UNDERSTANDING CMMC COMPLIANCE

AN E-BOOK

FROM MANAGED SERVICES PROVIDER

SIMPLE HELIX

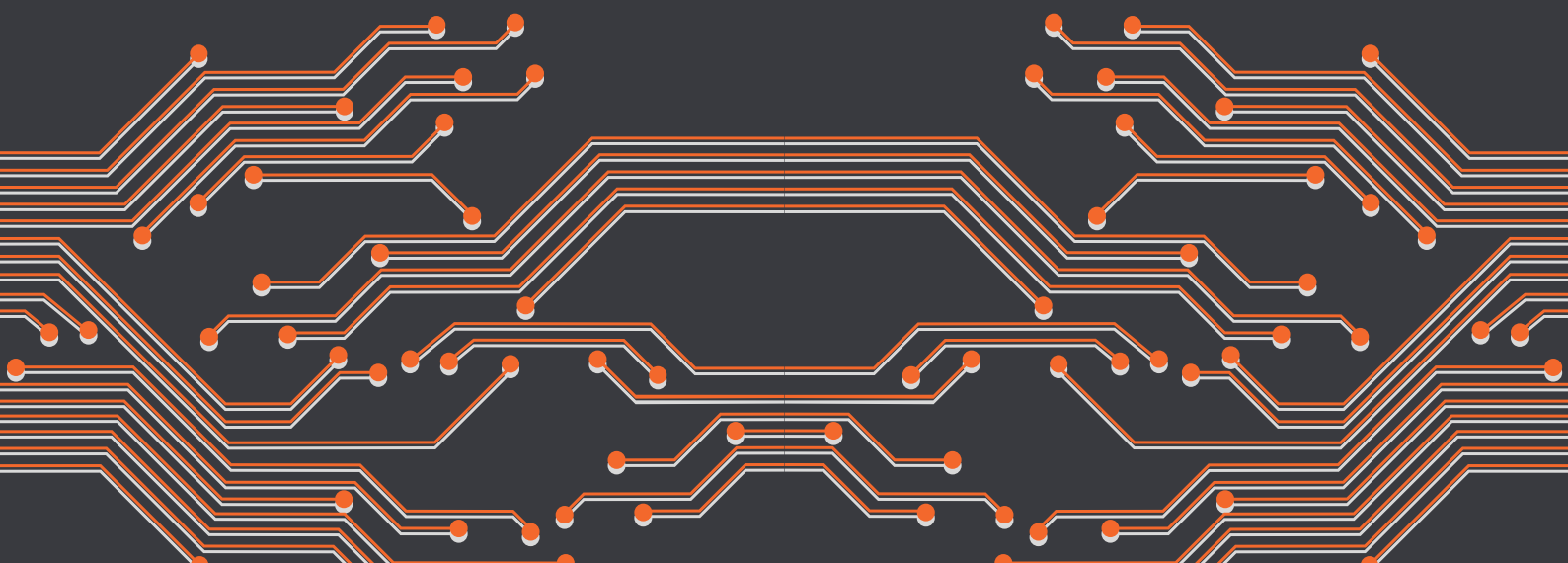
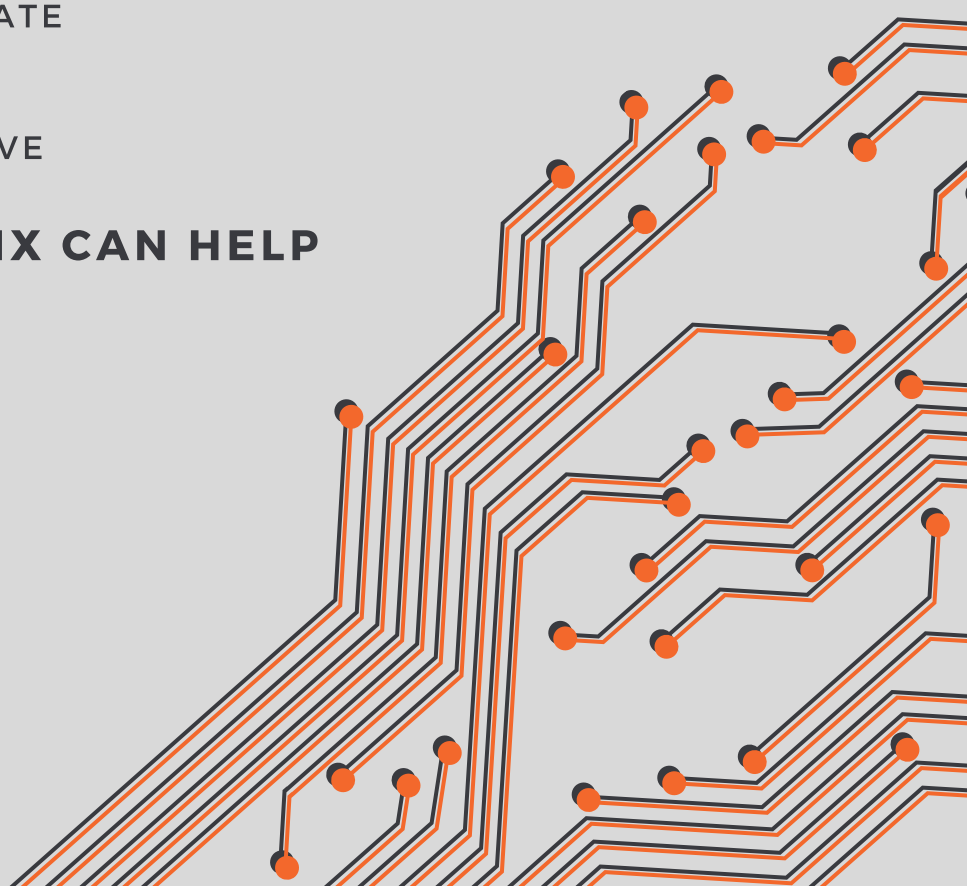


TABLE OF CONTENTS



CMMC FAQS

WHAT IS CMMC?

The Cybersecurity Maturity Model Certification or CMMC is a new standard of cybersecurity compliance developed by the Department of Defense (DoD). The compliance standard is an evolution of the DFARS 252.204-7012 & NIST 800-171 standards and is meant to protect the nation's most sensitive data from our adversaries. **All government contractors will have to become CMMC Compliant by 2026 in order to continue business with the U.S. Government.**

WHY IS THIS HAPPENING?

As the threat of data theft rises daily, so does the need to protect our nation's sensitive information. The Defense Industrial Base or DIB and DoD serve as major targets for cyber adversaries. These adversaries are most interested in gaining insight regarding our war machines and defense technologies. To prevent them from gaining this insight, our nation must seek to strengthen it's cyber security hygiene. Because of this CMMC was created. The new compliance standard ensures those companies that develop our greatest technologies can also keep them safe from those who would use them against us.

WHEN WILL CONTRACTORS HAVE TO BE CERTIFIED?

The CMMC roll-out will be a phased approach over a 5-year period starting with the release of 10 RFIs and RFPs in 2020. The number of new contracts requiring CMMC certification will grow in subsequent years until all contracts require CMMC Compliance in 2026. Contractors will have to meet CMMC Compliance in order to be awarded these contracts. Deciding when to start on the journey to compliance will depend on the release of the contractor's preferred RFI/RFP as well as what their business circumstances dictate. Contractors will be able to bid on opportunities prior to becoming CMMC compliant. However, they will not be awarded the contract unless they meet the compliance requirement.

ARE PRIME CONTRACTORS RESPONSIBLE FOR SUBS?

Prime contractors will have to ensure all sub-contractors working under them are CMMC compliant. However, the primes are not responsible for paying for the sub-contractors compliance journey. Primes are encouraged to provide subs with direction regarding CMMC Compliance.

WHAT'S THE DIFFERENCE BETWEEN CMMC & DFARS OR NIST 800-171?

Under NIST 800-171, contractors are responsible for self attesting their compliance. Now, contractors must be assessed and certified by CMMC assessors. **Under CMMC, DoD Contractors will be audited every 1 to 3 years depending on the level of compliance they achieve.** This ensures contractors are taking cyber security seriously and lowers the risk of data loss.

Here are some other differences between NIST 800-171 and CMMC:

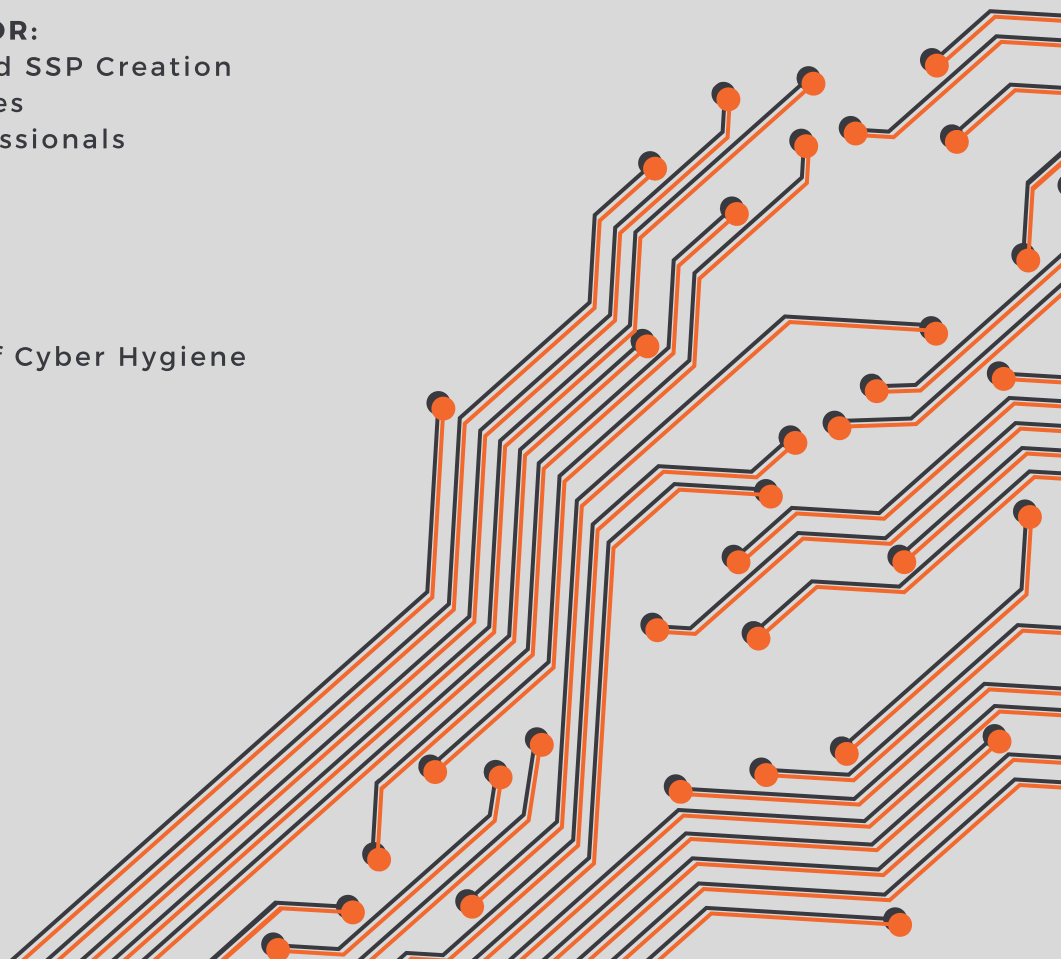
- The project plan (POA&M) must be complete before the assessment.
- Contractors must be certified prior to being awarded new contracts.
- Both Prime and Subcontractors will need to be CMMC Compliant.
- CMMC is not an all or nothing standard. Contractors can select the level that is appropriate for them based on the type of work they perform for the DoD.

HOW MUCH WILL THIS COST?

There isn't a defined cost to becoming compliant. **The cost depends on which level you choose to pursue/achieve.** The lower the level you achieve, the lower the cost. You can also decrease cost by selecting cost effective tools and processes while on your compliance journey.

COSTS TO PREPARE FOR:

- GAP Assessment and SSP Creation
  - Internal Resources
  - Third Party Professionals
- Implementation
  - Fees
  - Tools
  - Services
- Assessment
- Ongoing Maturity of Cyber Hygiene



HOW IS THE CMMC MODEL STRUCTURED?

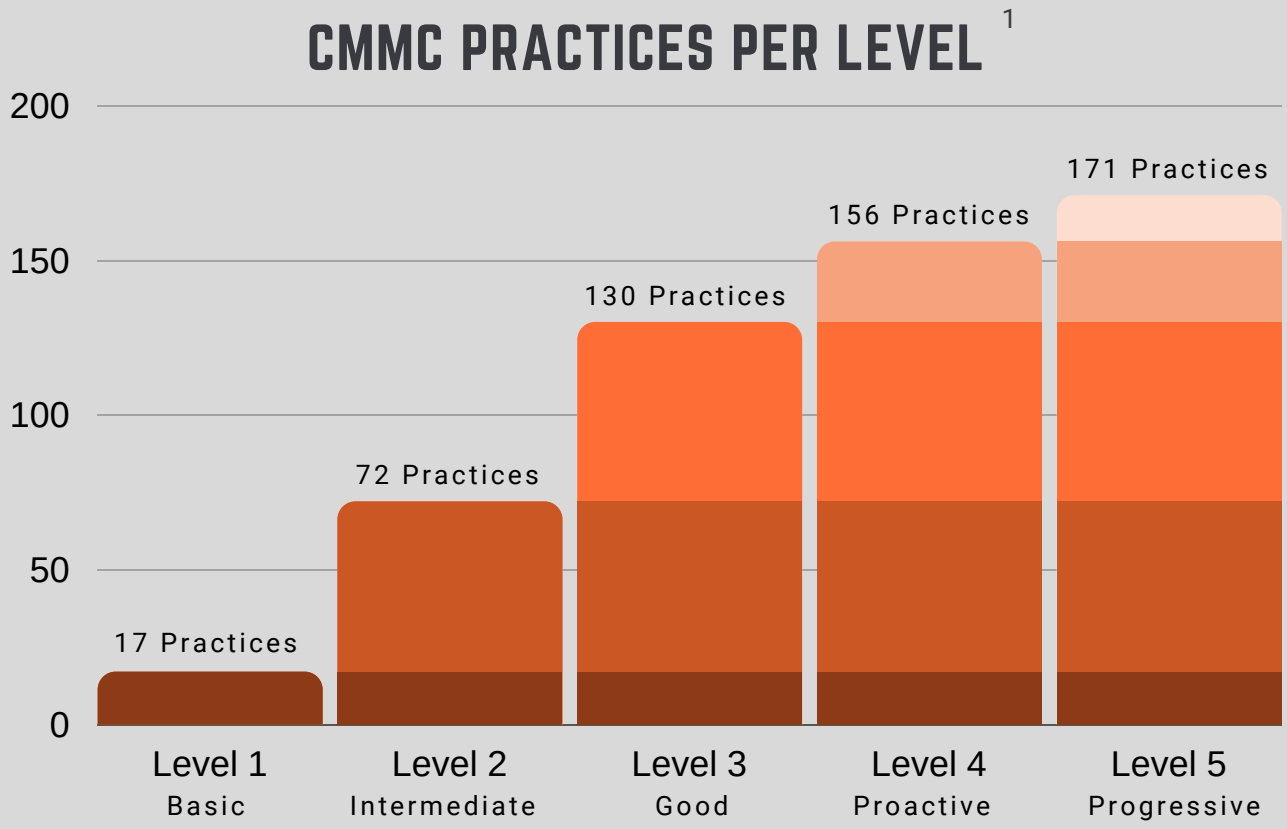
The CMMC Model is comprised of 17 domains. The domains are listed below with their coinciding capability.

DOMAIN	CAPABILITY	# OF PRACTICES COVERED *
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes	23/26
Asset Management (AM)	• Identify and document assets • Manage asset inventory	1/2
Audit & Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs	14/14
Awareness & Training (AT)	• Conduct security awareness activities • Conduct training	0/5
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management	10/11
Identification & Authentication (IA)	• Grant access to authenticated entities	10/11
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident	3/13
Maintenance (MA)	• Manage maintenance	6/6
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport	1/8
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions	1/2
Physical Protection (PE)	• Limit physical access	0/6
Recovery (RE)	• Manage backups • Manage information security continuity	4/4
Risk Management (RM)	• Identify and evaluate risk • Manage risk • Manage supply chain risk	2/12
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews	0/8
Situaltional Awareness (SA)	• Implement threat monitoring	2/3
Systems & Communications Protection (SC)	• Define security requirements for systems and communications • Control communicationsat system boundaries	20/27
Systems & Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • perform network and system monitoring • Implement advanced email protections	10/13

*The # of Practices Covered are based on how many practices Simple Helix can meet within the domain associated.

These domains match with a list of practices. Each practice is categorized within a level. The number of practices you are able to successfully implement will determine which level you achieve.

As the levels advance, they grow in number of practices and complexity. See the table below to view the number of practices within each level.



To create your SSP, you'll need to match each policy to a CMMC practice within the level you've selected. You can find the complete list of CMMC Practices on page 12 of the CMMC Model linked here.

THE 4 STEPS TO COMPLIANCE[1]

STEP 1: BASELINING

- Third party analyzes current contracts and assigns lowest level contractor must achieve
- Third party performs Gap Assessment
- Develop a System Security Plan (SSP) that meets all practices
- Create a project plan to close the gaps identified

STEP 2: IMPLEMENTATION

- Bring your Gap Assessment to an Implementer
- Complete project plan
  - Implementer will provide you with tools & services needed to gain compliance
  - Provide employees with training

Note: Simple Helix is considered an Implementer and can help guide contractors through Step 2.

STEP 3: ENACT

- Operate your SSP
  - You have the plan , tools, services, and training to ensure you're compliant. Now it's time to operate as a CMMC Compliant Contractor.
- Internally correct issues as they arise

Note: Simple Helix can also assist contractors throughout Step 3 by providing managed IT services and SOC monitoring services.

STEP 4: ASSESSMENT

- Prepare for the arrival of the Assessor
- Assessor arrives on site to review SSP & practices
- Assessor concludes with reporting their findings
  - If contractor passes, they will be awarded their Level of certification
  - If the contractor doesn't pass, they must correct the issues found and then be reassessed
- Contractor continues to improve cyber security practices in preparation for next audit

THE 5 LEVELS OF CMMC[1]

SIMPLE HELIX PROVIDES SOLUTIONS FOR THE PRACTICES BELOW AUGMENTED THROUGH MANAGED SERVICES.

LEVEL 1: BASIC CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
1	Spam Filtering	Office 365	11/17
	Password Encryption	Multi-factor Authentication by DUO	
	Antivirus	Webroot	

LEVEL 2: INTERMEDIATE CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
2	All previous practices	See previous tools/services	48/72
	Offsite, offline backups	Veeam Cloud-based Backups	

LEVEL 3: GOOD CYBER HYGIENE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
3	All previous practices	See previous tools/services	90/130
	DNS Filtering	Webroot or Palo Alto Firewalls	
	Encrypted Email & File Sharing	Office 365, Office 365 GCC High, or PreVeil	
	Retroactive monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

*The # of Practices Covered are based on how many practices Simple Helix can meet within the level associated.

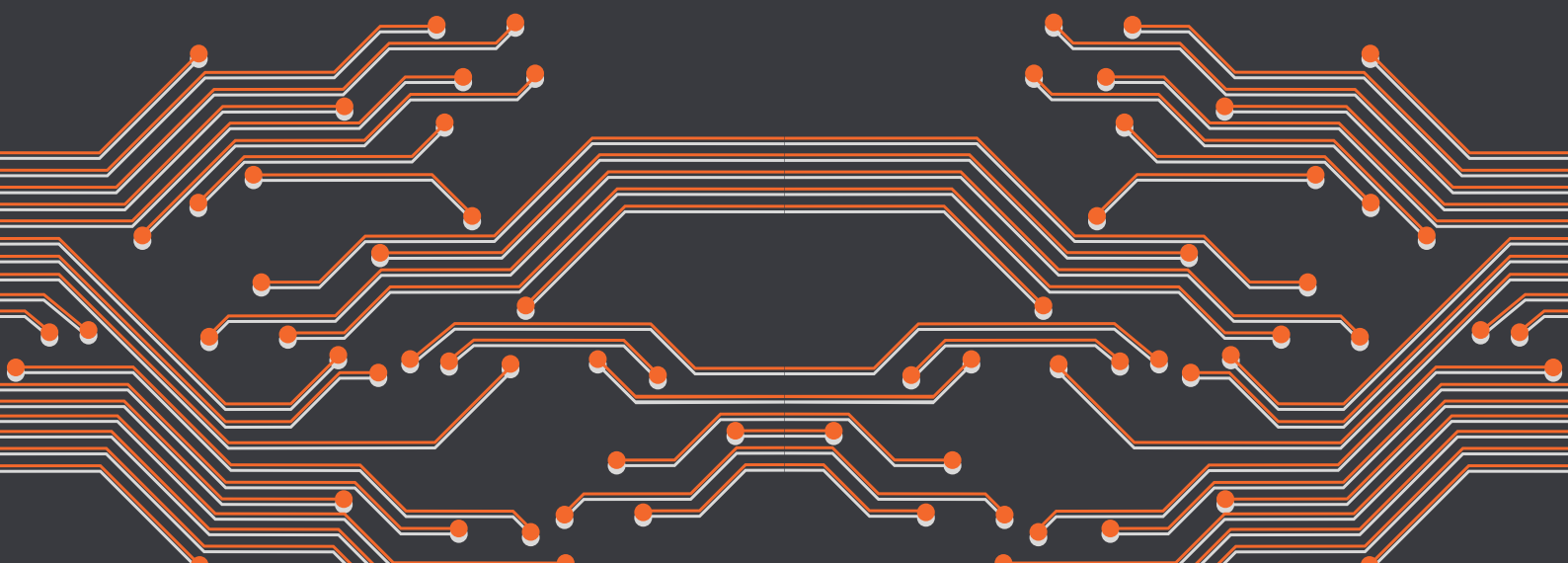
LEVEL 4: PROACTIVE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
4	All previous practices	See previous tools/services	105/156
	Proactive monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

LEVEL 5: ADVANCED/PROGRESSIVE

LEVEL	PRACTICE	SOLUTION	PRACTICES COVERED*
5	All previous practices	See previous tools/services	112/171
	24/7, real-time monitoring of Log Files	LogRhythm SIEM Solution	
		SOC Monitoring Services	

*The # of Practices Covered are based on how many practices Simple Helix can meet within the level associated.



HOW CAN SIMPLE HELIX HELP?

OUR SOLUTIONS

Below is a list of recommended tools we provide to help contractors meet CMMC compliance.

Simple Helix supports both Office 365 and Office 365 GCC High. Support options include licenses, implementation services, and managed services.

LogRhythm is a Security Information and Event Management (SIEM) tool that monitors and protects information security systems. It can be deployed on-site or within our hosted cloud environment with monitoring out of our Security Operations Center (SOC).

Simple Helix recommends Veeam for offsite and offline backups. This tool acts as a secure repository for your data. The software offers compression which allows users to fit more data within a smaller storage capacity - saving you money.

PreVeil is an email and file sharing encryption software solution that can pair with both Office 365 & G-Suite platforms. By deploying PreVeil to users as needed, PreVeil offers a simple, cost-effective solution that allows our customers to save money while also utilizing their existing email solution.

To meet the controls for password encryption, we recommed Multi-factor Authentication from DUO. Depending on which office suite your company uses, we may also be able to ensure the encryption tools native to your current technology run optimally.

OUR SERVICES

Simple Helix recommends our Managed Services and SOC/NOC Services to implement, support and maintain your compliance practices. Leverage our team to supplement your current IT department or make us your entire IT department. Regardless of what you choose, we'll be right there with you.

MANAGED SERVICES

Our team can serve as either an aid to your existing IT department or we can act as your entire IT department. We can implement, manage, and sustain your CMMC Compliant IT environment.

SOC SERVICES

Our SOC team is available to monitor your log files to ensure no your data is safe from adversaries.

Meeting log file practices in levels 3 through 5 doesn't have to be complicated with our team on your side.

NOC SERVICES

Our NOC Team manages our Veeam Cloud-based Environment in our Colocation Tier III Data Center to ensure you never go off-line.

FOR A FREE CONSULTATION, CONTACT US:

(256) 704-1041
SALES@SIMPLEHELIX.COM

OR VISIT US AT SIMPLEHELIX.COM

DUNS: 009815946 | CAGE: 7FNU2 | NAICS: 518210 (PRIMARY), 517311, 541513, 541519, 541690

SIMPLE HELIX

CITATIONS

1 Cybersecurity Maturity Model Certification (CMMC) Version 1.02 https://wplstage.simplehelix.host/wp-content/uploads/2020/07/CMMC_ModelMain_V1.02_20200318.pdf (last accessed July 23, 2020)