CMMC 2.0 and CPCSC cyber compliance support

In a defence market where Canada is committing over 80 billion dollars to modernize its forces and supply chain, programs like CMMC 2.0 and CPCSC are becoming increasingly important. How prepared is your organization to meet the challenge of protecting sensitive data and competing in this space?

Canada is planning billions of dollars in new defence investment, including NORAD modernization.

Cybersecurity certification will become mandatory for Canadian defence contracts, making a certified cyber posture a prerequisite.

What's on your mind?

Based on our client conversations, the most common questions related to CMMC 2.0/CPCSC include:

- **Where do we stand today** against CMMC 2.0 and CPCSC?
- **How do we scope our environment** so we're only certifying what really needs to be in-scope (CUI, CI, CDI, export-controlled data) and not our entire enterprise?
- **What's the most practical path** to get from current state to being audit-ready, without derailing day-to-day operations?
- **How do we prioritize remediation** when we have limited time and resources and still show a credible path to compliance?
- **Who should own CMMC/CPCSC** internally and how do we align IT, security, procurement and operations so accountabilities are clear?
- **How will we maintain compliance over time** including ongoing monitoring, change control and supplier risk, so we are not left managing issues reactively?

Actions your organization can take

Organizations can take several practical steps to improve risk management and enable certification at the same time:

- **Clarify what needs to be protected:** Identify where you handle CUI/CI/CDI, and other controlled data in your projects, systems and supply chains.
- **Right size your efforts:** Determine which tier applies to your contracts and then define a phased roadmap to achieve that.
- **Baseline your current posture:** Perform a gap assessment against NIST 800-171 controls, including, policies and technical safeguards, and all related documentation.
- **Establish governance, roles & ownership:** determine who should be involved at each phase, assign accountabilities, establish reporting and track progress.
- **Prioritize high-impact fixes:** Focus on areas such as access control, identity management, logging and monitoring and incident response to reduce risk and build towards certification.
- **Embed continuous readiness:** Establish ongoing monitoring, regular self-assessments, and strong governance so CMMC/CPCSC becomes part of how you operate, not an add-on.

© 2026 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Our CMMC 2.0/CPCSC Approach

	Activities	Outcomes
Gap assessment Current state snapshot to support the compliance journey and accelerate progress towards certification.	▪ Scope and boundary ▪ Data flow identification ▪ Asset classification ▪ Evidence reviews & interviews ▪ Control analysis/assessment	✓ Gap assessment report ✓ Supplier Performance Risk System (SPRS) score ✓ Remediation plan (if needed)
Remediation Targeted remediation and implementation support to close priority gaps, strengthen controls and embed repeatable processes.	▪ Roadmap and sprint planning ▪ Policy and procedure development ▪ Technical implementation guidance ▪ Remediation execution tracking	✓ System Security Plan (SSP) ✓ SPRS score ✓ Plan of Actions and Milestones (POA&M) (if needed) ✓ CMMC-compliant policies, procedures
Pre-Audit and readiness Independent pre assessment to validate control effectiveness, identify residual issues and rehearse for certification.	▪ Pre-audit controls testing ▪ Sampling and evidence walkthroughs ▪ Mock interviews and artefact reviews ▪ Issue logging and remediation guidance ▪ Readiness scoring	✓ Pre-Audit Readiness Report ✓ Assessor-style findings log ✓ Enhanced evidence set ✓ Clear “go/no-go” recommendation for certification
Continuous support Ongoing support to sustain compliance, monitor control performance and prepare for re assessment and evolving requirements.	▪ Annual SSP refresh ▪ Continuous controls monitoring ▪ Support services: vCISO, risk assessment, penetration testing, tabletop exercises	Example: ✓ SSP review ✓ Cyber reports and analysis ✓ Documentation review/updates ✓ Employee training materials

What makes KPMG different?

Aligned to your context and mandate

We tailor our approach to your business needs to streamline activities and produce efficient outcomes, while employing a personalized approach.

A local team

Our services are carried out by bilingual specialists who reside locally. In addition, as part of the KPMG global network, we have access to leading professionals globally.

Proven experience

Our team includes CMMC certified professionals, including Registered Practitioners Advanced (RPAs) and Registered Practitioners (RPs). This deep, specialized knowledge combined with your context translates into tailored solutions.

Cutting edge approach

We bring leading processes and tooling, including an ecosystem of AI enabled accelerators to drive efficiencies and enable better insights.

Contact us

Adil Palsetia
Partner,
Cyber Security
+1 647 501 8153
apalsetia@kpmg.ca

Peter Graham
Partner, National Industry Leader,
Aerospace and Defence
+1 416 777 8229
peterjgraham@kpmg.ca

© 2026 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.