ILLUMINATE THE CURRENT STATE WITH A GAP ASSESSMENT

A **Gap Assessment** is the essential first step toward achieving **CMMC Level 2** compliance. It objectively benchmarks your current cybersecurity posture against the 110 controls in **NIST SP 800-171**, identifies gaps, prioritizes risks, and delivers a clear, customized remediation roadmap. Starting with a thorough Gap Assessment saves time, reduces costs, and avoids surprises during formal assessments or certification, positioning your organization for efficient progress toward handling Controlled Unclassified Information (CUI) securely.

To make your Gap Assessment as efficient and effective as possible, prepare the following items:

☑ **Organizational scope and boundaries** — First, evaluate which contracts you have that include DFARS 252.204-7012. Second, ascertain which employees or contractors have a business need to support the contract that may have CUI. Do not forget to include your contracts department team members. Third, identify the computing assets associated with these individuals (Laptops, desktops, smartphones, printers, online storage locations, etc.). This will constitute the scope of what will be assessed.

☑ **Current System Security Plan (SSP)** — If you have one (even if draft or outdated), provide it; otherwise, note any existing high-level security documentation.

☑ **Policies and procedures** — Gather written documents covering access control, incident response, risk management, personnel security, physical security, system maintenance, audit logging, configuration management, identification/authentication, media protection, security awareness training, and more.

☑ **Asset inventory** — List of hardware, software, cloud services, and networked devices (including endpoints, servers, IoT/OT if relevant) that could store, process, or transmit CUI.

☑ **Network diagrams and data flow maps** — Visuals or descriptions showing how CUI moves through your environment (e.g., on-premises, cloud, third-party tools).

- ☑ **Access control lists and user accounts** — Details on user roles, privileges, MFA usage, remote access methods, and joiner/mover/leaver processes.
- ☑ **Technical configurations and evidence** — Screenshots, reports, or exports showing encryption (at rest/in transit), firewall rules, endpoint protection, backup/restore capabilities, vulnerability scanning results, patch management logs, and multi-factor authentication settings.
- ☑ **Incident response and continuity plans** — Any existing IR plan, business continuity/disaster recovery documentation, and recent test results or logs.
- ☑ **Training and awareness records** — Logs or rosters of security awareness training, phishing simulations, CUI training, insider threat training, or role-based training completion dates.
- ☑ **Third-party/vendor documentation** — Contracts, agreements, or assessments related to service providers, cloud vendors, or managed services that touch CUI (to evaluate supply-chain risks).
- ☑ **Recent risk assessments or self-assessments** — Any prior NIST 800-171 self-scores, gap analyses, or audit findings.
- ☑ **Key personnel contacts** — Names and roles of IT/security leads, compliance officers, and subject-matter experts who can answer questions during the analysis.

Here are a few useful tips that will save you time and lead to the most effective and efficient assessment we can provide:

01

Organize materials in a shared, secure folder (e.g., by NIST 800-171 family/domains) to speed up review.

02

Be transparent about what's missing or immature; honesty leads to the most accurate roadmap and realistic remediation plan.

03

Involve cross-functional stakeholders (IT, security, legal, leadership) early so decisions align with business realities.

04

Don't delay gathering items; even partial documentation helps start the process productively.

Ready to take the first step toward CMMC Level 2 compliance?

Contact Koniag Cyber to schedule your customized Gap Assessment. We'll benchmark your posture against NIST SP 800-171, then deliver a prioritized remediation roadmap tailored to your organization.

Let's efficiently and confidently secure your DoW opportunities. Let's talk → info@koniagcyber.com