MAY 28 WEBINAR POST-EVENT

CMMC PHASE 2 READINESS CHECKLIST

LESSONS FROM EXPERTS JAMES GOEPEL & ALI PABRAI

EXECUTIVE ACTIONS (DO THESE IMMEDIATELY)

- ☐ Assign a CMMC Program Owner
- ☐ Reserve a C3PAO assessment slot now
- ☐ Establish a realistic compliance budget
- ☐ Build a 6–12 month compliance timeline
- ☐ Identify all DoD contracts and subcontract relationships
- ☐ Review communications from prime contractors

CUI DISCOVERY & SCOPING

- ☐ Identify all sources of CUI
- ☐ Document how CUI enters your organization
- ☐ Map how CUI moves internally
- ☐ Identify every system storing, processing, or transmitting CUI
- ☐ Define assessment boundaries
- ☐ Define certification boundaries
- ☐ Identify Security Protection Assets (SPAs)
- ☐ Document cloud services touching CUI
- ☐ Identify Federal Contract Information (FCI)
- ☐ Reduce unnecessary CUI exposure whenever possible

DOCUMENTATION READINESS

- ☐ Create a complete System Security Plan (SSP)
- ☐ Ensure SSP aligns with CMMC Assessment Objectives
- ☐ Develop accurate network diagrams
- ☐ Develop data flow diagrams
- ☐ Document asset inventories
- ☐ Document authorization processes
- ☐ Ensure all policies match operational reality
- ☐ Link SSP references to supporting evidence

ASSESSMENT PREPARATION

- ☐ Review all 320 Assessment Objectives
- ☐ Verify evidence exists for each objective
- ☐ Conduct internal readiness reviews
- ☐ Validate user authorization processes
- ☐ Validate account management procedures
- ☐ Validate boundary protection controls
- ☐ Validate continuous monitoring controls
- ☐ Verify evidence collection processes
- ☐ Conduct mock interviews
- ☐ Prepare technical staff for assessor interviews

CELERIUM.com

CLOUD & THIRD-PARTY SERVICES

- ☐ Identify all cloud providers
- ☐ Determine whether CUI exists in each service
- ☐ Verify FedRAMP inheritance opportunities
- ☐ Review antivirus and security tooling
- ☐ Confirm whether security tools process CUI
- ☐ Document all inherited controls

ONGOING COMPLIANCE

- ☐ Establish annual affirmation process
- ☐ Create continuous monitoring procedures
- ☐ Implement evidence retention procedures
- ☐ Schedule quarterly compliance reviews
- ☐ Review scope changes immediately
- ☐ Track new cloud deployments
- ☐ Review AI-enabled tools for CUI exposure
- ☐ Maintain assessment-ready documentation year-round

RED FLAGS

- 🚩 SSP written only to NIST 800-171 controls
- 🚩 No data flow diagram
- 🚩 Unknown CUI locations
- 🚩 No evidence tied to controls
- 🚩 Assessment scheduled before readiness review
- 🚩 Vendor promises “guaranteed certification”
- 🚩 Vendor claims they can do everything for you
- 🚩 Organization relies entirely on consultants
- 🚩 Leadership assumes certification is a one-time project