SysArc

CMMC Compliance Solutions for Defense Contractors & Suppliers

YOUR **STRATEGIC PARTNER** IN CYBERSECURITY COMPLIANCE

As your strategic partner, SysArc empowers your organization to not only meet but exceed cybersecurity and compliance goals. Together, we can achieve a secure and compliant operational environment, setting the stage for a resilient and prosperous future.

CMMC Compliance Roadmap

SysArc can help Defense Contractors and their suppliers navigate the entire CMMC compliance journey from start to finish. From an initial CMMC Readiness Assessment through POAM remediation, Program Oversight and Monitoring to C3PAO selection and ongoing support of your cyber compliance program, SysArc has the team and solutions to help your enterprise not only achieve your certification, but more importantly reduce the risk of cyber breaches causing significant harm to your organization. SysArc partners with Microsoft along this journey to deliver some key solutions that complete 70-80% of the CMMC Level 2 requirements in NIST 800-171 including moving your sensitive workloads from M365 Commercial into M365 GCC High and providing outsourced SOC Services with the Microsoft Sentinel and Defender security stack.

CMMC Readiness Assessment

Our Compliance team can conduct a CMMC Level 2 readiness/mock assessment with resulting SSP, POAM and Remediation Recommendations deliverables.

01

CMMC Program Management Service

Our Compliance team can manage your compliance journey by providing oversight and guidance of the POAM tasks, required Policies, Procedures, SSP documentation, Evidence Collection, Audit Prep & Support.

02

Remediation with a Microsoft 365 GCC High Migration Project

SysArc is an experienced CMMC Consulting firm and approved Microsoft GCC High reseller, having successfully completed many large scale GCCH enclaves with custom CMMC hardening built into the solution. Migrating to GCCH can accelerate your compliance journey while making it easier to collaborate with your DoD customers and partners in a more secure environment.

03

Managed SOC Services for Mid-Sized Organizations

SysArc offers SOC services for U.S. enterprises, ensuring the highest security and compliance with experienced cybersecurity professionals and military-grade solutions using the Microsoft security stack including Sentinel and Defender

04

CMMC Certification Audit

SysArc can assist with C3PAO selection and be with you through the entire audit prep and onsite audit to ensure achievement of the certification. We have already successfully completed Joint Surveillance Program Audits (CMMC Pilot Program) with three of our enterprise customers. We have another 30+ customers that are in line to go through the audit process as soon as they are eligible.

05

Current Challenges

In today's regulatory landscape, ensuring data security and compliance is paramount, particularly for organizations managing sensitive information.

For government contractors, or organizations with stringent compliance needs, **migrating to Microsoft 365 Government Community Cloud (GCC)** High is often a necessity.

The migration to **Microsoft 365 Government Community Cloud (GCC)** High addresses specific compliance requirements, providing a secure and compliant environment tailored to the needs of government contractors.

Office 365 US Government
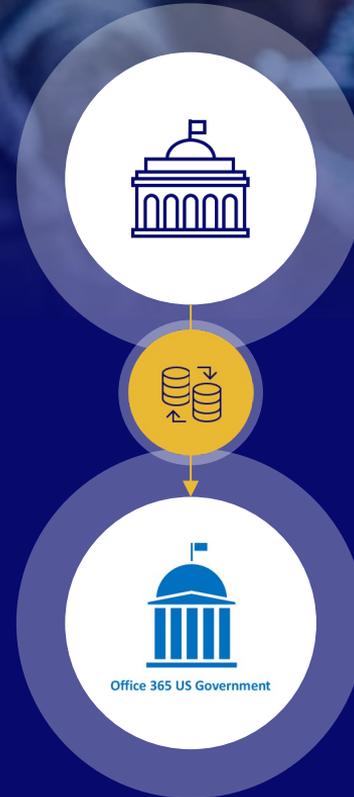
About the Solution

As your trusted IT advisor, **SysArc** can help your organization to meet these requirements with our **"Microsoft 365 GCC High Migration"** offering.

Our comprehensive solution facilitates seamless migration to Microsoft 365 GCC High, or Office 365 GCC High, enabling organizations to effortlessly address compliance and security challenges.

We specialize in helping organizations to meet compliance regulations such **as Cybersecurity Maturity Model Certification (CMMC), International Traffic in Arms Regulations (ITAR),** and more, while securely migrating organizations to Microsoft 365 Government Community Cloud (GCC) High.

Whether your organization is migrating from Google Workspace, Amazon Web Services, Microsoft 365 Commercial Cloud, and more. **We can help your team, no matter your starting point!**

Security Challenges

organizations

Compliance regulations

SysArc

Office 365 US Government

Deliverables

Initial Consultation

Our Compliance team can conduct a CMMC Level 2 readiness/mock assessment with resulting SSP, POAM and Remediation Recommendations deliverables.

Assessment and Planning

To prepare for the migration to Microsoft 365 GCC High, we will perform a thorough assessment of the existing infrastructure, evaluate the organization's compliance status, identify any compliance gaps for remediation, and develop a tailored migration plan that includes timelines, milestones, and resource allocations.

Configuration and Setup

We will configure the Microsoft 365 GCC High environment according to the migration plan, ensuring all settings, policies, and permissions are correctly set up, and provision user accounts with appropriate security settings to maintain data confidentiality, integrity, and availability within the GCC High environment.

Data Migration

We will employ industry-leading tools and methodologies for a seamless data migration from on-premises systems or other clouds to Microsoft 365 GCC High, while prioritizing data integrity and security to protect sensitive information throughout the process.

Testing and Validation

We will conduct comprehensive testing of the Microsoft 365 GCC High environment to ensure data integrity, functionality, and performance, address any issues found, and validate secure user access and authentication mechanisms.

Post Migration Support

We provide ongoing support and expert assistance post-migration to address any queries, resolve issues, or meet additional service needs, ensuring a secure, compliant, and seamless transition to Microsoft 365 GCC High.

Current Challenges

Organizations who do business with the United States Government face unique cybersecurity challenges due to stringent regulatory requirements, and the sensitive nature of government data.

Many of these organizations must adhere to the **Cybersecurity Maturity Model Certification (CMMC)**, which requires continuous monitoring and incident management.

SysArc manages and secures IT systems for enterprises throughout the United States, while helping them meet strict compliance requirements such as **DFARS, CMMC, FISMA, PCI DSS** and many others.

Incident Management

organizations

Continuous Monitoring
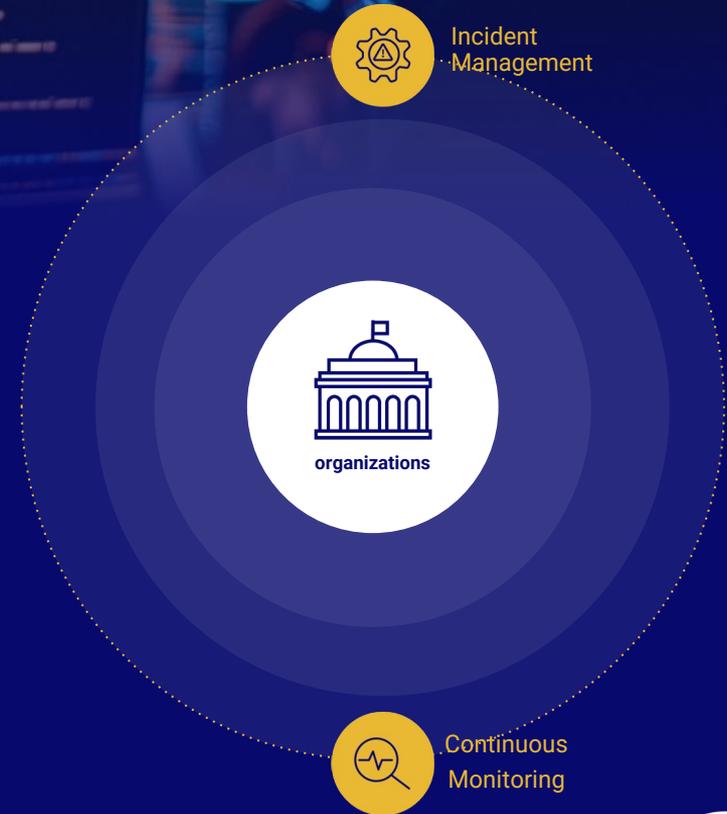
SysArc

About the Solution

To address these challenges, **SysArc** can help your organization to fulfill these requirements with our **"Managed XDR Service for Microsoft 365 Government Commercial Cloud (GCC) High environments"** offering.

We specialize in helping organizations to meet compliance regulations such as **Cybersecurity Maturity Model Certification (CMMC), International Traffic in Arms Regulations (ITAR)**, and more, while securely migrating organizations Microsoft 365 Government Community Cloud (GCC) High.

organizations

Compliance regulations
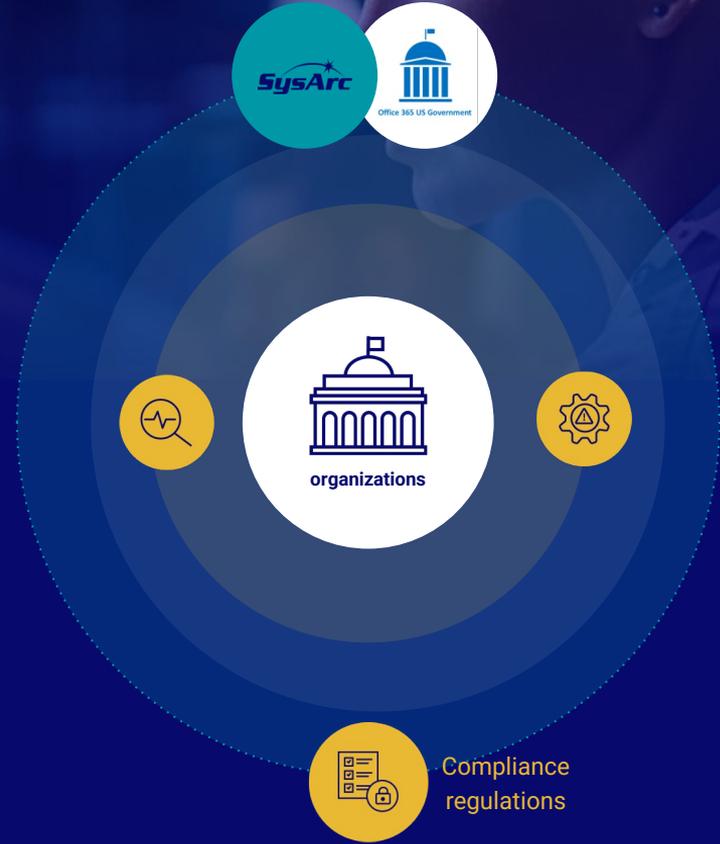
Deliverables

Implementation of Managed XDR Service Framework
We will establish a Managed XDR Service framework specifically tailored to meet the compliance requirements of U.S. Government contractors, incorporating policies, procedures, and workflows that comply with CMMC, ITAR, and other relevant regulations.

Tools Deployment
We will leverage the inherent security tools of Office 365 GCC High and Microsoft 365 GCC High, along with additional tools from the Microsoft Security suite, including Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud, to enhance protection.

Continuous Monitoring
We will implement real-time monitoring with advanced SIEM systems, utilize anomaly detection through sophisticated algorithms and machine learning, conduct alert triage to differentiate false positives from actual threats, engage in proactive threat hunting, and perform forensic analysis to investigate and understand potential security incidents.

Threat Detection and Incident Response
Our Managed XDR Service will deploy proactive measures using advanced threat detection systems for heuristic and behavioral analysis, alongside reactive measures for swift threat investigation and response, including incident protocols to contain, eradicate, and recover from genuine threats, complemented by a post-mortem analysis to prevent future incidents.

Threat Intelligence
We will analyze new threat patterns and behaviors, update our defense strategies based on strategic analysis, and conduct regular training and simulations to prepare for potential cyberattacks.

Vulnerability Management
We will conduct regular vulnerability scans, perform detailed security assessments, create threat models, formulate remediation strategies, and use continuous improvement practices to evolve our security posture and address emerging challenges.

SysArc

The journey towards uncompromising cybersecurity compliance starts with the right partner. SysArc's proven approach to Microsoft GCC High Migration and Managed XDR Services offers the pathway to success. Let's secure your organization's future together.

Contact Us

Sales: 240-453-4158

Customer Support: 800-699-0925 ext. 1