CMMC

SECURITY ASSESSMENT

Measure What Matters

The Security Assessment family helps you measure, document, and continuously strengthen your cybersecurity program. It focuses on verifying that your protections work, tracking and fixing gaps, and maintaining an up-to-date System Security Plan (SSP) that shows the DoD you're mission-ready.

Proof of Practice

Examples

- **System Security Plan (SSP)**
  Documents your system environment, components, boundaries, and how each CMMC control is implemented.
- **Plan of Action & Milestones (POA&M)**
  Lists identified gaps with assigned owners, target dates, and remediation steps to track progress over time.
- **Continuous Monitoring Records**
  Logs or screenshots proving regular review of alerts, patches, and configurations to detect and resolve issues early.

The Business Impact

Assessments turn effort into evidence. Consistent reviews protect contracts, reputation, and your place in the defense supply chain. Without them, gaps go unseen, documentation goes stale, and opportunities, and trust, can disappear when it matters most.

Available Resources

- **NIST SP 800-171: Excel, POA&M, & SSP Templates**
  https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
- **CISA: Cyber Security Evaluation Tool (CSET)**
  https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset
- **Project Spectrum Resources**
  https://www.projectspectrum.io/#/cyber-readiness-check
- **CYYNC: Your Mission. Your Team. Perfectly Synced.**
  https://www.cyync.com
- **Vanta: Trust Management Platform**
  https://www.vanta.com/products/cmmc

Quick Wins

1. Define system boundary and CUI scope.
2. Build a diagram of the system.
3. Perform a self-assessment of all controls & objectives.
4. Develop a Plan of Action & Milestones (POA&M).
5. Run short internal security sprints tackling one control family at a time.

CyberNEX Technology

www.CyberNEX.io