FREE ASSESSMENT TOOL

CSP Readiness Checklist for Defence Contractors

Contract Security Program Compliance Self-Assessment — Canada PSPC

Miller Contract Security Advisory | Ottawa, Ontario | millersecurityconsulting.ca

How to use this checklist: Work through each section and mark each item as *Complete*, *In Progress*, or *Not Started*. Items tagged **HIGH RISK** are the most common causes of audit findings or contract delays — prioritize these first. This tool is a general reference and does not substitute for a full gap analysis conducted by a qualified CSP advisor.

Section 1 — Organizational Registration & Sponsorship

Applicable to all organizations entering or currently within the CSP

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Organization is registered in the CSP and holds an active account with PSPC [HIGH RISK]	HIGH	
☐	A valid contract or Letter of Sponsorship from a Contracting Authority exists		
☐	Organization profile in PSPC's OLISS is current and accurate		
☐	FSC or DOS level is appropriate for contract requirements [HIGH RISK]	HIGH	
☐	Foreign ownership/control/influence (FOCI) assessment completed if applicable		
☐	Legal name, corporate structure, and address on file with PSPC match current registration		

Section 2 — Key Personnel & Security Responsibilities

Roles required under CSP and PSPC security requirements

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Chief Security Officer (CSO) appointed and notified to PSPC [HIGH RISK]	HIGH	
☐	CSO holds the required clearance level for their role		
☐	Alternate Security Officer designated and recorded in OLISS		
☐	Board/Senior Management screened to required clearance level [MED RISK]	MED	
☐	Process in place to notify PSPC of personnel changes within required timeframes		
☐	Security briefings documented for all personnel with access to protected/classified information		

Section 3 — Personnel Security Screening

Reliability Status, Secret, and Top Secret clearance administration

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Current register of all personnel clearances maintained, with expiry dates tracked [HIGH RISK]	HIGH	
☐	Clearance levels match or exceed the sensitivity designation on active contracts		
☐	Screening requests submitted through OLISS with complete and accurate TBS forms		
☐	Renewals initiated well before expiry — 90 days for Reliability, 6 months for Secret [HIGH RISK]	HIGH	
☐	Process exists for revoking access and notifying PSPC when personnel depart		
☐	Subcontractor personnel clearance requirements documented and verified		

Section 4 — Facility Security

Physical controls for protected and classified work environments

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Facility Security Plan (FSP) documented, current, reviewed within past 12 months [HIGH RISK]	HIGH	
☐	Physical access controls in place for areas where protected/classified work is conducted		
☐	Visitor control procedures documented and consistently applied		
☐	Approved storage containers in place for classified material [MED RISK]	MED	
☐	End-of-day security check procedures documented and followed		
☐	PSPC notified of facility address changes or significant security zone changes [HIGH RISK]	HIGH	

Section 5 — Document & Information Security

Handling, storage, transmission, and destruction of protected/classified materials

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Written procedures for marking, handling, and storing Protected and Classified documents [HIGH RISK]	HIGH	
☐	Document register maintained for classified materials received or generated under contract		
☐	Approved transmission methods used for protected/classified information		
☐	Secure destruction procedures in place — cross-cut shredding minimum for Protected B [MED RISK]	MED	
☐	IT systems handling government information assessed at the appropriate security level		
☐	Cloud storage and collaboration tools reviewed for GC IT security requirements		

Section 6 — Security Policy & Incident Reporting

Organizational security governance and reporting obligations

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Organizational Security Policy signed by senior management, communicated to all staff [HIGH RISK]	HIGH	
☐	Security incident reporting procedure documented (PSPC 24-hour notification rule understood)		
☐	Security incident log maintained with investigation records		
☐	Annual security awareness training conducted and records retained		
☐	Process for reporting foreign travel and reportable activities for cleared personnel [MED RISK]	MED	

Section 7 — Controlled Goods Program (CGP) — If Applicable

Complete this section only if your organization examines, possesses, or transfers controlled goods

✓	REQUIREMENT	RISK	STATUS / NOTES
☐	Organization is registered under the Controlled Goods Program (PSPC — CGD) [HIGH RISK]	HIGH	
☐	Designated Official (DO) appointed and registered; all CG-access persons registered		
☐	Security assessment of all individuals with CG access completed within required period		
☐	CGP Security Plan documented and current [HIGH RISK]	HIGH	
☐	Controlled goods register maintained with accurate inventory		
☐	Export compliance (ITAR/EAR) reviewed where applicable for goods held		

Scoring Your Results

25+ Complete: Strong compliance posture. Focus on renewal timelines and annual reviews.
15–24 Complete: Moderate gaps present. Prioritize HIGH RISK items before your next contract award or audit.
Under 15 Complete: Significant remediation needed. Consider engaging a CSP advisor before pursuing or renewing contracts.

About Miller Contract Security Advisory

Ron Miller, CD, brings over 20 years of hands-on federal security compliance experience to defence contractors across Canada. Our practice maintains a 100% client audit success rate. This checklist is a general reference tool and does not constitute formal legal or regulatory advice. Requirements may vary based on contract classification levels and PSPC program updates.

Ready for a full gap analysis? millersecurityconsulting.ca