SEAL : Cyber Risk Assessment (CRA) Report

Firm ID: **f619cda9**
Username: 2fc1ded1
Status: **Pre Assessment Request**
Total Score: 0
Assessor Score :
System Score:
Responsive Score: 5.0

Submission Date		**Artifacts EPA?**	Yes
Review Date	N/A	**Artifacts EPA**	Yes
Date of Audit		**Date of Artifacts deletion under EPA**	N/A
Certification Date	N/A		

Table of Contents

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	01 Jul 2025	Everyone	1. Acceptable_Use_Policy_Evidence.pdf
Access control Policy	01 Jul 2025	01 Jul 2025	Everyone	1. Access_Control_Policy_Evidence.pdf
Disaster Recovery	01 Jul 2025	01 Jul 2025	Everyone	1. Disaster_Recovery_Evidence.pdf
Business Continuity	01 Jul 2025	01 Jul 2025	Everyone	1. Business_Continuity_Evidence.pdf
Breach notification	01 Jul 2025	01 Jul 2025	Everyone	1. Breach_Notification_Policy_Evidence.pdf
Configuration and asset management	01 Jul 2025	01 Jul 2025	Everyone	1. Asset_Management_Policy_Evidence.pdf
Cryptography	01 Jul 2025	01 Jul 2025	Everyone	1. Cryptography_Evidence.pdf
Data/information classification and handling	01 Jul 2025	01 Jul 2025	Everyone	1. Data_Classification_Evidence.pdf
Information transfer	01 Jul 2025	01 Jul 2025	Everyone	1. Information_Transfer_Evidence.pdf
Information Security (Board level)	01 Jul 2025	01 Jul 2025	Everyone	1. Board_InfoSec_Evidence.pdf
Information security incident management	01 Jul 2025	01 Jul 2025	Everyone	1. Incident_Response_Evidence.pdf
Cryptographic key management	01 Jul 2025	01 Jul 2025	Everyone	1. Cryptography_Evidence.pdf
Networking	01 Jul 2025	01 Jul 2025	Everyone	1. Networking_Policy_Evidence.pdf
Patch management	01 Jul 2025	01 Jul 2025	Everyone	1. Patch_Management_Evidence.pdf
Physical and environmental	01 Jul 2025	01 Jul 2025	Everyone	1. Physical_Environment_Evidence.pdf
Secure configuration and handling of user endpoint devices	01 Jul 2025	01 Jul 2025	Everyone	1. Secure_Configuration_Evidence.pdf

Secure development	01 Jul 2025	01 Jul 2025	Everyone	1. Secure_Development_Evidence.pdf
Vulnerability management	01 Jul 2025	01 Jul 2025	Everyone	1. Vulnerability_Management_Evidence.pdf

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

Name	Purpose	Level of Access
PwC Legal	Tax advisory and structuring for client entities	Specific financial data access only (case-by-case basis)
Amazon Web Services (AWS)	Cloud hosting of client databases and internal applications	Full infrastructure-level access (encrypted data only)
Clio	Legal practice management (calendar, billing, case files)	Restricted client matter access

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

Standard	Compliance Status
ISO/IEC 27017	Certified
SOC 2 (Service Organization Control 2)	Certified
NIST CYBER SECURITY FRAMEWORK	Certified
NIST Special Publication 800-53	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
      - InfoSec_Officer_Training_Evidence.pdf
   2. Are they certified or trained in information security?
      Yes
   3. List training/certification(s):
      Cissp, cism, iso/iec 27001, nist cybersecurity framework workshop, giac security essentials (gsec)

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):
      - Third_Party_InfoSec_Services_Evidence.pdf
   2. List information security services provided to your firm by third parties:
      - Periodic review of security policies
      - Conduct penetration testing
      - Conduct vulnerability assessment
      - Information Security Risk Assessment
      - 24/7 Managed Security Operations Center (SOC)

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

1. Add Evidence
   - Cyber_Insurance_Coverage_Evidence.pdf
2. List all providers:

Provider	Amount Covered	Date of Expiry
Canadian Lawyers Association	500.00	31 Jul 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
   - Legal Document Management System

   1. Add Evidence
      - Client_Information_Storage_Evidence.pdf

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)
Microsoft Azure	Azure Blob Storage (Standard tier)	Yes	Yes	Canada

9. **Do you have a records retention plan?**
   Yes

   1. Add Evidence

- Records_Retention_Plan_Evidence.pdf

2. Date of last review:
   01 jul 2025

10. Do you conduct security background checks on personnel?

Yes

1. Add Evidence
   - Personnel_Background_Check_Evidence.pdf
2. On whom do you conduct background checks?
   - All full-time and part-time employees
   - Contractors and consultants with access to client or firm systems
   - Interns and temporary legal staff
   - Administrative and IT support personnel

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

- -Partners and Associates
- Paralegals and Legal Assistants
- IT and Support Staff
- Contract Attorneys and Consultants
- Administrative Staff with access to client schedules or billing records
- Interns and Temporary Employees
- Third-party service providers with data access privileges

1. Add Evidence
   - Confidentiality_Agreement_Evidence.pdf

12. 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
   - Access_Revocation_Policy_Evidence.pdf
   - InfoSec_Training_Module_July2025.pdf
   - User_Access_Audit_Report_Q2_2025.pdf
   - _Deactivation_Log_Export.pdf
   - Offboarding_Checklist_Template.pdf

13. What controls do you have for password protection?

- Minimum length: 12 characters
- Must include upper & lowercase letters, numbers, and symbols
- Passwords cannot contain the username or common dictionary words
- Multi-Factor Authentication (MFA) required for all remote, cloud, and privileged access
- SSO integration with Azure AD to centralize authentication and enforce consistency
- Passwords are hashed and salted using SHA-256 with adaptive key stretching (PBKDF2)
- Passwords expire every 90 days
- Account lockout after 5 failed login attempts
- Forced reset upon first login and after suspected compromise
- Annual secure password training and phishing simulations
- Password manager usage encouraged

1. Add Evidence
   - Password_Protection_Controls_Evidence.pdf

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

Yes

1. Add Evidence
   - InfoSec_Threat_Model_Evidence.pdf

2. Date of last review:
   01 jul 2025

15. Do you have an intrusion detection plan?

Yes

1. Add Evidence
   - Intrusion_Detection_Plan_Evidence.pdf
2. Date of last review:
   01 jul 2025
3. If tested, date of last tested:
   01 jul 2025

16. Do you have an incident response plan?

Yes

1. Upload
   - Incident_Response_Plan_Evidence.pdf
2. Date of last internal review:
   01 jul 2025
3. Date of last external review:
   01 jul 2025

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

Network Discovery	01 Jul 2025	-
Penetration Testing	01 Jul 2025	-
Vulnerability Assessment	01 Jul 2025	-
Hardware Refresh	01 Jul 2025	-
Hardware Inventory	01 Jul 2025	-

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

Yes

1. Add Evidence
   - CSIRT_Access_Evidence.pdf
2. CSIRT Team is:
   Both
3. Availability:
   24x7
4. Access:
   - Pre-approved but triggered on incident
   - Approved and provisioned
   - Approval required at the time of incident
   - Internal CSIRT led by Security Operations Manager
   - External CSIRT contracted via CyberSecure Response Group Inc. (on-call contract, 30 min SLA)

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

- Visitor log
- Specialised third party access controls
- Physical controls (locks, keypad access etc.)
- Restricted Keycard Access
- Surveillance Monitoring
- Visitor Access Protocol
- Security Signage and Entry Logs

- Environmental Safeguards
- Audit and Compliance

1. Add Evidence
    - File_Room_Access_Controls_Evidence.pdf

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

- Two-Factor Physical Entry Control
- 24/7 Surveillance
- Environmental and Intrusion Monitoring
- Access Logging and Reviews
- Visitor Access Procedure
- Backup Power and Redundancy

1. Add Evidence
    - Server_Room_Access_Controls_Evidence.pdf

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

- Access Authentication
- Unique Meeting Credentials
- Waiting Room & Lock Features
- Screen Share Restrictions
- Recording Controls
- Monitoring & Logging
- Training & Awareness

1. Add Evidence
    - Conference_Call_Access_Controls_Evidence.pdf

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

- Secure Handset Allocation
- Call Encryption
- Confidentiality Protocols
- Call Recording Controls
- Monitoring and Logging
- Awareness & Policy

1. Add Evidence
    - Telephone_Conversation_Controls_Evidence.pdf

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.)

- Secure Print Release (Follow-Me Printing)
- User Authentication and Logging
- Data Encryption and Erasure
- Physical Safeguards
- Network and Firmware Security
- Monitoring and Compliance

1. Add Evidence
    - Printer_Access_Controls_Evidence.pdf

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

- Data Loss Prevention (DLP) Tools
- USB and Removable Media Restrictions
- Email and File Transfer Restrictions
- Endpoint Protection
- Web Filtering and Proxy Control

- Audit and Compliance

1. Add Evidence
    - Data_Transfer_Prevention_Evidence.pdf

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
- Full-Disk Encryption
- Multi-Factor Authentication (MFA)
- Mobile Device Management (MDM)
- Automatic Lock and Timeout
- Restricted Local Storage
- *Incident Response Protocol
- Logging and Monitoring

1. Add Evidence
    - Lost_Device_Access_Controls_Evidence.pdf

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

- Mandatory Annual Training
- Onboarding Education
- Visual Aids and Guidelines
- *In-Line DLP Alerts
- Phishing Simulations & Awareness Campaigns
- Manager Reinforcement

1. Add Evidence
    - Confidential_Information_Identification_Training.pdf

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

- Annual Mandatory InfoSec Training
- Quarterly Awareness Refreshers
- Policy Acknowledgment Tracking
- New Hire Orientation
- Department-Specific Training
- Audit and Metrics

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

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

Yes

1. Add Evidence
    - Elevated_Access_Security_Training_Evidence.pdf
2. How do you test the preparedness of users with elevated access?
    - Specialized Privileged User Training
    - Access Awareness Onboarding
    - Simulated Attack Exercises
    - Peer Review & Change Validation
    - Audit Trail and SIEM Monitoring
    - Compliance Testing

Section : Technology

30. LEGAL APPLICATIONS

Yes

30.1 SERVER

Vendor	Platform	Version	Service Pack/Update/Build	Vendor Supported
Microsoft	SQL	2017	RTM-GDR	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