Request for Proposal (RFP)

Cybersecurity Assessment, Penetration Testing & Remediation Roadmap

Ontario Centre of Innovation (OCI)

Issue Date:	May 1, 2026
Questions Deadline:	May 11, 2026
Proposal Submission Deadline:	May 25, 2026
Evaluation Period:	May 28 – July 15, 2026
Award Notification:	July 16, 2026
Project Start Date:	July 20, 2026

1. Introduction

The Ontario Centre of Innovation (OCI) invites qualified cybersecurity consulting firms to submit proposals in response to this Request for Proposal (RFP). OCI is seeking a Canada-based, mid-tier cybersecurity firm to conduct a comprehensive assessment of its technology environment, perform penetration testing, and deliver a practical, actionable remediation roadmap.

2. Background

OCI has conducted annual penetration testing for the past three years in accordance with NIST SP 800-115. This engagement builds on that foundation and expands scope to include a full cybersecurity posture assessment, gap analysis, and a formal Cyber Resilience Program (CRP) framework. OCI operates a primarily cloud-based environment with approximately 100–150 users on Microsoft 365 and Azure-hosted services.

3. Purpose / Objectives

The objective of this engagement is to assess OCI's current cybersecurity posture, identify and validate key risks, and deliver a prioritized remediation plan and Cyber Resilience Program.

The selected vendor will:

- Assess current cybersecurity risks and vulnerabilities
- Identify and validate key risks through penetration testing
- Evaluate gaps against NIST CSF 2.0 as the primary framework (GO-ITS 42 as mandatory compliance baseline; CIS Controls v8 and ISO/IEC 27001:2022 as supplementary references)
- Develop a prioritized, actionable remediation roadmap
- Provide a Cyber Resilience Program (CRP) framework aligned to NIST CSF 2.0

Primary Standard: NIST CSF 2.0. Secondary references: GO-ITS 42 (mandatory compliance baseline), CIS Controls v8, ISO/IEC 27001:2022. Vendors should not produce lengthy framework checklists — OCI values clear,

practical recommendations above volume of findings.

4. Scope of Work

Phase 1 — Mandatory:

- Pre-Engagement Preparation and Scoping: Conduct discovery sessions with stakeholders to confirm systems in scope, rules of engagement, testing windows, and excluded assets. Develop and submit a Penetration Testing Plan including methodology, risk management, and communication protocols prior to testing commencement.
- Current-state cybersecurity assessment (NIST CSF 2.0)
- Comprehensive penetration testing (NIST SP 800-115 + MITRE ATT&CK)
- Risk assessment and gap analysis
- Prioritized remediation roadmap
- Board-level presentation

Phase 2 — Optional (separately priced):

- Remediation implementation support — vendors may propose a cost estimate for remediation on OCI's behalf as a separately quoted optional work package. Must be clearly separated in pricing.

Out of Scope:

- Physical security testing
- Ongoing managed security services
- Third-party or cloud platforms outside OCI's direct control (unless agreed in writing)
- Systems or segments not listed in the agreed scope

4.1 Penetration Testing

In-Scope Testing Areas:

- a. Network & Infrastructure
  - External and internal network testing
  - Network segmentation validation
  - Lateral movement simulation
  - Privilege escalation
- b. Cloud & Identity (Critical Priority)
  - Microsoft 365 and Azure environments
  - Entra ID / Active Directory (cloud and hybrid)
  - Identity attack paths (privilege escalation, conditional access bypass, token/session abuse)
  - Misconfiguration exploitation
- c. Endpoints
  - User endpoints (laptops)
  - EDR bypass attempts (where feasible)
  - Local privilege escalation
- d. Applications & APIs

– Web applications (internal, external, and cloud — including Smart Simple)

– APIs and integrations

– Authentication, session management, and authorization testing

– Business logic abuse scenarios (where applicable)

– Application-level vulnerability scanning

- e. Third-Party Systems (Mandatory)

– OCI's configuration, access controls, and integration points

– Configuration reviews and access path analysis where direct testing is restricted

Testing Methodology:

- Follow NIST SP 800-115 and align with MITRE ATT&CK
- Align with OWASP where applicable for web application testing
- Use both automated and manual techniques — automated scanning alone is not sufficient
- Simulate realistic, chained attack scenarios
- Include assumed breach and adversarial simulation scenarios
- Identify trust relationships and end-to-end escalation paths
- Simulate phishing and credential harvesting scenarios
- Evaluate the resilience of existing security controls and monitoring tools

Rules of Engagement:

- Pre-approved testing windows required
- No denial-of-service testing without explicit written approval
- No production disruption without explicit written approval
- Coordination with OCI Project Lead throughout
- Vendor must provide documented risk management and escalation procedures prior to testing commencement

Retesting: The vendor must include one round of retesting for remediated critical and high findings, including validation of remediation effectiveness and updated risk status.

5. Key Deliverables

All deliverables must be clear for both technical and non-technical audiences, actionable, and reusable without ongoing vendor dependency. OCI reserves the right to request revisions if deliverables lack sufficient detail, are generic, or do not align with scope.

1. Current-State Assessment (NIST CSF 2.0)

- Full mapping of OCI's environment across all CSF functions
- Maturity rating per function with defined scoring methodology
- Year-over-year trend comparison to prior assessments

Format:

– Primary report (PDF)

– Supporting control mapping (Excel)

2. Penetration Testing Report (NIST SP 800-115)

- Scope, methodology, and tools used
- Findings with PoC evidence for critical/high vulnerabilities, CVSS scoring, reproduction steps, attack path narratives, and business impact
- One round of retesting with validation results and updated risk status

Format:

– Full report (PDF)

– Raw findings data (Excel or CSV)

3. Risk Assessment (NIST SP 800-30 Rev. 1)

- Risk register including: threat source, vulnerability, likelihood/impact ratings, existing controls, and residual risk

Format:

– Risk register (Excel — mandatory)

– Summary report (PDF)

4. Gap Analysis (NIST CSF 2.0 / SP 800-53 / GO-ITS 42)

- Identification of control gaps and deficiencies
- Mapping across applicable frameworks
- Prioritized recommendations for remediation

Format:

– Control mapping and gap matrix (Excel)

– Summary report (PDF)

5. Cyber Resilience Program (CRP) Framework

- Target-state security posture aligned to NIST CSF 2.0
- Required security controls and capabilities
- Policy and governance recommendations (indicate whether provided as templates or recommendations only)
- Security awareness and training plan by role/function
- All recommendations implementable without proprietary vendor tools unless explicitly stated

6. Remediation Roadmap (Critical Deliverable)

- Prioritized, phased action plan (0–90 days / 3–6 months / 6–12 months)
- Per finding: exploitation likelihood, business impact, remediation actions, recommended owner, effort estimate
- Dependencies, sequencing, and required tools/resources

Format:

– Visual roadmap (PowerPoint or PDF)

– Detailed tracker (Excel)

7. Board-Level Presentation

- Non-technical; focused on business risk, impact, investment priorities, and next steps

• CSF 2.0 scorecard, overall maturity rating, top risks with business impact

• Vendor must conduct a formal debrief/presentation session with OCI stakeholders upon delivery of final findings

Format:

– PowerPoint — max 20–25 slides

8. Project Management Artifacts

• Work Breakdown Structure (WBS) with milestones, dependencies, and critical path

• Detailed project schedule (MS Project, Smartsheet, or equivalent)

• Weekly status reports (progress, risks/issues, decisions required from OCI)

• Meeting agendas and minutes within 24 hours of each session

9. Projected Solutions & Cost Estimates

• Estimated cost ranges for remediation

• Itemized breakdown (licensing, implementation, support)

• Annual pricing for any subscription-based services

Format:

– Optional quote: Continuous vulnerability management or subscription-based monitoring

– Optional quote: Threat intelligence services to inform testing scope

– Optional quote: Assistance with regulatory compliance or audit preparation (GO-ITS 42, SOC 2, ISO 27001)

6. Vendor Qualifications

Vendors must meet all of the following requirements to be considered:

• Canada-based: vendor offices must reside within Canada; the assessment must be delivered from within Canada; no offshore subcontracting permitted

• Experience with similar-sized organizations (100–200 users, cloud-first environments)

• Named project team with roles and resumes for senior technical leadership and key personnel

• Relevant certifications: CISSP, CISM, OSCP or equivalent

• Dedicated Project Manager as single point of accountability

• Firm fixed price for Phase 1; Phase 2 priced separately if offered

• Statement of how soon after contract execution the vendor can begin

Required with Proposal:

• 3–5 relevant project examples from the last 3 years (include completion date and client references)

• At least 2 anonymized sample deliverables

7. Proposal Requirements

Proposals must include all of the following sections in the order listed:

• 1. Cover Letter

• 2. Executive Summary — brief overview of the proposed approach and why the firm is well suited

- 3. Approach and Methodology — how the vendor will execute each phase
- 4. Work Plan and Timeline — detailed schedule with milestones
- 5. Team Structure and Resumes — named individuals and their roles
- 6. Relevant Experience — 3–5 case studies with completion dates and references
- 7. Sample Deliverables — minimum 2 anonymized examples (required)
- 8. References — minimum 2 client references from similar engagements
- 9. Pricing — fixed price for Phase 1; optional Phase 2 priced separately; itemized rate card; annual pricing for subscriptions
- 10. Assumptions and Exclusions
- 11. Signed Declarations

8. Evaluation Criteria

Proposals will be evaluated on:

- Approach & Methodology (25%) — clarity, practicality, and real-world applicability
- Relevant Experience (25%) — demonstrated work with similar-sized, cloud-first organizations
- Deliverable Quality (20%) — sample deliverable quality and clarity for non-technical audiences
- Team Qualifications (15%) — certifications, seniority, and named individuals
- Pricing & Value (15%) — competitiveness and transparency of fixed-price bid

Success Criteria: OCI values practicality, actionability, and clarity. Proposals that produce lengthy framework checklists rather than clear, implementable recommendations will be rated lower. Vendors must demonstrate the ability to deliver without creating ongoing dependency.

9. Timeline

Vendors should propose a realistic project timeline of 6–8 weeks from project start.

Milestone	Target Date
RFP Issued	May 1, 2026
Questions Deadline	May 11, 2026
Proposal Submission Deadline	May 25, 2026
Evaluation Period	May 28 – June 9, 2026
Award Notification	June 16, 2026
Project Start Date	June 19, 2026
Kick-Off Meeting	Within 5 business days of contract execution
Pre-work and consultations complete	June 30, 2026
Draft findings review	Mid-engagement
Final delivery	Within agreed project timeline (target: late August 2026)

10. Contract Terms and Conditions

• **Collusion** — Proposals must be independent, genuine, and free from collusion or unfair advantage.

• **Gratuities** — No gifts, incentives, or employment offers to OCI staff related to this RFP.

• **Review & Waiver of Protests** — Written questions/objections must be submitted by the deadline; late issues are waived.

• **Nondiscrimination** — Compliance with all applicable nondiscrimination laws is required.

• **Proposal Costs** — Proposers bear all costs associated with preparing and submitting a proposal.

• **Withdrawal** — Proposals may be withdrawn in writing and resubmitted before the submission deadline.

• **Errors** — Proposers are responsible for errors; no changes are permitted after the submission deadline.

• **Incorrect Information** — Materially incorrect information may lead to disqualification.

• **Proposer Terms** — Vendor standard terms and conditions are not acceptable and may result in rejection.

• **Assignment & Subcontracting** — Requires OCI written approval. All subcontractors must be disclosed and Canada-based. The prime vendor remains accountable. No offshore work is permitted.

• **Contract Negotiations** — OCI may negotiate with the selected or an alternate proposer.

• **Contract Execution** — The contract must be signed within 15 business days of award notification or OCI may proceed to the next proposer.

• **Right of Rejection** — OCI reserves the right to reject any or all proposals or cancel this RFP at its discretion. All deliverables become OCI property upon payment.

• **Governance** — The selected vendor must assign a dedicated Project Manager as single point of accountability. Weekly status meetings (30–60 min), a defined escalation path, and 2–3 business day decision turnaround are required. Full governance details will be incorporated into the contract and statement of work.

11. Data Security & Confidentiality

Vendors must:

- Store all OCI data within Canada
- Use secure transmission methods for all data exchange
- Ensure strict confidentiality of all findings, reports, and related materials
- Destroy all OCI data upon project completion (upon written request)
- Execute a Non-Disclosure Agreement at project kick-off

12. Submission Instructions & Contact Information

Proposals must be submitted electronically by:

Submission Deadline:	May 25, 2026 at 5:00 PM ET
Submission Format:	PDF (preferred) or Word document, submitted via email
Submission Email:	bparikh@oc-innovation.ca
Contact Name:	Bhavik Parikh, Director - IT

Receipt Confirmation:	All submissions will be acknowledged within 1 business day

Late submissions will not be accepted. OCI is not responsible for submissions not received due to technical issues. Proposals received after the deadline will be returned unopened.

13. Q&A Process

All questions regarding this RFP must be submitted in writing to the contact identified in Section 12 by the Questions Deadline of May 11, 2026 at 5:00 PM ET.

- Questions must be submitted by email with the subject line: “OCI Cybersecurity RFP — Question”
- Responses will be shared with all registered bidders in anonymized form within 3 business days of the deadline
- Verbal responses to questions are not binding
- OCI reserves the right to issue addenda to this RFP at any time prior to the submission deadline

---

Key Note to Vendors: *OCI is seeking a practical partner — not a theoretical assessment provider. Proposals that emphasize clear, actionable outcomes and real-world experience will be strongly preferred over overly complex or generic approaches.*