Gap assessment vs. compliance checklist for CPCSC readiness

When a Canadian defence supplier starts preparing for the Canadian Program for Cyber Security Certification (CPCSC) scoping, assessment, attestation, and certification, two approaches often come up: running through a compliance checklist or conducting a gap assessment. Both have their place, but they serve different purposes and produce different outcomes. Understanding the distinction helps you choose the right starting point and avoid wasted effort.

What a compliance checklist does

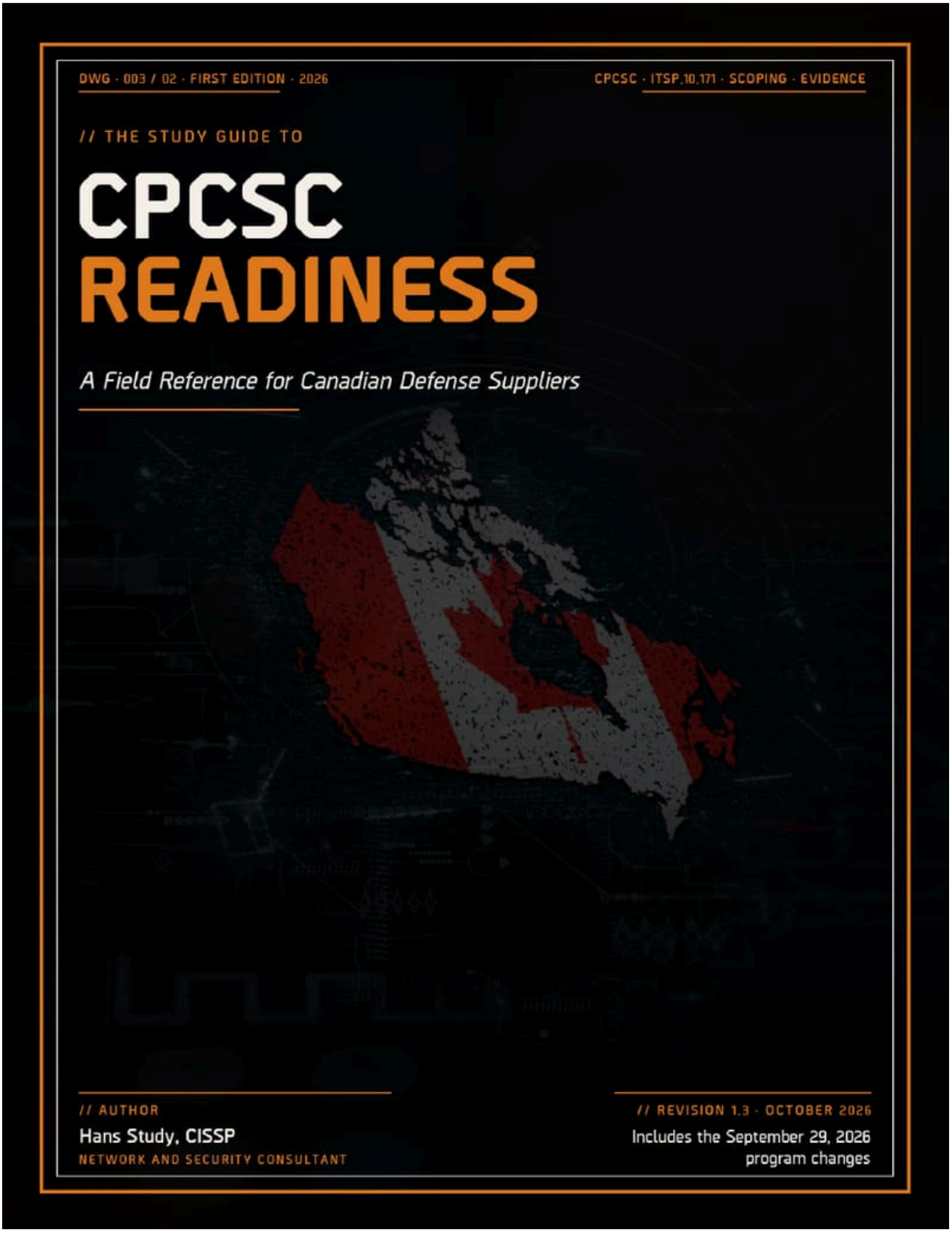
A compliance checklist is a list of requirements drawn from a standard or regulation. For the CPCSC context, that checklist might come from the NIST SP 800-171 framework, the Cyber Safe Canada standard, or your prime contractor's security requirements. You go down the list and tick yes or no: do you have a policy for access control? Is multi-factor authentication enabled for remote access? Do you maintain an asset inventory? Each item gets a pass or fail mark.

The strength of a checklist is speed. You can run through one in a few hours if you know your systems well. It gives a quick snapshot of where you clearly meet a requirement and where you clearly do not. It also provides a common language: your project manager, your IT lead, and your security officer can all look at the same list and agree on what it asks.

But a checklist has a blind spot. It treats each requirement in isolation. It does not ask how one control affects another, or whether your implementation actually works in practice. A checklist can tell you that you have an asset inventory, but it will not tell you whether that inventory is accurate, up to date, or covers all the categories the certifying body expects. It can confirm that you have a policy for protecting controlled unclassified information (CUI), but it will not reveal whether your staff actually follow it.

What a gap assessment does

A gap assessment takes a broader view. Instead of ticking boxes, it compares your current state against the target state defined by the certification framework. The output is not a pass-fail sheet but a gap register: a list of specific weaknesses, missing controls, or misalignments between what you have and what you need.



A good gap assessment looks at your security boundary, the network diagram, and the data flows that cross that boundary. It examines how protected information moves between systems, who has user accounts with privileged access, and where the risks actually sit. It

does not assume that having a firewall means your network is secure; it checks whether the firewall rules are properly configured and whether they align with your data classification.

The assessment also considers the relationships between controls. For example, you might have strong encryption for data in transit but weak access controls on the systems that store the decrypted data. A checklist would pass the encryption item and fail the access control item separately. A gap assessment would flag the combined weakness as a higher priority because the encryption is undermined by the access gap.

Another difference is depth. A gap assessment typically involves interviews with system owners, a review of actual configurations (not just policy documents), and sometimes technical testing. It produces a prioritized list of findings, often with suggested remediation steps. This makes it more resource-intensive, but also more useful for planning your certification timeline and budget.

When to use each approach

If you are at the very beginning of your CPCSC readiness journey and have never looked at the requirements, a compliance checklist can be a helpful warm-up. It gives you a sense of the scope: how many controls there are, which ones you already meet, which ones are clearly missing. It is a good way to get your leadership to see the gap in high-level terms without committing to a full assessment yet.

However, once you move past that initial awareness stage, a compliance checklist is rarely sufficient for certification preparation. The certifying body will expect evidence that your controls are actually effective, not just that you have them on paper. A checklist cannot provide that evidence. It can only tell you that you have checked the box.

A gap assessment, on the other hand, is designed to produce the kind of detail that feeds directly into a remediation plan. It tells you not only what is missing but also why it matters and how to fix it. It helps you allocate your limited resources to the gaps that pose the highest risk to your certification. This is especially important for small and medium-sized suppliers who cannot afford to waste time on low-priority issues.

View this on hans.study

There is also a timing factor. If your certification deadline is months away, a gap assessment early in the process gives you time to address the findings. If the deadline is weeks away, a checklist might be the only realistic option to confirm that you have at least addressed the basic requirements. But even then, you should treat the checklist result as a starting point, not a guarantee of passing the actual assessment.

Many suppliers find that they benefit from using both. Start with a checklist to get a rough sense of where you stand. Then commission a gap assessment to fill in the details and produce a prioritized action plan. After remediation, another round of the checklist can serve as a quick sanity check before the formal assessment.

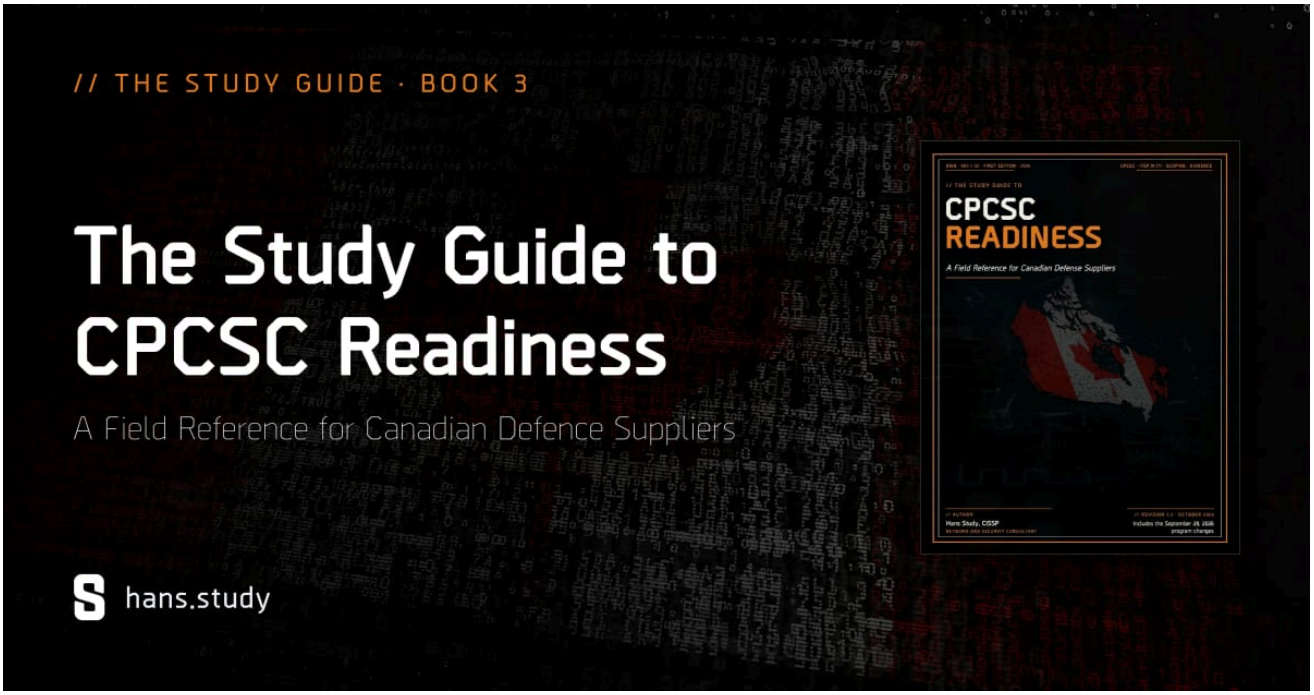
For those looking for a structured way to start, resources like Hans Study offer a free field guide that walks through the CPCSC process from scoping through certification. That guide can help you understand what a gap assessment should cover and how to interpret the results. It is worth reviewing before you decide which approach to take.

Common pitfalls to watch for

One common mistake is treating a compliance checklist as a gap assessment. You end up with a list of unmet requirements but no understanding of why they matter or how to close them. Another is skipping the checklist entirely and jumping straight into a gap assessment without any baseline. That can lead to a very long and expensive assessment that covers ground you could have handled in-house with a simple checklist.

Another pitfall is relying on a single approach for the whole certification lifecycle. The needs change as you move from scoping to assessment to attestation. In the scoping phase, you need to define your security boundary and identify which systems process CUI or other protected information. A checklist can help with the high-level identification, but a gap assessment will reveal whether your boundary definition is realistic or whether you are missing critical assets.

During the assessment phase, the certifier will expect to see evidence that your controls are implemented and effective. A gap assessment conducted before that phase gives you the evidence trail. A checklist alone will not satisfy the assessor, who will want to see network diagrams, configuration snapshots, user account reviews, and data flow analyses. These are outputs of a gap assessment, not a checklist.



Finally, do not treat the gap register as a static document. As you remediate findings, new gaps can appear. Changes to your network, new user accounts, or updated software versions can introduce weaknesses that were not there before. Revisiting the gap assessment periodically, especially after major changes, keeps your readiness on track.

Suppliers who combine both approaches in a thoughtful sequence tend to have a smoother certification journey. They use the checklist to build awareness and momentum, then invest in a proper gap assessment to build a solid remediation plan. They also understand that neither approach is a substitute for the actual on-site assessment by the certifying body. Both are preparation tools, not guarantees.

If you are unsure where to start, the **Hans Study** field guide includes guidance on how to scope a gap assessment and what to expect from it. That can help you decide whether a checklist or a full assessment is the right first step for your organization. The key is to choose deliberately, based on where you are in the process and what you need to learn next, rather than defaulting to one or the other out of habit.