

“Compliance at Scale: Building a Repeatable, Defensible CMMC Offering”



Presented by:
Leia Shilobod, Founder
CompliancyIT

Nathan Scott, CEO
Queen Consulting & Technologies



Our Story



- We believe in doing **meaningful work** with people dedicated to the mission
- **Compliance must be productized to scale** – always striving to improve our processes, while elevating our people
- *CMMC is hard enough. Doing it one-off for every client kills margins, increases risk, and burns out your team.*
- Principle Alignment = Opportunity for a Bigger Impact = a Joint Venture

Introducing our Joint Venture banner for
compliance consulting & events:



MISSION
COMPLIANT

Your Trusted Partners In Compliance

The Market Problem

- CMMC Products, MSPs, MSSPs, and consultants are out there promising the moon.
- “Get compliant in 2 weeks,” “all the documentation you need,” “we cover all 110 controls for you.”
- You CARE about the DIB want them to be successful
- BUT you refuse to make borderline unethical statements or promises you can't keep

Traditional Approaches Just Don't Work

- Custom documentation per client → unscalable.
- Scope creep and unclear contracts → liability.
- Overpromising “CMMC readiness” without governance.
- No cadence for ongoing compliance → clients regress.

What You Really Need

- A program, not a project.
- An actual culture, not a binder.
- A defined process for continuous compliance.
- A clear contract with a clear scope of work and outcomes, ensure clear roles and responsibilities
- A clear Roadmap for where to start to get to the end goal
- Certification.

**You Need To
Go From This...**



To This...



Our CMMC Compliance Process

The roadmap to get and keep you compliant



Identify Key Data, Business Processes, and Technology

CMMC is about protecting the data. You may take action in the wrong direction unless the data you need to protect is identified and how it flows in, is handled, and flows out are mapped.



Full Gap Analysis, Self-Assessment, SPRS Update

Our CMMC Subject Matter Experts will validate your Self-Assessment to assure nothing is missed and a complete POA&M.



Create Projects to Close POA&Ms

We create discrete projects from the POA&Ms, linking each item to one or more projects so you can clearly see what work must be accomplished to achieve compliance



Begin Risk Management Meetings

Risk Management Meetings are the key to accountability for compliance. Even before the POA&Ms are closed, Risk Management process provides evidence of compliance work and process maturity.



Begin Remediation Projects to Close POA&Ms

Kickstart the identified remediation projects to align with the NIST 800-171 controls. Meet biweekly to check on status and remove roadblocks.



Onboard and Integrate CMMC IT Documentation, Policies, and Procedures

Our CMMC IT Documentation Toolkit contains functional and easy to understand Policies, Plans, Procedures, and Lists required for CMMC Compliance.



Continue Risk Management Process to Maintain Compliance

Compliance is a journey, not a destination. As the organization grows, business processes change, and technology changes, items will be uncovered that must be added to the POA&Ms and gaps closed. The RM process assures continued compliance.

Compliance as a Service

- **Phase 1 – Gap Assessment:** Contract Review, Identify FCI/CUI flows & CUI type, clarifying scoping, evaluate documentation, produce POAM & roadmap.
- **Phase 2 – Documentation Onboard & Technical Alignment:** Documentation and technical remediation in parallel. Standardize policies, plans, and SOPs using the Toolkit (Policies = Principles, Plans = Strategy, Procedures = How-To). Parallel project work brings the environment into compliance.
- **Phase 3 – Program Pulse:** Bi-weekly meetings, governance cadence, shared responsibility matrices, and continuous improvement.
- **Phase 4 – Certification Prep & Assessment** – proven process to prepare artifacts, prep interviewees, and advocate for OSC implementation during assessment
- **Phase 5 – Continued Engagement** – Continuously work together based on Client needs to stay compliant over time, address compliance and security concerns, help the company to pivot and address new opportunities

The Key Is Establishing A Pulse

- Establish an ACTUAL Governance, Risk & Compliance (GRC) Program
- Risk Assessments & Security Assessments are tied in with Compliance checks with assigned responsibilities/accountabilities, and reported on during Risk Management Meetings (quarterly cadence)
- Deep dive into a sub-set of controls quarterly is your queue to review and update the SSP for those controls
- Write notes on the Agendas – your evidence of compliance management
- Create tickets/action items from the meeting for environment realignment, policy/process enforcement, and POAM closure tracking
- Certification Preparation and Support – a process to kick off two months prior to the actual certification
- It's not just "CMMC documentation." It's a living system of accountability



Client Risk Acceptance Form

Purpose: Provide clear communication about recommendations and risk acceptance to the [COMPANY] ownership and management. The strategies to address risk include: Risk Avoidance, Risk Mitigation, Risk Transfer, and Risk Acceptance.



Description of Risk:	<p><u>Violation of Microsoft Licensing Agreement.</u></p> <ul style="list-style-type: none">The machines "MONSTERV2A" & "MONSTERV3" utilize <u>RDPWrapper</u> to enable multiple concurrent Remote Desktop Protocol (RDP) sessions on Windows systems that typically only allow one.Per <u>c. Restrictions. (V)</u> this scenario violates Microsoft's Windows 10 EULA.Violating Microsoft Licensing Terms puts EME Associates at an increased risk for Fines and Penalties, Legal Action, regular Microsoft Audits, Reputation Damage, and legal <u>requirement</u> to align or disable the MONSTER environment. <p><u>Increased security risk.</u></p> <ul style="list-style-type: none"><u>RDPWrapper</u> does not receive regular security updates, leaving systems susceptible to known vulnerabilities that could be exploited by attackers.RDP services are common targets for malware and exploits, and using <u>RDPWrapper</u> may increase exposure to these threats.Since <u>RDPWrapper</u> is not an official Microsoft product, we do not have access to official support or patches, making it harder to address issues.
Impact of Risk:	<p><u>HIGH</u></p> <ul style="list-style-type: none">A licensing violation could result in <u>litigations</u>, fines, and increased costs.Security exploitation - The MONSTER environment is critical to business operations. Being without this environment due to a <u>vulnerability</u> exploitation could halt operations. The possibility for data

Phase

Select Primary ar

Gap Assessment

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Gap Assessment Ph

Select Primary ar

Program Onboard

Program Onboard P

Program Onboard P

Program Onboard P

Program Onboard P

Program Onboard P

Program Onboard P

Program Onboard Phase

Program Onboard Phase

Program Onboard Phase

Select Primary and Secondary Consultant for this Phase

Client Overview and Special Notes Template

Wednesday, April 02, 2025 12:04 PM

Client Code:

Agreement:

Products/Services in Scope:

Players:

- GRC Team and Roles:
 - Program Owner(s)
 -
 - MSP
 -
 - Other Important Contacts
 -

Primary & Secondary CIT Compliance Consultants

- Primary -
- Secondary -

Collaboration Platform:

- Platform and link

Compliance Requirement & Business Profile Notes

- Business type
- FCI and/or CUI
- CUI type
- Key players for FCI and CUI in the business process
- ESP's and contact info
- CSP's and contact info

Coordinates IT remediation pla

Updates SSP & POAM as remed

Why This Method Wins

Typical Consultant Challenges	CMMC IT Documentation Toolkit Model
One-off documents written from scratch	Pre-validated documentation system + templates
OR forcing companies into cookie-cutter documentation	Flexible core documents that are easy to customize to an OSC's culture, processes, and operations
Random meetings to work with the Client	Gap to regular bi-weekly program onboard meeting pulse
No project governance or cadence for compliance activities	Program governance through Risk Management meetings
No clear role structure for consultants	Defined Primary/Secondary consultant model
Subjective scope boundaries	Customer Responsibility Matrix clarifies what's in/out
Reactive compliance	Continuous "Program Pulse" accountability loop

We Want To Help YOU!

Because you attended CMMC LiftOff, you're already receiving our **CMMC Level 2 Prep Guide** – straight from the Toolkit.

We'd also like to help you out by providing you with the Compliance Clients Tracking spreadsheet – vital for us to keep track of each clients' most important info and status.

Just email **"SEND ME MY SPREADSHEET!"**
to
Compliance@compliancyit.io