AgileIT

ADAPTIVE • RESPONSIVE • STRATEGIC

Conrad Agramont
CEO
Agile IT

Cybersecurity Maturity Model Certification Overview

Delivered by **Agile IT**

We make IT easy

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

AgileIT

By being **100% unapologetically focused on Microsoft cloud services**, we can deliver strategic consulting & technical implementation through a single vendor to our customers

Microsoft Azure

Microsoft 365

AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Key Takeaways

- Defense Industrial Base = Cybersecurity Maturity Model Certification (CMMC)
- Cybersecurity is a lifestyle
- Cybersecurity is an organizational culture
- CMMC is a model and framework *not* an architecture
- Cloud Providers can share responsibility to reduce complexity
- Cloud Providers provide Enterprise capabilities available to more organizations
- Zero Trust principles and design aligns with Cybersecurity and CMMC

Bring on the acronyms

C3PAO	Certified Third-Party Assessor Organization
CISA	Cybersecurity and Infrastructure Security Agency
CDI	Covered Defense Information
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
ITAR	International Traffic in Arms Regulation
NIST	US National Institute of Standards and Technology
POA&M	Plan of Actions and Milestones
DIB	Defense Industrial Base
CMMC-AB RPO	CMMC Accreditation Body Registered Provider Organization

Who should care about CMMC

- Organizations doing business with the U.S. Department of Defense
- Required CMMC level for contractors and sub-contractors will be specified in the solicitation and in Requests for Information (RFIs), if utilized
- On Path with Executive Order 14028, on “Improving the Nation’s Cybersecurity”

Designated High Impact Service Providers

Department of Agriculture

1. Farm Services Agency
2. Forest Service
3. Food and Nutrition Service
4. Natural Resource Conservation Service
5. Rural Development

Department of Commerce

6. Census
7. United States Patents and Trademarks Office

Department of Education

8. Federal Student Aid

General Services Administration

9. USA.gov

Department of Health and Human Services

10. Centers for Medicaid and Medicare Services

Department of Homeland Security

11. Citizenship and Immigration Services
12. Customs and Border Protection
13. Federal Emergency Management Agency
14. Transportation Security Administration

Department of Housing & Urban Development

15. Housing and Urban Development

Department of the Interior

16. Bureau of Indian Affairs
17. Bureau of Trust Fund Administration
18. Fish and Wildlife Service
19. National Park Service

Agency for International Development

20. Agency for International Development

Department of Labor

21. Employment and Training Administration
22. Employee Benefits Security Administration
23. Occupational Safety and Health Administration
24. Office of Workers' Compensation Programs

Office of Personnel Management

25. Federal Employment Services
26. Retirement Services

Small Business Administration

27. Small Business Administration

Social Security Administration

28. Social Security Administration

Department of State

29. Passport Services

Department of Transportation

30. Build America Bureau

Department of the Treasury

31. Treasury Department
32. Internal Revenue Service

Department of Veterans Affairs

33. Veterans Benefits Administration
34. Veterans Health Administration

Cross-Agency Coordination

35. Recreation.gov

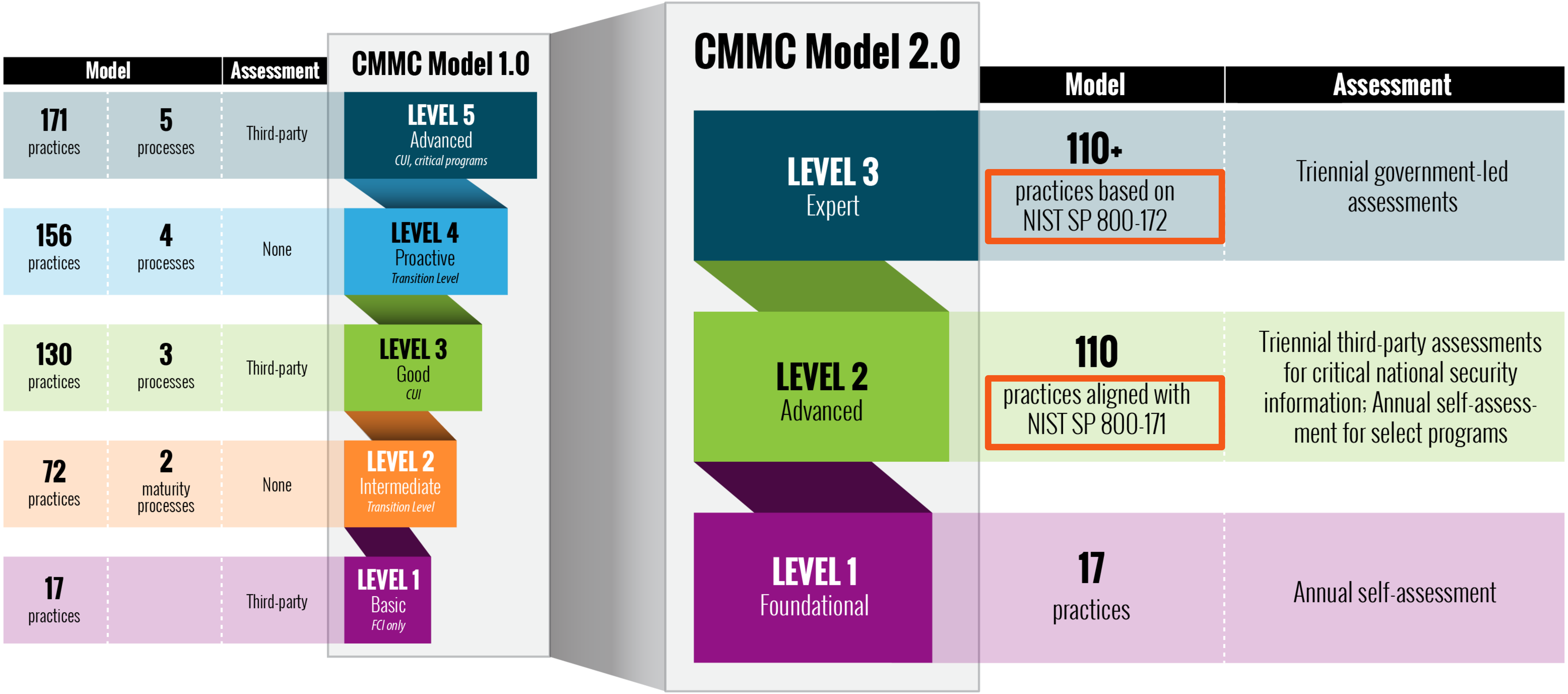
The included entities are identified as High Impact Service Providers (HISPs) and are subject to OMB Circular A-11 Section 280 activities including an annual enterprise-wide CX capacity assessment and action planning, designation of at least two high impact services, improved performance management for designated services, customer feedback collection and public reporting.

https://performance.gov/cx/

BY THE PEOPLE
FOR THE PEOPLE
WITH THE PEOPLE

CMMC Primary Goals

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards



Model		Assessment	CMMC Model 1.0
171 practices	**5** processes	Third-party	**LEVEL 5** Advanced *CUI, critical programs*
156 practices	**4** processes	None	**LEVEL 4** Proactive *Transition Level*
130 practices	**3** processes	Third-party	**LEVEL 3** Good *CUI*
72 practices	**2** maturity processes	None	**LEVEL 2** Intermediate *Transition Level*
17 practices		Third-party	**LEVEL 1** Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Scale and Scope

Variable

- **People**
- Number of users
- Culture
- Business process

- **Environment**
- Infrastructure
- Devices
- Application and Services

- **IT Management**
- Staffing size, maturity, and operations
- Collection of services, tools, and processes

Fixed

- **CMMC**
- Same requirements for all

- **Cybersecurity threats**
- Bad actors target all sizes and types of business
- People Hacking is REAL & Effective
- Good people trying to do good things, but did bad things

- **Insurance**
- Cybersecurity Insurance is getting specific

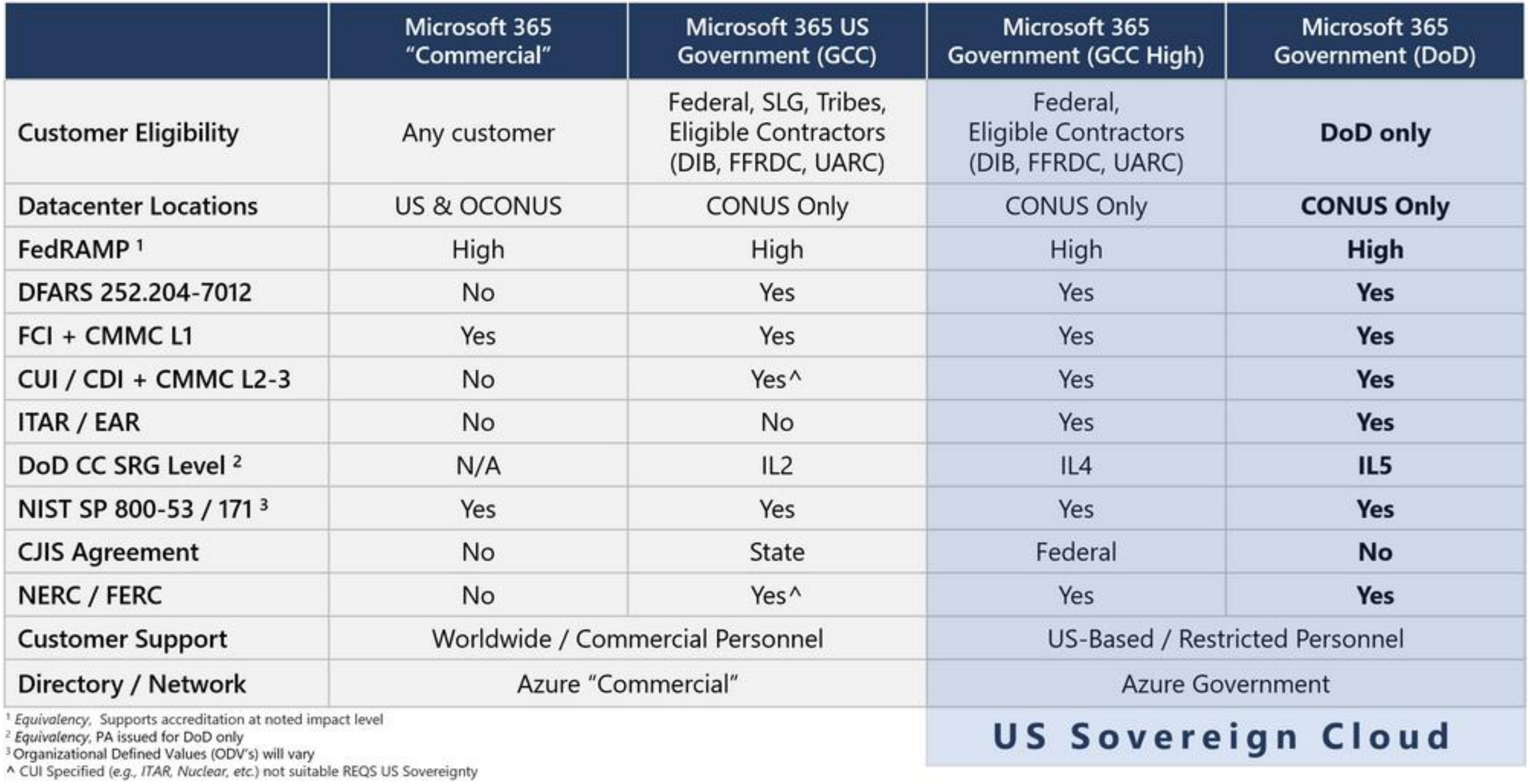
AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Shared Responsibility Model

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Microsoft Clouds



	Microsoft 365 "Commercial"	Microsoft 365 US Government (GCC)	Microsoft 365 Government (GCC High)	Microsoft 365 Government (DoD)
Customer Eligibility	Any customer	Federal, SLG, Tribes, Eligible Contractors (DIB, FFRDC, UARC)	Federal, Eligible Contractors (DIB, FFRDC, UARC)	**DoD only**
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	**CONUS Only**
FedRAMP [1]	High	High	High	**High**
DFARS 252.204-7012	No	Yes	Yes	**Yes**
FCI + CMMC L1	Yes	Yes	Yes	**Yes**
CUI / CDI + CMMC L2-3	No	Yes^	Yes	**Yes**
ITAR / EAR	No	No	Yes	**Yes**
DoD CC SRG Level [2]	N/A	IL2	IL4	**IL5**
NIST SP 800-53 / 171 [3]	Yes	Yes	Yes	**Yes**
CJIS Agreement	No	State	Federal	**No**
NERC / FERC	No	Yes^	Yes	**Yes**
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure "Commercial"		Azure Government	
			US Sovereign Cloud	

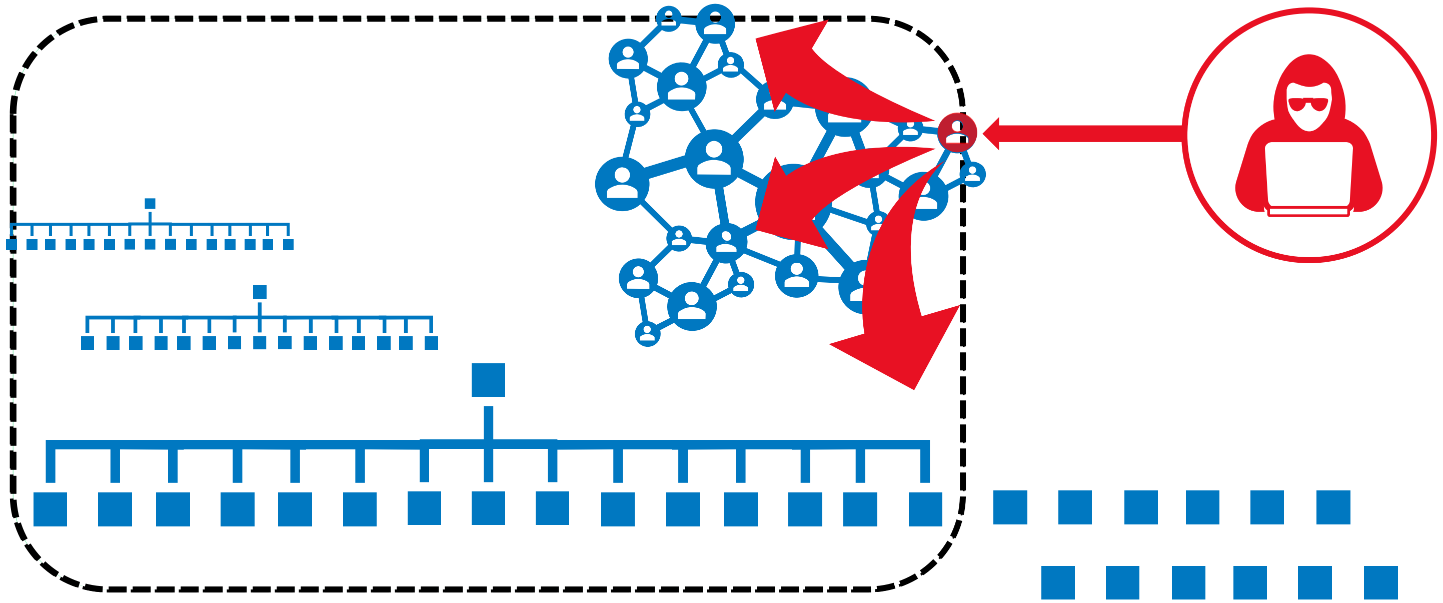
[1] *Equivalency*, Supports accreditation at noted impact level
[2] *Equivalency*, PA issued for DoD only
[3] Organizational Defined Values (ODV's) will vary
^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

https://techcommunity.microsoft.com/t5/public-sector-blog/understanding-compliance-between-commercial-government-and-dod/ba-p/3258326

AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Why are we having a Zero Trust conversation?

Keep **Assets** away from **Attackers**



1. IT Security is Complex
   - Many Devices, Users, & Connections
2. “Trusted network” security strategy
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within the network
3. Assets increasingly leave the network
   - BYOD, WFH, Mobile, and SaaS
4. Attackers shift to identity attacks
   - Phishing and credential theft
   - Security teams often overwhelmed

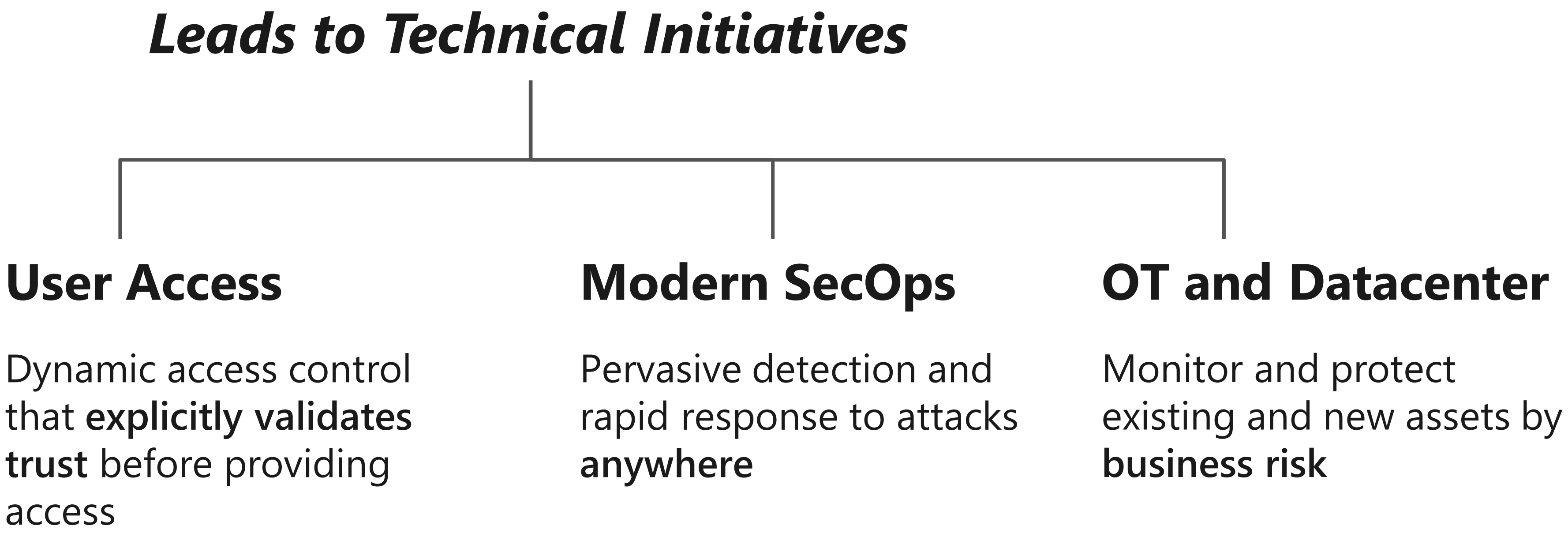
AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Zero Trust

- Simplify
- Integrate
- Automate
- Consolidate

Security Strategy for

- **business assets** (data, applications, devices)
- **everywhere** (private & public networks)



Leads to Technical Initiatives

User Access

Dynamic access control that **explicitly validates trust** before providing access

Modern SecOps

Pervasive detection and rapid response to attacks **anywhere**

OT and Datacenter

Monitor and protect existing and new assets by **business risk**

Increases security

Increases productivity

Zero Trust Rapid Modernization Plan (RaMP)

Prioritize rapid progress on highest positive impact

Roll out to IT Admins first

- Targeted by Attackers
- High potential impact
- Provide technical feedback

Top Priorities – critical security modernization steps

User Access and Productivity
Zero Trust Foundations

1. **Explicitly validate trust for all access requests (via Azure AD Conditional Access)**
   a. **User Accounts** - Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
   b. **Endpoints** - Require device integrity for access (configuration compliance first, then XDR signals
   c. **Apps -** Enable Azure AD for all SaaS, for VPN authentication, and for legacy apps (on-premises + IaaS) via App Proxy
   d. **Network -** Establish basic traffic filtering and segmentation to isolate business-critical or highly vulnerable resources

Data, Compliance & Governance
Align to business and mission

2. **Ransomware Recovery Readiness -** Ensure backups are validated, secure, and immutable to enable rapid recovery
3. **Data -** Discover and protect sensitive data (via Microsoft Info Protection, Defender for Cloud Apps, CA App Control)

Modern Security Operations

4. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Defender for Cloud)
5. **Unify Visibility** with modern Security Information and Event Management (SIEM via Microsoft Sentinel)
6. **Reduce manual effort** - using automated investigation/remediation (SOAR), enforcing alert quality, and threat hunting

As Needed – typically driven by cloud adoption or OT/IoT usage

Infrastructure & Development
Datacenter & DevOps Security

Security Hygiene – Rigorously monitor+remediate security configurations, permissions (CIEM), security updates, and more

Reduce Legacy Risk – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)

DevOps Integration – Integrate infrastructure + development security practices into DevOps with minimal friction

Microsegmentation – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

Align to cloud migration schedule

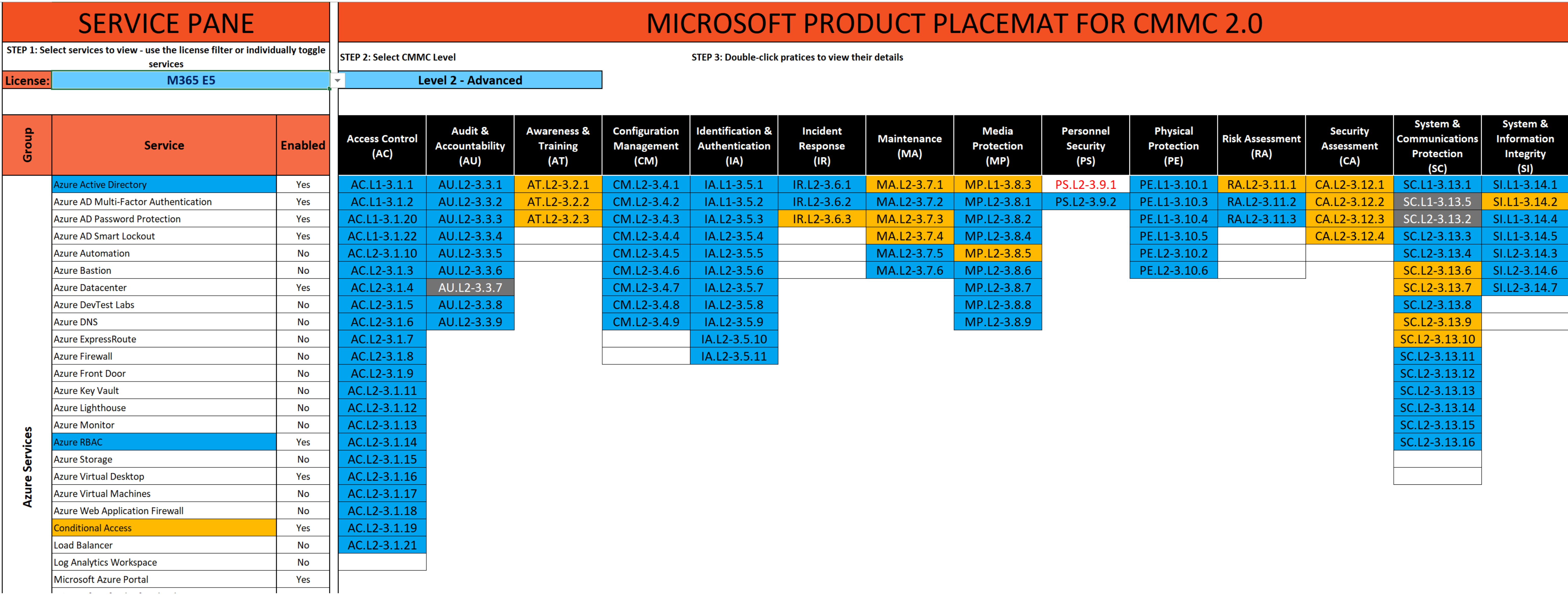
Operational Technology (OT) and Industrial IoT

Discover – Find & classify assets with business critical, life safety, and operational/physical impact (via Defender for IoT)

Protect – isolate assets from unneeded internet/production access with static and dynamic controls

Monitor – unify threat detection and response processes for OT, IT, and IoT assets (via Microsoft Defender for IoT)

Microsoft CMMC Product Placemat (Microsoft 365 E5)



SERVICE PANE

MICROSOFT PRODUCT PLACEMAT FOR CMMC 2.0

STEP 1: Select services to view - use the license filter or individually toggle services

License: M365 E5

STEP 2: Select CMMC Level

Level 2 - Advanced

STEP 3: Double-click pratices to view their details

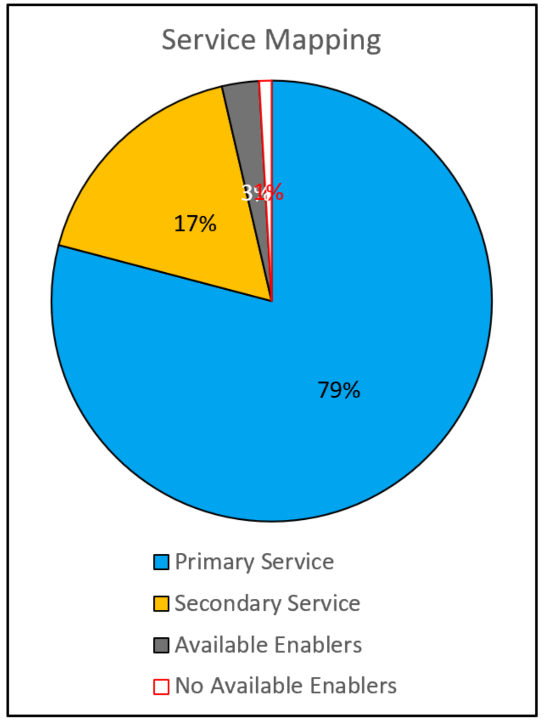
Group	Service	Enabled
Azure Services	Azure Active Directory	Yes
	Azure AD Multi-Factor Authentication	Yes
	Azure AD Password Protection	Yes
	Azure AD Smart Lockout	Yes
	Azure Automation	No
	Azure Bastion	No
	Azure Datacenter	Yes
	Azure DevTest Labs	No
	Azure DNS	No
	Azure ExpressRoute	No
	Azure Firewall	No
	Azure Front Door	No
	Azure Key Vault	No
	Azure Lighthouse	No
	Azure Monitor	No
	Azure RBAC	Yes
	Azure Storage	No
	Azure Virtual Desktop	Yes
	Azure Virtual Machines	No
	Azure Web Application Firewall	No
	Conditional Access	Yes
	Load Balancer	No
	Log Analytics Workspace	No
	Microsoft Azure Portal	Yes

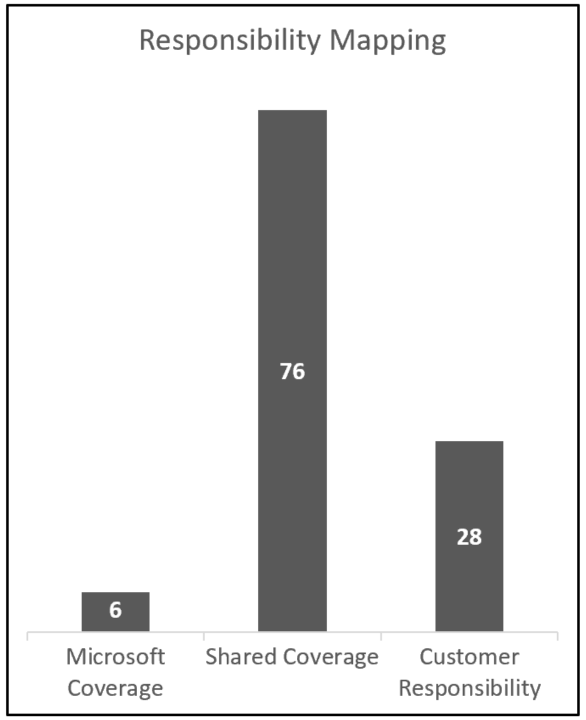
Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.11.2	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.2	SI.L1-3.14.4
AC.L1-3.1.22	AU.L2-3.3.4		CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5		CA.L2-3.12.4	SC.L2-3.13.3	SI.L1-3.14.5
AC.L2-3.1.10	AU.L2-3.3.5		CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2			SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6			SC.L2-3.13.6	SI.L2-3.14.6
AC.L2-3.1.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.7	SI.L2-3.14.7
AC.L2-3.1.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.8	
AC.L2-3.1.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.9	
AC.L2-3.1.7				IA.L2-3.5.10								SC.L2-3.13.10	
AC.L2-3.1.8				IA.L2-3.5.11								SC.L2-3.13.11	
AC.L2-3.1.9												SC.L2-3.13.12	
AC.L2-3.1.11												SC.L2-3.13.13	
AC.L2-3.1.12												SC.L2-3.13.14	
AC.L2-3.1.13												SC.L2-3.13.15	
AC.L2-3.1.14												SC.L2-3.13.16	
AC.L2-3.1.15													
AC.L2-3.1.16													
AC.L2-3.1.17													
AC.L2-3.1.18													
AC.L2-3.1.19													
AC.L2-3.1.21													

Microsoft CMMC Product Placemat: https://aka.ms/cmmc/productplacemat

Microsoft CMMC Product Placemat (Microsoft 365 E5)

Microsoft Azure Portal	Yes
Microsoft Defender for Cloud	No
Microsoft Defender for Identity	Yes
Microsoft Defender for IoT	No
Microsoft Sentinel	Yes
Named Locations	Yes
Network Security Groups	No
Privileged Identity Management (PIM)	Yes
Security Patterns	No
Virtual Network	No
VPN Gateway	No
Customer Key	Yes
Customer Lockbox	Yes
Entitlement Management	Yes
Exchange Admin Center	Yes
Insider Risk Management	Yes
Microsoft 365 Admin Center	Yes
Microsoft 365 Compliance Center	Yes
Microsoft 365 DLP	Yes
Microsoft 365 for Enterprise Test Lab	Yes
Microsoft 365 Groups	Yes
Microsoft 365 Lighthouse	Yes
Microsoft 365 Security Center	Yes
Microsoft 365 Web Apps	Yes
Microsoft Defender Antivirus Cloud Protection	Yes
Microsoft Defender for Cloud Apps	Yes
Microsoft Defender for Office 365	Yes
Microsoft Defender SmartScreen	No
Windows Hello for Business	Yes
Bitlocker	Yes
Intune/Microsoft Endpoint Manager	Yes
Microsoft 365 Defender	Yes
Microsoft Defender for Endpoint	Yes
Microsoft Graph	Yes
Microsoft Information Protection	Yes
Office 365 Message Encryption (OME)	Yes
Power Automate	Yes
Privileged Access Management	Yes
Secure Score	Yes
Teams	Yes
Threat and Vulnerability Management	Yes
GitHub Advanced Security (Add-On)	No
GitHub AE	No
GitHub Enterprise Cloud	No
App Locker	No
Direct Access	Yes
Distributed Key Manager	Yes





Microsoft Inherited Service Mapping			
Primary Service	🟦	87	79%
Secondary Service	🟨	19	17%
Available Enablers	⬛	3	3%
No Available Enablers		1	1%

CMMC Practice Details	
CMMC Practice	**AC.L1-3.1.1**
Description	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
Responsibility	Shared Coverage

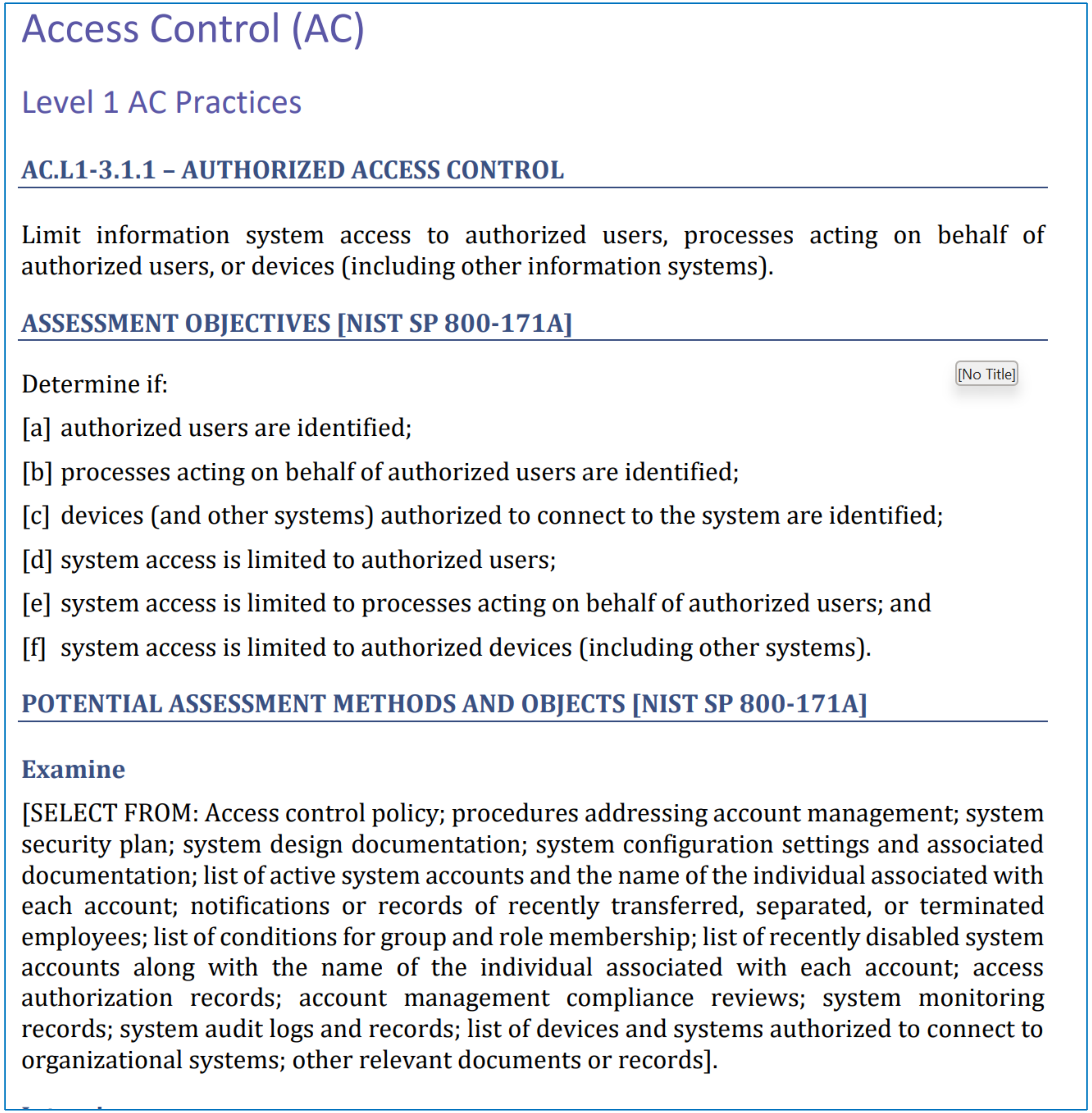
AC.L1-3.1.1 - Customer Implementation Guidance

It is good practice to assign permissions using the principle of least permissions; this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC.

RBAC helps in the creation and assignment of different permissions to different identities. This helps in segregating duties within teams, rather than everyone having all permissions. RBAC helps in making people responsible for their job because others might not even have the necessary access to perform it. It should be noted that providing permissions at a greater scope automatically ensures that child resources inherit those permissions. For example, providing an identity with read access for a resource group means that the identity will have read access to all the resources within that group, too.

Customer Responsibility:

- Responsible for authorizing access to the customer system.



Access Control (AC)

Level 1 AC Practices

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

[No Title]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

AC.L2-3.1.1

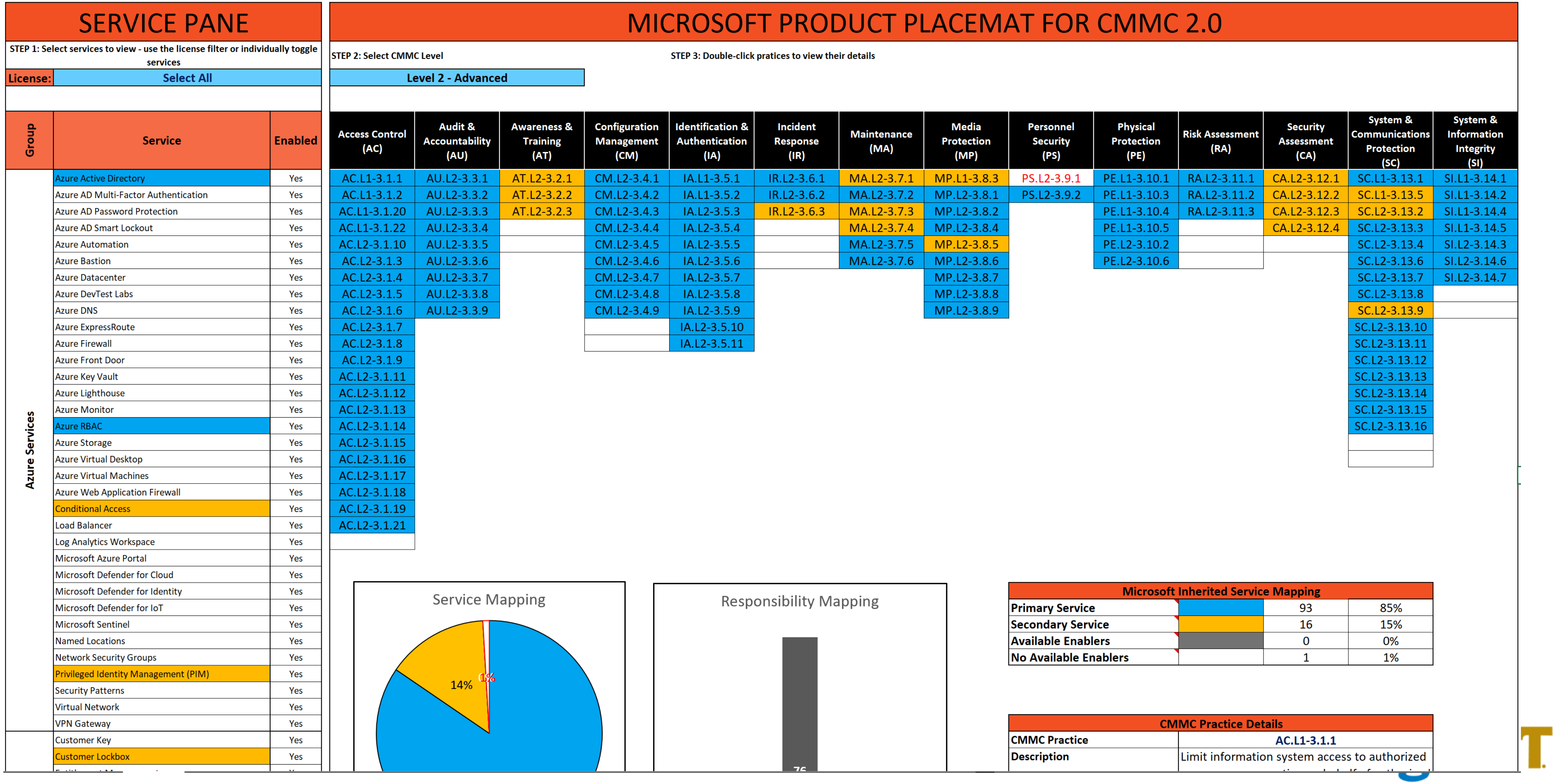
<table>
<tr><th colspan="2">Control Summary Information</th></tr>
<tr><td colspan="2"><b>NIST 800-53 Mapping:</b> AC-2, AC-3, AC-17</td></tr>
<tr><td colspan="2"><b>Control</b> : Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).</td></tr>
<tr><th>Primary Services</th><th>Secondary Services</th></tr>
<tr><td>Azure Active Directory
Azure RBAC
Intune/Microsoft Endpoint Manager</td><td>Microsoft Information Protection
Conditional Access
Customer Lockbox
Privileged Identity Management (PIM)
Security and Compliance Center
Microsoft 365 Web Apps
M365 Groups</td></tr>
</table>

Microsoft Technical Reference Guide for CMMC: https://aka.ms/cmmc/techrefguide

AC.L2-3.1.10

Control Summary Information	
NIST 800-171 Mapping: 3.1.10	
NIST 800-53 Mapping: AC-11, AC-11(1)	
Control : Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
Primary Services	**Secondary Services**
Azure Active Directory Conditional Access	Microsoft Azure Portal Azure Virtual Machines Microsoft 365 Web Apps Intune/Microsoft Endpoint Manager

Microsoft CMMC Product Placemat (All)



SERVICE PANE

STEP 1: Select services to view - use the license filter or individually toggle services

License: Select All

Group	Service	Enabled
Azure Services	Azure Active Directory	Yes
	Azure AD Multi-Factor Authentication	Yes
	Azure AD Password Protection	Yes
	Azure AD Smart Lockout	Yes
	Azure Automation	Yes
	Azure Bastion	Yes
	Azure Datacenter	Yes
	Azure DevTest Labs	Yes
	Azure DNS	Yes
	Azure ExpressRoute	Yes
	Azure Firewall	Yes
	Azure Front Door	Yes
	Azure Key Vault	Yes
	Azure Lighthouse	Yes
	Azure Monitor	Yes
	Azure RBAC	Yes
	Azure Storage	Yes
	Azure Virtual Desktop	Yes
	Azure Virtual Machines	Yes
	Azure Web Application Firewall	Yes
	Conditional Access	Yes
	Load Balancer	Yes
	Log Analytics Workspace	Yes
	Microsoft Azure Portal	Yes
	Microsoft Defender for Cloud	Yes
	Microsoft Defender for Identity	Yes
	Microsoft Defender for IoT	Yes
	Microsoft Sentinel	Yes
	Named Locations	Yes
	Network Security Groups	Yes
	Privileged Identity Management (PIM)	Yes
	Security Patterns	Yes
	Virtual Network	Yes
	VPN Gateway	Yes
	Customer Key	Yes
	Customer Lockbox	Yes

MICROSOFT PRODUCT PLACEMAT FOR CMMC 2.0

STEP 2: Select CMMC Level

Level 2 - Advanced

STEP 3: Double-click pratices to view their details

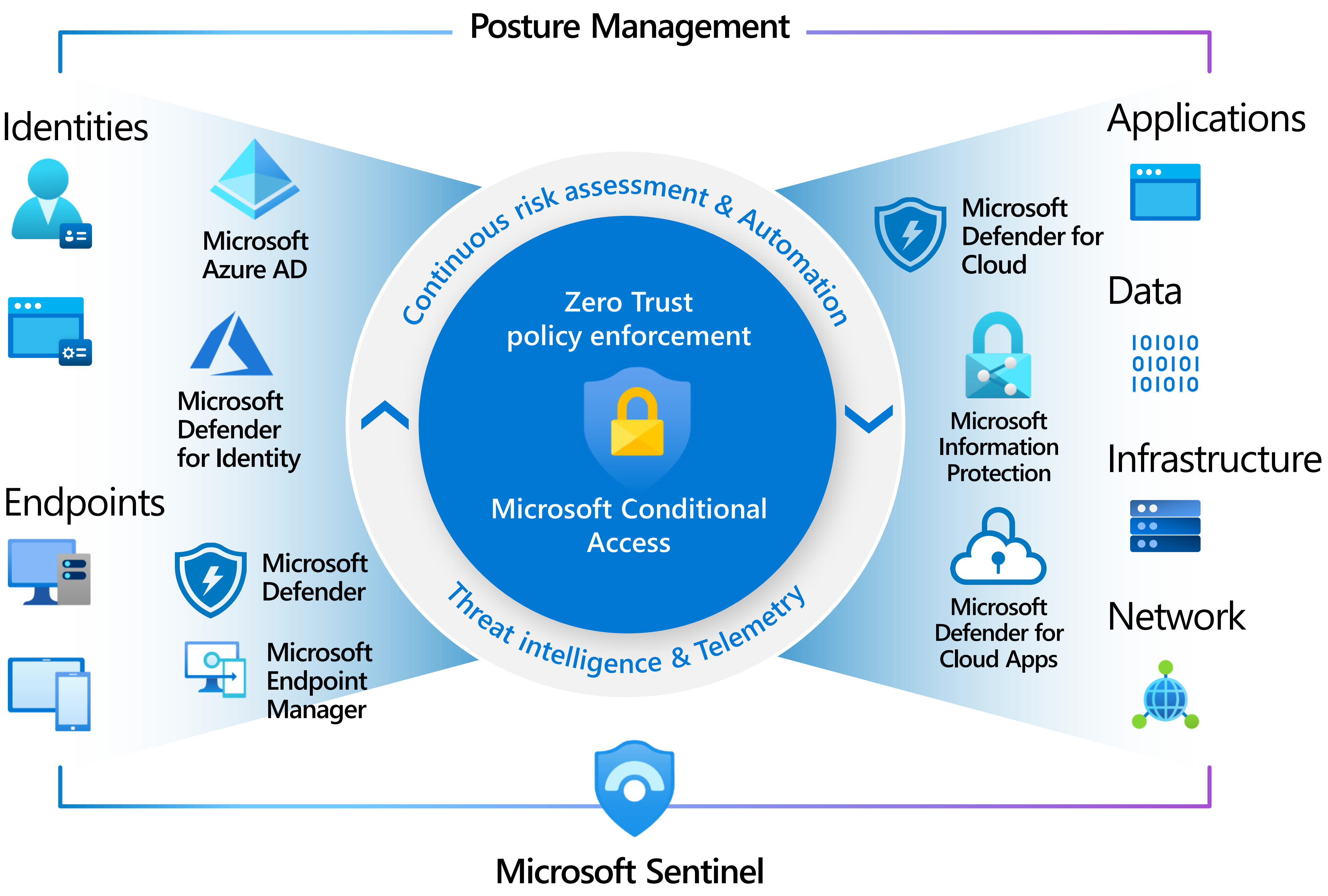
Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.11.2	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.2	SI.L1-3.14.4
AC.L1-3.1.22	AU.L2-3.3.4		CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5		CA.L2-3.12.4	SC.L2-3.13.3	SI.L1-3.14.5
AC.L2-3.1.10	AU.L2-3.3.5		CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2			SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6			SC.L2-3.13.6	SI.L2-3.14.6
AC.L2-3.1.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.7	SI.L2-3.14.7
AC.L2-3.1.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.8	
AC.L2-3.1.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.9	
AC.L2-3.1.7				IA.L2-3.5.10								SC.L2-3.13.10	
AC.L2-3.1.8				IA.L2-3.5.11								SC.L2-3.13.11	
AC.L2-3.1.9												SC.L2-3.13.12	
AC.L2-3.1.11												SC.L2-3.13.13	
AC.L2-3.1.12												SC.L2-3.13.14	
AC.L2-3.1.13												SC.L2-3.13.15	
AC.L2-3.1.14												SC.L2-3.13.16	
AC.L2-3.1.15													
AC.L2-3.1.16													
AC.L2-3.1.17													
AC.L2-3.1.18													
AC.L2-3.1.19													
AC.L2-3.1.21													

Microsoft Inherited Service Mapping			
Primary Service	🟦	93	85%
Secondary Service	🟨	16	15%
Available Enablers	⬛	0	0%
No Available Enablers		1	1%

CMMC Practice Details	
CMMC Practice	AC.L1-3.1.1
Description	Limit information system access to authorized

ADAPTIVE • RESPONSIVE • STRATEGIC

Microsoft Zero Trust Capabilities

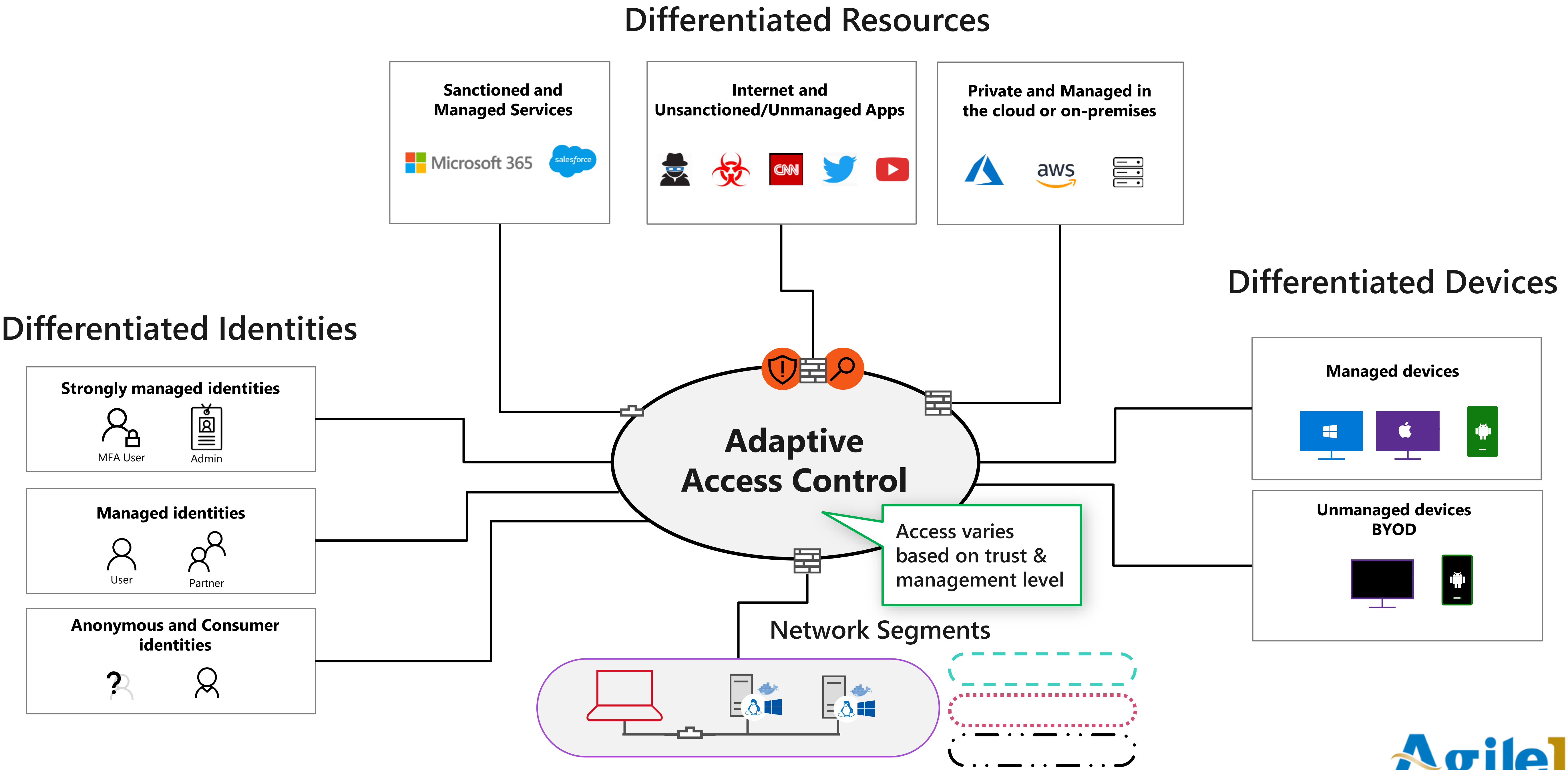


Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Microsoft Defender for Cloud
Microsoft Information Protection
Microsoft Defender for Cloud Apps
Applications
Data
101010
010101
101010
Infrastructure
Network
Microsoft Sentinel

AgileIT
ADAPTIVE • RESPONSIVE • STRATEGIC

Full Zero Trust End State

Bringing the best of both worlds



Differentiated Resources
Sanctioned and Managed Services
Microsoft 365
salesforce
Internet and Unsanctioned/Unmanaged Apps
CNN
Private and Managed in the cloud or on-premises
aws
Differentiated Identities
Strongly managed identities
MFA User
Admin
Managed identities
User
Partner
Anonymous and Consumer identities
?
Adaptive Access Control
Access varies based on trust & management level
Network Segments
Differentiated Devices
Managed devices
Unmanaged devices BYOD

Key Resources

- What is GCC High: https://www.agileit.com/news/what-is-gcc-high/
- CMMC DOD: https://www.acq.osd.mil/cmmc/index.html
- CMMC Assessment Guide, Level 2: https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf
- Cyber AB: https://cyberab.org/
- Microsoft CMMC Product Placemat: https://aka.ms/cmmc/productplacemat
- Microsoft Government
  - General Validation: https://azuregov.microsoft.com/general
  - Azure Government Trial Validation: https://azuregov.microsoft.com

Key Takeaways

- Defense Industrial Base = Cybersecurity Maturity Model Certification (CMMC)
- Cybersecurity is a lifestyle
- Cybersecurity is an organizational culture
- CMMC is a model and framework *not* an architecture
- Cloud Providers can share responsibility to reduce complexity
- Cloud Providers provide Enterprise capabilities available to more organizations
- Zero Trust principles and design aligns with Cybersecurity and CMMC

AgileIT

ADAPTIVE • RESPONSIVE • STRATEGIC

Thank You!

Questions?

We make IT easy