Solution Brief

CMMC Compliance With Microsoft Cloud

Security services to enable compliance success in Azure and M365

The Cybersecurity Maturity Model Certification (CMMC) is a program intended to establish a uniform level of cybersecurity throughout the Defense Information Base (DIB) or Department of Defense (DoD) supply chain. The DIB is made up of more than 300,000 product manufacturers, systems integrators, and service providers.

The DIB often has Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) shared with it by the DoD or primary contractors. CMMC introduces the use of an independent CMMC Third Party Assessment Organization (C3PAO) that has been trained to evaluate the cybersecurity of the systems used by the supply chain contractors that acquire, develop, process, or store CUI.

The goal of CMMC is to ensure that the DIB can effectively secure and mange CUI in a defined and consistent manner. Taking advantage of the shared responsibility provided by Azure® and M365 can allow businesses to achieve that goal with speed and simplicity.

Insight's CMMC services program

Insight's CMMC services program is designed to help clients understand DoD requirements, develop a strategy to achieve compliance in hybrid and cloud models, and execute to implementation and ongoing operations.

Assess

- Document current state, existing solutions, architecture, and design
- Identify Governance, Risk, and Compliance (GRC), business processes, and technical requirements
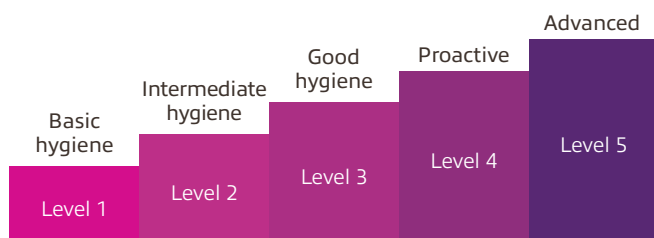- Identify and interview key stakeholders

Design

- Develop design strategy
- Design low-level architecture
- Begin solution selection process

Implement

- Execute strategic plan following roadmap
- Implement processes and methodologies in partnership with client
- Provide ongoing operations support

CMMC maturity

Why Insight for Microsoft

2020 Azure Security Deployment
Partner of Year

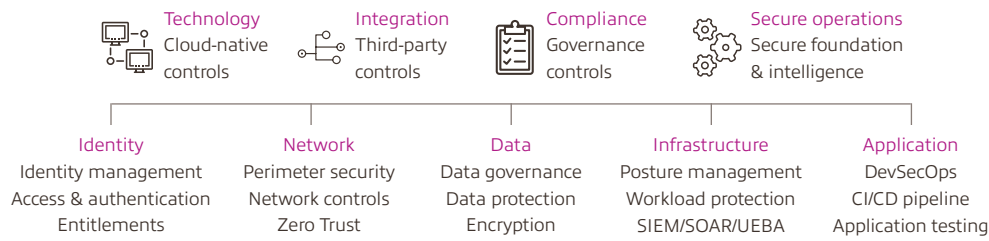**Gold competency** in Security

Advanced specializations

GRC resources made up of former CISOs and compliance directors with expertise **across multiple industry verticals**

Cloud security architects focused on integration and organizational infrastructure security
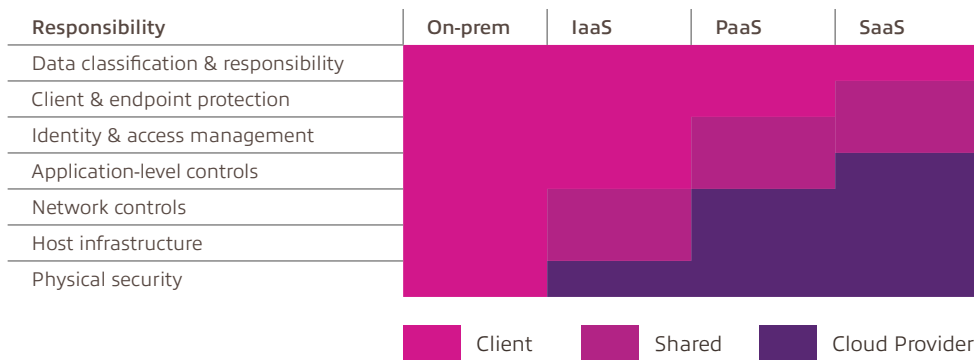
Microsoft® cloud architects with specialized competencies across Azure and M365 security

Insight's CMMC compliance & cloud security approach

Insight's compliance and cloud security approach allows for key technology and process considerations that will serve to inform and guide effective implementation and ongoing governance for your business. A wholistic approach will require decisions on use of cloud-native controls, third-party integration, compliance management, and ongoing security operations.

Technology
Cloud-native controls

Integration
Third-party controls

Compliance
Governance controls

Secure operations
Secure foundation & intelligence

Identity	Network	Data	Infrastructure	Application
Identity management	Perimeter security	Data governance	Posture management	DevSecOps
Access & authentication	Network controls	Data protection	Workload protection	CI/CD pipeline
Entitlements	Zero Trust	Encryption	SIEM/SOAR/UEBA	Application testing

Insight's compliance and cloud security experts have experience across multiple industry verticals and can provide the overall guidance needed to achieve a strategic plan as well as specialized advisory consulting across the key security domains for a more focused outcome.

Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification & responsibility				
Client & endpoint protection				
Identity & access management				
Application-level controls				
Network controls				
Host infrastructure				
Physical security				

■ Client   ■ Shared   ■ Cloud Provider

Outcomes and key deliverables

Depending on client current state and required services, deliverables can include:

Discovery workshops
- Executive summary
- Key Performance Indicators (KPIs)
- Environment current state
- Prioritized security strategy dashboard
- Strategic security roadmap
- Future state security solutions heatmap

Architecture & advisory
- Current & future state architecture
- Low-level design
- As-built design
- SSP completion
- POAM development
- Policy development
- Process & procedure development

Implementation & operations
- Secure tenant build
- Service blueprints development
- Deployment hardening
- As-built documentation & configuration
- Knowledge transfer
- Operationalization & training

Services methodology

Discovery workshops
Current state assessment and roadmap development

Advisory consulting
Flexible and focused consulting based on client need

Architecture & design
Strategy development and future state architecture

Technical deployment
Specialized experts to implement strategy and design

Training & operations
Ongoing enablement to achieve successful operations

Managed Security services
Support for businesses with limited security resources

Case study: U.S. shipbuilder

When a naval contractor engaged in a coalition with similar facilities to fulfill a DoD contract, the DoD and client partner organizations required evidence of NIST 800-171 and CMMC assessment and valuation. The facility's lack of compliance and security maturity presented roadblocks to business growth.

Insight's CMMC services program has helped the client overcome these maturity challenges with a modern architecture and solution design integrated into cloud and hybrid operating models through the following actions:

- Performing a CMMC maturity gap analysis, mapped NIST 800-171, and creating a single unified plan of action
- Working with the client to develop required policies, procedures, and processes
- Assisting the client in the selection of tools needed to achieve desired outcomes
- Performing a NIST 800-171 gap analysis and helping the client develop a roadmap

Getting started is easy.

Visit solutions.insight.com/contact-us to connect with our team.

solutions.insight.com | insight.com

⊹⊹ Insight.