CPCSC readiness: what small defence suppliers need to know before an assessment

What the CPCSC assessment actually checks

The Canadian Program for Cyber Security Certification (CPCSC) is the framework the government uses to qualify suppliers who handle controlled unclassified information. For a small defence contractor, the assessment can feel like a high-stakes audit of everything from password policies to physical locks on server cabinets. Understanding what the assessors look for before they arrive is the first step toward a smooth experience.

The process is built on the NIST SP 800-171 standard, which sets out 110 requirements across 14 families of security controls. An assessor will verify that your organisation has implemented each of these controls to a specified maturity level. For most small suppliers, the target is level 1 or level 2, which demands documented policies, consistent practices, and evidence that controls work as intended. The assessment is not a pass-fail test in the academic sense. It produces a score and a list of deficiencies. The government then uses that outcome to decide whether you can bid on certain contracts or access certain data.

How the assessment day unfolds

An assessment typically runs one to three days, depending on the size of your environment and the number of controls in scope. The assessor will start with a review of your system security plan and your plan of action and milestones. These documents tell them what you claim to have done and what you are still working on. From there, they move into interviews and demonstrations. They want to see that the policies on paper match the behaviour in the office. They will ask system administrators how they apply patches, how they manage user accounts, and how they detect unauthorised access. They will also inspect physical security measures such as locks on doors that lead to network equipment and the procedures for escorting visitors.

One area that catches small suppliers off guard is the requirement for multi-factor authentication on every user account that accesses covered data. Many small firms rely on simple passwords because they are easier to manage. The assessor will check for evidence that MFA is enabled and enforced. Another common gap is the lack of an up-to-date inventory of hardware and software. If you cannot list exactly what devices and applications touch protected information, the assessor will flag it as a finding.

Preparing your documentation ahead of time

The single most effective thing you can do before the assessment is to get your documentation in order. The CPCSC framework is heavily document-driven. Every policy must be written down, approved by management, and communicated to staff. The assessor will ask to see your incident response plan, your access control policy, your configuration management policy, and your media disposal procedures, among others. Many of these documents can be adapted from templates, but they must be tailored to your actual environment. A generic policy with the company name changed is a red flag.

Your system security plan is the centrepiece of the documentation package. It describes the boundary of the system that processes controlled unclassified information, the security controls implemented, and the connections to external networks. The plan of action and milestones is equally important. It lists each deficiency you have identified, the corrective actions planned, and the target completion dates. Assessors expect to see that you have a realistic plan to fix problems, not that you have fixed everything already. Honesty in the plan of action and milestones is valued more than a perfect score on the first try.

One practical step is to perform a self-assessment using the NIST SP 800-171 worksheet. Work through each of the 110 requirements and score your current state. Where you find gaps, document them in your plan of action and milestones. This self-assessment also helps you identify which controls will require the most evidence during the actual visit. For example, if you have a small IT team, the requirement for continuous monitoring of security events might be a challenge. The self-assessment lets you address that before the assessor sees it.

Common pitfalls for small suppliers

Small defence contractors often share a few weaknesses that assessors notice quickly. One is the separation of duties. In a team of three or four people, the same person who writes the security policy may also be the system administrator and the person who reviews audit logs. The framework expects some separation, or at least compensating controls such as automated alerts that detect the administrator logging in with a different account. Another pitfall is the lack of a formal training program. The framework requires that all personnel with access to controlled data complete security awareness training at least once a year. Many small firms skip this or rely on a single email. The assessor will ask for training records and evidence that the content covered the relevant topics.



Physical security is another area where small suppliers can be caught out. The CPCSC assessment includes a walkthrough of your facility. The assessor will look for unlocked server rooms, unsecured network jacks in common areas, and unattended workstations that are still logged in. They will also check that visitors are signed in and escorted. If your office shares a building with other tenants, the assessor will want to see that the network equipment is in a locked room that only authorised staff can enter.

A third common issue is the handling of media. The framework requires that any removable media containing controlled unclassified information be encrypted and tracked. USB drives, external hard drives, and even printed documents must be accounted for. Many small suppliers treat these items casually, assuming that a locked desk drawer is enough. The assessor will want to see a media sanitisation policy and records of when media was destroyed or cleared.

Working with a consultant to improve readiness

For a small defence supplier, preparing for a CPCSC assessment can feel overwhelming. The requirements are detailed, and the consequences of a low score can affect your ability to bid on contracts. Many firms choose to work with an independent consultant who specialises in compliance readiness. A consultant can help you perform a gap analysis, write the required policies, and coach your team on what to expect during the assessment. The goal is not to hide problems but to present a clear, honest picture of your security posture while addressing the most critical gaps.

One firm that provides this kind of independent support is Hans Study. As an IT and OT infrastructure consultant, Hans Study offers compliance readiness services, network security

consulting, physical security reviews, training, managed support, and fractional CISO services. For a small defence supplier, engaging a consultant like Hans Study early in the process can reduce the stress of the assessment and improve the final outcome. The consultant acts as a bridge between your team and the assessor, helping you understand what evidence will be required and how to present it clearly.

What happens after the assessment

Once the assessor submits their report, your organisation receives a score and a list of deficiencies. For any deficiency rated as high risk, you will need to submit a corrective action plan within a set timeframe, usually 30 days. The government may grant conditional approval while you work on the fixes. The key is to treat the assessment as a continuous improvement process rather than a one-time event. The CPCSC framework requires re-assessment at regular intervals, and each cycle builds on the previous one. Small suppliers that invest in good documentation, consistent practices, and regular self-assessments tend to improve their scores over time and become more competitive for defence contracts.

The whole experience is manageable if you approach it methodically. Start with the documentation. Perform a self-assessment. Address the most common gaps around MFA, inventory, and training. Consider working with a consultant who understands the framework. And remember that the assessor is looking for evidence of a genuine security program, not perfection. A well-prepared small supplier can pass the assessment and earn the certification that opens the door to government work.

Hans Study on social media Twitter LinkedIn Instagram YouTube