CMMC LEVEL 2 COMPLIANCE

COMPLETE AUDIT CHECKLIST

BREA NETWORKS

CMMC COMPLIANCE.US

BREA NETWORKS
CMMC COMPLIANCE.US

CONTROL FAMILIES

- ACCESS CONTROL
- AUDIT & ACCOUNTABILITY
- AWARENESS & TRAINING
- CONFIGURATION MANAGEMENT
- IDENTIFICATION & AUTHENTICATION
- INCIDENT RESPONSE
- MAINTENANCE
- MEDIA PROTECTION
- PERSONNEL SECURITY
- PHYSICAL PROTECTION
- RISK ASSESSMENT
- SECURITY ASSESSMENT
- SYSTEM & COMMS PROTECTION
- SYSTEM INTEGRITY

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

ACCESS CONTROLS

Access Control focuses on making sure only the right people can use your systems, view sensitive information, and perform specific actions. These controls protect CUI by limiting access to authorized users, devices, and sessions.

AC.L1-3.1.1 — Authorized Access Control

Do you limit access so that only approved users can get into your systems and data?

□ Yes □ No □ Not Sure

AC.L1-3.1.2 — Transaction and Function Control

Do you make sure users can only perform actions they are allowed to do in your systems?

□ Yes □ No □ Not Sure

AC.L1-3.1.20 — External Connections

Do you control and monitor all external connections into your network?

□ Yes □ No □ Not Sure

AC.L1-3.1.22 — Control Public Information

Do you make sure public information stays separate from sensitive information?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

ACCESS CONTROLS

AC.L2-3.1.3 — Control CUI Flow

Do you control how CUI moves in and out of your organization, including sharing, downloading, and transferring data?

□ Yes □ No □ Not Sure

AC.L2-3.1.4 — Separation of Duties

Do you separate responsibilities so no single person has too much control over sensitive tasks?

□ Yes □ No □ Not Sure

AC.L2-3.1.5 — Least Privilege

Does every user have only the minimum access they need to do their job?

□ Yes □ No □ Not Sure

AC.L2-3.1.6 — Non-Privileged Account Use

Do admins use regular accounts for normal work and only use admin accounts when needed?

□ Yes □ No □ Not Sure

AC.L2-3.1.7 — Privileged Functions

Do you tightly control who can perform high-risk or administrative actions?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

ACCESS CONTROLS

AC.L2-3.1.8 — Unsuccessful Logon Attempts

Do you lock accounts or trigger alerts after too many failed login attempts?

□ Yes □ No □ Not Sure

AC.L2-3.1.9 — Privacy and Security Notices

Do your systems display login banners or notices that warn users about authorized use only?

□ Yes □ No □ Not Sure

AC.L2-3.1.10 — Session Lock

Do devices lock automatically after being idle for a set amount of time?

□ Yes □ No □ Not Sure

AC.L2-3.1.11 — Session Termination

Do systems automatically log users out after a period of inactivity or at session end?

□ Yes □ No □ Not Sure

AC.L2-3.1.12 — Remote Access

Do you control and secure all remote access into your systems?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

ACCESS CONTROLS

AC.L2-3.1.14 — Remote Access Routing

Do remote connections go through approved and secure routes like VPN or managed gateways?

□ Yes □ No □ Not Sure

AC.L2-3.1.15 — Privileged Remote Access

Do you require extra security for admin-level users who access systems remotely?

□ Yes □ No □ Not Sure

AC.L2-3.1.16 — Wireless Access Authorization

Do you approve and control every wireless network and wireless access point?

□ Yes □ No □ Not Sure

AC.L2-3.1.17 — Wireless Access Protection

Do you secure wireless networks with strong encryption and authentication?

□ Yes □ No □ Not Sure

AC.L2-3.1.18 — Mobile Device Connection

Do you approve and manage any mobile devices that connect to your network or access CUI?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

ACCESS CONTROLS

AC.L2-3.1.19 — Encrypt CUI on Mobile Devices

Do you encrypt all CUI stored or accessed on mobile devices?

□ Yes □ No □ Not Sure

AC.L2-3.1.21 — Portable Storage Use

Do you control and approve any use of USB drives or portable storage devices?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

AUDIT & ACCOUNTABILITY

Audit and Accountability makes sure you record what happens inside your systems and can trace actions back to specific users. These controls help detect suspicious activity, respond to incidents, and prove compliance during an audit.

AU.L2-3.3.1 — System Auditing

Do you turn on system auditing so your systems record important events and activities?

□ Yes □ No □ Not Sure

AU.L2-3.3.2 — User Accountability

Can you link every action in the system back to a specific user?

□ Yes □ No □ Not Sure

AU.L2-3.3.3 — Event Review

Do you review logs and audit records to look for unusual or suspicious activity?

□ Yes □ No □ Not Sure

AU.L2-3.3.4 — Audit Failure Alerting

Do you get alerts when logging stops working or audit logs fail?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

AUDIT & ACCOUNTABILITY

AU.L2-3.3.5 — Audit Correlation

Can you compare logs from different systems to find patterns or track activity across multiple devices?

□ Yes □ No □ Not Sure

AU.L2-3.3.6 — Reduction and Reporting

Do you organize audit logs so they are easy to understand and report on?

□ Yes □ No □ Not Sure

AU.L2-3.3.7 — Authoritative Time Source

Do all your systems use the same trusted time source so timestamps in logs match?

□ Yes □ No □ Not Sure

AU.L2-3.3.8 — Audit Protection

Do you protect audit logs from being changed, deleted, or accessed by unauthorized users?

□ Yes □ No □ Not Sure

AU.L2-3.3.9 — Audit Management

Do you manage how logs are kept, stored, reviewed, and deleted based on your policies?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

AWARENESS & TRAINING

Awareness and Training makes sure your team understands cybersecurity risks, knows how to protect CUI, and can perform their security duties correctly. These controls ensure everyone is trained, informed, and prepared.

AT.L2-3.2.1 — Security Awareness Training

Do you train all employees on basic cybersecurity, safe practices, and how to protect CUI?

□ Yes □ No □ Not Sure

AT.L2-3.2.2 — Role-Based Security Training

Do employees who handle sensitive systems or CUI receive extra training for their specific job duties?

□ Yes □ No □ Not Sure

AT.L2-3.2.3 — Threat Awareness

Do employees learn how to spot phishing, suspicious behavior, and other common cyber threats?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

CONFIGURATION MANAGMENET

Configuration Management makes sure your systems, software, and settings are controlled, documented, and protected from unauthorized changes. These controls help you maintain secure and consistent system configurations across your organization.

CM.L2-3.4.1 — Establish Baseline Configurations

Do you keep a documented list of approved system settings and configurations for all your devices and systems?

□ Yes □ No □ Not Sure

CM.L2-3.4.2 — Control Changes

Do you review, approve, and track all changes made to systems, software, or configurations?

□ Yes □ No □ Not Sure

CM.L2-3.4.3 — Security Impact Analysis

Do you check how a change might affect security before you make that change?

□ Yes □ No □ Not Sure

CM.L2-3.4.4 — Manage System Components

Do you track and control what hardware, software, and tools are allowed on your systems?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

CONFIGURATION MANAGEMENT

CM.L2-3.4.5 — Allow Only Approved Components

Do you make sure only approved and secure software, tools, and devices are installed or used?

□ Yes □ No □ Not Sure

CM.L2-3.4.6 — Least Functionality

Do you disable features, services, and programs that are not needed so your systems stay secure?

□ Yes □ No □ Not Sure

CM.L2-3.4.7 — Unauthorized Software Prevention

Do you block or remove software that is not approved for use in your organization?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

IDENTIFICATION & AUTHENTICATION

Identification and Authentication ensures that only verified users and devices can access your systems. These controls require strong passwords, multi factor authentication, and unique identification for all users who handle CUI.

IA.L2-3.5.1 — Identify Users

Do you make sure every user has a unique ID so you always know who is accessing your systems?

□ Yes □ No □ Not Sure

IA.L2-3.5.2 — Authenticate Users

Do users need to prove who they are before they can access systems or data?

□ Yes □ No □ Not Sure

IA.L2-3.5.3 — Password Complexity

Do you require strong passwords that meet length and complexity rules?

□ Yes □ No □ Not Sure

IA.L2-3.5.4 — Password Change Frequency

Do you require passwords to be changed when needed or when there is a possible security risk?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

IDENTIFICATION & AUTHENTIFICATION

IA.L2-3.5.5 — Password Protection

Do you protect passwords from being shared, stored in plain text, or exposed in any way?

□ Yes □ No □ Not Sure

IA.L2-3.5.6 — Multi Factor Authentication

Do you require multi factor authentication for all users who access CUI or log in remotely?

□ Yes □ No □ Not Sure

IA.L2-3.5.7 — Identify and Authenticate Non User Entities

Do you identify and verify any devices, services, or systems that connect to your network?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

INCIDENT RESPONSE

Incident Response makes sure your organization can detect, report, respond to, and recover from cybersecurity incidents. These controls help you react quickly and reduce the impact of any security event involving CUI.

IR.L2-3.6.1 — Incident Response Plan

Do you have a written plan that explains how your team will respond to cybersecurity incidents?

□ Yes □ No □ Not Sure

IR.L2-3.6.2 — Incident Reporting

Do employees know how to report security incidents quickly and correctly?

□ Yes □ No □ Not Sure

IR.L2-3.6.3 — Incident Analysis

Do you investigate incidents to understand what happened, what was affected, and what needs to be done?

□ Yes □ No □ Not Sure

IR.L2-3.6.4 — Incident Response Activities

Do you take action during an incident to contain it, remove the threat, and protect your systems?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

INCIDENT RESPONSE

IR.L2-3.6.5 — Incident Response Testing

Do you test your incident response plan so you know it works and your team is prepared?

□ Yes □ No □ Not Sure

IR.L2-3.6.6 — Incident Reporting to External Parties

Do you report incidents to required external groups when needed, such as DoD or partners?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

MAINTENANCE

Maintenance ensures that systems are properly serviced, updated, and repaired in a secure way. These controls protect CUI by making sure only authorized personnel perform maintenance and that remote maintenance is controlled.

MA.L2-3.7.1 — Controlled Maintenance

Do you perform maintenance in a planned and approved way and keep records of what was done?

□ Yes □ No □ Not Sure

MA.L2-3.7.2 — Controlled Tools

Do you make sure only approved tools and equipment are used during maintenance?

□ Yes □ No □ Not Sure

MA.L2-3.7.3 — Authorized Maintenance Personnel

Do you verify that only authorized and trusted people perform maintenance on your systems?

□ Yes □ No □ Not Sure

MA.L2-3.7.4 — Nonlocal Maintenance Approval

Do you approve all remote maintenance sessions before they begin?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

MAINTENANCE

MA.L2-3.7.5 — Nonlocal Maintenance Monitoring

Do you monitor and log all remote maintenance activities while they are happening?

□ Yes □ No □ Not Sure

MA.L2-3.7.6 — Remote Maintenance Disconnection

Do you end or disable remote maintenance access when the task is complete?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

MEDIA PROTECTION

Media Protection makes sure that any physical or digital media containing CUI is properly controlled, stored, transported, and destroyed. These controls prevent sensitive information from being lost, stolen, or accessed by unauthorized people.

MP.L1-3.8.3 — Media Disposal

Do you destroy media containing sensitive information in a secure and approved way?

□ Yes □ No □ Not Sure

MP.L1-3.8.4 — Media Sanitization

Do you wipe or sanitize media before reusing or releasing it for other purposes?

□ Yes □ No □ Not Sure

MP.L1-3.8.5 — Access to Media

Do you limit access to media that contains sensitive information to authorized people only?

□ Yes □ No □ Not Sure

MP.L1-3.8.6 — Marking Media

Do you label media containing CUI so it is clearly identified and handled correctly?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

MEDIA PROTECTION

MP.L2-3.8.1 — Protect Information in Media

Do you protect sensitive information stored on media whether it is physical or digital?

□ Yes □ No □ Not Sure

MP.L2-3.8.2 — Limit Media Access

Do you restrict who can use, remove, or handle media containing CUI?

□ Yes □ No □ Not Sure

MP.L2-3.8.7 — Transport Protection

Do you protect media containing CUI when it is transported outside your facility?

□ Yes □ No □ Not Sure

MP.L2-3.8.8 — Media Control and Accountability

Do you track, control, and log who uses or moves media that contains CUI?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

PERSONNEL SECURITY

Personnel Security ensures that people with access to CUI are trustworthy and that access is removed quickly when someone leaves the company or changes roles. These controls help prevent insider threats and unauthorized access.

PS.L2-3.9.1 — Screen Personnel

Do you perform background checks or screening before giving someone access to CUI?

□ Yes □ No □ Not Sure

PS.L2-3.9.2 — Access Removal

Do you remove system and facility access quickly when an employee leaves or no longer needs access?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

PHYSICAL PROTECTION

Physical Protection ensures that only authorized people can enter areas where systems and information are stored. These controls help protect CUI from physical theft, tampering, or unauthorized viewing.

PE.L1-3.10.1 — Limit Physical Access

Do you control and limit who can enter areas where your systems and sensitive information are stored?

□ Yes □ No □ Not Sure

PE.L1-3.10.3 — Escort Visitors

Do you escort visitors inside secure areas and make sure they do not access sensitive information?

□ Yes □ No □ Not Sure

PE.L1-3.10.4 — Physical Access Logs

Do you keep records of everyone who enters and exits secure areas?

□ Yes □ No □ Not Sure

PE.L1-3.10.5 — Manage Physical Access Devices

Do you control things like keys, badges, and access cards so only authorized people can use them?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

PHYSICAL PROTECTION

PE.L2-3.10.2 — Protect and Monitor Access

Do you use alarms, cameras, or monitoring to protect areas where CUI or critical systems are located?

□ Yes □ No □ Not Sure

PE.L2-3.10.6 — Secure Media and Equipment

Do you secure laptops, servers, storage devices, and any equipment that contains CUI?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

RISK ASSESSMENT

Risk Assessment helps you identify threats, vulnerabilities, and weaknesses in your systems. These controls make sure you regularly review risks and test your security to keep CUI protected.

RA.L2-3.11.1 — Risk Assessment

Do you review your systems to identify risks, weaknesses, and potential threats to CUI?

□ Yes □ No □ Not Sure

RA.L2-3.11.2 — Vulnerability Scans

Do you run regular vulnerability scans to find security issues in your systems?

□ Yes □ No □ Not Sure

RA.L2-3.11.3 — Scan Remediation

Do you fix or address the problems found during vulnerability scans?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

SECURITY ASSESSMENT

Security Assessment ensures you review, test, and monitor your security practices on a regular basis. These controls help confirm that your policies are being followed and that your security program is working as intended.

CA.L2-3.12.1 — Security Assessments

Do you regularly assess your security policies and practices to make sure they are being followed and are effective?

□ Yes □ No □ Not Sure

CA.L2-3.12.2 — Plan of Action

Do you create a plan to fix security weaknesses and track progress until the issues are resolved?

□ Yes □ No □ Not Sure

CA.L2-3.12.3 — Continuous Monitoring

Do you monitor your systems on an ongoing basis to spot security issues or changes that could create risks?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

SYSTEM & COMMUNICATIONS PROTECTION

System and Communications Protection ensures your systems, networks, and data are protected while being stored, processed, and transmitted. These controls focus on encryption, boundary protection, monitoring, and securing communications that involve CUI.

SC.L1-3.13.1 — Boundary Protection

Do you protect your network by controlling the traffic that enters and leaves your systems?

□ Yes □ No □ Not Sure

SC.L1-3.13.5 — Public Access Protection

Do you keep public-facing systems separate from internal systems that store or process CUI?

□ Yes □ No □ Not Sure

SC.L2-3.13.2 — Encryption in Transit

Do you encrypt CUI when it is sent over networks so no one can read it during transmission?

□ Yes □ No □ Not Sure

SC.L2-3.13.3 — Cryptographic Protections

Do you use approved and secure cryptographic tools to protect CUI?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

SYSTEMS & COMMUNICATION PROTECTION

SC.L2-3.13.4 — Prevent Unauthorized Information Transfer

Do you block or control ways data could be moved out of your systems without authorization?

□ Yes □ No □ Not Sure

SC.L2-3.13.6 — Deny Untrusted Connections

Do you prevent connections from unknown or untrusted networks or devices?

□ Yes □ No □ Not Sure

SC.L2-3.13.7 — Monitor Communications

Do you monitor network traffic for unusual activity or possible security threats?

□ Yes □ No □ Not Sure

SC.L2-3.13.8 — Control Collaborative Computing Devices

Do you control devices like webcams, microphones, and conferencing tools to prevent unauthorized use?

□ Yes □ No □ Not Sure

SC.L2-3.13.9 — Specialized System Security

Do you apply extra security to systems that need additional protection due to their purpose or sensitivity?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

SYSTEMS & COMMUNICATION PROTECTION

SC.L2-3.13.10 — Address Boundary Filtering

Do you filter traffic at system and network boundaries to block harmful or unauthorized communications?

□ Yes □ No □ Not Sure

SC.L2-3.13.11 — Public Key Infrastructure Certificates

Do you use trusted certificates for secure connections and authentication?

□ Yes □ No □ Not Sure

SC.L2-3.13.12 — Remote Access Encryption

Do you encrypt all remote access sessions to protect data that is transmitted?

□ Yes □ No □ Not Sure

SC.L2-3.13.13 — Protect Voice and Video Communications

Do you secure voice and video calls when they involve CUI?

□ Yes □ No □ Not Sure

SC.L2-3.13.14 — Control Mobile Network Access

Do you control and secure how mobile devices connect to your network or access CUI?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

SYSTEMS & COMMUNICATION PROTECTION

SC.L2-3.13.15 — DNS Filtering and Monitoring

Do you protect your network by filtering and monitoring DNS requests to block malicious domains?

□ Yes □ No □ Not Sure

SC.L2-3.13.16 — Protect Data at Rest

Do you encrypt or otherwise protect stored CUI so only authorized users can access it?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

SYSTEM & INFORMATION INTEGRITY

System and Information Integrity ensures your systems are protected from malware, unauthorized changes, and security flaws. These controls help you detect problems quickly, fix vulnerabilities, and keep CUI safe from threats.

SI.L1-3.14.1 — Flaw Remediation

Do you find, track, and fix security flaws in your systems in a timely way?

□ Yes □ No □ Not Sure

SI.L1-3.14.2 — Malicious Code Protection

Do you use tools like antivirus or anti malware to protect your systems from harmful software?

□ Yes □ No □ Not Sure

SI.L1-3.14.4 — Update Malicious Code Protection

Do you keep your antivirus and anti malware tools updated so they can detect the latest threats?

□ Yes □ No □ Not Sure

SI.L1-3.14.5 — Spam Protection

Do you use tools to detect and block spam and harmful emails?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

SYSTEMS & INFORMATION INTEGRITY

SI.L1-3.14.6 — Monitor System Security Alerts

Do you monitor and respond to security alerts from your systems and security tools?

□ Yes □ No □ Not Sure

SI.L2-3.14.3 — Malicious Code Limits

Do you limit where code can run to reduce the risk of malware or unauthorized software?

□ Yes □ No □ Not Sure

SI.L2-3.14.7 — Identify Unauthorized Changes

Do you detect unauthorized changes to software, settings, or files on your systems?

□ Yes □ No □ Not Sure

SI.L2-3.14.8 — Monitor for Attack Indicators

Do you watch for signs of attacks or suspicious behavior inside your systems?

□ Yes □ No □ Not Sure

SI.L2-3.14.9 — End User Threat Reporting

Do employees know how to report suspicious activity, malware, or unusual system behavior?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

BREA NETWORKS

CMMC COMPLIANCE.US

SYSTEMS & INFORMATION INTEGRITY

SI.L2-3.14.10 — System and File Integrity Tools

Do you use tools that check system files and alert you if something changes unexpectedly?

□ Yes □ No □ Not Sure

ELIMINATE THE GUESSWORK, BOOK A CALL WITH A CERTIFIED RPO

BOOKING LINK

CMMC LEVEL 2

CMMC Level 2 is hard and the DoD/DoW are about to enforce it for real.

Most contractors are not ready. Their systems are weak, their documents are missing, and they have no plan. Every day they wait, they fall behind other contractors who are getting ready now. If you are not compliant, you will lose the right to bid or keep DoD/DoW contracts.

If you keep going after DoD/DoW work while you know you are not compliant, your company can face *False Claims Act* punishment. This can include very large fines that can reach 3x the contract value. It can also create serious legal trouble for company leaders. This is not a scare tactic. This is the new reality for DoD/DoW contractors.

You do not have to do this alone. Brea Networks is CMMC Level 2 certified and we passed our audit with a perfect score of 110 out of 110. We help you reach that level with our IT support, our security team, and full CMMC compliance help.

Hiring your own Cybersecurity Officer, Compliance Manager, and IT team can cost $350,000 to $550,000 each year.

You can work with our certified team for a fraction of that cost and with no learning curve or training delays. If you want to protect your contracts and lower your risk, book a call today.

BOOKING LINK

BREA NETWORKS