OSLER

A practical approach to enhancing cybersecurity trust: standards and validation programs for SMEs

FEBRUARY 10, 2025 6 MIN READ

Related Expertise

- Cybersecurity and Security Incident Response
- Emerging and High Growth Companies
- Privacy and Data Management
- Technology

Authors: Sam Ip, Justin P'ng, CIPP/C/US, Joseph Ierullo

On February 6, 2025, the Digital Governance Council, a not-for-profit organization that plays a critical role in setting Canadian standards, launched its new CyberReady Validation Program. This initiative aims to help small and medium-sized enterprises (SMEs)[1] in strengthening their cybersecurity posture by offering a service to review their cybersecurity practices for compliance with baseline requirements.

This launch is timely and coincides with the Government of Canada’s introduction of its new National Cyber Security Strategy to address the myriad cyber threats facing Canada. Given the increasing sophistication and frequency of cybersecurity incidents, and the vulnerability of smaller organizations due to limited resources, the CyberReady Validation Program potentially fills a gap in promoting and standardizing SME cybersecurity preparedness.

As cybersecurity threats become more prevalent, the need for SMEs to implement cybersecurity controls based on accessible, pragmatic and achievable standards is critical. In the AI industry, we have previously explored emerging AI security risks and comprehensive AI frameworks such the NIST AI RMF for AI developers and deployers. More broadly, many enterprises recognize the ISO/IEC 27001 as one of the more well-known information security standards, although its rigour and comprehensive requirements can be impractical for many SMEs.

To address this challenge, the CAN/DGSI 104:2021 / Rev 1: 2024 standard provides baseline cybersecurity controls to help SMEs navigate this risk environment. When paired with the CyberReady Validation Program, it potentially represents a cost-effective approach to address cyber risks and enhance stakeholder confidence.

Overview

CAN/DGSI 104:2021 / Rev 1: 2024 – Baseline Cyber Security Control for SMEs

The CAN/DGSI 104:2021 / Rev 1: 2024 standard (the SME cybersecurity standard), recently updated in December 2024, establishes a baseline of cybersecurity controls for SMEs. It encompasses a range of controls, from organizational aspects such as leadership and accountability to technical measures such as patch automation, user authentication and access controls.
Recognizing the diverse needs of organizations, particularly smaller organizations, the SME

cybersecurity standard adopts a two-tier approach: Level 1 for smaller organizations starting their cybersecurity journey and Level 2 for more mature organizations that seek to enhance their cybersecurity measures. The SME cybersecurity standard also includes practical appendices, such as a template for incident response, cybersecurity risk assessment and a vendor analysis questionnaire.

CyberReady Validation Program

According to the Digital Governance Council, the CyberReady Validation Program is designed to assist organizations with assessing and validating their cybersecurity readiness, ensuring their practices and controls meet the SME cybersecurity standard. To date, two services are offered, including a validation review based on self-reported information and a more in-depth validation audit.

With relatively modest associated costs, the program provides a relatively affordable option for SMEs looking to strengthen and demonstrate their posture. That said, while it supports certification, it is important to note that it is not itself a certification, although successful organizations will receive a statement of validation/verification and an associated Trustmark. Organizations interested in leveraging this service may wish to review these options to determine the appropriateness for their enterprise.

Broader implications

Tools such as the SME cybersecurity standard and programs such as the Digital Governance Council’s CyberReady Validation Program have broader implications, particularly for emerging and high-growth companies for which cybersecurity is often a challenge. Specifically:

- **Starting point for cybersecurity**. Many SMEs lack the resources to implement an enterprise-grade cybersecurity program on par with their larger counterparts. Enterprise frameworks such as ISO/IEC 27001 require significant financial investment and often involve fully dedicated organizational functions, making them impractical for smaller companies. Some SMEs are also intimidated by the complexity, while others do not view it as an immediate priority. On its face, the SME cybersecurity standard provides a relatively approachable baseline. When paired with initiatives such as the CyberReady Validation Program, it appears to offer a practical, structured approach to establishing an information security program and addressing common cybersecurity risks, such as ransomware, phishing and other types of data or system breaches.
- **Standardization of cybersecurity expectations for SMEs**. Given the variability of information security controls, many SMEs who do not already subscribe to an industry standard such as ISO/IEC 27001 follow a range of different approaches to securing their environment. The SME cybersecurity standard represents an integrated baseline — and one that serves as a practical subset of ISO/IEC 27001 — against which SMEs can benchmark themselves, as well as an opportunity to harmonize expectations and approaches for these types of organizations, including in critical areas such as incident response planning.
- **Independent accountability**. As is the case with other independent review programs, the CyberReady Validation Program raises expectations for SMEs by serving as an official

mechanism of third-party accountability for the SME cybersecurity standard. SMEs who want to ensure they achieve a successful verification or validation will be incentivized to materially improve their cybersecurity posture. Other SMEs who want to market their adherence to the SME cybersecurity standard will be pressured to demonstrate compliance by using the CyberReady Validation Program or otherwise have a credible basis for not agreeing to third-party review.

- **Establishing trust in the marketplace.** For many emerging high growth innovators, demonstrating cybersecurity readiness is essential. Many start-ups — especially those offering software-as-a-service-based solutions — handle large volumes of data and sensitive information. Aligning with a recognized cybersecurity standard such as the SME cybersecurity standard can provide assurances to potential and existing customers, business partners and even investors to reduce concerns and enhance trust and credibility.
- **Facilitating the procurement process.** Emerging and high-growth companies often struggle to close early sales with larger and sophisticated organizations and government entities due to cybersecurity concerns. The checklist-based appendices in the SME cybersecurity standard provide a useful starting point for addressing these concerns. Specifically:
  - Annex B (Cybersecurity Security Risk Assessment) helps SMEs evaluate and identify gaps in their security posture.
  - Annex C (Vendor Security Questionnaire) prepares SMEs for the kinds of questions they can expect from sophisticated enterprise customers.
- **Commercial contracting.** Startups often struggle with the complexity of varying security commitments in their contracts, as different clients may impose slightly different security requirements (e.g., AES encryption vs. other standards). By adhering to recognized standards such as the SME cybersecurity standard, SMEs can establish a baseline, making it more credible that their security practices align with industry expectations and should be deemed acceptable. Similarly, for those procuring solutions from SMEs, requiring them to comply with a recognized criteria like the SME cybersecurity standard provides a shorthand way to avoid lengthy and protracted negotiations on security provisions while obtaining a baseline level of security commitments in contract.
- **Tool in M&A transactions.** Cybersecurity risks are often key consideration for M&A, as buyers and investors seek to mitigate risks related to cyber vulnerabilities. While programs such as the CyberReady Validation Program will not replace traditional full security diligence, it could simplify cybersecurity assessments, help sellers demonstrate readiness beyond simply what is said during the diligence process and provide buyers with additional confidence in the security of acquisition targets.

Conclusion

The effectiveness of the SME cybersecurity standard and the CyberReady Validation Program remains to be seen, and its success will depend on its ability to stay aligned with well-known industry frameworks that evolve rapidly to address emerging cybersecurity threats. Additionally, striking a balance between cost-effectiveness and comprehensive validation is essential. Without rigorous validation, there remains the risk of fostering a false sense of security if controls are not thoroughly assessed for effectiveness.

That said, the SME cybersecurity standard and CyberReady Validation Program can offer a practical and structured solution for SMEs that lack the resources to implement and demonstrate adherence to a more comprehensive security program. By leveraging established standards such as CAN/DGSI 104:2021 / Rev 1: 2024, organizations can take meaningful steps toward improving their cybersecurity posture, enhancing stakeholder trust and ensuring compliance with evolving security expectations.

More broadly, the SME cybersecurity standard and the CyberReady Validation Program are just two of the many available tools designed to support cybersecurity resilience. While programs like these provide structured guidance, SMEs should carefully evaluate and adopt cybersecurity frameworks that align with their specific needs, resources and risk profile.

---

[1] The CAN/DGSI 104:2021 / Rev 1: 2024 standard characterizes SMEs as typically having fewer than 500 employees.