Cybersecurity Services

Our cybersecurity services are designed to help governments and civic-minded organizations identify and mitigate risks while protecting the confidentiality, integrity, and availability of their data. Whether you want a comprehensive needs assessment, a roadmap for improvement, or targeted implementation support, we adapt our approach to match your capacity and goals.

What we do

Cybersecurity risk assessment

We help you build a comprehensive understanding of your organization's risk profile, vulnerabilities, and security posture. Our approach evaluates security and privacy needs across the data lifecycle while considering your organization's size, capacity, and technological maturity. Typical activities include:

- Conducting stakeholder interviews and workshops to surface cybersecurity risks to key data assets, flows, and use cases.
- Evaluating existing policies, practices, and tools for addressing data security and privacy needs.

What you gain: A clear understanding of your organization's readiness to detect, respond to, and mitigate cyber threats.

Roadmap development

Based on your risk profile, existing security measures and vulnerabilities, we work with you to design a roadmap for improvement that includes:

- Defining Specific, Measurable, Actionable, Relevant, and Time-bound (SMART) goals to guide improvement efforts.
- Creating action plans to guide implementation of priority initiatives, with timelines, resource requirements, and milestones to monitor progress.

What you gain: A focused strategy outlining sequenced, practical steps to mitigate risk and enhance your cybersecurity practices.

Targeted implementation support

We support you in implementing your roadmap through tailored, hands-on assistance, including:

- Audit services: Verifying compliance with specific security standards and evaluate existing controls.
- Stress-testing policies, actions, and procedures in a controlled and safe environment before broader deployment.
- Policy and standards development: Co-creating policy and procedures for long-term and sustainable approaches to emerging and evolving cybersecurity threats.
- Team training: Fostering a culture of proactive risk awareness and mitigation in daily activities.

What you gain: Progress toward your cybersecurity goals with effective solutions, strong governance, and teams equipped to respond to future threats.

Why work with Open North?

At Open North, we combine deep expertise in data with a multidisciplinary approach. Our team includes urban planners, software engineers, community organizers, data scientists, cyber and IT audit specialists, sociologists, geographers, and technology lawyers, bringing diverse perspectives to every project.

We are passionate about our work and committed to continuous learning, investing regularly in the professional development of our team members through recognized training and certifications, while adapting this knowledge to meet the unique needs of diverse contexts.

What sets us apart:

- **Accessible, right-sized solutions:** As a small not-for-profit organization, we understand the unique constraints faced by smaller organizations and work to tailor solutions to your organization's capacity and resources.
- **Commitment to knowledge sharing:** We believe in learning in the open by publishing free resources, guides, tools, and courses.
- **Building capacity for autonomy:** We focus on equipping your organization with the capacity to succeed on its own, without dependence on outside support.

Contact us today to learn how we can help your organization unlock the potential of your data, achieve your goals, and contribute to advancing the common good through responsible and impactful data practices.

Email us at info@opennorth.ca
Visit our website: opennorth.ca

OPEN NORTH