BL King Consulting

CMMC

Simplify Your CMMC Compliance With Our Services

COMPLIANCE BASED ON TECHNICAL SERVICES, POLICY DEVELOPMENT, PROCEDURAL DOCUMENTATION, AND PERIODIC PROGRAM AUDITS

BL King Consulting's pay-per-endpoint model provides technical services that provide the heavy-lift technical controls at a fraction of the cost of DIY solutions. As your trusted partner, we manage mandated policies and procedures so you can focus on winning defense department contracts.

Key CMMC Notes:

DFARS 252.204-7012

- Already requires self-attestation of compliance with NIST SP 800-171 (security control/protocol catalog)
- Finalized in 2016 and applied to contracts

DFARS 252.204- 7019

- Requires self-assesment results to be uploaded to DoD Supplier Performance Risk System (SPRS)

DFARS 252.204-7020

- Defines 3 levels of assessment for DFARS 7012
- Basic Assessment - self conducted
- Medium assessment - Gov't review of contractor's self assessment
- High Assessment - Full Gov't audit using NIST 800-171a (test procedures)

DFARS 252.204-7021

- Actual CMMC Requirement
- Requires CMMC certification every 3 years
- Requires all subcontractors to have appropriate level of CMMC certification

Federal Approval Timeline

- As of 11/24/23 In final processes for formal rule making
- OMB (OIRA) concluded review of CMMC
- Next step is publication

Contract Timelines

- Late 2024 first RFP requirements
- Original plan included a 5-year phase-in period with select OUSD(A&S) approved pilot contracts
- Subject to change in CMMC 2.0 rollout

KEY BENEFITS

- Erase the Confusion of Complex Protocols
- Real-World Tested Policies and Procedures
- Technology Hand-Picked for CMMC Compliance
- No Painful Learning Curve
- One-Stop-Shop or Co-Managed IT/ Security Services

NVBDC CERTIFIED
SERVICE DISABLED
VETERAN OWNED BUSINESS

E-Mail: Info@BLKing.net | Phone: +1(978) 688-1739 | Web: www.BLKing.net

CMMC for SMBs

BL King Consulting

COMPLIANCE MEANS WINNING MORE BUSINESS WITH THE DEPARTMENT OF DEFENSE

With years of experience in Gov't contracting, we fully understand your bid & proposal, contract performance, and the Gov't side of acquisitions. We help your small business navigate the complex process of information security and the nuances of Gov't contracting. Our services are tailor-made for CMMC compliance to ensure a smooth and swift implementation

Security Operations Center
- 24x7 AI monitoring
- Staffed 8x5 for SMB budgets
- Fused with open source threat intelligence
- Most important for reducing time to notice an attack

Training And Breach Testing/Monitoring
- Training tailored to each individual's level of knowledge
- Extensive catalog
- 3-5 Minutes each prevents training burnout
- Extensive catalog of phishing pages
- Phishing based on real world examples
- Educate employees to prevent phishing and ransomware
- Monitor the dark web for your employees company email addresses

Unlimited Incident Response
- We respond and continue through all phases of the incident to include a thorough after action analysis
- After action analysis required for reporting or understanding the full effects of an attack could take weeks
- No surprise charges for incident response
- We respond within minutes of initial notification
- We're committed to you through the duration of the incident

Vulnerability And Patch Management
- The #1 best defense is patch management
- All attacks start by exploiting a weakness that usually has a patch available
- Not all patches are applied by patch management systems
- 3rd party patches are not always updated by their auto-update system
- Vulnerability scanning finds missing patches and alerts staff to weaknesses

Cloud Collaboration And Server Monitoring
- Just because it's in the cloud doesn't mean its secure
- Our technology monitors Google, Microsoft, and Amazon for misconfiguration and attacks using the same technology we deploy on your computers
- Adds network monitoring (intrusion detection) to your cloud infrastructure

Continuous Monitoring
- Software and hardware baseline auditing ensures that only approved software is installed, reducing your attack surface
- Governance and policy auditing ensures your policies reflect what is actually happening and corrects deficiencies in processes
- System configurations and security services monitored for continued compliance

ABOUT CMMC
- DoD Security Requirements Policy For Contractors That Process DoD Information
- Compliments DFARS 252.204-7012
- 3rd Party Audit
- In Contracts About Q3FY24
- 2 Levels
  - Level 1
    - Federal Contract Information (FCI)
  - Level 2
    - Controlled Unclassified Information (CUI)
- Uses NIST SP 800-171 And SP 800-171a
- NIST SP 800-171 Revision 3 Is Draft And Has Significant Changes
- Great Governance For SMBs With No Other Governance Requirements