Insurance for Financial Technology Companies

Markel Fintech 360 Canada

Application Form

Important Notice

1. This is an application for a contract of insurance and various provisions within the policy will restrict coverage
2. This is a proposal for a contract of insurance. You have a legal duty to provide a fair presentation of the risk. Failure to do so may make the contract of insurance voidable or severely prejudice your rights in the event of a claim.
3. This proposal must be completed signed and dated. All questions must be answered to enable a quotation to be given but completion does not bind you or insurers to enter into any contract of insurance. If space is insufficient to answer any questions fully, please attach a signed addendum sheet. You should retain a copy of the completed proposal (and of any other supporting information) for future reference.
4. You are recommended to request a specimen copy of the proposed policy wording from your insurance broker and to consider carefully the terms, conditions, limitations and exclusions applicable to the cover.

Section A: General Information

Name of applicant:	
Principal Address:	
Province of Incorporation	
Website URL:	
Total Employees:	
Date of Establishment:	

MARKEL

Please provide a full description of your business activities and detail if there are any anticipated changes to the activities in the next 12 months:

A1. Type of Business Entity (please check the applicable description):

☐ Corporation ☐ Limited Partnership/Limited Liability Company

☐ Not for Profit/Tax Exempt Company ☐ Partnership/Joint Venture

If other, please specify:

A2. Does the Applicant act as a general partner, partnership manager or participate in any joint ventures? ☐ Yes ☐ No

If 'Yes', and coverage is required, please attach a list of these entities and indicate for each the nature of business and percentage ownership held by the Applicant.

A3. Are there any entities owned less than 51% for which coverage is requested? ☐ Yes ☐ No

If 'Yes', and coverage is required, please attach a list of these entities and indicate for each the nature of business and percentage ownership held by the Applicant.

A4. Has the Applicant in the past 12 months completed or agreed to, or does it contemplate within the next 12 months, any of the following, whether or not such transactions were or will be completed:

a) A merger, acquisition, consolidation or tender offer? ☐ Yes ☐ No

b) Does the Applicant have any subsidiaries outside of Canada? ☐ Yes ☐ No

If 'Yes', please attach a list of these entities and indicate for each the nature of business and percentage ownership held by the Applicant.

MARKEL

Please provide annual financial details for the past year, current year and the projected income for the next financial year.

	Currency	Past Year	Current Year	Next Year
Revenue				
Total Assets				
Current Assets				
Current Liabilities				
Total Debt				
Cash Flow from Operations				
Profit (Loss)*				

* Please provide a copy of latest annual financial report

Please confirm geographical split of fee income / turnover by client / customer base:

	Past Year	Current Year (estimate)	Next Year (estimate)
Canada			
USA			
UK			
Europe			
Rest of the World (ROW)			
If you have entered a Rest of the World number, please list applicable countries below:			

Section B: Requested Insurance

Coverage Type	Limit	Past Year	Policy Period			Current Retroactive Dates
Errors & Omissions Liability				to		
Directors and Officers				to		
Employment Practices Liability				to		
Theft Insurance				to		
Cyber Liability and Loss Insurance				to		
Commercial General Liability				to		
Directors and Officers				to		

MARKEL

Section C: Financial Services and Technology Errors & Omissions Liability Module

If you require coverage under Financial Services and Technology Errors & Omissions Liability, please complete the following questions:

C1. Is the company authorised and regulated by the Financial Consumer Agency of Canada? ☐ Yes ☐ No

C2. Is the company authorised and regulated by any other regulator? ☐ Yes ☐ No

If YES, please name the regulator:

C3. Is the company an authorised representative of another company? ☐ Yes ☐ No

If YES, please name the principal:

C4. Please provide an approximate percentage breakdown of how your revenue/fees are generated from your products and services:

Products & Services	Percentage Revenue/Fees
	%
	%
	%
	%
	%

C5. If you engage in business to business (B2B) contracts then please list the five largest contracts undertaken during the last 3 years:

Client	Industry	Nature of your Product/Service	Fee	Start Date	End Date

C6. Do you always carry out work under a written contract? ☐ Yes ☐ No

MARKEL

C7. What percentage of your contracts are under your own standard terms and conditions? *Please provide a copy of your standard terms and conditions. %

C8. Have your standard contractual terms and conditions been reviewed by internal/external legal counsel? ☐ Yes ☐ No

C9. Are all client, non-standard or amended contracts reviewed by legal counsel before being signed? ☐ Yes ☐ No

C10. Do you exclude liability for consequential, special or indirect losses and loss of profit? ☐ Yes ☐ No

C11. Do you cap your overall liability? ☐ Yes ☐ No If Yes, please provide amount:

C12. Do you only warrant a performance standard no greater than reasonable care and skill? ☐ Yes ☐ No

C13. Do you ensure your contracts allow you to subrogate claims from outsourced service providers? ☐ Yes ☐ No

C14. Do ensure your contracts include a dispute resolution procedure? ☐ Yes ☐ No

C15. Do you only provide indemnities in respect of intellectual property rights, data protection, confidentiality, death, bodily injury or property damage? ☐ Yes ☐ No

C16. If you engage in payments, trading or money transfer, then please answer questions (a), (b) and (c):

(a) Total volume of transactions annually

(b) What is the largest value per transaction during the last 12 months?

(c) What is the average value per transaction during the last 12 months?

C17. If you engage in business to consumer (B2C) or business to business to consumer (B2B2C), then please state the number of individual personal identifiable information you store and process:

C18. Please describe the impact on your clients if your technology products or services failed or you were unable to deliver your products or services:

C19. a) Do you seek legal advice relating to intellectual property protection and breaches prior to the release of any new products or technology? ☐ Yes ☐ No

b) Have you registered the intellectual property rights for your products and technology? ☐ Yes ☐ No

c) If you use third party owned intellectual property, do you obtain appropriate licenses and indemnifications? ☐ Yes ☐ No

If NO to any of the above, please detail below what alternative controls are in place with regard to the management of intellectual property rights:

MARKEL

C20. Are all publications and online material issued by the company reviewed by an in-house legal department and/or outside legal advisers? ☐ Yes ☐ No

C21. What percentage of your work is sub-contracted to others? ☐ None ____ %

C22. Do you obtain hold harmless and/or indemnity agreements from your sub-contractors? ☐ Yes ☐ No

C23. Do you require that your sub-contractors provide you with proof that their professional liability and cyber insurance coverage is current? ☐ Yes ☐ No

---

Section D: Directors & Officers and Company Liability Module

If you require coverage under Directors & Officers Liability, please complete the following questions:

D1. Can you confirm the statements for the applicant and all of its subsidiaries:

(a) Are not contemplating a share offering or rights issue in the next 12 months? ☐ Yes ☐ No

(b) Involved in any issuance of debt or convertible securities? ☐ Yes ☐ No

(c) Are not publicly listed on any stock exchange or other securities exchange? ☐ Yes ☐ No

(d) Have not had any material change to its capital structure ☐ Yes ☐ No

(e) Have not sold any part of the company in the last 12 months and do not anticipate making any acquisitions or disposals in the next 12 months? ☐ Yes ☐ No

(f) Have not had the CEO or CFO leave the company in the last 12 months? ☐ Yes ☐ No

(g) Do not have any shareholders that own 5% or more of the company that are not directors? ☐ Yes ☐ No

(h) Do not any have any shareholders that own 20% or more of the voting shares directly or beneficially? ☐ Yes ☐ No

If you have answered No to any of the questions above, please give details here:

D2. Has the applicant sought protection under the Companies' Creditors Arrangement Act (CCAA) or Bankruptcy and Insolvency Act in Canada or Chapter 11 in the U.S.A., or reorganization or arrangement with creditors under provincial or state law or similar provisions in any other jurisdiction? ☐ Yes ☐ No

MARKEL

Section E: Employment Practices and Third Party Discrimination Liability Module

	Canada	USA	Other	Specify Country if Other
Number of Full Time Employees				
Number of Part Time Employees				
Number of Contract Employees (the company has assumed liability of)				
Number of Volunteers				

	Texas	California	New York	New Jersey	Michigan	Illinois	Florida
Number of USA Employees by State							

E1. Employee Turnover as % of total.

12 Months ____ %

24 Months ____ %

E2. Total percentage of current employees with annual compensation greater than $100,000. ____ %

E3. Does the Applicant have an Human Resources Department? ☐ Yes ☐ No

If 'No', does the applicant have other qualified staff members serving equivalent functions. ☐ Yes ☐ No

If 'No' how are Employment Concerns handled and by whom?

E4. Does the applicant issue all employees with an employee handbook that addresses workplace conduct and grievance procedures? ☐ Yes ☐ No

If Yes, do you require all employees to sign back with acknowledging their acceptance? ☐ Yes ☐ No

E5. Does the Applicant have a written Human Resources Manual in place? ☐ Yes ☐ No

E6. Does the Applicant have a written procedure for preventing discrimination and harassment? ☐ Yes ☐ No

E7. Does the Applicant have a written procedure for dealing with complaints about discrimination and harassment? ☐ Yes ☐ No

MARKEL

E8. Does the Applicant have a written process for disciplinary procedures ? ☐ Yes ☐ No

E9. Does the Applicant have a written grievance procedure ? ☐ Yes ☐ No

E10. Does the Applicant have a complaints procedure from allegations from any person who is not an employee of the applicant? ☐ Yes ☐ No

E11. Does the Applicant have a standardized performance management process? ☐ Yes ☐ No

E12. Does the Applicant provide regular written performance evaluations? ☐ Yes ☐ No

E13. Does the Applicant provide a standardized application form for employment that includes a full job description? ☐ Yes ☐ No

E14. Does the Applicant have a standardized severance program for terminations and layoffs? ☐ Yes ☐ No

E15. Are any layoffs or terminations of employees anticipated or being contemplated in the next 18 months or has occurred in the past 18 months? ☐ Yes ☐ No

If 'Yes' please answer the following:

a) What percentage of employees will be affected? ____ %

b) Will Outside Counsel be utilized? ☐ Yes ☐ No

c) Will severance be offered to all affected employees? ☐ Yes ☐ No

d) Are procedures in place to assist affected employees find work? ☐ Yes ☐ No

Section F: Fiduciary/Pension Trust Liability Module

Plan Summary

Plan Name	Plan Type	Plan Assets	Number of Plan Participants	Country	Year Established

Types of Plans:

DC = Defined Contribution Plan
ESOP = Employee Stock Ownership Plan
DB = Defined Benefit Plan
WP = Welfare Plan
RRSP/SP = RRSP/Savings Plan

MARKEL

Plan Operations

F1. If any plan for which coverage is requested holds or invests in securities of the Applicant, please provide details, including name of plan, number of shares held and most recent share value. ☐ Yes ☐ No

If no such plan, check here: ☐ No Plan

F2. In the past 18 months has the Applicant merged, spun-off, transferred or terminated any employee benefit plans(s) or is any such merger, spin-off, transfer or termination being contemplated in the next 18 months? ☐ Yes ☐ No

If 'Yes', provide details including transaction date, status of asset distribution, whether similar benefits are being offered, and name of insurance carrier if terminated plan benefits are secured by insurance.

F3. Are all plans in compliance with plan agreements or ERISA? ☐ Yes ☐ No

F4. Has any amendment to any plan been made or contemplated within the past two (2) years, or is any amendment now contemplated, which has resulted or might result in any reduction of benefits including, but not limited to an increase in participant's share of cost? ☐ Yes ☐ No

F5. Do any plan(s) employ outside providers to perform services in the following disciplines? ☐ Yes ☐ No

If Yes, provide the service provider name:

Service	Usage	Name of Service Provider
Investment	☐ Yes ☐ No	
Accounting	☐ Yes ☐ No	
Actuarial	☐ Yes ☐ No	
Legal	☐ Yes ☐ No	
Administrative/Books	☐ Yes ☐ No	
Record Keeping	☐ Yes ☐ No	

MARKEL

F6. Provide details of any reviews completed regarding any administrative, record-keeping, investment management, or advise, commissions or marketing fees charged to or paid by, whether directly or indirectly, any sponsored defined contribution:

F7. Is benchmarking performed? ☐ Yes ☐ No

a) How frequently are these fees reviewed/benchmarked?

b) How frequently are investment options reviewed/benchmarked, evaluated for performance?

c) Provide details of the review/benchmark process:

Section G: Theft Module

If you require coverage under Theft, please complete the following questions:

G1. Are the duties of each employee arranged so that no one employee is permitted to control any transaction/process from start to finish? ☐ Yes ☐ No

G2. Is there segregation of duties between those responsible for bank reconciliation and deposits, cheque signing and payroll? ☐ Yes ☐ No

G3. Are background checks performed on all new employees? ☐ Yes ☐ No

G4. Are company bank accounts reconciled weekly? ☐ Yes ☐ No

G5. Are all passwords securely changed when staff leave? ☐ Yes ☐ No

G6. Is the use of IT terminals restricted only to authorised personnel? ☐ Yes ☐ No

G7. Are remote IT terminals kept in a physically secure location accessible to authorised personnel only? ☐ Yes ☐ No

If you have answered No to any of the previous questions in this section above, please give details here:

G8. Please provide details on the risk management procedures for avoiding and mitigating fraud/theft against the company and its customers (eg encryption, passwords, testing and other message authentication, call back, contractual disclaimers):

*Please provide a copy of your procedures manual

G9. Can you confirm the company adheres to the following best practices and minimum security standards?

(a) All electronic payments and sensitive data (including bank/credit card details) are encrypted? ☐ Yes ☐ No

(b) Payments to customers are only made to customer bank accounts as recorded on the company's systems? ☐ Yes ☐ No

(c) Prior to amending personal details (including bank account details) in your records, secondary confirmation is obtained from customers via a source different from the original communication and evidential proof of such changes is obtained? ☐ Yes ☐ No

(d) Customers can only access their accounts on your systems via a password? ☐ Yes ☐ No

If NO to any of the above, please detail below along with mitigating comments:

Section H: Cyber 360 Liability and Loss Module

If you require coverage under Cyber Liability and Loss , please complete the following questions:

H1. (a) How many personally identifiable information (PII) records or unique consumer records does the company currently hold (including employees)? ☐ Yes ☐ No

(b) Does the company hold or process any of the following types of sensitive data? ☐ Yes ☐ No

Financial Information (including credit / debit card records)

Medical information

Identity Information (including NI number or passport details)

Names, addresses, telephone numbers

H2. Can you confirm the company adheres to the following best practices and minimum security standards? ☐ Yes ☐ No

(a) Have a dedicated individual responsible for information security and privacy. ☐ Yes ☐ No

(b) Have a written incident response plan. ☐ Yes ☐ No

(c) Perform background checks on all employees and contractors with access to sensitive data. ☐ Yes ☐ No

(d) Have restricted access to sensitive data (including physical records). ☐ Yes ☐ No

(e) Have a process to delete systems access within 48 hours after employee termination. ☐ Yes ☐ No

(f) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training. ☐ Yes ☐ No

(g) Only use operating systems that continue to be supported by the original provider. ☐ Yes ☐ No

(h) You do not use any software or hardware that is no longer supported or is considered “end-of-life” (EOL) by the manufacturers. ☐ Yes ☐ No

(i) You use anti-virus, anti-spyware and anti-malware software and update them regularly. ☐ Yes ☐ No

(j) You use firewalls and other security applications between the internet and sensitive data. ☐ Yes ☐ No

(k) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored. ☐ Yes ☐ No

(l) You ensure all sensitive data on your system and removable media is encrypted. ☐ Yes ☐ No

(m) You ensure sensitive data is permanently removed (e.g. physical destruction not merely deleting) from hard drives and other storage media and paper records are shredded or confidentially disposed of. ☐ Yes ☐ No

MARKEL

If NO to any of the previous questions in this section, please detail below along with mitigating comments:

H3. (a) Do you have a disaster recovery plan (DRP) and/or business continuity plan (BCP) in place? ☐ Yes ☐ No

(b) In your DRP / BCP, how long would it take for you to be fully operational again following an incident? ☐ Yes ☐ No

(c) How often do you test your DRP / BCP? ☐ Yes ☐ No

H4. Please provide details of your Critical Service Providers for the following services:
(or check box if it is managed and operated in-house)

Service	Critical Service Providers	In-House
(a) Internet service provider		☐
(b) Cloud / hosting / data centre provider		☐
(c) Payment processing		☐
(d) Data or information processing (such as marketing or payroll)		☐
(e) Offsite archiving, backup and storage		☐
(f) Any other critical service providers? (list below)		

MARKEL

H5. Do you typically require such critical service providers to:

(a) Demonstrate adequacy of their IT security and risk management procedures. Is this audited regularly? ☐ Yes ☐ No

(b) Procure and evidence relevant insurance for the services they provide to you ☐ Yes ☐ No

(c) Indemnify you contractually in respect of their errors or negligence (including data breach and system downtime)? ☐ Yes ☐ No

Please provide further details on these controls:

H6. How often is vendor access rights reviewed and updated?

☐ Monthly ☐ Quarterly ☐ Annually ☐ Other

H7. How is vendor access monitored on your network?

H8. Do you have the following email controls and authentication protocols:

☐ SPF ☐ DKIM ☐ DMARC ☐ Sandboxing ☐ Attachment/URL Filtering External Tagging

H9. Do you use O365 in your organisation?

☐ Yes. Have the following been implemented:

☐ MFA ☐ ATP ☐ Macros disabled by default

☐ No. Which product do you use for email monitoring (e.g. Proofpoint)

H10. Do all administrative/privileged accounts have unique credentials? ☐ Yes ☐ No

H11. Do you allow local admin rights on workstations? ☐ Yes ☐ No

H12. Do administrative/privileged accounts enforce MFA and/or use a privilege access management (PAM) tool (e.g. CyberArk)? ☐ Yes ☐ No

Which PAM product(s) do you use:

MARKEL

H13. Do you use an endpoint protection (EPP) product? ☐ Yes ☐ No

If so, which product(s):

H14. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of: ☐ Yes ☐ No

☐ Servers ☐ Endpoints

If so, which product(s):

If the EDR tool offers AI/automated rules-based enforcement, has this been enabled? ☐ Yes ☐ No ☐ N/A

H15. Does all remote access to your network and corporate email require multifactor authentication (MFA)? ☐ Yes ☐ No

H16. Have you disabled remote desktop protocol (RDP)? ☐ Yes ☐ No

If No, have you implemented the following: ☐ VPN ☐ MFA ☐ RDP Honeypots

H17. Do you operate a SIEM monitored 24/7/365 by an internal SOC or MSSP? ☐ Yes ☐ No

H18. Does your incident response plan (IRP) specifically address ransomware scenarios? ☐ Yes ☐ No

H19. How frequently do you back up critical data?

☐ Daily ☐ Weekly ☐ Monthly ☐ Other

H20. Do you keep a copy of your critical backups offline and inaccessible from your network? ☐ Yes ☐ No

H21. Which of the following are used to store backups?

☐ Cloud ☐ Secondary data centre ☐ Offline ☐ Within a separate network segment

H22. Have the following been implemented to secure your backup environment? ☐ Yes ☐ No

☐ Segmentation ☐ Encryption ☐ MFA ☐ Vaulted Credentials

H23. Do you use any commercial backup solutions (e.g. Commvault)? ☐ Yes ☐ No

Which product(s) do you use:

H24. Does your backup strategy include the use of immutable technologies? ☐ Yes ☐ No

H25. Is the integrity of these backups and your recovery plans regularly tested (annually) ☐ Yes ☐ No

H26. In what time frame do you install critical and high severity patches across your enterprise?

☐ 0-3 days ☐ 3-7 days ☐ >7 days ☐ >14 days ☐ >30 days ☐ 30-60 days

MARKEL

H27. What % of the enterprise is covered by your scheduled vulnerability scans? ☐ Yes ☐ No

If NO to any of the above, please detail below along with mitigating comments:

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):

H28. Can you confirm the applicant adheres to the following best practices to mitigate Cyber Crime & Social Engineering:

(a) Does the applicant provide mandatory regular training on social engineering, phishing, to all employees that release company or client assets? ☐ Yes ☐ No

(b) Prior to transferring funds to an account not previously used (new payee or changing payee accounts). Do verify the new account details with the recipient using a method of authentication distinct from the original request method? ☐ Yes ☐ No

(c) Is senior management approval always required before the change or new payee is processed, such approval being given after review of the underlying request and the record of its verification? ☐ Yes ☐ No

(d) Do you have dual controls in place so that at least two people are required to process financial transactions? ☐ Yes ☐ No

(e) Is the first payment to a new supplier bank account always capped and confirmation of receipt always obtained before any further payment are made to that account? ☐ Yes ☐ No

Section I: Claims History

i1. After having made full enquiries, including of all directors, partners and principals, can you confirm that:

(a) No claims (successful or otherwise) have been made against or have been threatened to made against:

(i) the company or any of its predecessors in respect to any negligence, breach of duty of care, infringement of any intellectual property right, libel or slander, dishonesty of any employee or to any other act, error or omission that has or might have given rise to a claim? ☐ Yes ☐ No

(ii) any director, partner or officer in respect to any wrongful act committed by them whilst acting in such capacity? ☐ Yes ☐ No

(b) In the last 5 years the company or any director/employee has not been subject to any regulatory investigation? ☐ Yes ☐ No

(c) In the past 5 years, has the company or any director/employee applying for this insurance been involved in any litigation or proceedings related to employment including, but not limited to, wrongful dismissal? ☐ Yes ☐ No

(d) The company has not suffered from any attempt, successful or otherwise:

(i) to steal any money, financial instruments or any other asset that it either owns or for which it is legally responsible. ☐ Yes ☐ No

(ii) of extortion against it by a threat to commit a theft, cyber-attack or other malicious or criminal event. ☐ Yes ☐ No

(e) The company has not received complaints, whether oral or in writing, regarding its Fiduciary or Benefit plan fees and expenses or the performance of plan investments, defined contribution plan fees or investments? ☐ Yes ☐ No

(f) The company has not received complaints, whether oral or in writing, regarding its services performed, products or solutions sold or provided, or advice given? ☐ Yes ☐ No

(g) The company has not been adversely affected by or suffered any loss from any:

(i) privacy breach, virus, distributed denial of service (DDOS), telephone phreaking or hacking incident? ☐ Yes ☐ No

(ii) unforeseen down time to its website or IT network of more than 5 hours? ☐ Yes ☐ No

(h) You are not aware of any circumstance or problem that might in the future give rise to a claim against or a loss for the company or any of its directors, officers or partners that is covered under the proposed insurance policy? ☐ Yes ☐ No

If NO to any of the above, please provide full details:

MARKEL

Section J: Declarations

I the undersigned hereby confirm that I am duly authorised and do give consent to the use of information as set out above.

I also hereby declare that I am authorised to complete this proposal on behalf of the company. I undertake to inform insurers of any material alteration or addition to these statements or particulars which occurs before the

commencement of the period of insurance. It is hereby acknowledged and agreed that the terms conditions limitations and exclusions of the policy may be subject to alteration at any time prior to the commencement of the period of insurance should any such material alterations or additions arise. Signing of this proposal does not bind insurers to offer nor the applicant to accept insurance.

Any material change in Insurers exposure must be reported prior to coverage applying.

NOTE: The signatory must be a director, senior officer, or a partner of the company.

Signature:	
Name:	
Company Position:	
Agent/Broker Contact Details:	
Date:	

Section K: Your Data

Markel are committed to protecting your privacy. Insurance involves the use and disclosure of your personal data to various insurance participants such as intermediaries, insurers and reinsurers. If you would like to know how Markel deals with any personal data you have provided us, please contact your Agent or Broker who will provide you with our contact details. Alternatively, please visit our privacy page at: www.markel.com/privacy-policy

Markel Cyber 360 Canada
Guardian 360 Pre-Breach Services

Did you know eligible policyholders can be granted access to one of the following Guardian 360 offering alongside their pre-breach onboarding call and Black Kite access; each includes a curated menu of cyber and privacy services, with policyholders able to select one preferred service. Speak to your broker for more information.

Guardian 360 Core

Breach partners may provide updates on Privacy, Cyber and AI, or an initial cyber risk consultation or contract review, including:

1. Weekly privacy updates plus quarterly Privacy, Cyber & AI roundtables with industry experts
2. High-level review of cybersecurity governance, with regulatory guidance and identification of key risks
3. Review of up to two critical contracts with insights on potential risks

Guardian 360 Plus

Breach partners may provide cyber risk assessments, tabletop exercises or contract reviews, including:

1. Assessment or development of an incident response plan, with identification of regulatory gaps
2. A virtual one-hour tabletop exercise with key stakeholders
3. Customized checklist mapping relevant federal and provincial cyber regulations
4. Review of up to five critical contracts with insights on potential risks

Guardian 360 Pro

Breach partners may offer policy or contract reviews, tabletop exercises, and regulatory checklists, including:

1. Review of up to two key policies, with expert recommendations for compliance and best practices
2. A tailored two-hour tabletop exercise followed by a debrief to strengthen preparedness.
3. Customized checklist outlining applicable federal and provincial cyber regulations
4. Review of up to five critical contracts, offering insight into potential risks and recommended clause enhancements to support compliance and resilience

Guardian 360 Ultra

Breach partners may provide a full cyber readiness assessment, incident response plan drafting, custom tabletop exercises, regulatory gap analyses, board/executive training or vendor management consultancy, as detailed below:

1. Full review of cyber policies, procedures, and contracts, with stakeholder interviews to assess preparedness
2. A three-hour immersive tabletop exercise with real-time feedback, followed by key takeaways and an action plan
3. A regulatory compliance review: expert gap analysis of your alignment with applicable cyber laws and regulations
4. Customized cyber risk training for executives and boards, covering legal obligations and real-world case studies
5. Vendor management guidance with risk assessment templates and standard cyber contract clauses for ongoing resilience.

Access is subject to terms and conditions and will be agreed on a policy by policy basis.