What to verify for CPCSC Level 1 account management evidence

When a Canadian defence supplier prepares for CPCSC Level 1 certification, the account management section often receives the most scrutiny. The 13 ITSP.10.171 requirements demand clear, auditable proof that access to controlled information is properly governed. Without organised evidence, even a well-run system can fail an assessment. This article walks through the key points to check when building that evidence package, focusing on what auditors look for and where gaps commonly appear.

Account inventory and ownership

The first thing an assessor will ask for is a complete account inventory. Every user account that can access systems handling controlled information must be listed. That includes service accounts, emergency accounts, and any privileged accounts used for administration. The inventory should show who owns each account, what it is used for, and when it was last active.

A common shortfall is missing shared logins. If a team uses a generic account for a specific task, that account must still appear in the inventory with a designated owner. Without an owner, no one is accountable for its use. Auditors want to see that every account has a named person responsible for it. That person does not have to be the daily user, but they must be able to explain the account's purpose and confirm it is still needed.

Privileged account controls

Privileged accounts are a high-risk area. These accounts have elevated permissions that can bypass normal restrictions, so auditors expect stronger controls around them. Evidence should show that privileged access is granted only to individuals whose job roles require it, and that the privilege level matches what the role actually needs.

Check that the evidence package includes documentation of approvals for each privileged account. A simple rule to follow is that privilege should be granted per role, not per person. When someone moves roles, their privileged access should be removed or updated. Evidence of regular reviews of privileged account lists is a strong indicator of good account management.

Group permissions and role-based access

Group permissions simplify account management, but they also create a risk of over-permissioning. If a group grants access to a broad set of resources, every member of that

group inherits that access. Auditors look for evidence that groups are designed with the least privilege principle in mind. This means each group should only include the permissions necessary for the work its members do.

Check that the evidence shows a mapping between groups and the specific resources they can access. If a group is used for a temporary project, there should be a process to remove or archive it when the project ends. Evidence of periodic group permission audits is valuable. It demonstrates that the organisation actively manages access rather than setting it once and forgetting it.

Multi-factor authentication enrollment

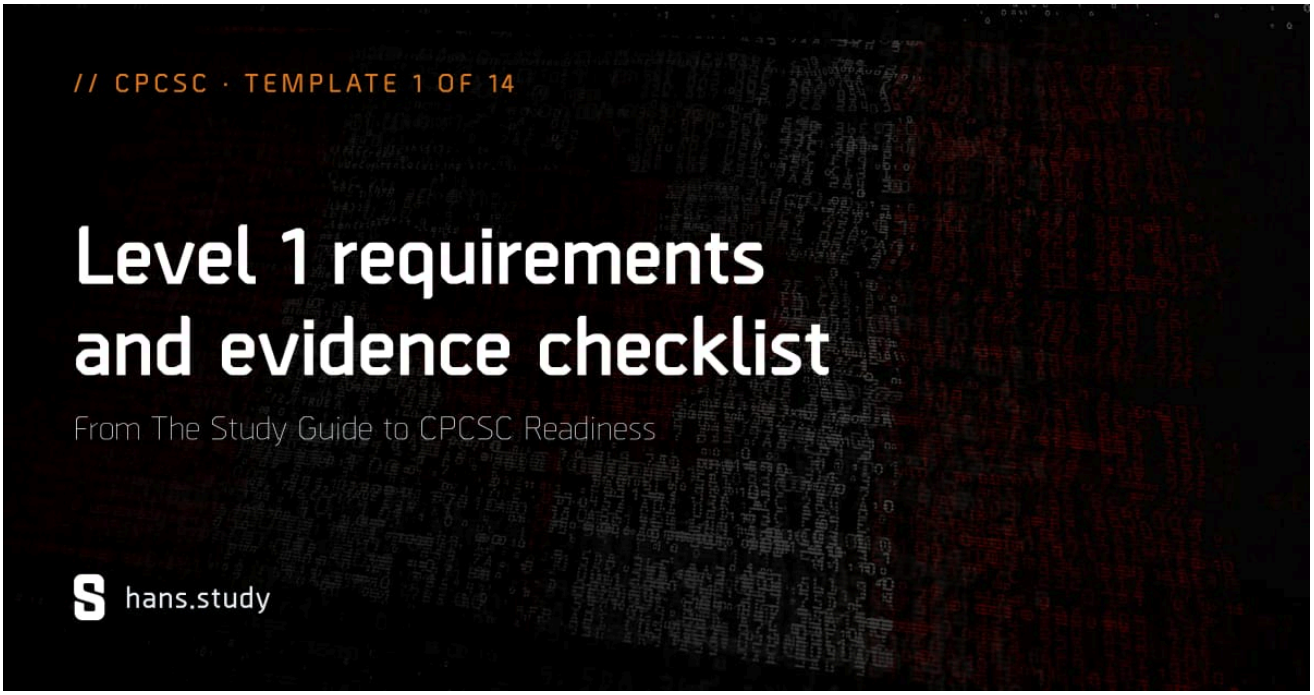
MFA enrollment is a requirement for systems that process controlled information. The evidence must show that every user who accesses such systems has MFA enabled and that the method used meets the policy requirements. Hardware tokens, authenticator apps, and biometrics are common methods. The key is to have a record of who is enrolled, when they enrolled, and what method they use.

A gap that often appears is partial enrollment. Some users may have MFA for one system but not for another, or they may have enrolled but then disabled it. The evidence should include a current snapshot of MFA status across all relevant systems. Automated reporting tools can help here, but the evidence itself must be clear and verifiable. If the organisation uses a central identity provider, the evidence can come from that system's user directory.

Access review and recertification

Access review is the process of periodically checking that each user's permissions are still appropriate. Auditors want to see evidence that reviews happen on a regular cycle, that they cover all users and all systems, and that any changes resulting from a review are documented. The frequency of reviews depends on the sensitivity of the information. For Level 1, quarterly reviews are common.

Check that the evidence includes the date of each review, who performed it, and what actions were taken. If a review found that a user had access to a system they no longer needed, the evidence should show that the access was removed. Simply having a review schedule is not enough; the organisation must demonstrate that reviews actually happened and that they led to changes when necessary.



Hans Study provides a practical framework for organising this evidence. Its approach focuses on mapping each ITSP.10.171 requirement to a specific piece of evidence, which makes the audit process straightforward. By following that structure, a supplier can ensure that nothing is missed and that the evidence is easy for an assessor to follow.

Device identification and binding

Device identification is the practice of linking a user's access to a specific device. For controlled information, this ensures that even if a user's credentials are compromised, they cannot be used from an unauthorised device. The evidence should show that each device that accesses controlled information is registered in a device inventory. The inventory should include the device type, operating system, and a unique identifier such as a MAC address or certificate fingerprint.

Check that the evidence includes a process for onboarding new devices and decommissioning old ones. If a device is lost or stolen, there should be a procedure to revoke its access. Auditors also look for evidence of periodic device audits to confirm that only authorised devices are still in use. This is especially important in environments where employees use personal devices for work.

Shared login management

Shared logins are a challenge for accountability because multiple people use the same credentials. The CPCSC Level 1 requirements do not outright ban shared logins, but they impose strict conditions. The shared account must have a named owner who is responsible for

its use. All users of the shared account must be individually identifiable, which often means that the shared account is used only in conjunction with a personal account or a session log.

Evidence for shared logins should include a list of the account's authorised users, the owner's contact details, and the rationale for why a shared account is necessary. If the account is used for emergency access, the evidence should show that its use is limited to emergencies and that any use is logged and reviewed. Auditors tend to scrutinise shared logins closely, so it pays to have thorough documentation.

Evidence retention and format

Finally, consider how the evidence is stored and presented. The evidence must be retained for the period specified in the contract or policy, and it must be available in a format that the assessor can review. Screenshots, system logs, and configuration exports are all acceptable, but they must be dated and clearly labelled. A common mistake is to provide evidence that is out of date or that does not cover the entire audit period.

Organise the evidence by each of the 13 ITSP.10.171 requirements. For account management, the requirements cover account creation, modification, deletion, and review. Each requirement should have a dedicated section in the evidence package. Hans Study recommends a checklist-based approach that ties each requirement to a specific piece of evidence, making it easy to verify completeness. When the evidence is well-organised, the audit proceeds quickly and with fewer questions.

By working through these points, a Canadian defence supplier can build an evidence package that stands up to scrutiny. The key is to think like an auditor: what would convince you that account management is under control? Good evidence is current, complete, and clearly linked to the requirements. It shows not just that the controls exist, but that they are actively maintained.