

CYBERSECURE CANADA CERTIFICATION



**FOR MORE INFORMATION
CONTACT US**

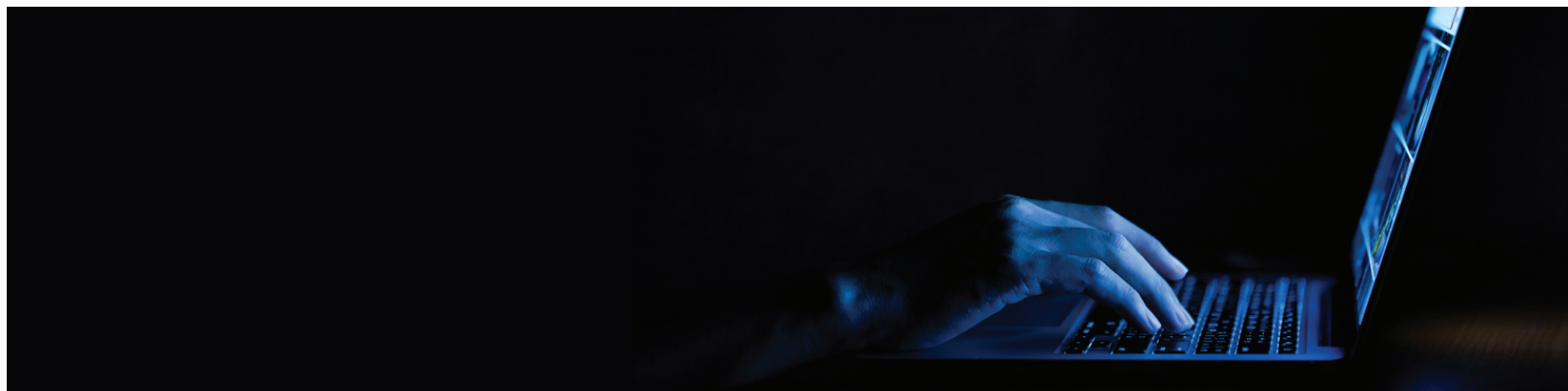
 www.sourcetekit.com

 sales@sourcetekit.com

 1(844)818-4646



CYBERSECURE CANADA CERTIFICATION AUDIT PROCESS



WHO WE ARE

Founded in 2009, SourcetekIT's Security as a Service team is dedicated to getting ahead of cyber threats before they can stop business. Our subject matter experts are sought-after authorities in IT security, risk mitigation, compliance, gap analyses and threat remediation, with decades of experience consulting, auditing, training and implementing enterprise security across multiple industries and for multiple resellers.

Our principal consultants literally wrote the book on compliance frameworks like NIST. They have trained thousands of CISSPs to be CISSPs, and authored books on the fundamentals of information systems security. As a result, we have contractual relations with more than 100 CISSPs who specialize in multiple market sectors, including healthcare (HIPAA/HITECH), retail (PCI-DSS), government contracting (ISO/NIST) & European markets (GDPR).



CYBERSECURE CANADA CERTIFICATION

AUDIT PROCESS

1. APPLICATION SUBMISSION

Applications can be submitted through: website period once these applications are submitted, a questionnaire along with baseline controls is sent to the applicant. This questionnaire details key information pertaining to the audit, that the auditing body will require in reviewing the application.

2. APPLICATION REVIEW, AUDIT QUOTATION, AND TIMELINE

Our internal body will review the answers on the questionnaire based on this the quotation will be shared. If there are any questions from the applicant needed answered by the auditing body a call can be set up for the applicant to clear any doubts.

3. PROPOSAL APPROVED, AUDIT PLAN, ASSESSMENT TEAM MEET & GREET

Once the business has approved the proposal the certification body will formulate an audit plan. This plan will outline procedures and timelines of the entire audit process customized for the business. The plan will be presented and shared with the business during the initial meet and greet.

4. PRE-AUDITING ACTIVITIES

The client/business that is undergoing the audit will then provide the auditor with all the information pertaining to policies and all other relevant documentation they can share in regards to the policy controls against which they will be audited.



CYBERSECURE CANADA CERTIFICATION

AUDIT PROCESS

5. CONDUCT AUDIT

STAGE 1: DOCUMENTATION AUDIT

1. The assigned auditor will then review each response and assess the level of compliance. A detailed review of all the policies, documents and the contracts will be conducted. This review includes any contracts with external vendors to whom any IT service has been outsourced to by the business.require in reviewing the application.

RESULTS :

Based on the review, if the auditor finds that there are major high-risk in regard to security non compliance. The auditor will immediately inform the management of this business to ensure this is resolved right away. At this point the audit will go on hold. The business will then have to provide a time period in which they are to make the required changes. The auditor can reinstate the audit upon the resolution of the high-risk security non-compliance. Once the assessed material adherers to the compliance requirements successfully or with minor non-compliances the auditor will generate a report to be shared with the organizations. The minor changes will be highlighted to the organization for the required corrections to be made. Upon completion, the auditor will re-evaluate the correction and score the organization.

STAGE 2: IMPLEMENTATION AUDIT

1. The implementation audit can only take place once the documentation audit has been successfully completed and passed by the organization.
2. In this stage of the audit the policies to which the organization has provided will be tested in the actual environment. This is done in two ways:
 - The auditor will perform an internal/external pen test checking the environment for vulnerabilities. This step will allow the auditor to see if the technical infrastructure is up to date with policies in place. The auditor will provide sampling in which the organization will understand the existing vulnerabilities.



CYBERSECURE CANADA CERTIFICATION

AUDIT PROCESS

5. CONDUCT AUDIT

- The second part of the implementation audit involves assessing compliance. The auditor will conduct interviews with members of the organization. The auditor will also be collecting sampling of the various reporting systems, to assess how if the business is adhering to controls based on mandatory documentation ex. how onboarding of new employees is conducted. The interviewee's will be selected based on their roles and responsibilities within the organization;
 - ▶ Member or members of management will be assessed on how and what they do to enforce the policies they have in place for there employees and security infrastructure.
 - ▶ Employees may be assessed on there knowledge of cyber security. With this the auditor will be able to determine the success of the knowledge transfer given to employees by management.
 - ▶ Members of the technical team will be assessed on the processes they follow to up keep the technical infrastructure.

Evaluation of stage 2 will follow the same procedure of that in stage 1: Based on the review, if the auditor finds that there are major high-risk in regard to security non compliance. The auditor will immediately inform the management of this business to ensure this is resolved right away. At this point the audit will go on hold. The business will then have to provide a time period in which they are to make the required changes. The auditor can reinstate the audit upon the resolution of the high-risk security non-compliance.

Once the assessed material adherers to the compliance requirements successfully or with minor non-compliances the auditor will generate a report to be shared with the organizations.



CYBERSECURE CANADA CERTIFICATION

AUDIT PROCESS

The minor changes will be highlighted to the organization for the required corrections to be made. Upon completion, the auditor will re-evaluate the correction and score the organization.

6. CERTIFICATION DECISION

AUDIT REPORT:

At the end of audit, the auditor will send an executive audit report to the business's management. A member of management team from the business has to provide an acceptance on these findings. Once accepted this report will be presented to the internal auditing body who will provide an approval on the findings given that they conclude the business has satisfied the requirements of the certification based on these findings.

Upon the success of this process the certification will be awarded. The Certification mark is issued by government of Canada however the certificate itself will be issued by certification body.

7. CERTIFICATION DECISION

Upon receipt of the certification the business is required to follow guidelines outlined by Cyber Secure Canada and enforced by the certification body. These guidelines are crucial for the business to adhere to in order to remain certified and most importantly, secure. The Cyber Secure Canada Certification is valid for two years, upon completion of this two-year period the business is required to undergo a reassessment.