



What's New in CMMC Preparedness?

Presented by KTL Solutions

March 31, 2021



Housekeeping

- Feel free to ask questions in the chat box. We will answer as many as we can during our Q&A session at the end of the webinar. If we don't get to your questions today, a KTL consultant will reach out to you to provide answers.
- Our webinar is being recorded and you will be sent a link to the recording after the webinar, as well as a PDF copy of the deck.

Agenda

- Town Hall News
- CMMC Practices and Processes
- Microsoft Offerings
- GCC vs GCC-High
- Shared Responsibility
- Microsoft CMMC Acceleration Program
- KTL Consulting and Implementation



Speakers



Richard Wakeman

Senior Director

Aerospace & Defense

Azure Global Engineering, Microsoft



David Bedard, CMMC-RP

Senior Account Manager

Aerospace & Defense

KTL Solutions

KTL Solutions

- Certified Microsoft Gold Partner
- CMMC Registered Provider Organization (CMMC-RPO)
- Work with many government contractors
- We offer a suite of CMMC products and services
- Contact Us: info@ktsolutions.com



CMMC-AB Town Hall News

February Highlights

- PM's instructed to follow the DOD 5000.90 – Released Dec 31, 2020
 - Currently guidance to PM's is to only verify a score is in SPRS. Award determinations have not be instructed to be based on how high the score is at this time. - Lt Col Bryan Lamb (February Town Hall)
- DCMA starting to assess 5 C3PAO's against CMMC in March. Potentially ready to start assessments of DIB involved in the initial Pilot program

March Highlights

CMMC Practices and Processes

- The Cybersecurity Maturity Model Certification (CMMC) is a new cybersecurity framework and accompanying certification by the [US Department of Defense \(DoD\)](#).
- In 2021, DoD will roll out requirements for some new contracts.
- By 2026, **all contracts** will require CMMC certification.
- There are five levels of CMMC certification.
- **Certification is valid for three years.**

				Level 5 (171)
			Level 4 (157)	Advanced
		Level 3 (130)	Proactive	15
	Level 2 (72)	Good	26	26
Level 1 (17)	Intermediate	58	58	58
Basic	55	55	55	55
17	17	17	17	17
Performed	Documented	Maintained	Reviewed	Optimized

NIST 800-171 & CMMC

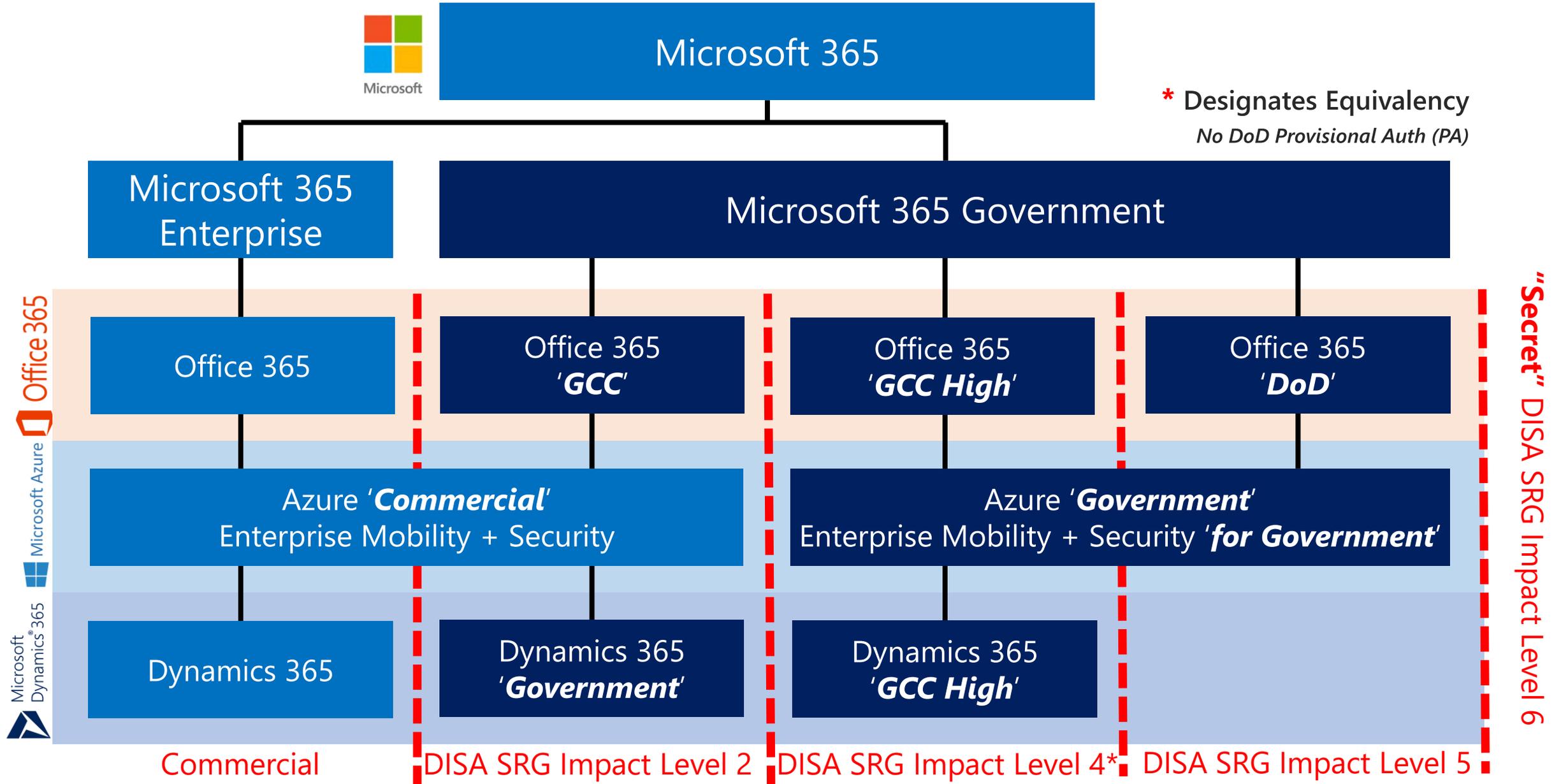
- By 2026 all company that bids on a DoD contract that contains Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) will be required to be CMMC compliant at the CMMC level mandated in a contract.
- Commercial off-the-shelf products will not require CMMC compliance.
- **Early adopters will have a competitive advantage.**



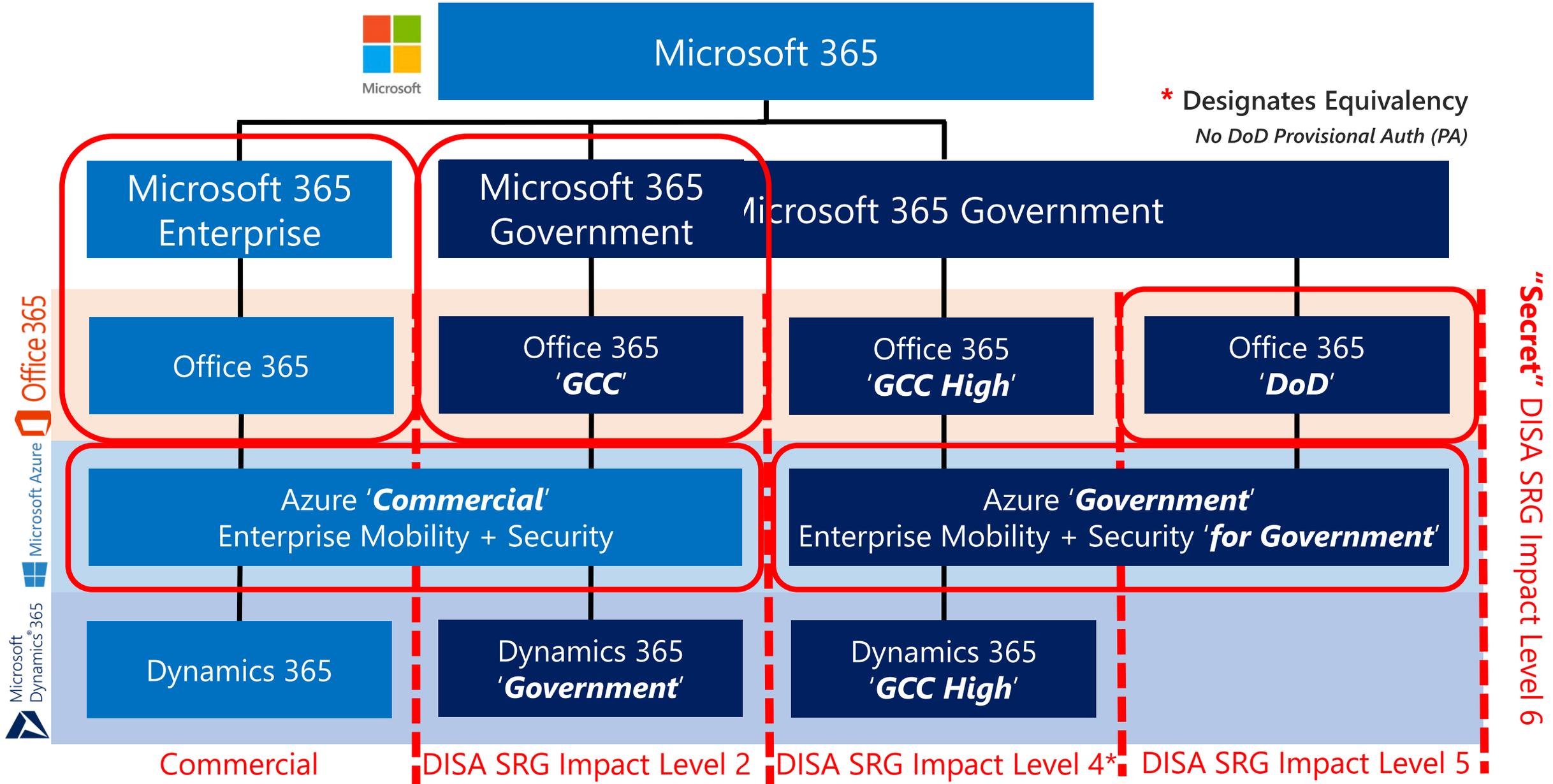


Microsoft Offerings & Shared Responsibility

History of Microsoft Cloud Service Offerings leading to the US



History of Microsoft Cloud Service Offerings leading to the US



Service Offering Differentiation



	Commercial	M365 "GCC"	M365 "GCC High"	M365 "DoD"
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	DoD only
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	CONUS Only
FedRAMP *	High	High	High	High
DFARS 252.204-7012	No	Yes	Yes	Yes
FCI + CMMC L1-2	Yes	Yes	Yes	Yes
CUI / CDI + CMMC L3-5	No	Yes^	Yes	Yes
ITAR / EAR	No	No	Yes	Yes
DoD CC SRG Level **	N/A	IL2	IL4	IL5
NIST SP 800-53 / 171 ***	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				



* *Equivalency*, Supports accreditation at noted impact level

** *Equivalency*, PA issued for DoD only

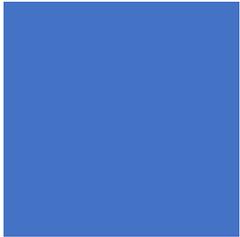
*** Organizational Defined Values (ODV's) will vary

^ CUI Specified (e.g. ITAR, Nuclear, etc.) not suitable REQS US Sovereignty

GCC vs GCC-High

- **GCC High** is built to meet the needs of the Defense Industry Base that cover stringent cybersecurity requirements of NIST 800-171 and DFARS 252.204-7012 (with flow-downs) and the protection of CUI.
- On Feb 23, Microsoft announced that the Government Community Cloud (GCC) offering now meets the reporting requirements stated in paragraphs C - G of DFARS 7012.
- **Why should I go to GCC High instead of GCC now that DFARS flow-downs are covered?**

Shared responsibility model



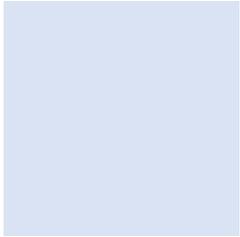
Customer management of risk

Data Classification and data accountability



Shared management of risk

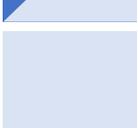
Identity & access management | End Point Devices



Provider management of risk

Physical | Networking

 Customer  Cloud Provider

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host Infrastructure				
Physical Security				

Examples of shared responsibilities: NIST

NIST 800-171

Access to production environment

Set up access controls that strictly limit standing access to customer's data or production environment

Protect data

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

Personnel control

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process



Access to production environment

Set up access control policy and SOP, leveraging Customer Lockbox / identity management solutions

Protect data

Encrypt data based on org's compliance obligations. E.g. encrypt PII in transit between users, using its own encryption key, etc.

Personnel control

Allocate and staff sufficient resources to operate an organization-wide privacy program, including awareness-raising and training

Office 365



Microsoft
CMMC
Acceleration
Program

Microsoft CMMC Strategy for Products



Blogs

[Microsoft CMMC Acceleration Program Update – January 2021](#) by Richard Wakeman

[Accelerating CMMC compliance for Microsoft cloud \(in depth review\)](#) by Richard Wakeman

[CMMC with Microsoft Azure: Access Control \(1 of 10\)](#) by TJ Banasik



Certifying with the Microsoft Cloud; how Microsoft products meet CMMC

Focus on products, not the enterprise

Allowable reciprocity for NIST SP 800-53 / FedRAMP

Allowable reciprocity for DoD CC SRG Impact Level 4 in Government clouds

Demonstrate compliance with DFARS 252.204-7012 in Government clouds

Demonstrate adoption of NIST Cybersecurity Framework (CSF)

Intend to include all Microsoft Cloud offerings

CMMC Acceleration Program



**First release in
Q4 CY20**



**Targeting
CMMC Level 3**



**Recommend
Azure Government +
M365 GCC High
Not Required*



**Pre-configured for
cloud-native
environments**

Pre-configured environment
Fully hosted environments –
Primarily SMB
DIB cloud shared enclaves –
Aligned to Mission or Prime
supply chain
Segmented environments –
Isolated business units



**Scaffolding
for partners to build
managed solutions on**

CMMC Acceleration Program Update - [Jan 2021](#)



[Reciprocity & Inheritance](#)



[Microsoft Product Placemat for CMMC](#)



[Azure Sentinel: CMMC Workbook](#)



[STIG Automation](#)



[Compliance Manager CMMC Levels 1-5 Assessment Templates](#)



[Azure Blueprint for CMMC Level 3](#)



[Azure Security Benchmark Foundation](#)



[Microsoft Cybersecurity Reference Architecture](#)

More to come!



Microsoft

Microsoft Product Placemat for CMMC

Illustrates CMMC Practices with Microsoft product coverage

Interactive with drill down of implementation statements

Select based on SKU (E5, E3, etc)

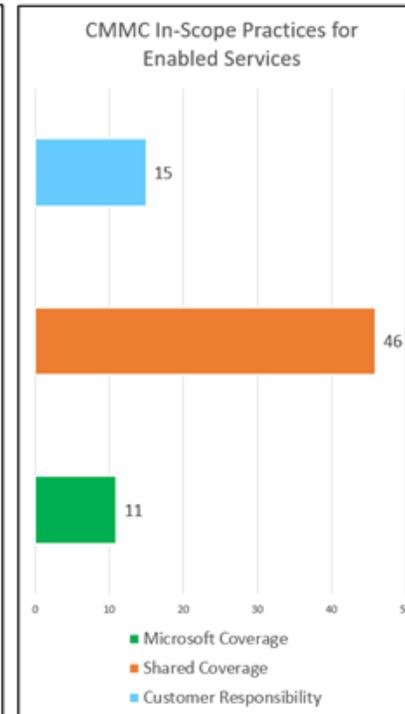
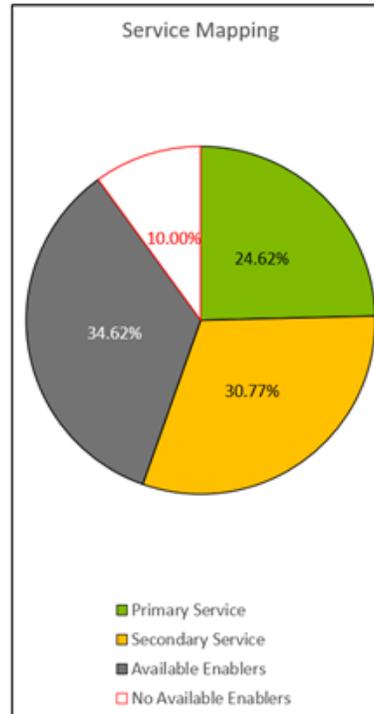
M365 E5 covers 18 practices outright and 74 have Shared Coverage

Shared Coverage means that the customer is required to implement and configure the practice to the standard for your tenant

MICROSOFT PRODUCT PLACEMAT FOR CMMC LEVEL 3

All Practices														
Access Control (AC)	Asset Management (AM)	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)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)
AC.1.001	AM.3.036	AU.2.041	AT.2.056	CM.2.061	IA.1.076	IR.2.092	MA.2.111	MP.1.118	PS.2.127	PE.1.131	RE.2.137	RM.2.141	CA.2.157	SA.3.161
AC.1.002	AM.4.226	AU.2.042	AT.2.057	CM.2.062	IA.1.077	IR.2.093	MA.2.112	MP.2.119	PS.2.128	PE.1.132	RE.2.138	RM.2.142	CA.2.158	SA.4.162
AC.1.003		AU.2.043	AT.3.058	CM.2.063	IA.2.078	IR.2.094	MA.2.113	MP.2.120		PE.1.133	RE.3.139	RM.2.143	CA.2.159	SA.4.163
AC.1.004		AU.2.044	AT.4.059	CM.2.064	IA.2.079	IR.2.096	MA.2.114	MP.2.121		PE.1.134	RE.5.140	RM.3.144	CA.3.161	SA.4.164
AC.2.005		AU.3.045	AT.4.060	CM.2.065	IA.2.080	IR.2.097	MA.3.115	MP.3.122		PE.2.135		RM.3.146	CA.3.162	SA.4.165
AC.2.006		AU.3.046		CM.2.066	IA.2.081	IR.3.098	MA.3.116	MP.3.123		PE.3.136		RM.3.147	CA.4.163	SA.4.166
AC.2.007		AU.3.048		CM.3.067	IA.2.082	IR.3.099		MP.3.124				RM.4.148	CA.4.164	SA.4.167
AC.2.008		AU.3.049		CM.3.068	IA.3.083	IR.4.100		MP.3.125				RM.4.149	CA.4.227	SA.4.168
AC.2.009		AU.3.050		CM.3.069	IA.3.084	IR.4.101						RM.4.150		SA.4.169
AC.2.010		AU.3.051		CM.4.073	IA.3.085	IR.5.102						RM.4.151		SA.4.170
AC.2.011		AU.3.052		CM.5.074	IA.3.086	IR.5.106						RM.5.152		SA.4.171
AC.2.013		AU.4.053				IR.5.108						RM.5.155		SA.4.172
AC.2.015		AU.4.054				IR.5.110								SA.4.173
AC.2.016		AU.5.055												SA.4.174

Microsoft Inherited Service Mapping		
Primary Service	xxx,xxxx	32
Secondary Service	xxx,xxxx	40
Available Enablers	xxx,xxxx	45
No Available Enablers	xxx,xxxx	13
Out of Scope for Level 3	xxx,xxxx	41



CMMC Practice Details	
CMMC Practice	IA.3.084
NIST 800-171 Mapping	3.5.4
Description	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
Primary Services	Azure Government Portal Azure Active Directory Azure MFA Intune/Microsoft Endpoint Manager
Secondary Services	
Responsibility	Microsoft Coverage

Microsoft Compliance Manager

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 Compliance Center](#)

[Assessment Templates](#) include NIST SP 800-171 and CMMC Levels 1-5

Available in Microsoft 365 Commercial, Government (GCC & GCC High)

** Automated Testing not available in GCC High*

Compliance Manager

[Overview](#) [Improvement actions](#) [Solutions](#) [Assessments](#) [Assessment templates](#)

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Overall compliance score

Your compliance score: 63%

15021/23532 points achieved

Your points achieved ⓘ
246/8757

Microsoft managed points achieved ⓘ
14775/14775

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Key improvement actions

Not completed	Completed	Out of scope
1002	23	0

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remain
Audit	0/135 points	33
Azure	0/3 points	2
Azure Active Directory	162/504 points	52

[View all solutions](#)

Microsoft Compliance Manager *Improvement Actions*

- Suggests actions to meet intent of each CMMC Practice requirements
- Links to reference documentation and how-to support articles
- Improves Compliance Score as actions are implemented
**Compliance Score not associated with NIST SP 800-171A nor with SPRS*
- Allows for assignment to individuals
- Allows for uploading of documentation

Enable multi-factor authentication for non-admins

This action is automatically monitored. [Learn more](#)

Overview

Implementation Status: Partially Implemented
Test Status: Partially tested

Points achieved: 27/27
Group: CMMC-L3

Documents: 0

Assigned to: None

Implementation Testing Standards and Regulations

Implementation status: Select Implementation status...
Implementation date: Thu Jan 21 2021

How to implement

Microsoft recommends that organization enable multi-factor authentication (MFA) for all users. Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan. Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator

Implement account lockout

Overview

Implementation Status: Not Implemented
Test Status: None

Points achieved: 0/27
Group: CMMC-L3

Documents: 0

Assigned to: None
[Assign action](#)

Implementation Testing Standards and Regulations Documents

Implementation status: Select Implementation status...
Implementation date: Select a date...

How to implement

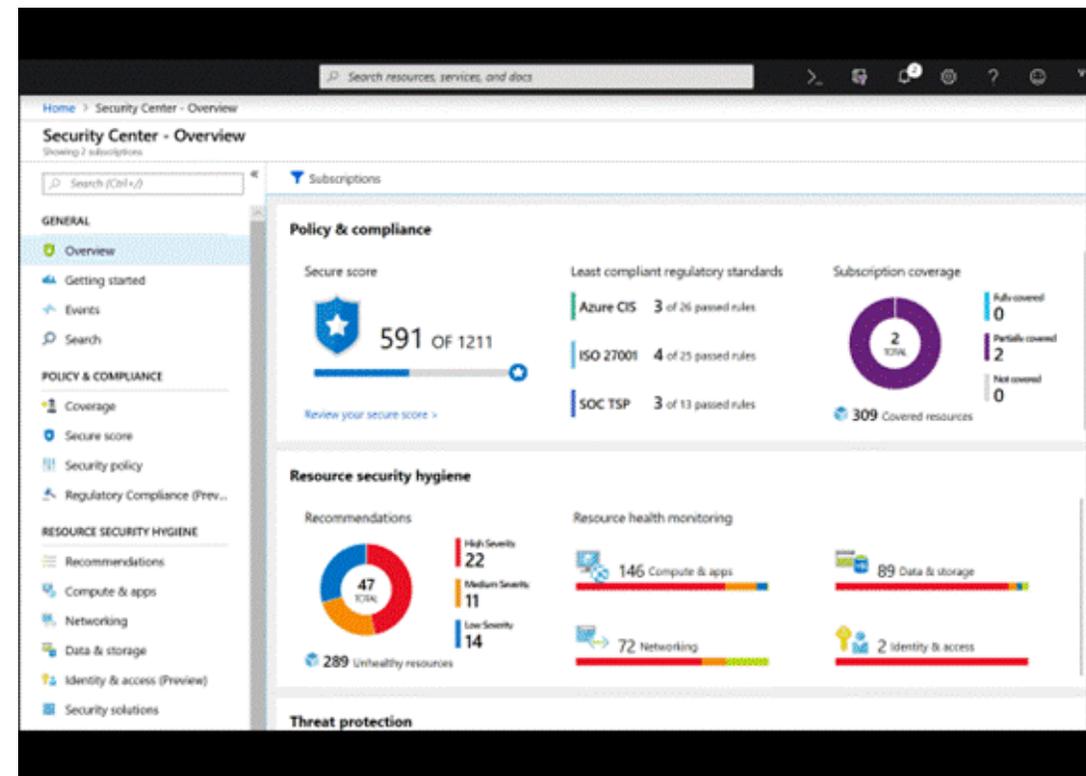
Microsoft recommends that your organization lock accounts for a specified time period after the maximum number of failed logon attempts has been reached. For cloud service accounts in Azure Active Directory, after 10 unsuccessful sign-in attempts with the wrong password, the user is locked out for one minute. Further incorrect sign-in attempts lock out the user for increasing durations of time. Use Active Directory to manage user accounts to implement an account lockout policy that enforces a limit for consecutive failed logon attempts during an organizationally-defined time period. If your organization has not defined a lockout time period, we recommend using at least 15 minutes or until an administrator enables the user ID. Select **Launch Now** to access the **Authentication methods - Password protection** page in the Azure Active Directory admin center to implement account lockout.

Azure Security Center

[Azure Security Center](#)
is integrated with
[Azure Defender](#)

[Azure Blueprints](#) include samples for
[NIST SP 800-171](#) and projected
requirements for CMMC Levels 3

*CMMC Level 3 Azure Blueprint sample
public preview [available now](#)*



Azure Security Benchmark Blueprint

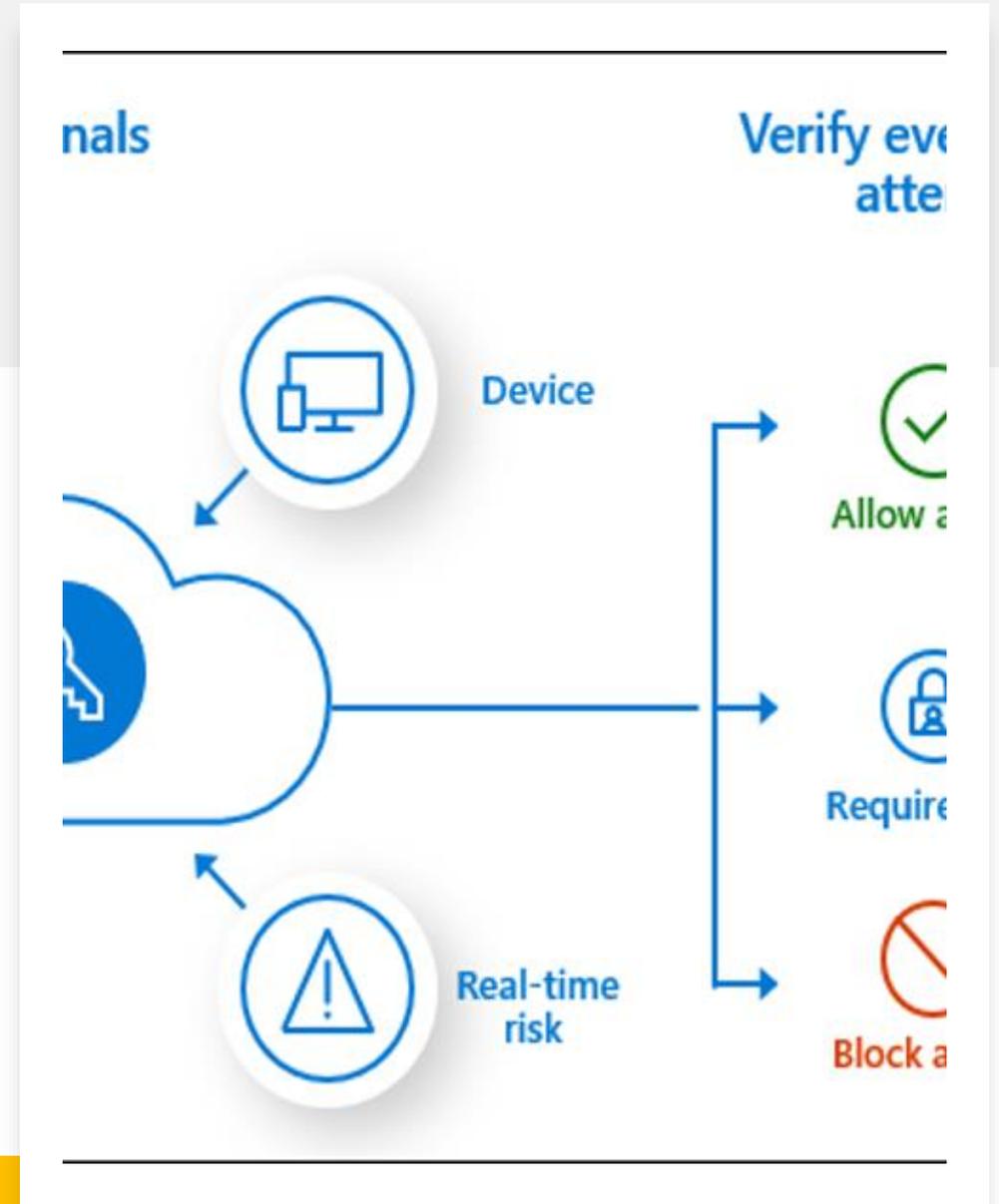
To help organizations stay secure in a

zero trust environment

Azure Security Benchmark Foundation

is a Blueprint that providing a set of baseline infrastructure patterns to assist in building a

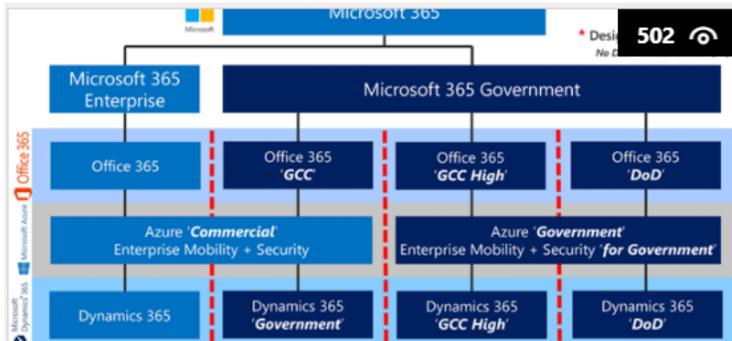
secure and compliant Azure environment



Public Sector Community Blog



History of Microsoft Cloud Service Offerings leading to the US



History of Microsoft Cloud Offerings leading to the US...

RichardWakeman on 02-23-2021 07:36 AM

Microsoft has evolved our cloud service offerings to include the US Sovereign Cloud with Azure Government, Microsoft 365...

	Any customer	GCC	GCC High	651
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	CONUS Only
FedRAMP *	High	High	High	High
DFARS 252.204-7012	No	Yes	Yes	Yes
FCI + CMMC L1-2	Yes	Yes	Yes	Yes
CUI / CDI + CMMC L3-5	No	Yes^	Yes	Yes
ITAR / EAR	No	No	Yes	Yes
DoD CC SRG Level **	N/A	IL2	IL4	IL5
NIST SP 800-53 / 171 ***	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	

Understanding Compliance Between Commercial, Government...

RichardWakeman on 02-23-2021 07:34 AM

Understanding compliance between Commercial, Government and DoD offerings: There remains much confusion as to what servi...

Understanding Compliance Between Microsoft 365 Commercial, Government and DoD Offerings

The Microsoft 365 US Government (GCC High) Conundrum - DIB Data Enclave vs Going All In



The Microsoft 365 US Government (GCC High) Conundrum - DIB...

RichardWakeman on 10-30-2019 10:00 AM

The DIB (Defense Industrial Base) are embracing M365 GCC High to achieve compliance with U.S. defense regulations. Howev...



KTL Solutions: Consulting & Implementation

KTL CMMC Packages

Consultation: Discuss compliance requirements for your organization

Gap Analysis: Analyze current state of your cybersecurity

Roadmap: Propose products and solutions to achieve compliance

Licensing & Migration: Offer GCC-High and Azure Government licenses

Pre-audit Review: Assess all controls in place

Azure Configuration: Tailor Azure Sentinel for your organization

vCISO: Provide ongoing coaching so you remain CMMC compliant

KTL 360: Deliver managed services for government contractors

Consultation

- **CMMC Consultation:** Take advantage of this no cost initial consultation with a KTL CMMC-RP. This discussion will provide a clear understanding of compliance requirements and help determine the best path forward for your organization.
- **Discuss:**
 - Cloud: GCC vs GCC high
 - Licensing options: Azure and GCC high
 - KTL Solutions: Products and Services

CMMC Gap Analysis

- **CMMC Gap Analysis:** KTL will review all information gathered in the investigative process to include policies, documented practices, interviews, and any additional relevant information and produce a CMMC Gap Analysis Report that will articulate the following:
 - Executive Summary of organization's Current State: Overview of the current state of cybersecurity maturity as compared to CMMC requirements, as if an assessment were performed today.
 - Detailed Control Analysis: An exhaustive list of CMMC required security controls and the current ability of your organization to satisfy those controls in a pass/fail context.
- **For each practice or process to which your organization is discovered to be non-compliant, KTL will recommend a course of action to remediate these shortcomings.** Those areas requiring improvement will be clearly identified, documented, and presented in a format that can be leveraged by executive management to serve as a foundation for formal security program improvement and compliance attainment.

CMMC Gap Analysis *cont.*

Your organization will be assessed for gaps to CMMC ML3/NIST 800-171 requirements. The assessment will cover all of the CMMC ML3/NIST 800-171 domains:

- Access Controls (AC)
- Asset Management (AM) – Specific to CMMC Only (1 Control)
- Audit & Accountability (AU) – 2 Controls specific to CMMC
- Awareness & Training (AT)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR) – 4 Controls specific to CMMC
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE) – 2 Controls specific to CMMC
- Risk Management (RM) – 3 Controls specific to CMMC
- Security Assessment (CA) – 1 Control specific to CMMC
- Situational Awareness (SA) – Specific to CMMC Only (1 Control)
- System & Communication Protection (SC) – 3 Controls specific to CMMC
- System & Information Integrity (SI) – 3 Controls specific to CMMC

CMMC Roadmap

- **CMMC Roadmap:** Utilizing a Gap Analysis, KTL will remediate each of the practices or processes that were identified as non-compliant. KTL will help you build your information security program to the desired CMMC compliance level. We will assist you in creating a detailed CMMC roadmap, create missing policies and procedures, and work with your team to implement the proper practices.
- **Following the completion of the project, you will have technical documentation to complete your System Security Plan (SPP) and prepare for your CMMC Assessment.**

CMMC Roadmap

The CMMC Roadmap includes the following:

Areas addressed

- Policies
- Practices
- Procedures
- Plans
- Controls

Systems Improvement

- Architecture
- Migration
- Configuration

Additional Support

- Provide training for your team
- Offer ongoing support



CMMC Implementation Timeframe

- The implementation timeframe depends on:
 - The level of certification required for your organization
 - The current state of your NIST 800-171 implementation
 - The size and scope of your system.
- *Example: a CMMC Level 3 implementation could take 6+ months while a CMMC Level 1 compliance can be accomplished in a shorter time-frame.*
- **The time to begin exploring CMMC certification is now.**



Licensing & Migration

- **Licensing for GCC-High and Azure Government:** KTL offers a full range of licensing, migration and configuration services.
- KTL will address policies, practices, procedures, plans and controls in order to:
 - Architect, migrate, and/or configure systems
 - Provide training for your team
 - Offer ongoing support
- Speak with one of our CMMC-RPs to ensure you have the proper licenses in place for your journey to CMMC compliance.





Q&A

For more info, contact us at info@ktsolutions.com