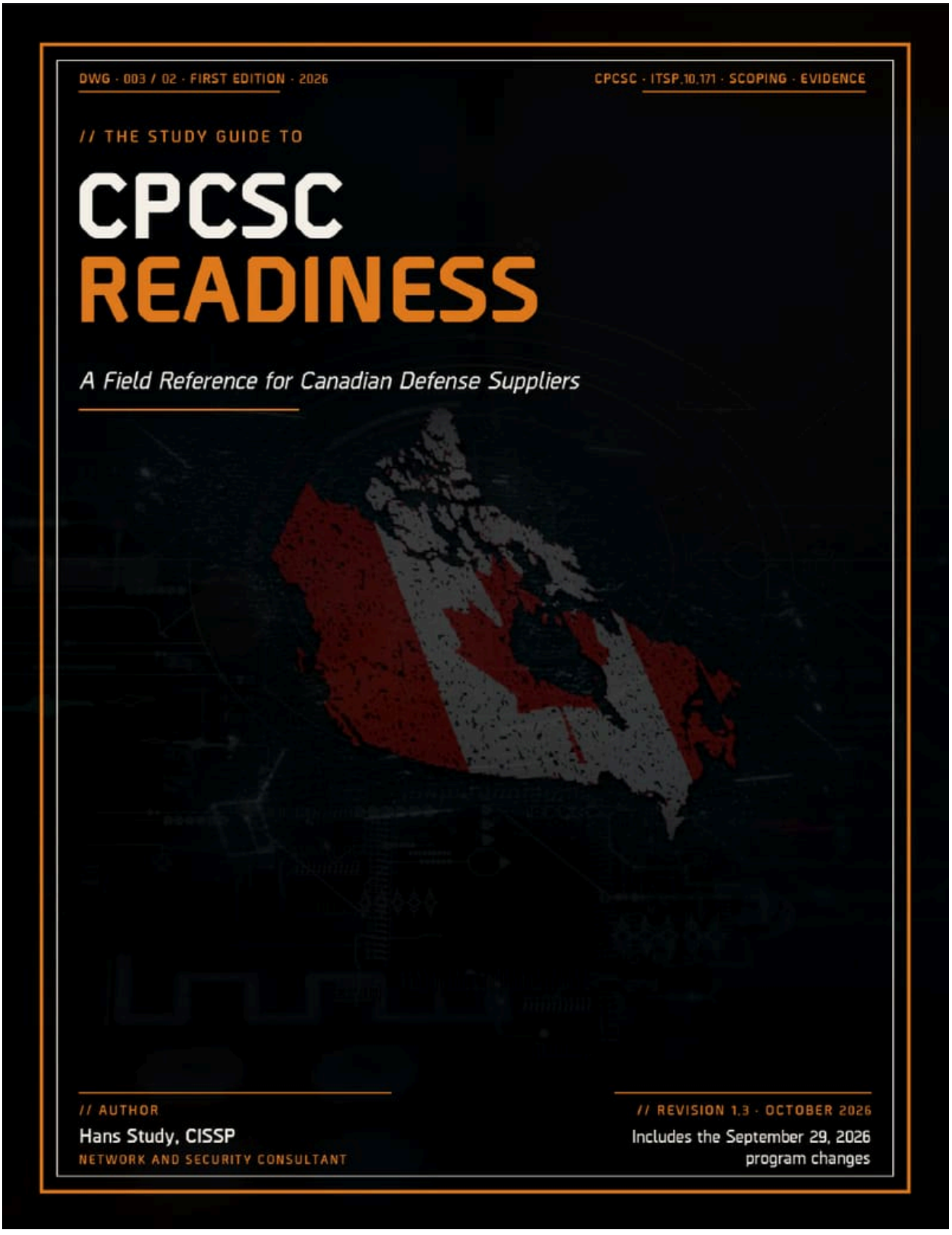
Key Points to Verify When an MSP Offers CPCSC Support

Canadian defence suppliers working toward the Canadian Program for Cyber Security Certification (CPCSC) often turn to a managed service provider (MSP) for help. The right MSP can simplify scoping, assessment, and certification, but not every provider understands the program's specific requirements. Asking the right questions early helps avoid mismatched expectations, wasted budget, and gaps in your compliance posture.

Below are the areas worth probing before you commit. Each question targets a common weak point in MSP offerings and gives you a practical reason to ask it. Use this list as a conversation starter, not a script, and adapt it to your organisation's size and existing security maturity.

Does the MSP Already Work With Defence Supply Chains?

CPCSC draws heavily from the NIST SP 800-171 framework, but it has its own scoping rules and attestation timelines. An MSP that claims general cybersecurity expertise may still be unfamiliar with the program's particularities. Ask whether they have guided other Canadian suppliers through the formal CPCSC process, not just through a generic security assessment. A provider with direct experience will know where the audits tend to focus - for example, how they handle remote access, data flow diagrams, and the boundary between managed and unmanaged devices. Without that experience, you risk paying for a consultant who learns on your time.



How Do They Define Their Role in the Responsibility Matrix?

CPCSC certification requires a clear responsibility matrix that shows who owns each control. When an MSP manages parts of your network, some controls fall under their scope. The question is whether they can document that split clearly and provide evidence for the controls they operate. Ask for a sample responsibility matrix from a past engagement. If the answer is vague or they cannot show one, you may end up with a gap that your own team cannot fill because the MSP controls the relevant logs or configurations. A good MSP will understand that the matrix is not just paperwork but the foundation of a successful assessment.

What Security Policies Do They Follow Themselves?

An MSP that helps you meet CPCSC requirements should also operate under a strong security policy internally. Ask for their own certifications or audit reports, such as SOC 2 Type II or ISO 27001, and check whether those reports cover the services they will provide to you. If their own house is not in order, you cannot rely on their systems to produce compliant evidence. Also ask how they handle staff training. The people managing your environment need to understand not just technical controls but also the documentation and evidence demands of the program. A provider that invests in ongoing security training for its team is more likely to keep your certification on track.

How Do They Support a Manageable CPCSC Preparation Plan?

Building a manageable CPCSC preparation plan requires more than a checklist. It calls for a realistic timeline, a budget that accounts for remediation, and a clear escalation path when something goes wrong. Ask the MSP how they break the work into phases. Do they start with a gap analysis, then move to remediation, then support the assessment itself? Or do they offer only the assessment support, leaving you to guess what to fix first? A provider that can show a phased approach - scoping, remediation, pre-assessment, and attestation support - is more likely to help you stay on schedule and within budget.

What Happens When Remediation Is Needed?

Few organisations pass their first CPCSC assessment without some remediation. The MSP's willingness to help with fixes matters. Ask whether they treat remediation as part of the original engagement or as a separate project with its own costs. Also ask how they prioritise findings. Some providers apply a standard severity rating that may not match the program's actual risk appetite for your sector. A good MSP will work with you to create a remediation plan that addresses the most critical controls first and that keeps you moving toward certification without unnecessary delays.

View this on hans.study

How Do They Handle Budget and Scope Creep?

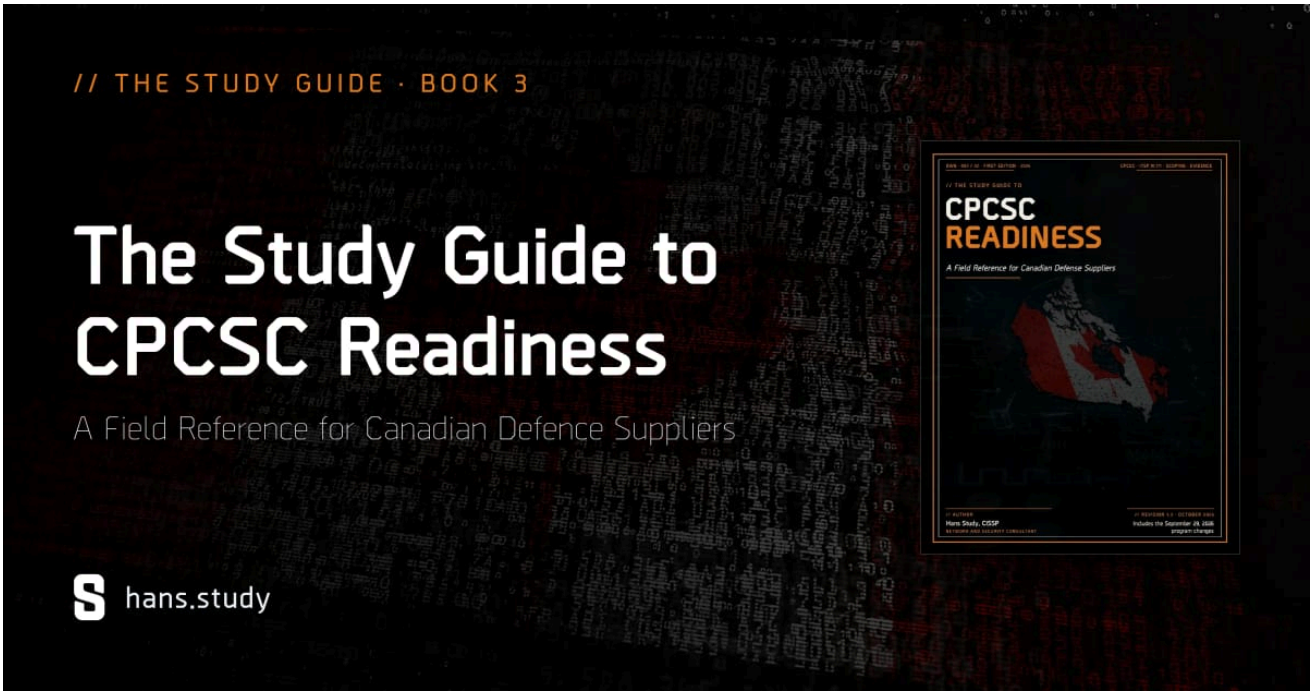
Managed services contracts often bundle a fixed set of activities, and CPCSC support can push beyond those boundaries. Ask the MSP how they handle scope changes. Do they have a formal change order process? What is their hourly rate for work outside the original agreement? A clear policy on scope creep protects both sides. Without it, you may find that the support you thought was included - such as helping draft a system security plan or reviewing your incident response procedure - triggers additional charges. A provider that is upfront about these limits is easier to plan with.

Can They Provide References From Similar-Sized Organisations?

Small businesses face different challenges than large primes when pursuing CPCSC certification. An MSP that has only worked with large defence contractors may not understand the resource constraints of a smaller supplier. Ask for references from organisations of roughly your size and complexity. Listen for stories about how the MSP handled tight timelines, limited IT staff, and budget pressure. A provider that has successfully guided a small business through the process will have practical advice on how to build **a manageable CPCSC preparation plan** without overstretching your team.

What Is Their Exit Strategy?

Finally, ask how you would move your data and compliance evidence if you decide to switch providers. CPCSC certification depends on continuous monitoring and evidence collection. If the MSP holds your logs, configuration baselines, or incident reports, you need a clear way to retrieve them. A good contract defines data portability and transition assistance upfront. The MSP should be willing to document how they will transfer your information in a usable format. This question also reveals how the provider thinks about the long-term relationship. A confident MSP will have a standard process for offboarding, not a vague promise.



Asking these questions does not guarantee a perfect partnership, but it does surface the most common mismatches early. The goal is to find an MSP that treats CPCSC support as a defined service, not an add-on, and that can explain exactly where their responsibility ends and yours begins. With the right provider, certification becomes a structured process rather than a guessing game.