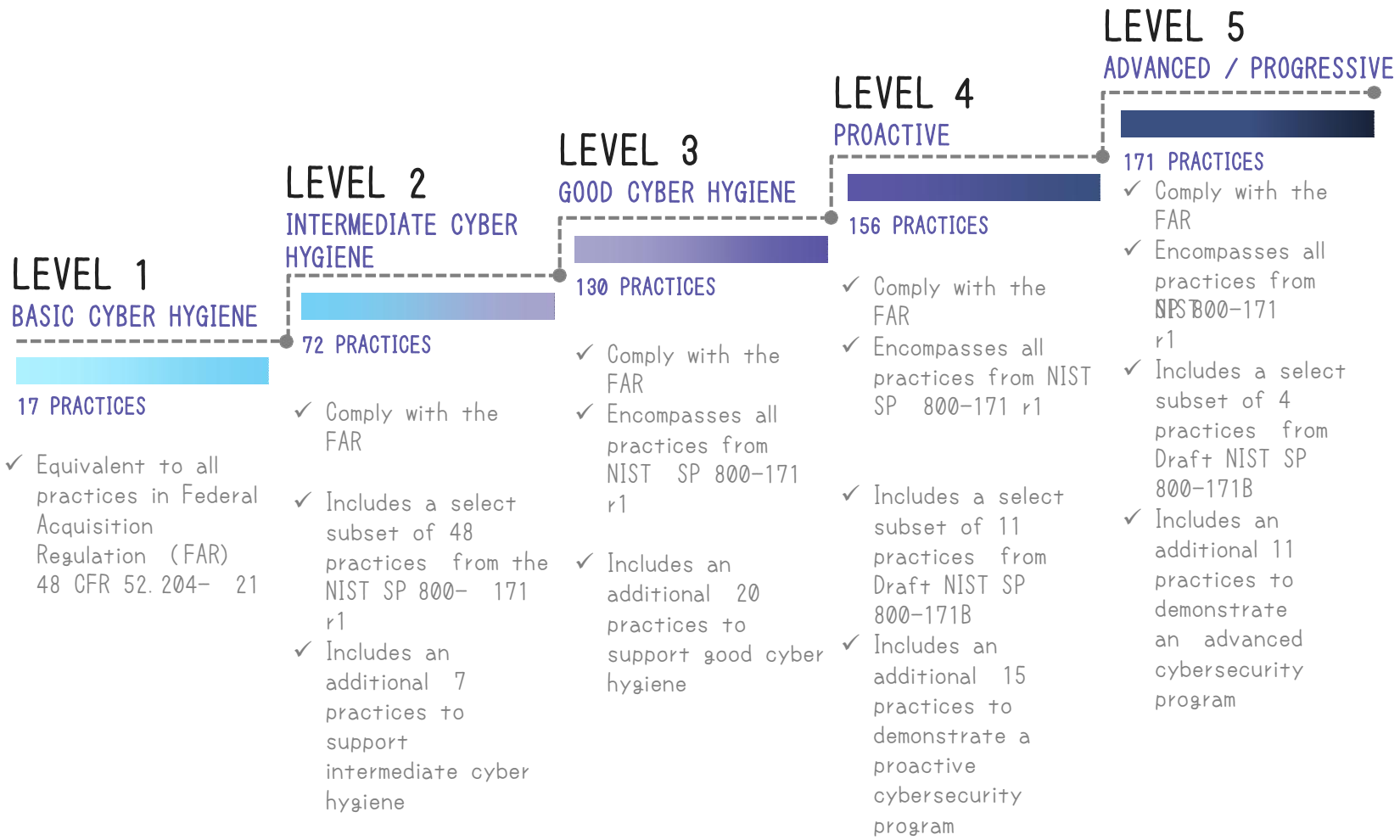


CMMC Maturity Process Progression

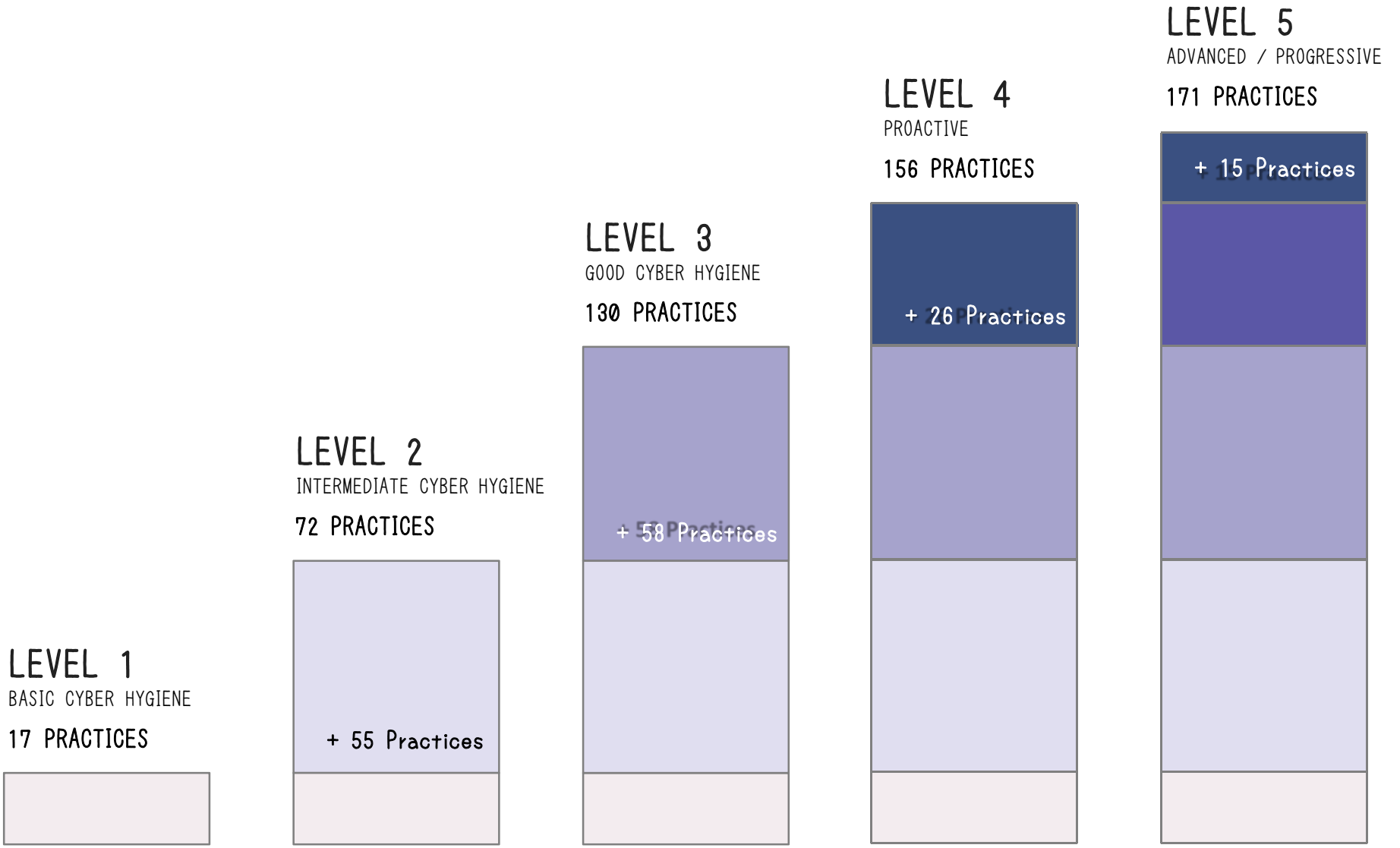


*Planning activities may include mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders

CMMC Practice Progression



CMMC Practices Per Level



CMMC Model v1.0 Source Counts

CMMCモデルは複数の情報元を参照し、活用する
- CMMCレベル1は、FAR条項52.204-21のプラクティスのみに対応している
- CMMCレベル3には、NIST SP 800-171r1およびその他のすべてのプラクティスが含まれる
- CMMCレベル4および5には、ドラフトNIST SP 800-171Bに加えてその他のプラクティスのサブセットが組み込まれている
- UK Cyber EssentialsやAustralia Cyber Security Center Essential Eight Maturity Modelなどの追加ソースも検討され、モデルで参照されている

Draft CMMC Model v1.0: Number of Practices per Source

CMMC Level	Total Number Practices Introduced per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B **	Other
Level 1	17	15*	17*	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11

* Note: 15 safeguarding requirements from FAR clause 52.204-21 correspond to 17 security requirements from NIST SP 800-171r1, and in turn, 17 practices in CMMC

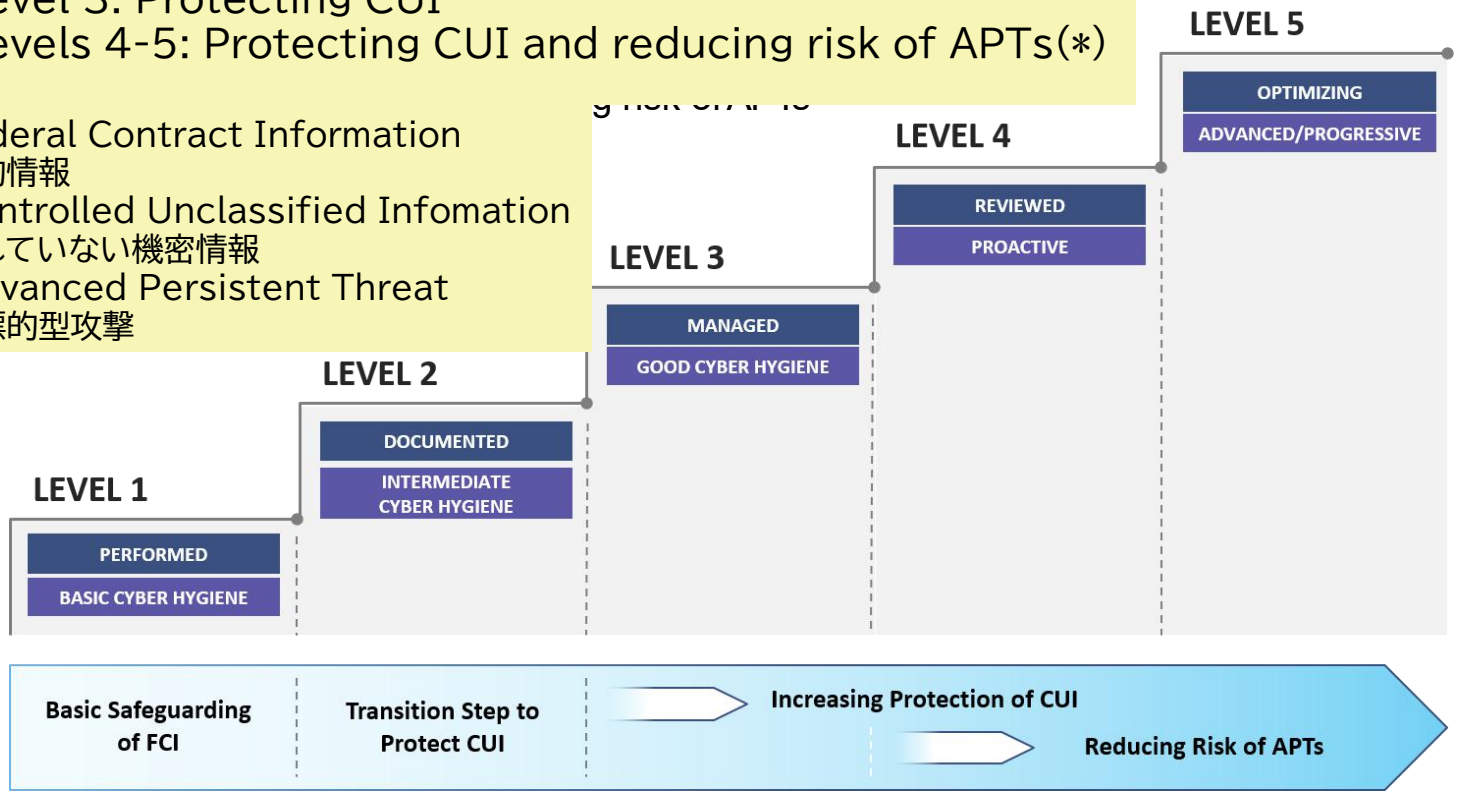
** Note: 18 enhanced security requirements from Draft NIST SP 800-171B have been excluded from CMMC Model v1.0

Summary

・CMMCは将来のDoDのための
　統一されたサイバーセキュリティを確立する
・CMMCは下記焦点のレベルと一致する
　　- Level 1: Basic safeguarding of FCI(*)
　　- Level 2: Transition step to protect CUI(*)
　　- Level 3: Protecting CUI
　　- Levels 4-5: Protecting CUI and reducing risk of APTs(*)

oD acquisitions

* FCI: Federal Contract Information
　連邦契約情報
* CUI: Controlled Unclassified Infomation
　管理されていない機密情報
* APT: Advanced Persistent Threat
　持続的標的型攻撃



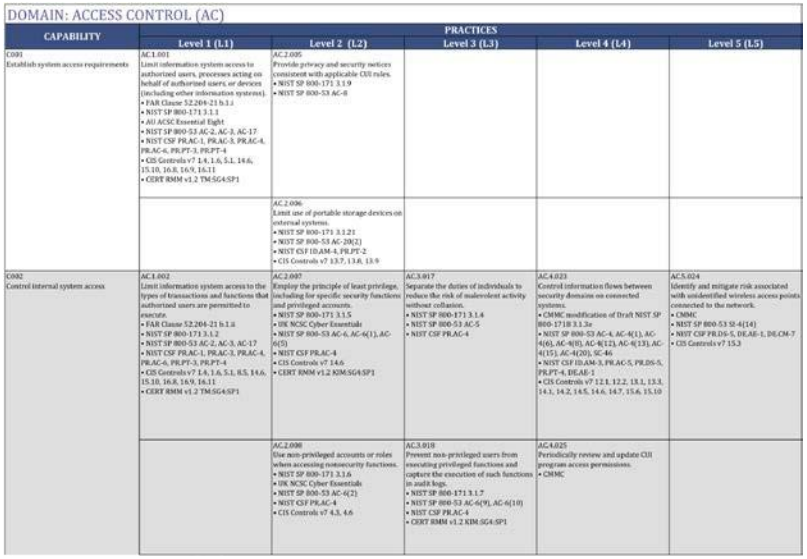
Backups

Supporting Documentation Summary

- **CMMC Model v1.0 document consists of the following:**
  - Introduction, CMMC Model, and Summary
  - Appendix A: CMMC Model v1.0
  - Appendix B: Process and Practice Descriptions
  - Appendix C: Glossary
  - Appendix D: Abbreviations and Acronyms
  - Appendix E: Source Mapping
  - Appendix F: References

Appendix A: CMMC Model v1.0

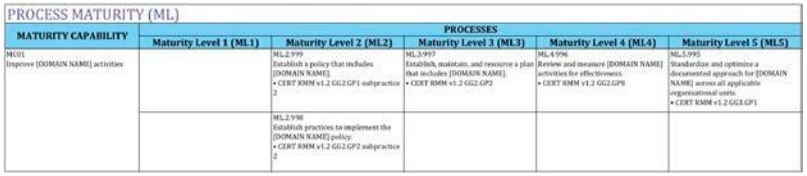
- **Appendix A provides the model in tabular form with all practices organized by Domain (DO), Capability, and Level (L)**
  - Practices are numbered as DO.L.###, with a unique number ###
  - Each practice includes up to nine sources
- **Appendix A also includes maturity level processes**
  - Processes are generalized but apply to all domains
  - Processes are numbered as ML.L.99#



DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight • NIST SP 800-53 AC-2, AC-3, AC-17 • NIST CSF PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CIS Controls v7 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • CERT RMM v1.2 TM:SG4:SP1	AC.2.005 Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 3.1.9 • NIST SP 800-53 AC-8			
		AC.2.006 Limit use of portable storage devices on external systems. • NIST SP 800-171 3.1.21 • NIST SP 800-53 AC-20(2) • NIST CSF ID.AM-4, PR.PT-2 • CIS Controls v7 13.7, 13.8, 13.9			
C002 Control internal system access	AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 3.1.2 • NIST SP 800-53 AC-2, AC-3, AC-17 • NIST CSF PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CIS Controls v7 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • CERT RMM v1.2 TM:SG4:SP1	AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 3.1.5 • UK NCSC Cyber Essentials • NIST SP 800-53 AC-6, AC-6(1), AC-6(5) • NIST CSF PR.AC-4 • CIS Controls v7 14.6 • CERT RMM v1.2 KIM:SG4:SP1	AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4 • NIST SP 800-53 AC-5 • NIST CSF PR.AC-4	AC.4.023 Control information flows between security domains on connected systems. • CMMC modification of Draft NIST SP 800-171B 3.1.3e • NIST SP 800-53 AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20), SC-46 • NIST CSF ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1 • CIS Controls v7 12.1, 12.2, 13.1, 13.3, 14.1, 14.2, 14.5, 14.6, 14.7, 15.6, 15.10	AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CMMC • NIST SP 800-53 SI-4(14) • NIST CSF PR.DS-5, DE.AE-1, DE.CM-7 • CIS Controls v7 15.3
		AC.2.008 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 3.1.6 • UK NCSC Cyber Essentials • NIST SP 800-53 AC-6(2) • NIST CSF PR.AC-4 • CIS Controls v7 4.3, 4.6	AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 3.1.7 • NIST SP 800-53 AC-6(9), AC-6(10) • NIST CSF PR.AC-4 • CERT RMM v1.2 KIM:SG4:SP1	AC.4.025 Periodically review and update CUI program access permissions. • CMMC	

Appendix A Practices



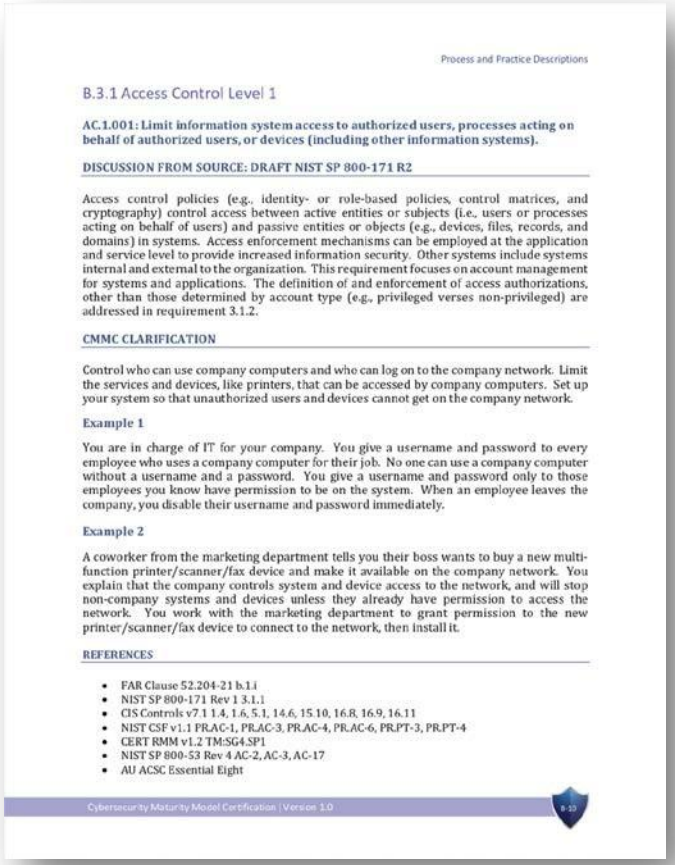
PROCESS MATURITY (ML)

MATURITY CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
MC01 Improve [DOMAIN NAME] activities		ML.2.999 Establish a policy that includes [DOMAIN NAME] • CERT RMM v1.2 GG2.GP1 subpractice 2	ML.3.997 Establish, maintain, and resource a plan that includes [DOMAIN NAME]. • CERT RMM v1.2 GG2.GP2	ML.4.996 Review and measure [DOMAIN NAME] activities for effectiveness. • CERT RMM v1.2 GG2.GP8	ML.5.995 Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organizational units. • CERT RMM v1.2 GG3.GP1
		ML.2.998 Establish practices to implement the [DOMAIN NAME] policy. • CERT RMM v1.2 GG2.GP2 subpractice 2			

Appendix A Processes

Appendix B: Process and Practice Descriptions

- **Appendix B Process and Practice Descriptions include:**
  - Discussion, derived from source material where available
  - Clarification with examples
  - A list of references
- **Same framework as model**
  - Processes are generalized but apply to all domains
  - Practices are ordered by domain and level



Process and Practice Descriptions

B.3.1 Access Control Level 1

AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

DISCUSSION FROM SOURCE: DRAFT NIST SP 800-171 R2

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.

CMMC CLARIFICATION

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

A coworker from the marketing department tells you their boss wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

REFERENCES

- FAR Clause 52.204-21 b.1.i
- NIST SP 800-171 Rev 1 3.1.1
- CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11
- NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
- CERT RMM v1.2 TM:SG4.SP1
- NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17
- AU ACSC Essential Eight

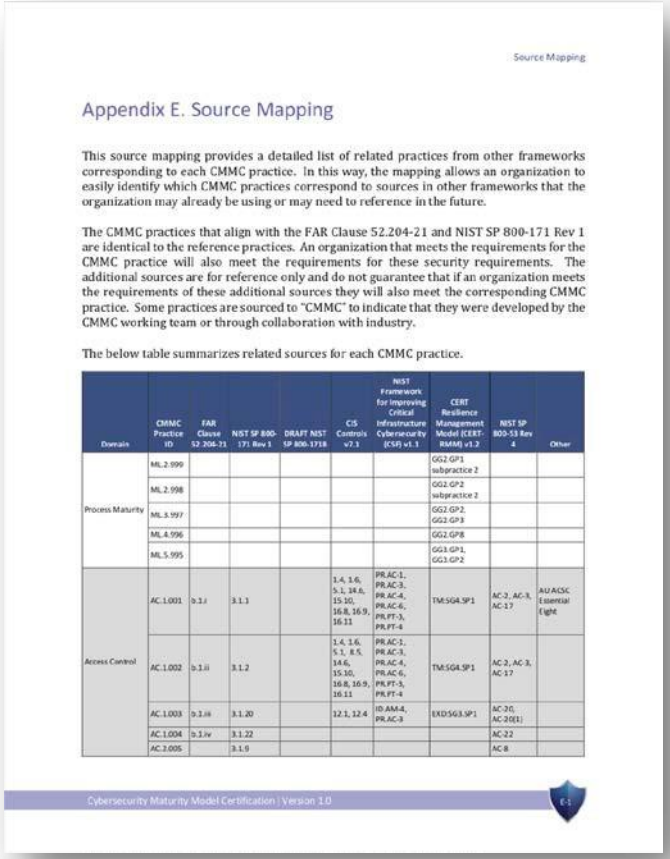
Cybersecurity Maturity Model Certification | Version 1.0

Appendix B Practice & Process Descriptions

Appendix E: Source Mapping

- **Appendix E Source Mapping summarizes the list of sources for all five processes and 171 practices**

- **Sources include:**
  - FAR Clause 52.204-21
  - NIST SP 800-171 Rev 1
  - Draft NIST SP 800-171B
  - CIS Controls v7.1
  - NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1
  - CERT Resilience Management Model (CERT RMM) v1.2
  - NIST SP 800-53 Rev 4
  - Others such as CMMC, UK NCSC Cyber Essentials, or AU ACSC Essential Eight



Source Mapping

Appendix E. Source Mapping

This source mapping provides a detailed list of related practices from other frameworks corresponding to each CMMC practice. In this way, the mapping allows an organization to easily identify which CMMC practices correspond to sources in other frameworks that the organization may already be using or may need to reference in the future.

The CMMC practices that align with the FAR Clause 52.204-21 and NIST SP 800-171 Rev 1 are identical to the reference practices. An organization that meets the requirements for the CMMC practice will also meet the requirements for these security requirements. The additional sources are for reference only and do not guarantee that if an organization meets the requirements of these additional sources they will also meet the corresponding CMMC practice. Some practices are sourced to "CMMC" to indicate that they were developed by the CMMC working team or through collaboration with industry.

The below table summarizes related sources for each CMMC practice.

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 1	DRAFT NIST SP 800-171B	CIS Controls v7.1	NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1	CERT Resilience Management Model (CERT-RMM) v1.2	NIST SP 800-53 Rev 4	Other
Process Maturity	ML.2.999						GG2.GP1 subpractice 2		
	ML.2.998						GG2.GP2 subpractice 2		
	ML.3.997						GG2.GP2, GG2.GP3		
	ML.4.996						GG2.GP8		
	ML.5.995						GG3.GP1, GG3.GP2		
Access Control	AC.1.001	b.1.i	3.1.1		1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4	TM:SG4.SP1	AC-2, AC-3, AC-17	AU ACSC Essential Eight
	AC.1.002	b.1.ii	3.1.2		1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4	TM:SG4.SP1	AC-2, AC-3, AC-17	
	AC.1.003	b.1.iii	3.1.20		12.1, 12.4	ID.AM-4, PR.AC-3	EXD:SG3.SP1	AC-20, AC-20(1)	
	AC.1.004	b.1.iv	3.1.22					AC-22	
	AC.2.005		3.1.9					AC-8	

Cybersecurity Maturity Model Certification | Version 1.0

E-1

Appendix E Source Mapping