CAIQ-Lite Self-Assessment

Movahedi Solutions, 1000823315 ONTARIO INC., Mississauga, Ontario, Canada

Date: October 28, 2026 | Contact: mohammad@movahedi.ca

This document is a self-assessment, not a certification, audit, or third-party verification.

This document is a self-assessment by 1000823315 ONTARIO INC., operating as Movahedi Solutions. It is not a CSA assessment, not a certification, and not an audit. It is not a third-party verification.

Company: 1000823315 ONTARIO INC., operating as Movahedi Solutions, Mississauga, Ontario, Canada.

Contact: mohammad@movahedi.ca

Date: October 28, 2026

Scope: the public website movahedi.ca, and the handling of client material in engagements. This document does not cover a client system.

Structure: the questions below follow the domain structure of the Cloud Security Alliance CAIQ-Lite questionnaire, which covers 16 control domains. The wording of the questions is original to this document and paraphrases the topic of each domain; no proprietary template text is reproduced. Only questions answered from verified evidence are included. Items not listed here are not claimed.

Services: AI and agent inventories; EU AI Act readiness assessments; custom AI governance frameworks; risk assessments; privacy advisory; Law 25 compliance support; knowledge-base design and build.

Client data rules: client data is used only for its engagement, access is limited, and client data is removed at the end of the engagement, or returned or deleted on client instruction. There is no sale of client data, no use of client data for model training, and no public naming of a client without written permission.

Founder credentials are personal only: ISC2 CC, CIPP/C, Six Sigma Black Belt. No company certification is held, and none is claimed here.

1. Application and Interface Security

1. Is the public site served over HTTPS only, through its delivery provider? Yes. The public site is

served over HTTPS through Cloudflare. Evidence: DNS and SSL Checks, October 28, 2026; SSL Labs grade A, assessed October 28, 2026, 01:00:26 UTC.
2. Are security headers in place on the public site? Yes. A Security Headers scan returned grade A+ on October 28, 2026, 00:59 UTC, and a re-check on October 28, 2026, 02:09 UTC returned the same header set. Evidence: https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on. This is a header scan, not a penetration test.

2. Audit Assurance and Compliance

1. Is this document presented as a self-assessment, with its limits stated? Yes. The status paragraph above states that this is a self-assessment, not a certification or an audit.
2. Are the firm's registrations recorded with dates, so a reader can check them? Yes. Registrations recorded October 27, 2026 are listed in the companion cybersecurity self-assessment, including UNGM Basic, MERX Basic Free, and CanadaBuys / SAP Ariba.

3. Business Continuity and Operational Resilience

1. Can the public site be redeployed from its source after a correction? Yes. The site is built and deployed from GitHub, so recovery does not depend on a single live copy.
2. Is the handling of client material at the end of an engagement defined? Yes. Client data is removed at the end of the engagement, or returned or deleted on client instruction, under terms agreed for that engagement.

4. Change Control and Configuration Management

1. Is the source for the live site held in version control? Yes. The public site is built and deployed from GitHub.
2. Are changes to the live site traceable to that source? Yes. The GitHub source gives a record of what was deployed, so a change to the live site can be traced to its source.

5. Datacenter Security

1. Is physical datacenter security for the public site handled by the delivery provider? Inherited. Delivery is through Cloudflare; physical security of Cloudflare facilities is a matter for Cloudflare, and no datacenter claim of the firm's own is made here.
2. Does the firm operate its own datacenter for the public site? Not applicable. The firm does not

operate a datacenter for movahedi.ca.

6. Data Security and Information Lifecycle Management

1. Is client data used only for its engagement? Yes. That rule is stated for every engagement, with access limited.
2. Is client data removed, returned, or deleted at the end of an engagement or on client instruction? Yes. That step follows the terms agreed for the engagement.

7. Cryptography, Encryption, and Key Management

1. Is the public site served over HTTPS? Yes. Evidence: DNS and SSL Checks, October 28, 2026; SSL Labs grade A.
2. Is a strict transport header in place? Yes. The Security Headers scan returned Strict-Transport-Security with max-age 31536000, includeSubDomains, and preload.

8. Governance, Risk, and Compliance

1. Is accountability for the public site and for engagement handling rules assigned? Yes. The founder is accountable for the public site and for the engagement handling rules stated in this document.
2. Are engagement handling rules stated in writing for each engagement? Yes. Scope, data flows, and deliverables are named in writing before work that depends on them begins, and handling rules are stated for that engagement.

9. Human Resources Security

1. Is access to the firm's own accounts and tools limited to the people who need it for the work at hand? Yes. That rule is stated in the Security Practices document.
2. Is access removed when a person no longer needs it for an engagement? Yes. Removal is part of closing the engagement, as stated in the Security Practices document.

10. Identity and Access Management

1. Is access to client data limited? Yes. Access is limited, and client data is used only for its engagement.
2. Is access to the firm's own accounts kept to those who need it? Yes, as stated under Human

Resources Security above.

11. Infrastructure and Virtualization Security

1. Is the public site delivered through a named provider? Yes. Delivery is through Cloudflare, over HTTPS.
2. Is the site built and deployed from a named source? Yes. The site is built and deployed from GitHub.

12. Interoperability and Portability

1. Is the public site source held in version control, so the site is not tied to a single live copy? Yes. The site is built and deployed from GitHub.
2. Are engagement deliverables provided to the client under that engagement's terms? Yes. Deliverables, scope, and handling are named in writing for each engagement.

13. Mobile Security

1. Does the firm publish a mobile application for clients? Not applicable. No mobile application is published as part of the services listed above.
2. Is a mobile device management claim made here? No claim is made. No mobile device management product is named in this document, and none is claimed.

14. Security Incident Management

1. Is there a published method for reporting a security issue on the public site? Yes. Reports go to mohammad@movahedi.ca, under the Responsible Disclosure page in this project, with scope limited to movahedi.ca and no bounty unless separately approved and funded.
2. Is there a published handling sequence for a confirmed issue on the public site? Yes. A confirmed issue is handled through the site source in GitHub and redeployment of the corrected site, with the reporter told the outcome for their report.

15. Supply Chain Management, Transparency, and Accountability

1. Is a subprocessor table published? Yes. The Subprocessor Transparency Table in this project lists Cloudflare for delivery over HTTPS and GitHub for build and deployment, with no location stated where none was verified.

2. Are engagement tools agreed per engagement rather than presented as a single standing list? Yes. Tools for an engagement are confirmed during scoping for that engagement.

16. Threat and Vulnerability Management

1. Is there a published contact for security reports on the public site? Yes. Reports go to mohammad@movahedi.ca, and a security.txt file is prepared for https://movahedi.ca/.well-known/security.txt with that contact.
2. Are email authentication records in place for the firm's domain? Yes. SPF, DKIM for the Google selector, and DMARC at quarantine policy were verified from DNS on October 28, 2026. Evidence: DNS and SSL Checks, October 28, 2026. No strict DMARC rejection policy is claimed.

Summary

Questions answered: 32, across 16 domains, 2 per domain.

Answers: Yes, 28; Inherited, 1; Not applicable, 2; No claim made, 1 (Mobile Security, question 2, which states only that no claim is made).

Evidence links: https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on; https://www.ssllabs.com/ssltest/analyze.html?d=movahedi.ca. Other evidence is cited by document title within this project: Security Practices, Responsible Disclosure, Subprocessor Transparency Table, DNS and SSL Checks, and the companion cybersecurity self-assessment dated October 28, 2026.

Limits: this self-assessment does not claim a company certification, a penetration test, a monitoring platform, a response time, or an availability figure. It does not cover a client system.