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

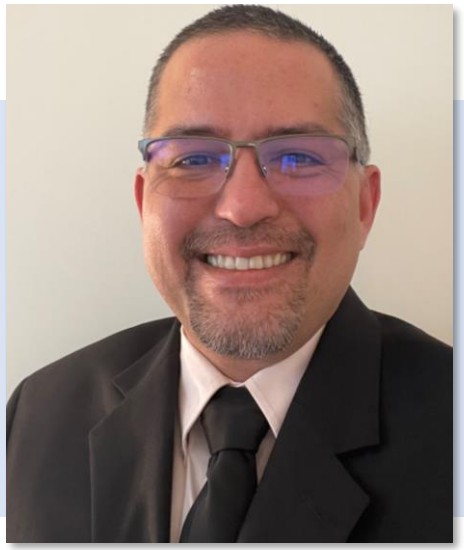
Speakers

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@ktlsolutions.com

Microsoft Gold Partner

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

KTL SOLUTIONS

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

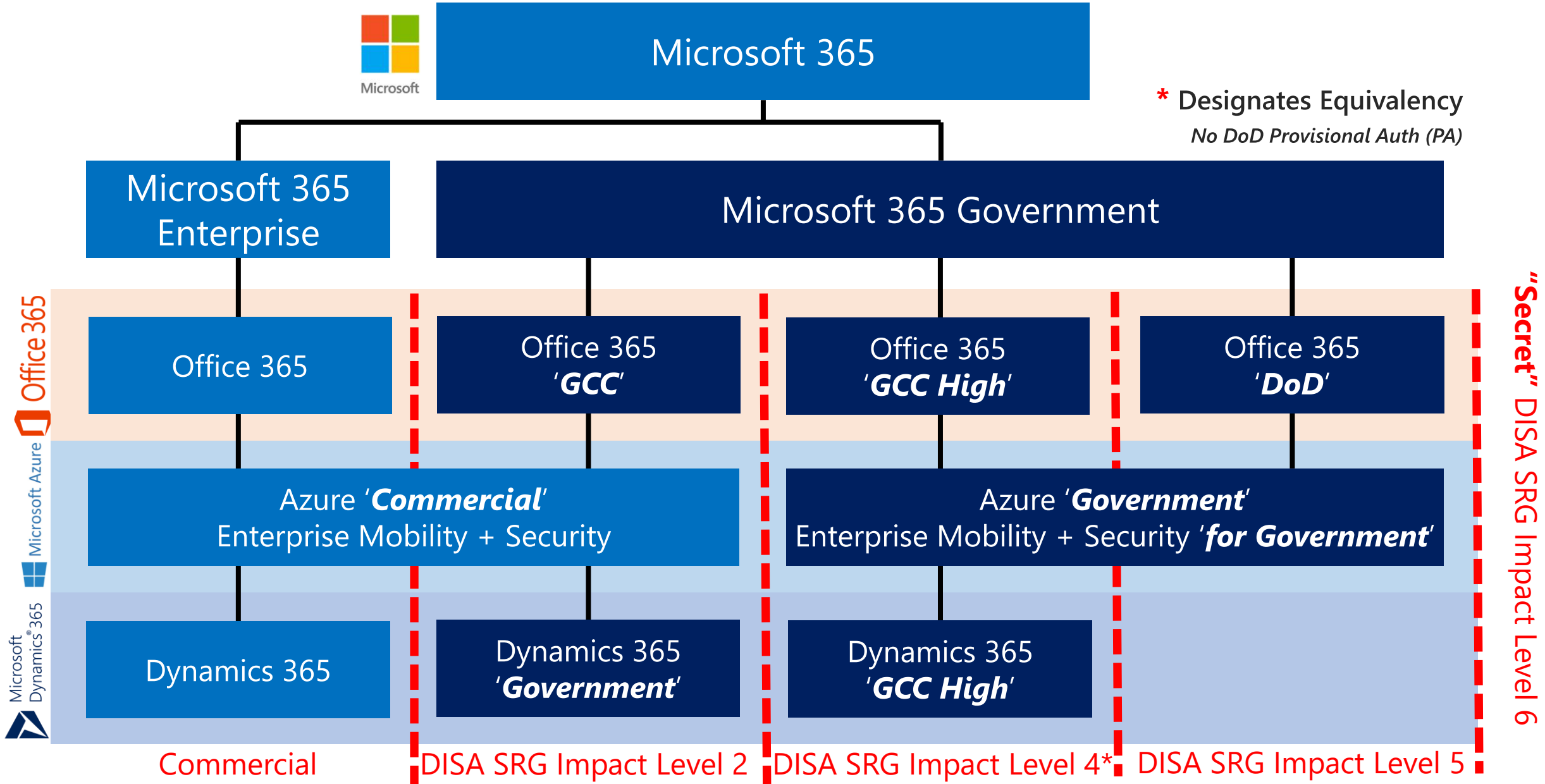
NIST 800-171 & CMMC

- 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.**

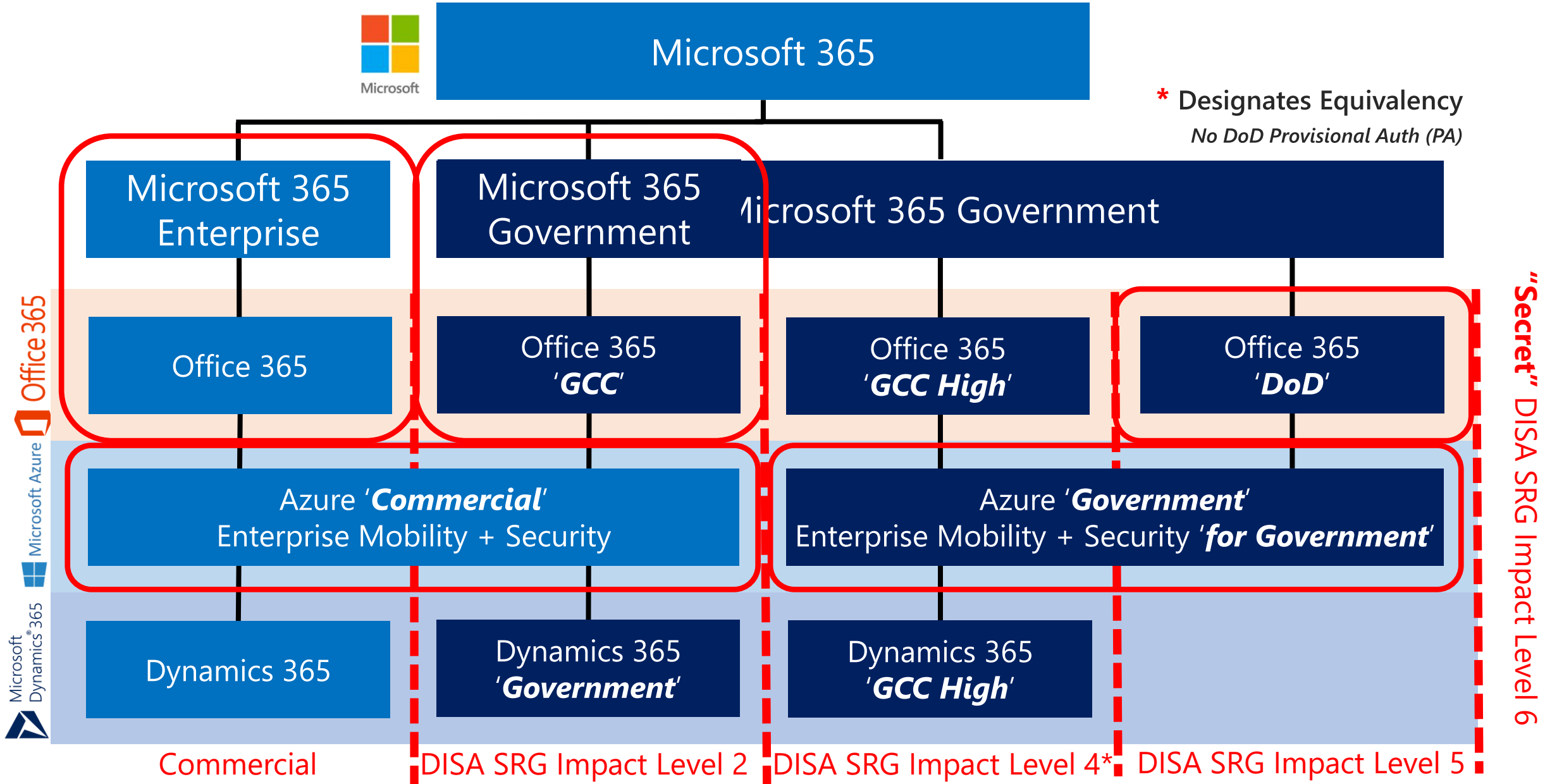
KTL SOLUTIONS

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

[Public Sector Blog]

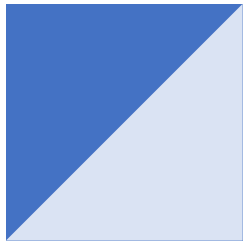
GCC vs GCC-High

- **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

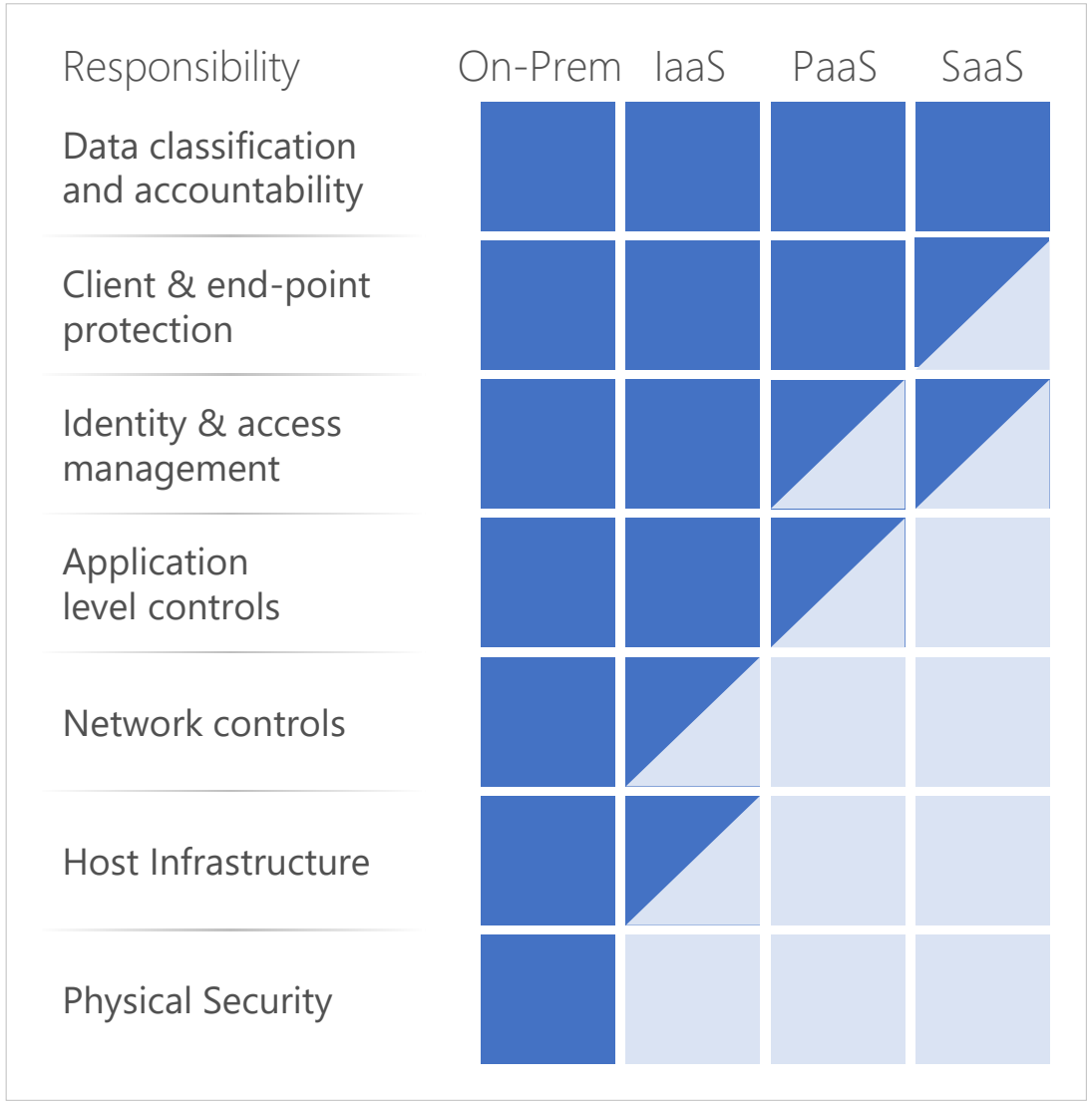


Shared management of risk

Identity & access management | End Point Devices

Provider management of risk

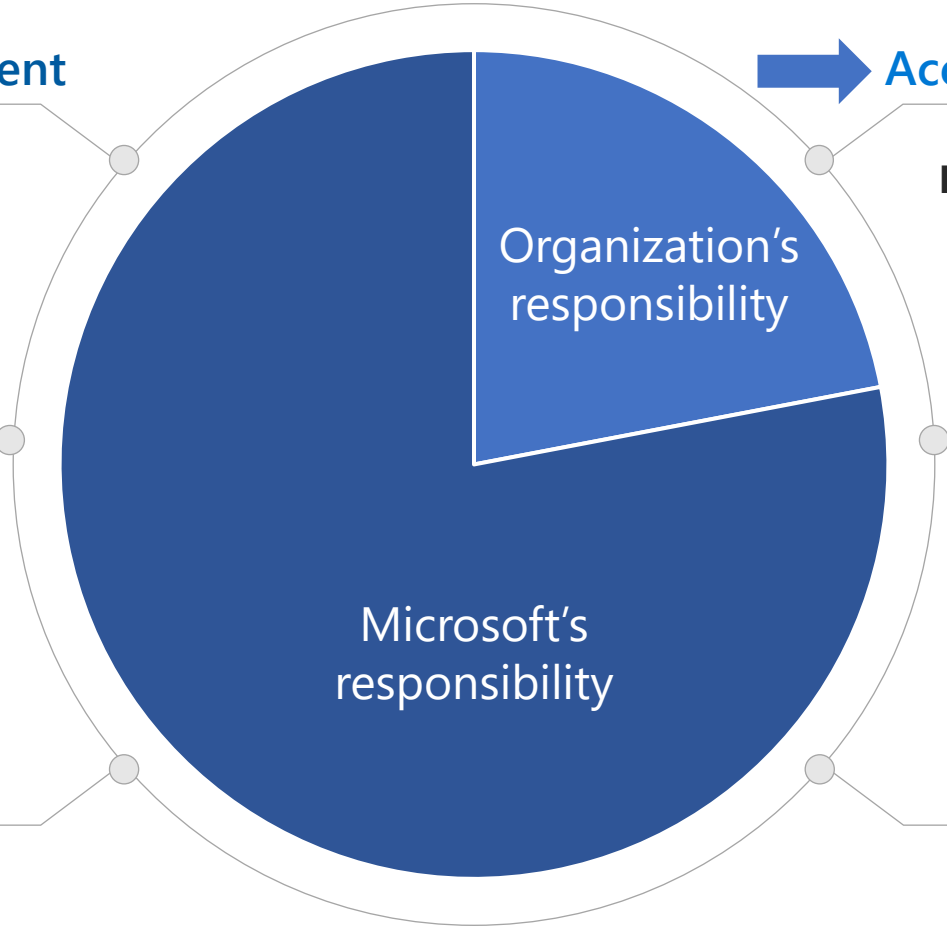
Physical | Networking



Customer **Cloud Provider**

Examples of shared responsibilities: NIST

NIST 800-171



Office 365

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

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

Microsoft

- 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

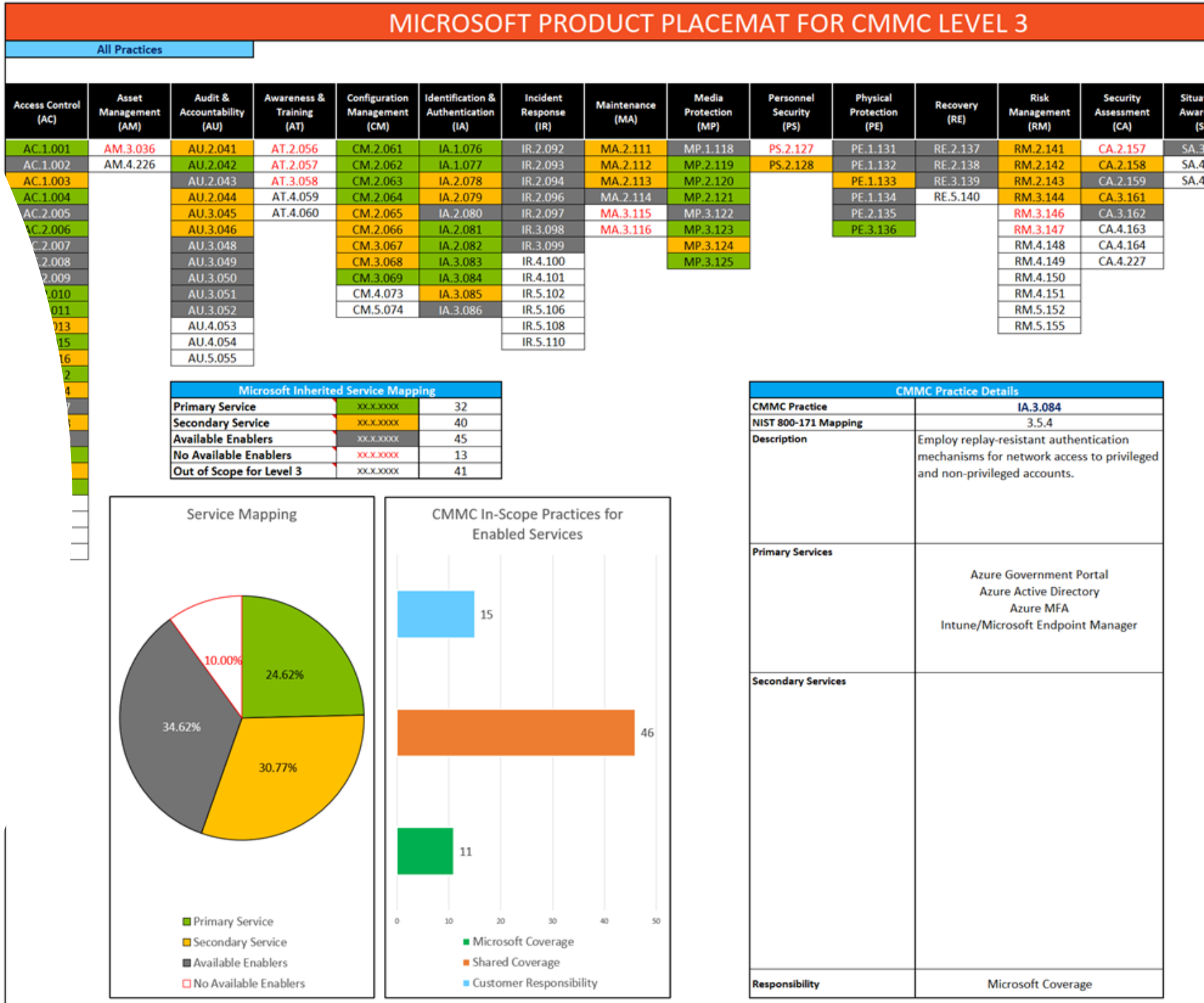
Illustrates CMMC Practices with Microsoft product coverage

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



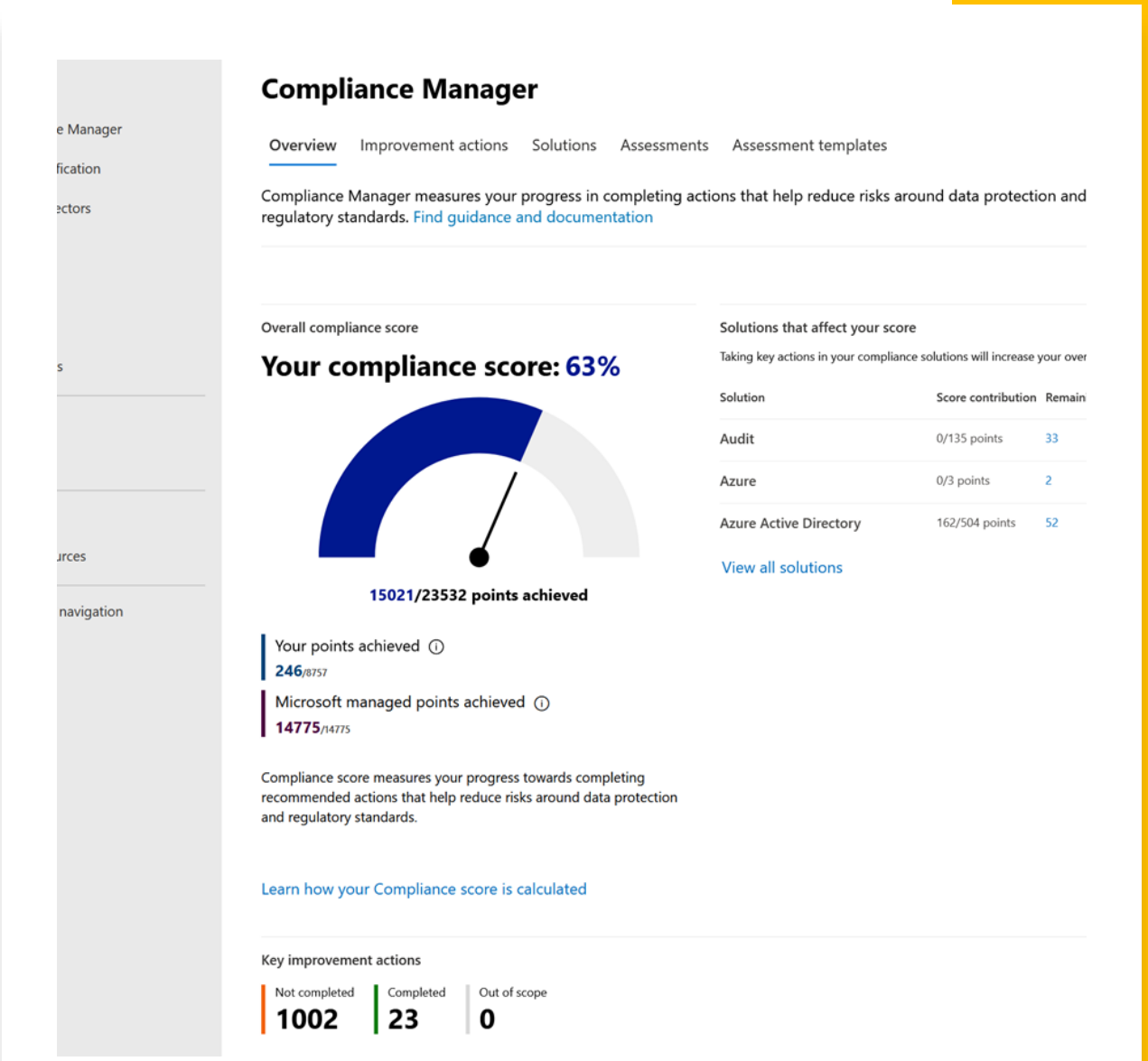
Microsoft Compliance Manager

Microsoft Compliance Manager
is a feature in the
Microsoft 365 Compliance Center

Assessment Templates include
NIST SP 800-171 and CMMC Levels 1-5

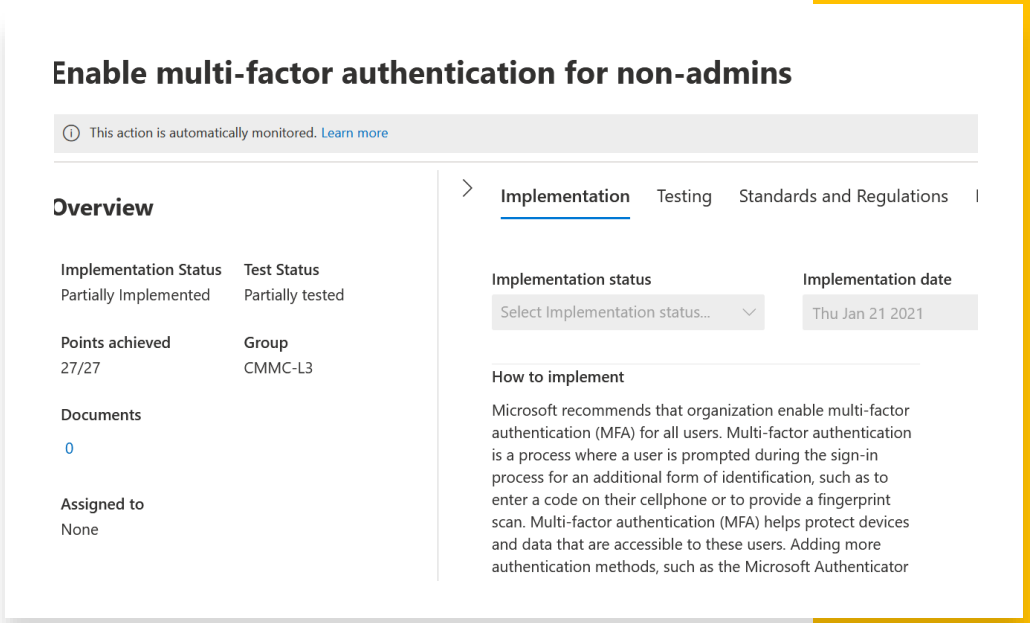
Available in Microsoft 365 Commercial, Government (GCC & GCC High)

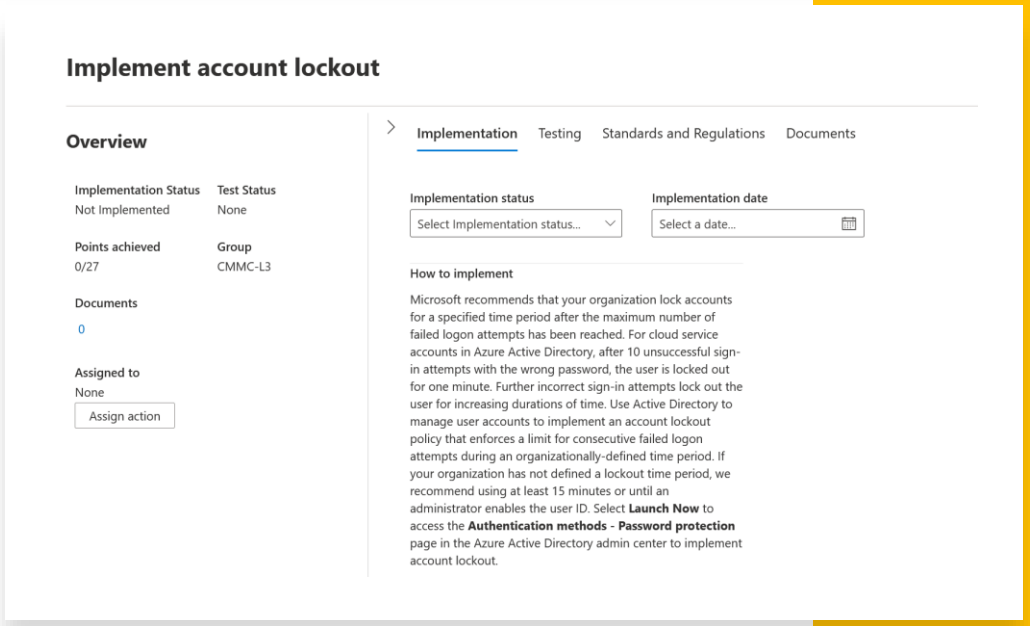
** Automated Testing not available in GCC High*



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



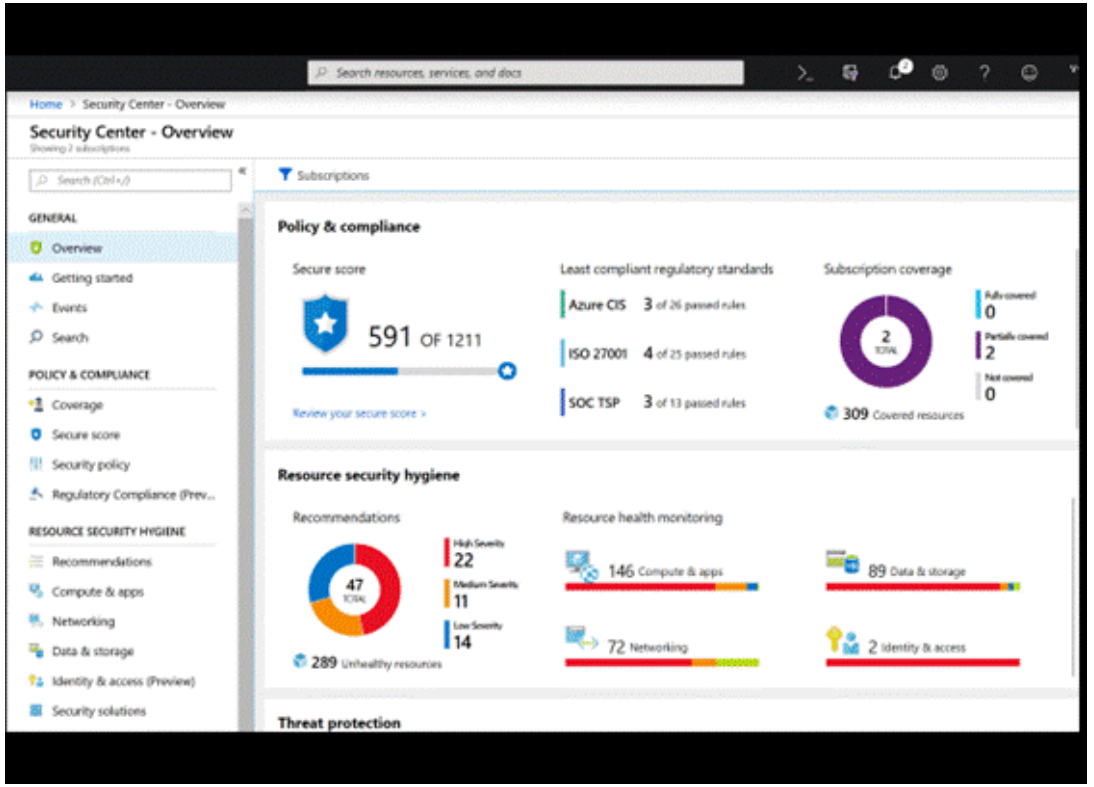


Azure Security Center

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

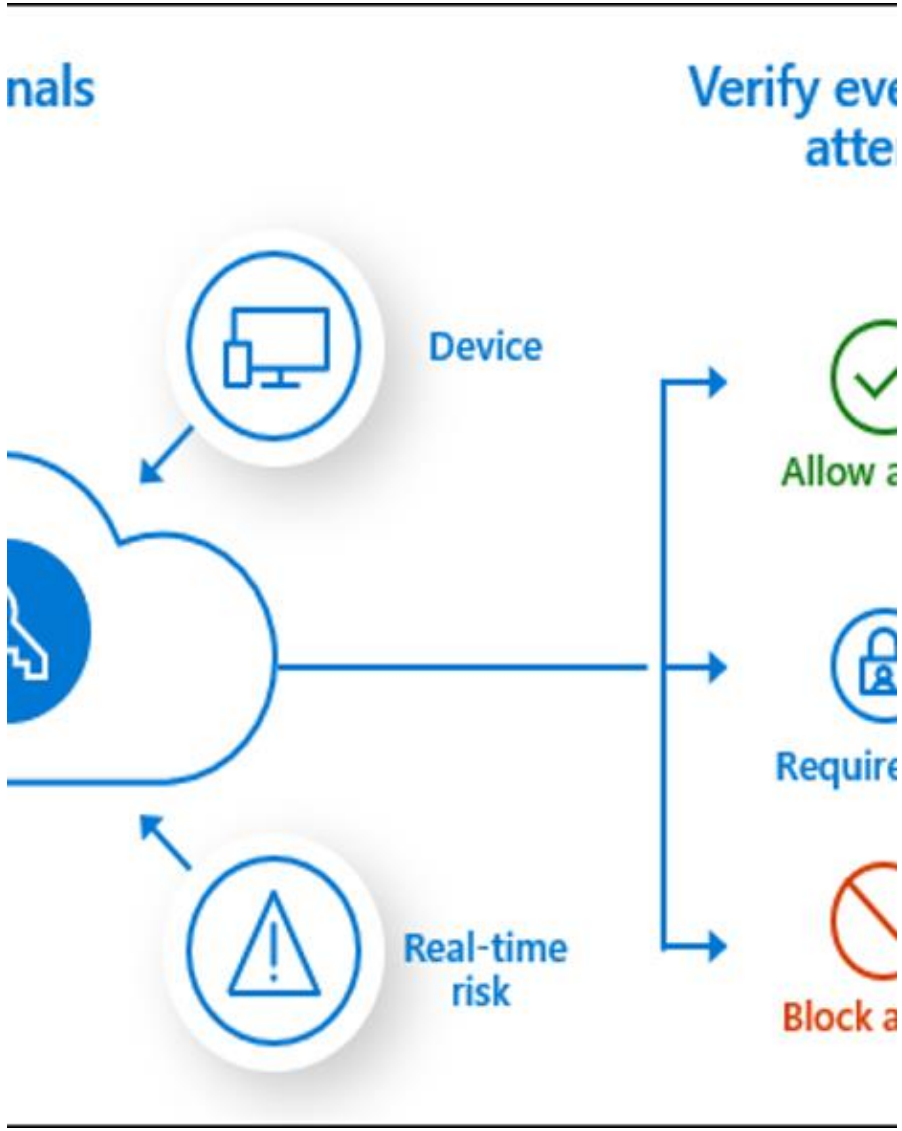
To help organizations stay secure in a

zero trust environment

Azure Security Benchmark Foundation

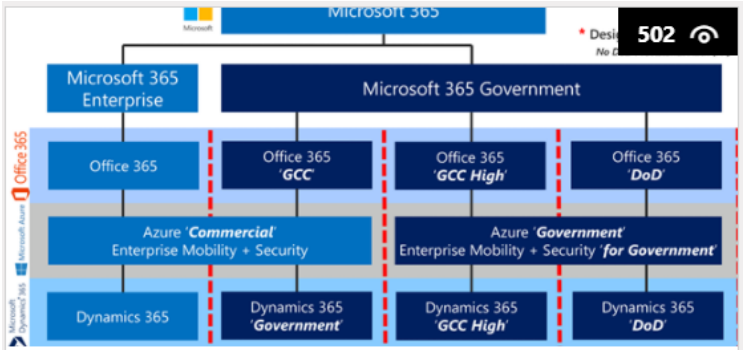
is a Blueprint that providing a set of baseline infrastructure patterns to assist in building a

secure and compliant Azure environment



Public Sector Community Blog

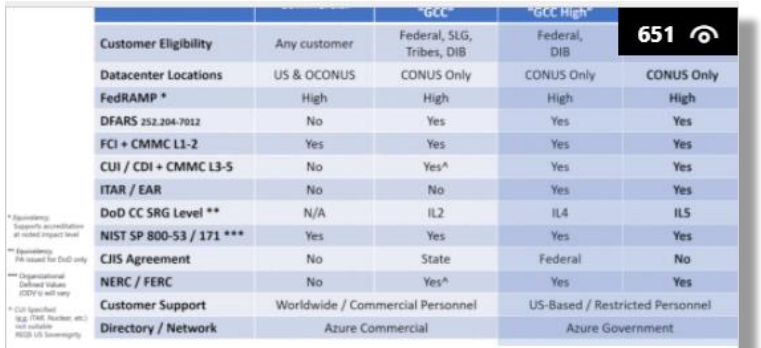
[History of Microsoft Cloud Service Offerings leading to the US]



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...



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

KTL SOLUTIONS

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 polices, 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

KTL SOLUTIONS

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.

Microsoft Gold Partner

KTL SOLUTIONS

Q&A

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