

SEAL : Cyber Risk Assessment (CRA) Report

Firm ID: d2a295e7

Username: ea3e8341

Status: Certified

Total Score: 2.5

Assessor Score :

System Score: 1.19

Responsive Score: 5

Submission Date		Artifacts EPA?	Yes
Review Date	Sep 08, 2025	Artifacts EPA	Yes
Date of Audit	Sep 08, 2025 11:33 AM	Date of Artifacts deletion under EPA	Sep 11, 2025 11:33 AM
Certification Date	Sep 08, 2025 11:33 AM		

Table of Contents

1. SEAL Assessment Form
2. Assessor Notes
3. Artifacts

List of questions and answers received from law firms as part of SEAL Process.

Section: Policy

1. List all information security related policies in force in your organization

Policy / Standard / Plan Type	Last Reviewed	Last Updated On	Socialized with	Upload Policy
Acceptable use or Code of Conduct/Ethics Policy	01 Jul 2025	21 Jul 2025	Everyone	1.ACCEPTABLE_USE_POLICY_1_.docx

2. List other organizations that you have shared client information with.

Name	Purpose	Level of Access
Apex Law Associates	Contract drafting & legal review	Read-only (client files)

3. List all information security standards that your firm follows OR has achieved certification in:

Standard	Compliance Status
COBIT	Certified

1. If you follow any other standard, please provide details:

N/A

4. Do you have information security officer(s)?

Yes

1. Add Evidence

- N/A

2. Are they certified or trained in information security?

Yes

3. List training/certification(s):

Cissp

5. Have you retained a third party service provider to assist with your firm's information security?

Yes

1. Upload evidence from your third party (e.g. reports, tests, etc):

- N/A

2. List information security services provided to your firm by third parties:

- Conduct risk assessment
- Periodic review of security policies
- Conduct penetration testing
- Review incidence response plan
- Conduct vulnerability assessment

6. Do you have an insurance policy that covers cyber risk and protects against losses resulting from breaches of information?

Yes

1. Add Evidence

- N/A

2. List all providers:

Provider	Amount Covered	Date of Expiry
Canadian Lawyers Association	100.00	30 Jun 2026

3. Is the client named as additional insured on this policy?

Yes

4. Select all coverages that apply:

- Defamation
- Cyber theft
- Data loss
- Data destruction
- Denial of service
- Reputational risk
- Failure to safeguard data
- Damage to business
- Damage to customers
- Damage to third parties
- Post incidence public relations expenses
- Investigative expenses
- Standard insurance offerings
- Security liability
- Privacy liability
- Multimedia liability
- Privacy regulatory defence and penalties
- Privacy breach response costs, customer notification expenses and customer support and credit monitoring
- Network asset protection
- Cyber extortion
- Cyber terrorism
- Loss of digital assets

7. Where is client information stored?

- Cloud
- On premises
- File room
- Storage vendor
- Colocated
- Removable storage
- Off-site

1. Add Evidence

- N/A

8. If you use the services of a cloud provider to store client information, please complete the following:

Provider	Service Name	Encrypted (In Flight)	Encrypted (At rest)	Location of Data (Country)
Google Cloud Platform	Google Cloud Storage	Yes	Yes	Canada

9. Do you conduct security background checks on personnel?

Yes

1. Add Evidence

- N/A

2. On whom do you conduct background checks?

- All current personnel
- New personnel hired by your firm directly

- New personnel hired through third parties or agencies
- All vendor supplied personnel
- All non lawyer staff
- All non paralegal staff

10. For personnel that have access to client information, who is required to sign a confidentiality agreement?

- Lawyers
- Contractors
- Paralegals
- Vendors
- Non-lawyer staff

1. Add Evidence

- N/A

11. What is your policy for revoking access for personnel (ie. Contractors, full time, part time employees) who leave the firm (Incl. Resignations, termination, Mat leaves, Long term disability etc.)?

After communicating intent but before end of employment/contract

1. Add Evidence

- N/A

12. What controls do you have for password protection?

- Password required to be changed every 90 days
- Training users on the best practices for password management
- Password complexity required more than 8 char with capital letters and special characters

1. Add Evidence

- N/A

13. Do you have an InfoSec threat model for your organization?

Yes

1. Add Evidence

- N/A

2. Date of last review:

02 sep 2025

14. Do you have a records retention plan?

Yes

1. Add Evidence

- N/A

2. Date of last review:

N/A

15. Do you have an intrusion detection plan?

Yes

1. Add Evidence

- N/A

2. Date of last review:

N/A

3. If tested, date of last tested:

N/A

16. Do you have an incident response plan?

Yes

1. Upload

- N/A

2. Date of last internal review:

N/A

3. Date of last external review:

N/A

17. Provide most recent date for each of the following activities:

Network Discovery	02 Sep 2025	-
Penetration Testing	02 Sep 2025	-
Vulnerability Assessment	02 Sep 2025	-
Hardware Refresh	02 Sep 2025	-
Hardware Inventory	02 Sep 2025	-

18. Do you have an access to a Computer Security Incident Response Team (CSIRT)?

No

1. Add Evidence

• N/A

2. CSIRT Team is:

N/A

3. Availability:

N/A

4. Access:

19. What controls do you have to prevent unauthorized access to file rooms?

- Access to select personnel only
- Visitor log
- Specialised third party access controls
- Monitoring (video, motion sensors etc.)
- Physical controls (locks, keypad access etc.)

1. Add Evidence

• N/A

20. What controls do you have to prevent unauthorized access to server rooms?

- Access to select personnel only
- Monitoring
- Specialised third party controls
- Physical controls

1. Add Evidence

• N/A

21. What controls do you have to prevent unauthorized access to conference calls?

- Announcing user name when joined
- Beeping user name when joined
- Ability to check users on the call
- Ability to prevent recording by attendees
- Access using passcode

1. Add Evidence

• N/A

22. What controls do you have to prevent unauthorized access to telephone conversations?

- Encrypted communication
- Restricted access to PBX/VoIP servers
- Restricted call forwarding
- Voice mail password strength
- Call Recording with system announcement
- Conferencing with system announcement

1. Add Evidence

- N/A

23. What controls do you have to prevent access to printers? (i.e.: unauthorized printing, unauthorized access to printer memory, unauthorized access to printed material, etc.)

- Scan to self
- Scan to others
- Scan to external emails restricted
- Access controlled

1. Add Evidence

- N/A

24. What controls do you have to prevent unauthorized data transfer?

- DVD/CD copying restricted
- Use of personal cloud storage restricted
- Use of external VPN restricted
- Encryption enforced on USB/external hard drives
- System monitoring

1. Add Evidence

- N/A

25. What controls do you have to prevent unauthorized access to a lost device with client information?

- Password protection
- Encrypted content
- Auto wiping on multiple failed attempts
- Remote wiping
- Ability to disable access remotely

1. Add Evidence

- N/A

26. What do you do to ensure that your personnel can identify confidential information?

- Testing
- Published guideline
- Published tips
- Regular training
- Simulation

1. Add Evidence

- N/A

27. How do you ensure that your personnel is familiar with and trained on your Information security policies and procedures?

- Training
- Reminders
- Seminars
- Instructional videos
- In person training
- Tip sheets

1. Provide evidence that such training occurs on a regular basis:

- N/A

28. Do you provide security training to personnel with elevated/broad access (i.e. System administrators, Office administrators etc)?

No

1. Add Evidence

- N/A

2. How do you test the preparedness of users with elevated access?

Section : Technology

30. LEGAL APPLICATIONS

Yes

30.1 SERVER

Vendor	Platform	Version	Service Pack/Update/Build	Vendor Supported
Redhat	Linux	7.9	4	Yes

30.2 CLIENT

Vendor	Platform	Version	Service Pack/Update/Build	Vendor Supported
Drupal	Redhat Linux	7	3	Yes

Assessor Notes:

- Law firm declined to upload document without an NDA.
- Conducted Audit via Webex and Phone.
- Verified Policies and evidence for references.
- Infosec Training is provided via a third party system that hasn't been reviewed for currency for 3 years.
- Penetration report reviewed. Remediation is underway. Remediation report not available.
- Incidence response plan: Communicated only to IT staff

Artifacts Reviewed:

- Incidence Response Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Records Retention Policy
- Acceptable Use Policy
- Privacy Policy
- ISO Certification
- Penetration Test Report
- Incidence Response Plan
- Evidence of:
- Evidence of:
 - Network Discovery
 - Penetration Testing
 - Vulnerability Assessment
 - Hardware Refresh
 - Hardware Inventory
 - Software Inventory
 - CSIRT Team Access
 - Background checks
 - Confidentiality Agreement (one)
 - User Training – Schedule and delivery method.
- Intrusion Detection Plan