CONSEIL DE GOUVERNANCE NUMÉRIQUE | DIGITAL GOVERNANCE COUNCIL

Verification Statement

(Issuance No: DGC-VV-2026-24)

Issued To:
CanITSM Consulting
1200 Bay St. Suite 1201
Toronto, ON
Canada M5R 2A5

Issuer:
Digital Governance Council
500-1000 Innovation Dr.
Ottawa, ON
Canada, K2K 3E7
dgc-cgn.org

Verification Claims

Digital Governance Council has assessed the claims declared by CanITSM Consulting ("CanITSM") concerning the implementation of cybersecurity controls within the assessed environment supporting its Managed IT Services ("Solution") and reviewed the supporting evidence in accordance with the policies and procedures of the DGC Digital Trust Verification Program. The claims were assessed in accordance with the following:

- **Assessment Type:** Verification Review
- **Scope:** Cybersecurity
- **Sub-Scope:** Baseline cyber security controls for small and medium organizations
- **Focus/Specialization:** Control-implementation information mapped to Level 1 and Level 2 requirements
- **Applicable Standard(s)/Assessment Tool(s):** CAN/DGSI 104:2021 / Rev 2:2026, *Baseline cyber security controls for small and medium organizations*
- **Accreditation Standard(s):** ISO/IEC 17029:2019, *Conformity assessment — General principles and requirements for validation and verification bodies*
- **Assessed Verification Report:** CanITSM's control-implementation disclosures recorded in its Statement of Conformance, dated 15 September 2026.

The object of verification was CanITSM's declared information concerning cybersecurity-control implementation, including the scope of implementation and disclosed limitations. The verification was limited to the organizational units, systems, services and operating environments identified in the assessed documentation. Customer environments were included only where expressly identified within those boundaries.

The objective of the verification was to determine whether CanITSM's claims were truthfully stated against the specified verification criteria. Based on the verification activities performed, DGC confirms, as of the date of issuance, that the following claims declared by CanITSM are truthfully stated within the assessed boundaries:

1. CanITSM has implemented cybersecurity controls addressing the following Level 1 and Level 2 requirements of CAN/DGSI 104:2021 / Rev 2:2026, *Baseline cyber security controls for small and medium organizations*, within the assessed environment supporting its Solution, subject to the exception identified in Claim 2:
    a. Organizational controls (Section 4)
        i. Leadership (4.1)
        ii. Accountability (4.2)
        iii. Cyber security training (4.3)
        iv. Cyber security risk assessment (4.4)
    b. Baseline controls (Section 5)
        i. Incident response plan (5.1)
        ii. Automatically patch operating systems and applications (5.2)
        iii. Enable security software (5.3)
        iv. Implement and maintain a secure configuration process (5.4)

v. Use strong user authentication (5.5) – subject to Claim 2.
vi. Backup and encrypt data (5.6)
vii. Establish basic perimeter defences (5.7)
viii. Implement access control and authorization (5.8)

c. Baseline controls by operating environment (Section 6)
i. Secure mobility (6.1)
ii. Secure cloud and outsourced IT services (6.2)
iii. Secure websites (6.3)
iv. Secure portable media (6.4)
v. Point of sale (POS) and financial systems (6.5)
vi. Computer Security Log Management (6.6)

2. CanITSM has not yet implemented phishing-resistant authentication in accordance with clause 5.5.3.2 for administrator access to critical systems, identity services and cloud consoles. CanITSM currently enforces multi-factor authentication for applicable administrative access through Microsoft Entra ID, supported by separate administrative accounts and role-based access controls. Phishing-resistant authentication has been formally considered, and its implementation is planned as part of CanITSM's future cybersecurity enhancements.

DGC Statement of Assurance

DGC assures that the verification and assessment process was conducted impartially, fairly and transparently using evidence provided in accordance with the DGC Digital Trust Verification Program, subject to approved DGC policies and procedures publicly available. This verification statement does not constitute an endorsement by DGC. Until such time that the DGC Digital Trust Verification Program receives accreditation, this verification statement shall be relied on as an interim acknowledgement only. Once accreditation is received, this verification statement shall be reviewed and considered for formal recognition. This is a third-party verification.

Date of Issuance: 2026-10-22

Signature:

Keith Jansa, CEO, Digital Governance Council

DIGITAL TRUST VERIFIED