2W Technologies' Role in CMMC 2.0 Compliance

2W Technologies, INC.

Overview: 2W Technologies serves as a specialized **External Service Provider (ESP)** for defense contractors pursuing **CMMC 2.0 Level 2**. In other words, **2W operates within your CMMC assessment scope**, but **you (the client) are the Organization Seeking Certification (OSC)** responsible for overall compliance. Our role is **to help scope your CUI, design, implement, and manage secure cloud environments and technical controls** to meet **NIST SP 800-171** and related **DFARS** requirements on your behalf, while **you retain ownership** of organizational policies, personnel practices, and ultimately the certification process. This clear division of responsibilities — documented in a **Shared Responsibility Matrix (SRM)** ensures nothing falls through the cracks and provides a **clean, auditable separation of duties** from an assessor's perspective.

2W's Services: What We Provide to Support CMMC Level 2

Secure Cloud Architecture & Technical Controls: 2W **designs and operates a dedicated cloud environment** tailored for CMMC Level 2 (CUI data) compliance. We typically deploy your systems in **Microsoft Azure Government (GCC High)** – a FedRAMP High authorized platform (DoD Impact Level 5) with U.S.-only data residency and support personnel. This provides a compliant foundation to meet **DFARS 252.204-7012** cloud requirements (FedRAMP Moderate-equivalent) out of the gate. On top of this, 2W implements a full suite of **security controls aligned to NIST SP 800-171** families:

- **Identity & Access Management:** We configure **Microsoft Entra ID (Azure AD)** with **Conditional Access policies and Phishing resistant Multi-Factor Authentication (MFA)** (e.g., FIDO2 security keys) and Microsoft Defender for Identity to enforce strict access control for CUI systems. Only authorized, verified users can access your environment, and privileged/admin accounts are tightly governed (including support for Azure Privileged Identity Management if needed). We ensure all **enforcement of least privilege and account management** controls on the technical side. *You approve and create user accounts (who gets access) while 2W enforces how that access occurs.*
- **Endpoint & Network Security:** We deploy **Microsoft Intune** to manage and secure endpoints (user PCs, devices) with compliance policies so that only **trusted devices** can reach the CUI environment. We lock down network traffic with an "**allow-list**" approach — **using AVD Deployment**, **Azure Firewall,**

Network Security Groups (NSGs), and VPN gateways — to permit only authorized connections into the enclave. The default posture is **"deny-all, allow by exception."** This addresses many of the **Access Control (AC)** requirements in NIST 800-171 by segmenting and restricting network access to CUI systems.

- **Threat Monitoring & Incident Response Preparedness:** All systems in our managed environment have **Microsoft Defender for Endpoint and Defender for Cloud** enabled for continuous threat detection, vulnerability scanning, and security posture management. We set up **centralized logging** (with custom retention per your needs) so security events are captured and can be audited. Optionally, we can integrate logs with a **Microsoft Sentinel SIEM** in GCC High for advanced correlation and alerting. We maintain a **documented Incident Response Plan** aligned with DFARS 7012 (72-hour breach reporting) and NIST 800-171's incident handling controls. If a security incident occurs in the hosted environment, **2W acts immediately**: we notify your team per our SLA, assist with triage and forensics, preserve relevant logs and systems, and help you meet the **72-hour DoD reporting requirement** by providing the necessary technical details and evidence. (The client still submits the official report to DIBNet as required by DFARS 7012, but we ensure you have the information needed to do so.)
- **Data Protection & Backup:** We help implement **data encryption** (AES-256, FIPS140-2/140-3 validated, for data at rest; TLS 1.2+ for data in transit) in line with CMMC's System & Communications Protection (SC) requirements. We configure **sensitivity labeling and Data Loss Prevention (DLP)** policies via **Microsoft Purview** to mark and control CUI in your environment (satisfying requirements around marking and media protection). IRM / AIP (Information Rights Management and Azure Information Protection) Regular, **immutable backups** of critical systems are performed in Azure Government, with periodic restore tests to validate your disaster recovery readiness.
- **Technical Compliance Documentation:** For every **security control we implement**, 2W maintains **mappings and evidence**. We document how each NIST 800-171 requirement is addressed by the environment (e.g., in the **System Security Plan** sections we contribute) and **collect artifacts** such as configuration screenshots, baseline settings, log excerpts, and system inventories that demonstrate compliance. This significantly reduces the burden on your team to generate technical evidence during an audit, since we provide ready-to-go **evidence packages** for all controls under our management.

Shared Responsibility & Control Mapping: Because **CMMC Level 2 spans 110 controls**, not every requirement is managed by 2W. We map out exactly **who is responsible for each requirement** via a Shared Responsibility Matrix (**SRM**). The SRM lists all NIST 800-171 controls and indicates if it is fulfilled by **Microsoft (cloud**

platform and GCC-H Microsoft licensing), **2W Technologies (the MSP)**, **Epicor** (if applicable for an ERP application like Kinetic), or **you (the client)**. For example, **Microsoft** covers physical data center security and underlying infrastructure controls; **2W** covers system patching, logging, and access control configurations; **the client** covers policies, user training, and decisions on user access; and **Epicor** covers application-level support. The SRM is tailored to your environment and kept up-to-date and has even been **successfully used as evidence in formal C3PAO assessments**. This ensures **no control is unaccounted for** — every requirement has an owner, and we assist with whatever belongs to us or the platform. Table 1 below highlights a few key divisions of responsibility between 2W and the client (OSC):

Table 1 – Key Responsibility Areas: 2W Technologies vs. Client (OSC)

Compliance Area	2W Technologies (MSP/ESP) – Our Role	Client (OSC) – Your Role
Secure Cloud Environment & Infrastructure	Design and deploy the **Azure Government (GCC High)** environment; enforce secure configurations, network segmentation, and baseline technical controls (firewalls, MFA, encryption, backups) to meet CMMC requirements. Maintain cloud resources (VMs, storage, networks) and apply updates according to best practices.	Define overall system needs and scope (which systems and data are in the CMMC boundary). Approve any major architectural decisions. **Rely on 2W's secure architecture** as the compliant foundation for housing CUI data.
Identity, Access & Data Management	Implement and enforce **identity** policies (Azure AD Conditional Access, MFA) and **data protection** measures (encryption, access control lists, monitoring of data flows) in the environment. Ensure only authorized, verified users and compliant devices access CUI systems.	**Decide and manage "who has access"** – assign user roles, approve accounts, and maintain up-to-date user lists. Classify which data is CUI and ensure it stays within the secure environment (e.g., use labeling). Follow best practices for handling CUI in your business processes.
Security Operations (Monitoring & Maintenance)	**Run daily security operations** for the hosted environment: system maintenance, vulnerability scanning, **patch management**, anti-malware updates, log collection, and continuous security monitoring with Microsoft Defender tools. Investigate alerts and maintain	**Oversee and stay informed** of your environment's security posture via 2W's reports or dashboards. Work with 2W on risk-based decisions (e.g., scheduling of updates, acceptance of any residual risk). Provide 2W with timely information on changes (new

	incident response readiness (collect forensic data, preserve evidence). Perform regular backup and recovery tests.	users, new data types) so we can adjust security controls as needed.
Policies, Compliance & Governance	**Support** your compliance program by aligning technical measures to your policies and compliance needs (e.g., implementing controls as per policy, providing technical input for SSPs and POA&Ms). **Provide evidence and documentation** for technical controls (SSP sections, architecture diagrams, screenshots). *Optionally, 2W can offer* SSP or PO*A&M awareness training, policy templates or vCISO services via a separate engagement if you need help developing governance documents*.	**Own your organizational security policies, procedures, and training programs**. Develop and enforce policies on access control, incident response processes, personnel vetting, physical security, etc. Maintain required compliance documentation (SSP, policies, etc.) and manage your **Plan of Action & Milestones (POA&M)** for any compliance gaps. **Train your employees** on security awareness (with optional 2W training platform if needed). **Lead the overall compliance program** – you drive internal audits, risk acceptance, and readiness tracking.
Assessment & Certification	**Prep and support technical audit evidence**: ensure our controls meet audit standards, provide evidence packages for the controls we manage, and (if engaged) **participate in informal or formal assessments** to explain technical details to the C3PAO. Update the Shared Responsibility Matrix and any documentation as needed for audit prep.	**Engage the C3PAO** for your CMMC assessment and coordinate audit activities. **Present the full picture** to the assessor: provide policies, training records, and business context (with 2W's technical evidence integrated). **Own the CMMC certification** process end-to-end as the OSC – you interface with the assessor and ensure all requirements (technical and non-technical) are satisfied to their approval.

*In addition, core elements like **physical facility security**, **supplier/subcontractor compliance**, and **organizational risk acceptance decisions** are fully **client-side responsibilities** – 2W's scope is limited to the cloud and IT domain.*

Notice that many of the client responsibilities (policies, training, physical, supply chain governance) are **non-technical controls** that **no MSP can take over** – they require management decision-making and internal enforcement. Meanwhile, 2W shoulders the **technical heavy lifting** so that your in-house team can focus on these governance areas.

What We Do *Not* Provide (and why): By design, **2W does not cover certain domains** of compliance that fall outside an MSP's typical role. These include:

- **Physical security controls** (secure rooms, badge systems, cameras, on-site facility safeguards) – the client's facilities or security team must implement these.
- **Supplier & subcontractor compliance** (vetting vendors, managing flow-down DFARS clauses, authorizing external CUI sharing) – the client is responsible for managing its supply chain's compliance.
- **Organizational risk management & policy decisions** – the client's executives must perform risk assessments and formally accept any residual risks; we do not unilaterally make those business decisions.
- **CMMC program management & audit coordination** – you lead scheduling and orchestrating C3PAO assessments; we support with evidence, but we are not the ones managing the assessor's process or your POA&M tasks.
- Background checks, term procedures, and NDA.
- **Security training program administration** – ensuring your users complete regular **security awareness training** and keeping records is considered an **OSC responsibility** under CMMC. However, **2W can provide a turnkey training and phishing-simulation platform** as a separate service.

This clear **boundary is intentional**. It **gives you, as the client, full control and accountability** over policies, personnel, and compliance management, while **2W focuses on operating a secure technical environment**. Auditors appreciate this clarity – it delineates exactly who manages what, making the certification process more straightforward.

In summary, **2W provides and maintains the compliant IT infrastructure so that you can meet CMMC's technical requirements without building everything in-house**. Meanwhile, you retain responsibility for business-side controls and the overall compliance program, with a detailed matrix documenting the handoffs. The combined result covers **all 110 NIST 800-171 controls** with no gaps: some controls are fully managed by 2W or the cloud platform, and others remain with you (or are shared), but **every requirement is addressed by the proper party**.

How 2W Supports You Through the Compliance Journey

Achieving and maintaining CMMC Level 2 is an ongoing journey. 2W is an active partner to your organization at **each stage: from initial preparation, through assessment, and beyond**. Table 2 summarizes **the key phases of the compliance lifecycle** and how 2W engages in each:

Table 2 – Compliance Lifecycle Phases: 2W's Role at Each Stage

Phase	2W's Role & Key Activities
Plan & Build (Pre-Compliance)	**Scoping & Enclave Design:** We collaborate with you to define the **CUI boundary** – identifying which systems and data will fall in scope – and plan an appropriate architecture (often a **cloud enclave in GCC High**) to contain those systems. **Gap Assessment & Remediation:** We assist with or support a **NIST 800-171 gap assessment** (often via a third-party consultant or our own services) to pinpoint missing controls. And help develop the SPRS Score Calculation. Then, we **implement technical remediations** in our domain (e.g., enabling needed logging, encryption, MFA, etc.) to close gaps. We also provide guidance for controls outside our scope, helping prioritize what you need to address on your end.
Operate & Monitor (Ongoing)	**Day-to-Day Security Operations:** 2W runs the CUI environment with a focus on **continuous compliance**: we apply patches promptly, monitor system health and alerts (via Microsoft Defender and Sentinel), and maintain secure configurations. We issue **periodic reports** or reviews on your enclave's security posture (e.g., summary of updates applied, any notable alerts or changes). If threat alerts or incidents occur, we manage first-level response actions as described earlier (notify, contain, preserve evidence). In short, we keep the lights on securely, so your environment always remains audit-ready.
Assessment Preparation & Documentation	**Evidence & Documentation:** In the lead-up to an audit (or during routine self-assessments), 2W **supports mock audits**, supplies the **technical artifacts** needed: **SSP contributions** detailing how our environment meets each control, updated **Shared Responsibility Matrix**, **network diagrams** showing your CUI boundary, **configuration screenshots,** and **log samples** for proof of control implementation. We assist with **POA&M inputs** by identifying any residual gaps on the technical side and suggesting remediation steps. We can also coordinate with your internal team or consultants to ensure all documentation aligns – i.e., that what is written in policies and SSP matches what is in the system.
Formal Assessment (C3PAO Audit)	**On-site/Virtual Assessment Support:** If you request it, 2W **participates in mock audits and the formal C3PAO assessment** for our scope components. This involvement is typically arranged via a separate agreement and includes our experts **explaining technical controls** to the assessor, demonstrating configurations, and clarifying how responsibilities are split (without overstepping into policy areas). We provide quick responses to auditor questions about our managed systems and, if any issues are found, we work swiftly to address them or provide additional evidence.

	Our goal is to ensure the parts of the assessment covering the IT environment **go smoothly and have zero findings**.
Sustainment & Re-Certification	**Ongoing Compliance Maintenance:** After initial certification, we continue to maintain and improve the environment to keep pace with evolving threats and standards. We will assist with **annual self-attestations** (e.g., updating your SPRS score based on any changes) by ensuring documentation and controls remain current. If there are significant changes (new CUI systems, etc.), we update the SRM and configuration accordingly. When it is time for **re-certification (every 3 years)**, we are there to refresh evidence and support the next assessment cycle. *(For clients needing extra help with broader compliance tasks, 2W also offers a **Comprehensive Compliance Assistance Program** – including policy maintenance and vCISO advisory – as an add-on, but many clients manage those aspects internally.)*

Throughout all these stages, **2W works in close partnership with your team and any third-party compliance advisors** you engage. We tailor our involvement to your needs – some clients lean heavily on us for technical evidence and leave policy work to a consultant, while others involve us end-to-end including strategy. In every case, **you remain at the helm of your compliance program**, and **2W serves as the technical backbone and subject-matter expert** to streamline your path to CMMC success.

No Guarantees, but a Reliable Path: It is important to note that **only an accredited C3PAO and the DoD can grant CMMC certification**, and they make that decision based on an independent assessment of your entire scope. *No service provider can "guarantee" you will be certified.* What 2W guarantees is that **our solutions will meet the technical requirements and provide solid evidence**, positioning you for success. In other words, **we cannot do the audit for you, but we ensure our part holds up under audit**. By combining our secure infrastructure and expertise with your organization's commitment to policy and process, you are equipped to navigate CMMC 2.0 Level 2 with confidence and credibility.