CYBERSECURITY CONSULTING

GRC & Compliance Readiness

Governance programs and audit preparation that turn compliance from a scramble into a formality, SOC 1/2, ISO 27001, PCI DSS, CMMC, NIST, and Canadian privacy.

CyberX One builds the governance backbone and gets you audit-ready. We map your controls to the frameworks that matter to your sector, close the gaps with the right policies and procedures, and assemble the evidence, so external audits become a formality rather than a fire drill.

Objectives

- Identify the standards that apply to your sector and scope the program accordingly.
- Measure current controls against the target framework through a structured gap analysis.
- Close gaps with policies, procedures, and practical technical controls.
- Assemble documentation and evidence and prepare teams for assessors.
- Establish a governance cadence that keeps you compliant between audits.

Outcomes & benefits

- **Audit-ready**, evidence and documentation assembled before the assessor arrives.
- **Clear scope**, the right frameworks selected for your sector and obligations.
- **Complete controls**, a full policy and procedure suite that maps to the standard.
- **Prioritized remediation**, gaps closed in the order that matters most.
- **Sustained compliance**, a repeatable cadence, not a once-a-year panic.

Scope of service

- Control mapping to the selected framework(s).
- Policy and procedure framework development.
- Gap analysis and a prioritized remediation roadmap.
- Evidence collection support and audit liaison.
- A readiness assessment or mock audit before the real one.

Frameworks & standards we work across

- **SOC 1 / SOC 2 Type II**, service-organization controls for security, availability, and confidentiality.
- **ISO/IEC 27001**, the global standard for managing information security.
- **PCI DSS**, controls for organizations storing, processing, or transmitting cardholder data.
- **NIST CSF & 800-53**, U.S. cybersecurity framework and control catalogue.
- **CMMC**, maturity model for organizations in defense supply chains.
- **PHIPA**, Ontario law protecting personal health information.
- **PIPEDA**, Canadian law regulating personal information in the private sector.
- **GDPR**, European data-protection regulation with global reach.
- **SOX & SOC audits**, financial-reporting IT controls and service-organization assurance.
- **OSFI, FINTRAC & CASL**, Canadian financial, anti-money-laundering, and anti-spam obligations.
- **IEC 62443 & NERC CIP**, controls for industrial systems and critical infrastructure.

Our process

1. **Scope**
   Select the applicable frameworks and define audit scope.
2. **Gap analysis**
   Measure current controls against the target standard.
3. **Remediate**
   Develop policies, procedures, and controls to close gaps.
4. **Ready**
   Assemble evidence and run a readiness assessment / mock audit.

What you receive

- Framework gap analysis
- Policy and procedure suite
- Prioritized remediation roadmap
- Evidence pack and audit-readiness assessment

Engagement at a glance

TYPICAL DURATION	LED BY	SERVICE TYPE
~4-8 weeks per framework	**CISA-certified consultant**	**Program & audit prep**

SOC 1 / SOC 2 · ISO 27001 · PCI DSS · NIST CSF · CMMC · PHIPA / PIPEDA

Ready to start?

Email **shah@cyberxone.ca** · **LinkedIn**
CyberX One Inc. · Markham, Ontario · Serving Canada

Book a discovery call