

## SEAL Methodology

Version 1.2

Last updated: March 31, 2024

Author: Peter Davis, CISSP, CISA, CISM, CGEIT, COBIT Certified Assessor, CFRA, ISO Certified Assessor.

Owner : Rajneesh Chhabra, CISSP, CISA, PLDA (Harvard Univ), ACSC (Stanford Univ.)

Contributor : Jolie Lin, Sr. Counsel

Replaces: 1.0

## Table of Contents

1.	Purpose .....	5
2.	Introduction .....	5
3.	CRA and PANEL .....	5
4.	Audience .....	7
5.	Obligations .....	8
6.	Third-Party Risks .....	9
7.	SEAL Components .....	10
7.1	Cyber Risk Assessment (CRA) Domain.....	12
7.1.1	<i>List all information security related policies in force at your law firm.</i> .....	12
7.1.2	<i>List other firms that you have shared information with (such as eDiscovery firms, process servers, legal process outsourcers, consulting firms, other law firms etc.).</i> .....	13
7.1.3	<i>List all information security standards that your firm follows OR has achieved certification in.....</i>	14
7.1.4	<i>Do you have information security officer(s)? Are they certified or trained in information security?</i> .....	15
7.1.5	<i>Have you retained a third-party service provider to assist with your firm's information security?..</i>	16
7.1.6	<i>List information security services provided to your firm by third parties.</i> .....	17
7.1.7	<i>Do you have an insurance policy that covers cyber-risk and protects against losses resulting from breaches of information?</i> .....	18
7.1.8	<i>If you use the services of a cloud provider to store bank information, please provide it?</i> .....	19
7.1.9	<i>Where is client information stored?</i> .....	20
7.1.10	<i>When do you revoke access for terminated personnel (i.e., contractors, lawyers, vendors, non-lawyers)?</i> .....	21
7.1.11	<i>What controls do you have to prevent unauthorized access to file rooms?</i> .....	22
7.1.12	<i>Do you conduct security background checks on personnel? On whom do you conduct background checks?</i> .....	23
7.1.13	<i>What controls do you have to prevent unauthorized access to server rooms?</i> .....	24
7.1.14	<i>For personnel that have access to client information, who is required to sign a confidentiality agreement?.....</i>	25
7.1.15	<i>Do you have an intrusion detection plan?</i> .....	26

## **SEAL Methodology: Version 1.2**

7.1.16	<i>Do you have an InfoSec threat model for your firm?</i> .....	27
7.1.17	<i>What controls do you have for password protection?</i> .....	28
7.1.18	<i>Do you have an incident response plan?</i> .....	29
7.1.19	<i>Do you have access to a Computer Security Incident Response Team (CSIRT)?</i> .....	30
7.1.20	<i>When do you revoke access for terminated personnel (i.e., contractors, lawyers, vendors, non-lawyers)?</i> 31	
7.1.21	<i>Do you have a records retention plan?</i> .....	32
7.1.22	<i>What controls do you have to prevent unauthorized access to conference calls?</i> .....	33
7.1.23	<i>What controls do you have to prevent unauthorized access to telephone conversations?</i> .....	34
7.1.24	<i>What controls do you have to prevent unauthorized access to fax machines and scanners?</i> .....	35
7.1.25	<i>What controls do you have to prevent unauthorized data transfer?</i> .....	36
7.1.26	<i>What do you do to ensure that your personnel can identify confidential information?</i> .....	37
7.1.27	<i>Do you provide security training to personnel with elevated/broad access (i.e. System administrators, Office administrators etc)?</i> .....	38
7.1.28	<i>How do you ensure that your personnel are familiar with and trained on your Information security policies and procedures?</i> .....	39
7.1.29	Technology.....	40
7.2	Preferred Accredited Network of Law firms (PANEL) Domain.....	40
7.2.1	<i>Does your firm prepare, track and share budgets with us?</i> .....	40
7.2.2	<i>Does your firm have a formal process for developing value-based pricing or alternative fee arrangements (AFAs)?</i> .....	41
7.2.3	<i>Is your firm a customer of Bank or any of our subsidiaries (including any subsidiaries or affiliates)?</i> 42	
7.2.4	<i>How many years has your firm provided legal services to us?</i> .....	43
7.2.5	<i>What is our average annual legal spend with you over the last three years?</i> .....	44
7.2.6	<i>To which department(s) did you provide legal services and who are your main contact(s)?</i> .....	44
7.2.7	<i>Does your firm make referrals to us?</i> .....	45
7.2.8	<i>Aside from routine audit reporting, does your firm provide annual or quarterly reporting to us? ...</i> 46	

## **SEAL Methodology: Version 1.2**

7.2.9	<i>Has your firm represented a party adverse to our firm (including any of our subsidiaries or affiliates) in a matter or a dispute at any time within the last 10 years?</i> .....	47
7.2.10	<i>Would any prior or ongoing engagement prevent your firm from acting for us?</i> .....	48
7.2.11	<i>How do you manage conflict of interest at your firm?</i> .....	49
7.2.12	<i>Is your firm's management led by a majority of women/minority professionals and individuals?</i> ..	50
7.2.13	<i>Does your firm have an annual internal program for regularly tracking diversity within your firm?</i> 50	
7.2.14	<i>Does your firm have any representation goals or targets for diversity?</i> .....	51
7.2.15	<i>Does your firm consider the diversity of staffing on bank matters?</i> .....	52
7.2.16	<i>Do the relationship partner(s) assigned to us self-identify as diverse?</i> .....	53
7.2.17	<i>Does your firm have internal process improvement initiatives?</i> .....	54
7.2.18	<i>Does your firm have bank-facing process improvement initiatives?</i> .....	55
7.2.19	<i>Has your firm conducted process improvement initiatives with our bank?</i> .....	56
7.2.20	<i>Does your firm share innovation best practices with your banks?</i> .....	57
7.2.21	<i>Does your firm use non-standard technology (such as document automation, machine-learning contract review, e-discovery tools etc.) for delivery of legal services?</i> .....	58
7.2.22	<i>Does your firm propose improvements to legal documents and strategy on our matters?</i> .....	59
7.2.23	<i>Does your firm hold "voice of client" sessions with us?</i> .....	60
7.2.24	<i>Does your firm hold post-matter reviews with us?</i> .....	61
7.2.25	<i>Does your firm use legal process outsourcing (LPO) or alternative legal services providers (ALSP)?</i> 62	
7.2.26	<i>Does your firm use alternative internal legal professional sourcing (non-partnership track lawyers; paralegals, etc.)?</i> .....	63
7.2.27	<i>Does your firm use project managers on our matters? If yes, does your firm charge us for the project managers?</i> .....	64
7.2.28	<i>Do you provide free continuing professional development/legal education to us?</i> .....	65
7.2.29	<i>Do you provide clients with secondments of your lawyers?</i> .....	66
7.2.30	<i>Do you provide clients with opportunities for student(s) to spend a rotation with them?</i> .....	67
7.2.31	<i>Do you provide clients with other value-add services?</i> .....	68
8.	Glossary, Initialisms and Acronyms .....	69
9.	References.....	71
4	Classification: Internal	

## 1. Purpose

The Secure Engagement and Assessment of Law firms (SEAL) methodology developed by SecureEngage is a set of processes and procedures used to assess an organization's risk associated with sharing information with external law firms. It is a structure composed of two domains that fit together to address cyber and legal risks. This document describes SEAL's methodology to provide an overview of how the components work together.

Figure 1: SEAL Wheel



This document does not purport to explore all components of the SEAL Wheel; this document describes and contextualizes its two domains: Cyber Risk Assessment (CRA), and Preferred Accredited Network of Law firms (PANEL). This document does not purport to explore all components of the SEAL Wheel.

## 2. Introduction

As the world becomes more complex and interconnected, attempts to disrupt businesses through cyber-attacks have become ever more sophisticated. All organizations, but certainly organizations like Canadian

banks, are more than ever focused on protecting their reputation, their customer and employee PII (Personally Identifiable Information), their proprietary information—essentially all critical assets, including computerized devices and information. But protecting information has become increasingly a challenge. Implementing cybersecurity across a progressively unstructured and decentralized network is one of the most troublesome technology concerns. The risk associated with doing business on digital platforms has never been greater. The media abounds with stories about advanced persistent threats, hijacking, spoofing, command and control botnets, zombies, phishing, spear-phishing, whaling, and malware; that is, virus, worm, Trojan horse, and spyware, that result in data breaches. The list is endless and entirely unpredictable.

Banks in particular, are subject to regulatory frameworks that impose a responsibility to conduct due diligence on their third-party service providers, including law firms, to ensure they are reputable, reliable, and capable of providing the required services. Given the interconnectedness of banks and their outside law firms, these firms have significant potential impact on that bank's regulatory compliance. This is not just an issue of third-parties, the risk extends to fourth- and fifth-parties.

Law firms handle a wide range of data, including confidential and sensitive information, financial data, PII, and intellectual property. A data breach at a law firm can have serious consequences for their client organizations, including reputational damage and legal liability.

It is, therefore, critical that organizations assess and understand the cyber-position of their outside law firms (as third party service providers). Conducting this assessment now forms an essential component of good risk management and compliance.

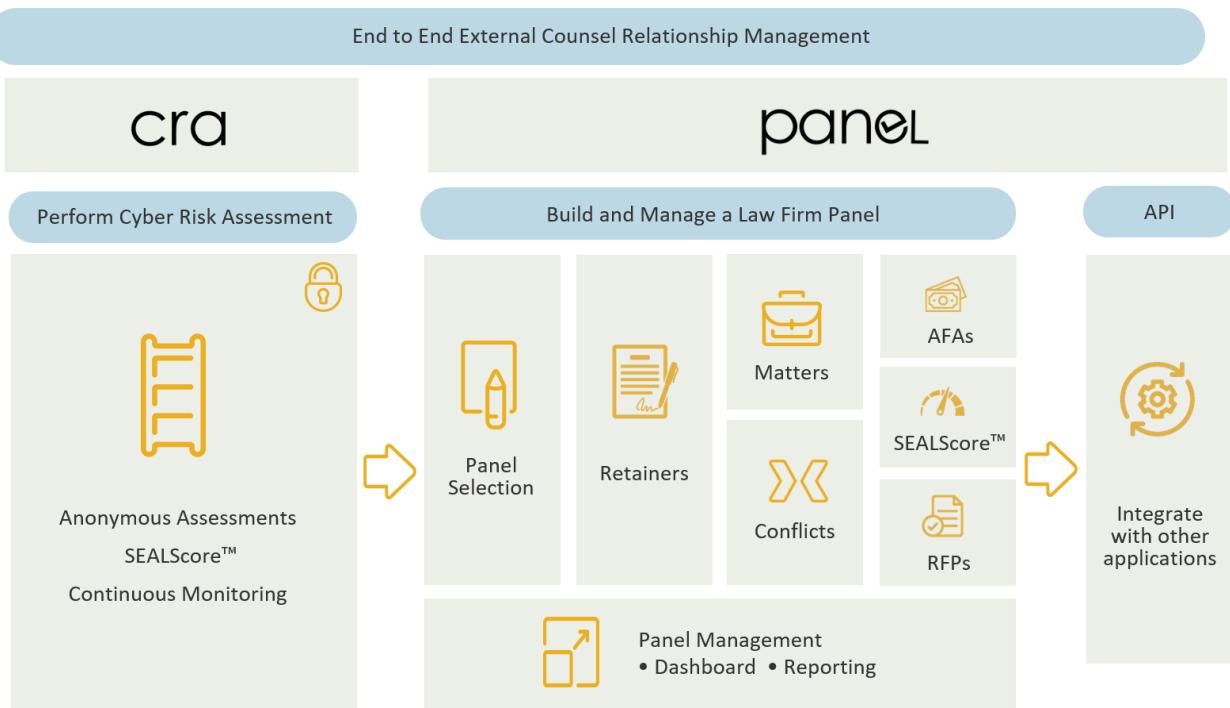
SEAL's objective is to foster effective communication, collaboration, and accountability between an organization and its outside law firms. The assessments and ongoing reviews help establish and maintain a strong working relationship, define roles and responsibilities, address any concerns or issues, and ensure mutual understanding of expectations.

### **3. CRA and PANEL**

Secure Engage developed the SEAL methodology comprised of the Cyber Risk Assessment (CRA) and Preferred Accredited Network of Law firms (PANEL) domains to increase the capability and capacity of organizations to engage a consistent panel of law firms and manage the risk associated with their third-party providers of legal services.

Figure 2 depicts the two domains of SEAL. The remainder of this document will provide the SEAL ontology and decompose the components of the domains.

Figure 2: SEAL Domains



The CRA domain leverages existing guidance, including OSFI B-10, OSFI B-13, Center for Internet Security Critical Security Controls 18, and ISO/IEC 27001:2022. SEAL itself was designed and developed with security that not only meets but exceeds industry best practices.

The PANEL domain provides a single-decision support system for weeding out low-performing relationships and rewarding high-performing ones. PANEL also leverages good practice for legal practice management, law society regulations and guidance, and regulatory guidelines for managing the risk associated with third-party service providers.

Section 9 lists documents used in the preparation of this document.

The SEAL platform achieves two objectives: (1) create a trusted, secure platform where both assessors and law firms can confidently exchange sensitive information, and (2) automate an objective assessment, including scoring, while allowing some ability to add subjective evaluations.

SEAL automatically learns from responses and assessments and adapts to the changing security assessment landscape.

## 4. Audience

Secure Engage developed this document to assist interested stakeholders, such as banks, law firms, and regulators, in understanding the key components of SEAL and how the components work together to address cyber and legal risks.

Readers may read the entire document or those sections of interest.

Secure Engage used the following principles to develop the SEAL methodology:

1. Focus on the business.

2. Deliver value and quality to stakeholders.
3. Establish governance for and management of third-party law firm risk.
4. Comply with relevant legal and regulatory requirements.
5. Provide timely and accurate information on performance.
6. Evaluate current and future threats.
7. Promote continuous improvement.
8. Adopt a risk-based approach.
9. Concentrate on critical business relationships.
10. Foster a risk-positive culture.

For every question, SEAL provides additional control objectives aligned with these principles. See Section 6 for more details.

## 5. Obligations

Every organization has obligations to its stakeholders. Stakeholders may include:

- **Customers:** Expect their information to be protected—in the case of banks, customers expect their bank to protect their information when they use services such as deposits, loans, credit cards, and investment products.
- **Shareholders:** Expect organizations to reduce financial losses from cyber and legal risks.
- **Employees:** Expect the organizations not to engage in activities that may impact their job security and growth opportunities.
- **Regulators and government agencies:** Expect organizations under their oversight jurisdiction to follow regulations and guidelines.
- **Board of Directors:** Expect the organization to make decisions regarding third-party risks that ensure their stability and long-term success.
- **Suppliers and Service Providers:** Expect organizations to apply rigour and fairness in the evaluation of third-party risks of all suppliers and service providers.
- **Creditors:** Expect organizations to protect their financial interests.
- **Communities and Society:** Expect organizations to act responsibly and ethically.
- **Competitors:** Expect organizations to meet their financial obligations in a timely manner

Of course, the specific stakeholders and priorities may vary depending on an organization's size, business model, geographic reach, regulatory regime, and the goods/services it offers.

For Canadian financial institutions, the Office of the Superintendent of Financial Institutions (OSFI) published the [Third-Party Risk Management Guideline \(osfi-bsif.gc.ca\)](https://osfi-bsif.gc.ca) or Guideline B-10 for Federally regulated financial institutions (FRFIs). This Guideline states:

“OSFI expects the FRFI to manage the risks related to all third-party arrangements and emphasizes that the FRFI retains accountability for business activities, functions and services outsourced to a third party.”

The guideline also states:

“Therefore, OSFI expects the FRFI to understand the risk and criticality of all its third-party arrangements ...”

It is worth noting that the Guideline specifically mentions the “use of independent professional consultants”.

### **6. Third-Party Risks**

A corporate legal department often has to outsource work to outside law firms, whether for specialized expertise, cost effectiveness, flexibility, scalability, access to a broader network, confidentiality, objectivity, efficiency, time savings and mitigation of risk. While outsourcing legal work can bring various benefits, an organization needs to carefully evaluate and select law firms based on their reputation, track record, expertise, technology footprint, and alignment with the organization’s values and objectives.

For financial institutions, OSFI defines third-party risk as:

“the risk to the FRFI due to a third party failing to provide goods, business activities, functions and services, protect data or systems, or otherwise exposing the FRFI to negative outcomes. Third-party risk scenarios could include, but would not be limited to:

- insolvency of the third party;
- operational disruption at the third party due to people, inadequate or failed processes and systems, or from external events (e.g., cyber incidents);
- political, geographic, legal, environmental, or other risks impeding the third party from providing services according to its arrangement with the FRFI;
- insolvency or operational disruption at a subcontractor;
- risks arising from interconnections between multiple third parties and multiple FRFIs;
- corruption of FRFI data or FRFI data breaches; and
- loss of data by the third party.”

Technology and cyber-risks in third-party arrangements present elevated vulnerabilities to any organization. Cyber incidents continue to be identified as the greatest risk to the Canadian financial system. The Bank of Canada’s 2019 Financial System Review points to cyber threats and financial interconnections as vulnerabilities for the Canadian financial system. To mitigate these risks, organizations need to develop appropriate third-party risk management programs to address all third-party relationships, including those with their outside law firms. It is important that organizations conduct due diligence on outside law firms to ensure that they have appropriate controls in place to manage the cybersecurity risks associated with their services.

Overall, organizations need to be aware of the risks (including cybersecurity risks) presented by third-parties and take active steps to reduce those risks. This includes understanding the legal and regulatory framework, implementing third-party risk management procedures and controls, the nature of outsourced work, the law firms doing the work, and staying up-to-date on cybersecurity-related staff notices and bulletins. The use of SEAL aids in meeting third-party risk management obligations, including those specifically applicable to financial institutions.

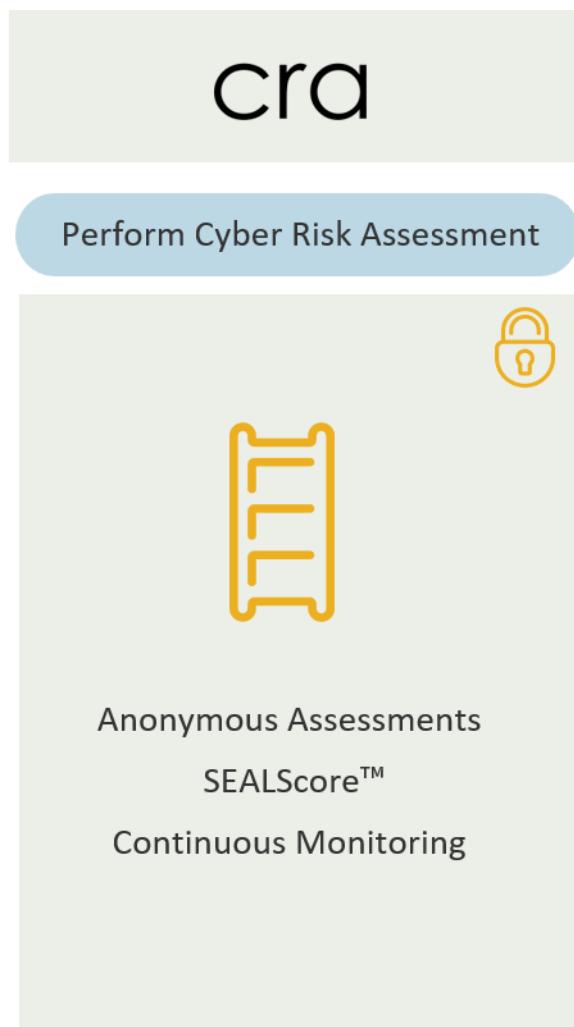
Cyber incidents are unlike traditional operational disruptions in both their dynamism and impact and are not adequately captured by backward-looking proxies, such as historical losses. In addition, there is a

mismatch between the traditional risk-based supervision, which relies on annual risk-rating of a law firm, and the quickly changing nature of cybersecurity risks.

### **7. SEAL Components**

A methodology is a collection of concepts and practices and how they fit or work together to achieve a specific goal or objective. The SEAL methodology has two domains: CRA) and PANEL. The CRA component is based upon COBIT 2019, SOC 2 (domain specific) , ISO/IEC 27002:2022, NIST Cybersecurity Framework, OSFI B-10, and OSFI B-13. The use of a framework like COBIT aids in the definition and measurement of the effectiveness of information technology controls.

Figure 3: Cyber Risk Assessment Domain



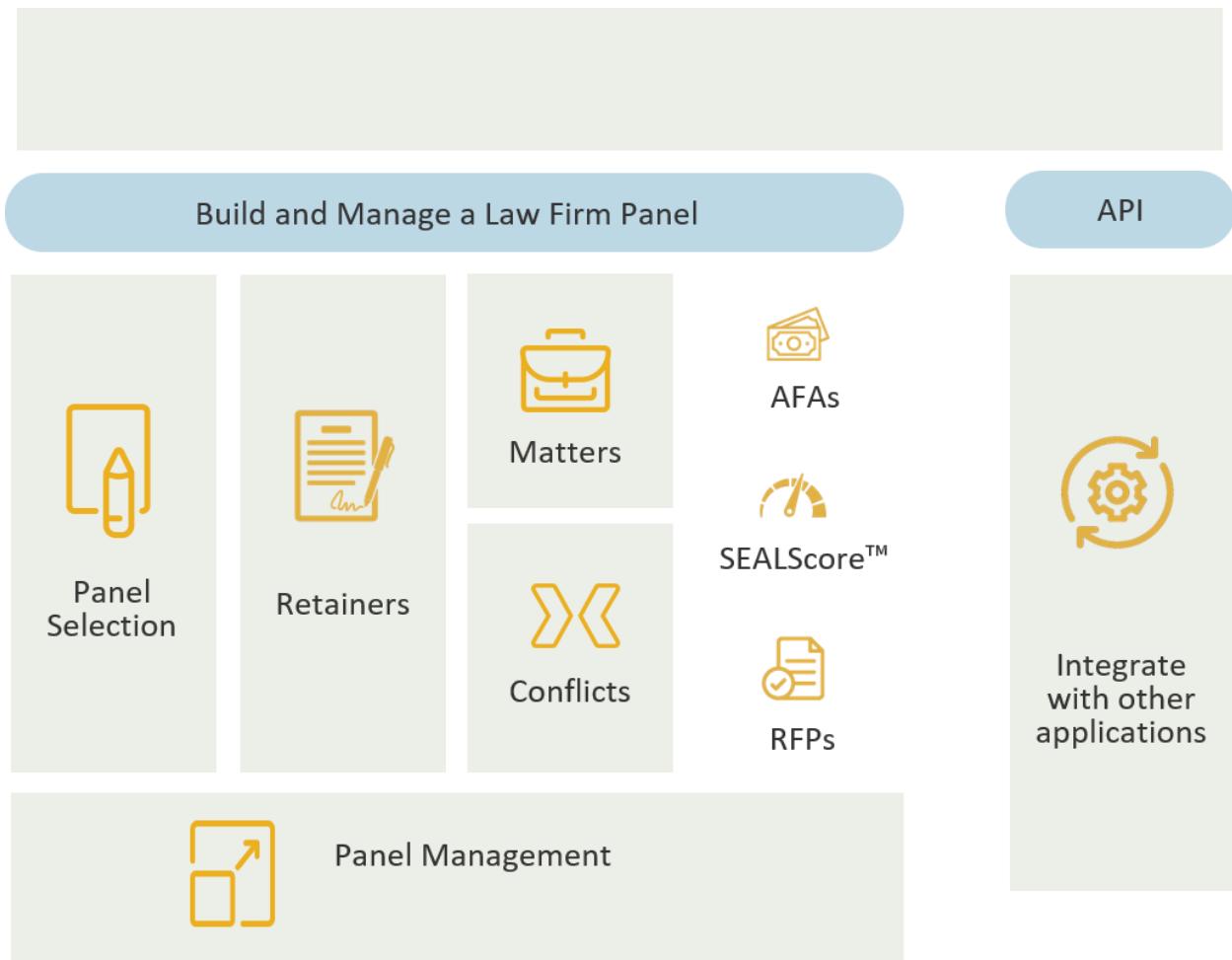
CRA is offered as a sectoral cybersecurity assessment methodology for an organization outsourcing work to outside law firms.

The use of CRA helps to answer risk questions, such as:

## SEAL Methodology: Version 1.2

1. What is the organization's exposure to cybersecurity risk, and what is the potential impact of a breach?
2. What is the likelihood of cyber attacks occurring, and what is the impact they may have on the organization's assets?
3. What is the law firm's risk profile, and how can it be improved?

Figure 4: PANEL Document Structure



The following sub-sections define the detail for the domains, CRA and PANEL. For the domain detail, we will provide the question, objective, the rationale and the expected practices for the requirement. When completing the questionnaires, a law firm may find it helpful to review the documented practices.

### **7.1 Cyber Risk Assessment (CRA) Domain**

#### **7.1.1 List all information security related policies in force at your law firm.**

##### **7.1.1.1 Objective**

To maintain on-going appropriateness, sufficiency, and effectiveness of management guidance and assistance for cyber or information security aligning with business needs and legal, statutory, regulatory, and contractual obligations.

##### **7.1.1.2 Rationale**

It helps the assessor ensure that management direction and support for cyber and information security remain robust, adaptable, and aligned with various requirements, ultimately safeguarding the organization's assets and interest.

##### **7.1.1.3 Practices**

1. Policy Identification: The question aims to identify and document all the information security-related policies that are in place at the law firm. It provides an opportunity for the firm to list and specify each policy separately, ensuring a comprehensive understanding of the policies that govern information security.
2. Policy Compliance: By requesting a list of information security policies, the question seeks to assess the law firm's compliance with established policies and industry best practices. It allows the firm to demonstrate its commitment to following a set of defined policies designed to protect sensitive information and mitigate security risks.
3. Policy Documentation: The question encourages the law firm to maintain well-documented and up-to-date cyber and information security policies. It highlights the importance of having written policies that clearly outline the firm's expectations, procedures, and guidelines for managing cyber and information security.
4. Policy Scope: By listing the information security-related policies, the law firm can communicate the breadth and scope of its policies. It helps identify policies that cover various aspects of information security, such as access control, data protection, incident response, data retention, and employee awareness.
5. Policy Review and Update: Asking for a list of information security policies prompts the law firm to periodically review and update its policies to align with evolving security threats, technological advancements, and regulatory requirements. It encourages the firm to ensure that policies are regularly reviewed, maintained, and kept relevant to the changing information security landscape.
6. Policy Communication and Awareness: By documenting the information security policies, the law firm can assess its efforts in communicating and promoting policy awareness among its personnel. It prompts the firm to consider how effectively the policies are disseminated, understood, and followed by employees, fostering a culture of information security awareness.
7. Policy Integration: The question assists in understanding how information security policies are integrated into the law firm's overall governance structure. It provides insights into how policies are aligned with other legal, regulatory, and compliance frameworks, ensuring a cohesive and comprehensive approach to information security.

**7.1.2 List other firms that you have shared information with (such as eDiscovery firms, process servers, legal process outsourcers, consulting firms, other law firms etc.).**

### **7.1.2.1 Objective**

To assess information security risks, ensure compliance with data protection regulations, manage vendor relationships, maintain client trust, and enhance incident response preparedness.

### **7.1.2.2 Rationale**

It helps the assessor determine whether the firm effectively manages risks, complies with OSFI guidelines, if applicable, complies with privacy regulations, manages vendors, maintains transparency and trust with clients, enhances incident response capabilities, and supports internal audits and assessments for continuous improvement in cybersecurity practices.

### **7.1.2.3 Practices**

1. Risk Management: Sharing information with third-party organizations introduces potential risks to the confidentiality, integrity, and availability of that information. By identifying these organizations, an organization can assess and manage the associated risks more effectively. This helps in implementing appropriate security measures, monitoring the handling of data, and ensuring that confidentiality is maintained throughout the information sharing process.
2. Compliance with Privacy Regulations: Canada has stringent data protection and privacy regulations that govern the sharing of personal information. By identifying the organizations involved in data sharing, an organization can ensure compliance with applicable laws and regulations. This includes obtaining necessary consents, implementing data protection agreements, and verifying that the recipient organizations have appropriate security measures in place.
3. Vendor Management: Understanding the organizations involved in handling information allows for effective vendor management. It helps an organization evaluate the capabilities, reputation, and security practices of these third-party entities. This evaluation is important for selecting trustworthy partners, establishing clear contractual obligations, and ensuring that adequate safeguards are in place to protect client data.
4. Transparency and Trust: Disclosing the organizations with whom information is shared demonstrates transparency. It allows an organization to understand how their data is being handled and the measures in place to protect its confidentiality. This transparency helps build trust between the law firm and the clients, enhancing the reputation and credibility of the firm.
5. Incident Response and Remediation: In the event of a security incident or data breach, knowing the organizations that have access to bank information enables a faster and more coordinated response. An organization can quickly identify the potential impact, notify the relevant parties, and collaborate with the involved organizations to mitigate the incident effectively. This helps in minimizing the damage caused by the incident and maintaining trust.
6. Internal Audits and Assessments: The information gathered about shared organizations can be used for internal audits and assessments. It enables the firm to evaluate its information sharing practices, assess the effectiveness of controls, and identify any gaps or areas for improvement. This proactive approach helps strengthen information security measures and ensures ongoing compliance with policies and regulations.

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

### **7.1.3.1 Objective**

To verify compliance, mitigate risks, enhance reputation and trust, align with regulatory requirements, foster continuous improvement, support vendor and partner selection, and facilitate benchmarking and comparison within the industry.

### **7.1.3.2 Rationale**

It helps the assessor understand whether the firm is following and maintaining certification to information standards that help mitigate the risk of data breaches and other security incidents, protecting their client's reputation and maintaining the trust of clients, partners, and stakeholders.

### **7.1.3.3 Practices**

1. **Compliance Verification:** By listing the information security standards followed or certified by the firm, the question helps verify whether the firm is meeting specific compliance requirements. It allows the assessor to assess whether the firm has implemented the necessary controls, processes, and policies aligned with the selected standards.
2. **Risk Mitigation:** Adhering to established information security standards helps mitigate risks by providing a framework for identifying, assessing, and addressing potential vulnerabilities and threats. Following recognized standards ensures that the firm has implemented industry best practices to protect its information assets and minimize security risks.
3. **Industry Reputation and Trust:** Achieving certification in widely recognized information security standards enhances the law firm's reputation and builds trust among the clients, partners, and stakeholders. It demonstrates the firm's commitment to maintaining robust security practices, protecting sensitive information, and meeting industry benchmarks for information security.
4. **Alignment with Regulatory Requirements:** Certain information security standards are aligned with regulatory requirements specific to industries or jurisdictions. By adhering to these standards, an organization can ensure compliance with relevant laws and regulations governing data protection, privacy, and security. This helps avoid penalties, legal liabilities, and reputational damage resulting from non-compliance.
5. **Continuous Improvement:** Following information security standards supports a culture of continuous improvement. These standards often require organizations to conduct regular assessments, audits, and updates to their security practices. By listing the standards followed or certified, firms can demonstrate their commitment to ongoing improvement and staying up to date with evolving security threats and challenges.
6. **Vendor and Partner Selection:** Listing the information security standards followed or certified by the firm helps potential clients, partners, and vendors evaluate the firm's security posture. It enables them to assess the firm's ability to protect sensitive information and align with their security requirements when considering partnerships or collaborations.
7. **Benchmarking and Comparison:** Knowing the information security standards followed or certified by the firm allows for benchmarking and comparison with industry peers. It helps firms understand how their security practices align with industry norms, identify areas for improvement, and adopt best practices from other organizations that follow similar standards.

### **7.1.4 Do you have information security officer(s)? Are they certified or trained in information security?**

#### **7.1.4.1 Objective**

To establish a clear, authorized, and comprehensible organizational structure with the necessary responsibility, authority, and competence for implementing, operating, and managing information security.

#### **7.1.4.2 Rationale**

It helps the assessor understand whether there is an established, defined, approved, competent, and known structure for cybersecurity that provides the law firm with a proactive and systematic approach to protect the information provided to them by their clients.

#### **7.1.4.3 Practices**

1. Identification of Information Security Officer(s): The question aims to determine whether the firm has designated specific individuals as information security officers. This helps in understanding the organizational structure and responsibilities related to information security management.
2. Qualifications and Certification: By asking whether the information security officers are certified or trained in information security, the questionnaire seeks to assess the level of expertise and knowledge possessed by the individuals responsible for overseeing information security. Certification or training in information security demonstrates a commitment to professional development and a deeper understanding of the subject matter.
3. Competence in Information Security: The questions help evaluate the competency of the information security officers by determining their qualifications and training. Having knowledgeable and skilled individuals in these roles increases the likelihood of effective information security practices, risk management, incident response, and compliance with relevant standards and regulations.
4. Compliance and Best Practices: By verifying the certification or training of information security officers, the question assesses the firm's commitment to compliance with industry best practices and standards in information security management. It indicates a proactive approach to staying abreast of evolving threats, technologies, and regulatory requirements.
5. Leadership and Accountability: Identifying information security officers and their qualifications helps establish clear lines of responsibility and accountability for information security within the firm. It promotes a culture of leadership, ownership, and responsibility for safeguarding sensitive information.
6. Expertise in Information Security Management: The questions provide insights into the level of expertise and knowledge possessed by the information security officers, which is crucial for effective planning, implementation, and management of information security controls, risk assessments, incident response, and overall governance of information security practices.

### **7.1.5 Have you retained a third-party service provider to assist with your firm's information security?**

#### **7.1.5.1 Objective**

To assess the outsourcing of security functions, evaluate vendor management practices, leverage external expertise and resources, conduct risk assessments, ensure compliance and contractual obligations, and enhance security effectiveness and assurance.

#### **7.1.5.2 Rationale**

It helps the assessor ascertain whether the firm has access to specialized expertise, optimizes resource allocation, achieves cost efficiency, enhances scalability and flexibility, receives independent assessments, mitigates risks, meets compliance requirements, and ensures effective vendor management. It allows a firm to leverage external capabilities and support to strengthen their information security practices while focusing on their core business objectives.

Note: For a small firm, one would expect that they use a third-party to help with information security.

#### **7.1.5.3 Practices**

1. Access to Expertise: Engaging a third-party service provider allows the law firm to tap into specialized expertise that may not be available internally. These providers often have a deep understanding of information security best practices, industry standards, and emerging threats. By leveraging their knowledge and experience, a firm can enhance their security capabilities and stay up to date with the evolving threat landscape.
2. Resource Optimization: Information security can be complex and resource-intensive. Outsourcing certain security functions to a third-party provider allows a firm to optimize their resource allocation. It enables the firm to focus on its core competencies while relying on the expertise and dedicated resources of the service provider to manage and support their information security needs effectively.
3. Cost Efficiency: Building and maintaining an in-house information security team can be costly. Engaging a third-party service provider can offer cost advantages by leveraging economies of scale. Service providers typically work with multiple organizations, spreading the costs of their specialized resources and infrastructure across their base. This can result in cost savings for the firm while still receiving high-quality security services.
4. Scalability and Flexibility: Information security needs can vary over time, requiring the firm to scale their capabilities up or down as needed. Third-party service providers offer scalability and flexibility to align with the firm's changing requirements. They can quickly adjust their services to accommodate increased workloads, new projects, or changing security priorities, allowing the firm to adapt more efficiently.
5. Independent Assessments: Engaging a third-party service provider for information security can provide independent assessments and validations of the firm's security practices. These providers often conduct audits, assessments, and penetration testing to evaluate the firm's security posture objectively. The independent perspective and expertise of the service provider can help identify vulnerabilities, gaps, and areas for improvement that may go unnoticed internally.
6. Risk Mitigation: Outsourcing information security functions introduces certain risks, such as data breaches or loss of control over sensitive information. However, the rationale for engaging a third-party provider includes the ability to mitigate these risks. Reputable service providers typically

have robust security measures in place, including advanced threat detection and incident response capabilities. By selecting a trusted provider and ensuring proper contractual agreements, a firm can effectively manage and mitigate potential risks associated with outsourcing.

7. Compliance and Regulatory Requirements: Engaging a third-party service provider for information security can help the firm meet specific compliance and regulatory requirements. Many industry regulations and frameworks require independent assessments or certifications. By working with a service provider that has the necessary certifications and expertise, the firm can ensure compliance with relevant standards and regulations.
8. Vendor Management: Engaging third-party service providers for information security purposes involves proper vendor management practices. This includes conducting due diligence, selecting reputable providers, and establishing clear contractual agreements that address data protection, confidentiality, service levels, and liability. The rationale for this control is to ensure that the firm maintains control over its sensitive information and holds the service provider accountable for meeting security obligations.

### ***7.1.6 List information security services provided to your firm by third parties.***

#### **7.1.6.1 Objective**

To assess vendor assessment and management practices, understand the scope and coverage of security services, evaluate risk assessment and mitigation efforts, ensure compliance and contractual obligations, evaluate vendor performance, and promote continuous improvement in information security.

#### **7.1.6.2 Rationale**

It helps the assessor gain insight into the firm's reliance on external expertise and the effectiveness of its information security program.

#### **7.1.6.3 Practices**

1. Vendor Assessment: The question aims to assess the firm's reliance on third-party vendors for information security services. It seeks to identify the specific services that the firm has outsourced to external providers, such as managed security services, penetration testing, security monitoring, vulnerability assessments, incident response, or security consulting.
2. Vendor Management: Engaging third-party vendors for information security services requires proper vendor management practices. By asking this question, the assessor can evaluate whether the firm has established appropriate vendor management processes, including due diligence, contract negotiations, and ongoing monitoring of the third-party providers' performance and compliance with security requirements.
3. Security Service Coverage: The question helps determine the scope and coverage of information security services provided by third-parties to the firm. It allows the assessor to understand the extent to which the firm relies on external expertise to support its information security needs. This information is valuable for assessing the firm's overall security posture and the effectiveness of its security controls.
4. Risk Assessment and Mitigation: Engaging third-party vendors for information security services introduces certain risks, such as data breaches, service disruptions, or confidentiality breaches. By asking this question, the assessor can assess whether the firm has conducted appropriate risk

assessments and implemented mitigating controls to manage the risks associated with using external providers for security services.

5. Compliance and Contractual Obligations: Depending on the nature of the engagement, there may be specific compliance and contractual obligations associated with the information security services provided by third-party vendors. The objective of this question is to determine whether the firm has considered and addressed these obligations, including contractual provisions related to data protection, confidentiality, liability, and compliance with applicable laws and regulations.
6. Performance Evaluation: Asking about the information security services provided by third parties allows the assessor to evaluate the effectiveness and performance of these external providers. It helps identify the quality of the services rendered, the level of expertise demonstrated, and the extent to which the services meet the firm's requirements and expectations. This information may guide future decision-making when selecting and retaining third-party vendors.
7. Continuous Improvement: The question addresses the firm's approach to continuous improvement in information security. By engaging third-party vendors for specialized security services, the firm can leverage external expertise to identify vulnerabilities, implement best practices, and enhance their security posture. Understanding the information security services provided by third parties allows the assessor to evaluate whether the firm actively seeks opportunities for improvement and collaboration with external experts.

### *7.1.7 Do you have an insurance policy that covers cyber-risk and protects against losses resulting from breaches of information?*

#### 7.1.7.1 Objective

To assess risk mitigation efforts, coverage and protection against cyber-risks, compliance with industry or regulatory requirements, financial resilience, risk assessment and underwriting processes, and incident response and business continuity planning.

#### 7.1.7.2 Rationale

It helps the assessor evaluate the firm's approach to managing financial risks associated with cyber-incidents and their preparedness for potential losses resulting from information breaches or cyberattacks.

#### 7.1.7.3 Practices

1. Risk Mitigation: The question aims to evaluate the firm's risk management approach regarding cyber incidents. Having a dedicated cyber insurance policy demonstrates a proactive stance towards mitigating financial losses associated with data breaches, cyberattacks, or other cyber-incidents. It indicates that the firm has considered the potential financial impact of such events and taken steps to transfer or mitigate the associated risks.
2. Coverage and Protection: By asking about the existence of a cyber insurance policy, the assessor seeks to understand the extent of coverage provided by the policy. This includes assessing whether the policy offers protection against various types of cyber-risks, such as data breaches, network security failures, cyber extortion, business interruption, legal liabilities, and other related financial losses. It helps evaluate whether the firm has taken appropriate measures to safeguard its financial interests in the event of a cyber incident.
3. Compliance and Risk Transfer: Depending on the industry or regulatory requirements, the firm may be obligated to have cyber insurance coverage. The question addresses whether the firm has considered any compliance obligations related to cyber-risk insurance. Additionally, having a

cyber insurance policy can also transfer some of the financial risks associated with cyber-incidents to the insurance provider, reducing the firm's overall exposure to such risks.

4. Financial Resilience: The question aims to assess the firm's financial resilience in the face of cyber incidents. Having a cyber insurance policy provides an added layer of financial protection, which can help the firm cover costs related to incident response, remediation, legal liabilities, regulatory fines, notification and credit monitoring services, public relations, and potential business interruption. It helps evaluate whether the firm has considered the financial implications of cyber incidents and taken steps to mitigate their impact.
5. Risk Assessment and Underwriting: Obtaining a cyber insurance policy often involves a risk assessment and underwriting process. By asking this question, the assessor seeks to understand whether the firm has undergone a risk assessment to determine the appropriate coverage and premiums for the policy. It indicates that the firm has actively engaged with insurance providers to evaluate its cyber-risk profile and obtain tailored coverage based on its specific needs and exposures.
6. Incident Response and Business Continuity: Having a cyber insurance policy can also be an indication that the firm has established incident response and business continuity plans. Insurers often require organizations to have these plans in place to ensure effective incident management and minimize potential losses. The question helps evaluate whether the firm has considered these aspects of cyber-risk management and taken steps to align its insurance coverage with its incident response and business continuity strategies.

### **7.1.8 If you use the services of a cloud provider to store bank information, please provide it?**

#### **7.1.8.1 Objective**

To gather information about the specific providers engaged by the firm, assess risk assessment and due diligence efforts, evaluate compliance with legal and regulatory obligations, understand security and privacy controls implemented by the providers, review vendor management practices, and assess considerations regarding data residency and jurisdiction.

#### **7.1.8.2 Rationale**

It helps the assessor gain insights into the firm's approach to leveraging cloud services for storing information and the measures taken to ensure the security and integrity of that data.

#### **7.1.8.3 Practices**

1. Cloud Service Provider Identification: The question aims to identify the specific cloud service providers utilized by the firm for storing information. It seeks to gather information about the names or identities of the cloud service providers engaged by the firm.
2. Risk Assessment and Due Diligence: The question indirectly addresses the firm's risk assessment and due diligence processes related to cloud service providers. It aims to assess whether the firm has evaluated the security and reliability of the chosen cloud service providers before entrusting them with bank information. This information helps the assessor understand whether the firm has taken appropriate measures to mitigate potential risks associated with using cloud services.
3. Compliance and Legal Obligations: The question evaluates whether the firm considers compliance and legal obligations when selecting cloud service providers. It aims to determine whether the firm ensures that the chosen providers meet the necessary requirements for storing information in accordance with applicable laws, regulations, or industry-specific standards.

4. Security and Privacy Controls: The question indirectly addresses the security and privacy controls implemented by cloud service providers. It aims to gather information about the security measures, data protection practices, and privacy safeguards offered by the chosen providers. This information helps assess the firm's efforts to ensure the confidentiality, integrity, and availability of information stored in the cloud.
5. Vendor Management: The question addresses the firm's vendor management practices concerning cloud service providers. It aims to assess whether the firm has established contractual agreements, service level agreements (SLAs), or other governance mechanisms with the cloud providers to ensure compliance, security, and accountability. This information helps evaluate the firm's oversight and control over the cloud services used.
6. Data Residency and Jurisdiction: The question indirectly addresses the issue of data residency and jurisdiction. It aims to determine whether the firm considers the location where information is stored and whether it aligns with legal and contractual requirements regarding data residency or jurisdiction. This information helps assess the firm's awareness of potential legal and regulatory implications related to data storage in the cloud.

### 7.1.9 *Where is client information stored?*

#### 7.1.9.1 Objective

To create a data inventory, assess data security measures, ensure compliance with legal requirements, conduct risk assessments, establish data governance practices, and support incident response and business continuity planning.

#### 7.1.9.2 Rationale

It helps the assessor gain insight into how the firm manages and protects client information across various storage locations, ensuring data confidentiality, integrity, and availability.

#### 7.1.9.3 Practices

1. Data Inventory: The question aims to identify and assess the locations where client information is stored within the firm's infrastructure. It helps create a data inventory by documenting the various storage locations, which may include on-premises servers, cloud services, data centers, or other storage facilities. This information provides insight into the firm's data management practices and the potential exposure of client information to different environments.
2. Data Security Assessment: By understanding the locations where client information is stored, the assessor can evaluate the security measures and controls implemented to protect the data. Different storage locations may have varying levels of security and associated risks. The question helps assess whether appropriate security measures, such as access controls, encryption, monitoring, and physical security, are in place to safeguard bank information across all storage locations.
3. Compliance and Legal Requirements: Depending on the industry or jurisdiction, there may be specific compliance and legal requirements regarding the storage of client information. The question addresses whether the firm is aware of and adhering to these requirements by storing client information in compliant locations. It helps evaluate the firm's commitment to data privacy and protection, as well as its ability to meet relevant regulatory obligations.
4. Risk Assessment and Mitigation: The question helps identify potential risks associated with storing client information in different locations. By understanding where the data is stored, the assessor

can evaluate the inherent risks, such as physical security vulnerabilities, network risks, or jurisdictional concerns. This information enables the firm to conduct a risk assessment and implement appropriate risk mitigation measures to protect information effectively.

5. Data Governance and Control: Understanding the storage locations of client information is essential for effective data governance and control. The question addresses whether the firm has established proper data governance practices to manage the storage, access, retention, and disposal of client information across different locations. It allows the assessor to assess the firm's ability to maintain data integrity, enforce data protection policies, and ensure regulatory compliance in relation to data storage.
6. Incident Response and Business Continuity: Knowing where client information is stored is crucial for incident response and business continuity planning. In the event of a data breach or other security incidents, it is important to quickly identify the affected storage locations and take appropriate remedial actions. The question helps evaluate whether the firm has incident response plans and business continuity strategies that consider the storage locations of client information.

### **7.1.10 When do you revoke access for terminated personnel (i.e., contractors, lawyers, vendors, non-lawyers)?**

#### **7.1.10.1 Objective**

To ensure that access rights are given exclusively to authorized users, software components and services.

#### **7.1.10.2 Rationale**

It helps the assessor determine whether a firm understands that removing access rights from terminated employees is crucial for preventing unauthorized access, meeting compliance requirements, optimizing resource allocation, reducing costs, protecting data from unauthorized exposure or misuse.

#### **7.1.10.3 Practices**

1. Security and Risk Mitigation: The question aims to assess the firm's practices for ensuring the security of its systems and data by promptly revoking access rights when personnel, such as contractors, lawyers, vendors, or non-lawyers, are terminated. Revoking access helps mitigate the risk of unauthorized access, data breaches, or misuse of information by individuals who no longer have a legitimate need for access.
2. Compliance with Policies and Regulations: By asking about the timing of access revocation, the questionnaire seeks to evaluate the firm's adherence to its internal policies, legal requirements, and industry best practices. Timely revocation of access aligns with data protection regulations, confidentiality agreements, and security standards that govern the handling of sensitive information.
3. Preventing Unauthorized Access: The question intends to assess whether the firm has appropriate procedures in place to remove terminated personnel's access promptly. Revoking access ensures that individuals who are no longer associated with the firm cannot continue to access sensitive data, systems, or resources, thus reducing the risk of unauthorized access and potential malicious activities.
4. Data Loss Prevention: Revoking access rights of terminated personnel helps prevent potential data loss or data leakage incidents. By revoking access promptly, the firm can minimize the risk of confidential or sensitive information being compromised or shared inappropriately.

5. Protecting Intellectual Property: Access revocation ensures that terminated personnel do not retain access to valuable intellectual property, trade secrets, or proprietary information. It helps safeguard the firm's assets and reduces the possibility of unauthorized disclosure or misuse of confidential data.
6. Operational Efficiency: By gathering information about when access is revoked for terminated personnel, the firm can assess the efficiency of its access management processes. This information helps identify areas for improvement in access revocation procedures and streamline the overall offboarding process for departing personnel.

### **7.1.11 What controls do you have to prevent unauthorized access to file rooms?**

#### **7.1.11.1 Objective**

To assess access control measures, physical security practices, compliance with regulatory requirements, risk assessment and mitigation efforts, incident response capabilities, and employee awareness and training programs.

#### **7.1.11.2 Rationale**

It helps the assessor evaluate the firm's physical security posture and its commitment to protecting sensitive information stored in physical file rooms.

#### **7.1.11.3 Practices**

1. Access Control Assessment: The question aims to assess the effectiveness of access controls implemented by the firm to protect server rooms. It seeks to understand whether the firm has established measures to limit and monitor access to server rooms, such as access cards, biometric authentication, key control, security codes, or security personnel. This information helps evaluate the firm's ability to prevent unauthorized individuals from accessing critical IT infrastructure and systems.
2. Physical Security Evaluation: By asking about controls for preventing unauthorized access to server rooms, the assessor can evaluate the firm's physical security practices. This includes assessing the adequacy of physical barriers, such as locked doors, secure entry points, surveillance cameras, or intrusion detection systems. It also encompasses the use of security technologies to detect and deter unauthorized access attempts, such as alarm systems or video monitoring.
3. Compliance and Regulatory Requirements: Depending on the industry or regulatory obligations, there may be specific requirements for securing server rooms and protecting critical IT assets. The question addresses whether the firm has considered these compliance and regulatory requirements and implemented controls accordingly. It helps evaluate the firm's commitment to safeguarding IT infrastructure and meeting legal obligations.
4. Risk Assessment and Mitigation: The question helps identify potential risks associated with unauthorized access to server rooms. By understanding the controls in place, the assessor can evaluate the effectiveness of risk mitigation measures, such as access logs, visitor registration procedures, security audits, or employee training programs. This information allows for assessing the firm's ability to identify vulnerabilities and implement appropriate measures to prevent unauthorized access.
5. Incident Response and Reporting: The question also addresses incident response and reporting capabilities related to unauthorized access to server rooms. By asking about controls, the assessor can assess whether the firm has established procedures to respond to security incidents, such as

reporting breaches, conducting investigations, or implementing corrective actions. It helps evaluate the firm's preparedness to address and mitigate the impact of unauthorized access incidents.

6. Employee Awareness and Training: The question indirectly assesses the firm's employee awareness and training programs regarding physical security and access control. Adequate controls require educating employees on the importance of safeguarding server rooms and the proper use of access control mechanisms. The question provides insight into whether the firm has implemented training programs to educate employees on security protocols, access control procedures, and the risks associated with unauthorized access to server rooms.
7. Business Continuity and Disaster Recovery: Server rooms often house critical IT infrastructure and systems that are essential for business operations. By asking about controls to prevent unauthorized access, the assessor can evaluate the firm's business continuity and disaster recovery strategies. It helps assess whether the firm has implemented appropriate controls to protect the availability and integrity of IT systems and ensure the continuity of business operations.

### *7.1.12 Do you conduct security background checks on personnel? On whom do you conduct background checks?*

#### 7.1.12.1 Objective

To guarantee personnel that handle confidential and financial data meet the necessary qualifications and suitability for their designated roles during the hiring process and throughout their employment.

#### 7.1.12.2 Rationale

It helps the assessor ensure that law firm personnel are eligible and suitable for their roles and responsibilities, and maintain their eligibility and suitability throughout their employment, which is vital for organizational performance of the contract with the client, risk mitigation, compliance, employee satisfaction, and overall success.

#### 7.1.12.3 Practices

1. Security and Risk Mitigation: The question aims to assess the firm's commitment to mitigating security risks by conducting background checks on their personnel. Background checks help identify any potential risks associated with individuals who may have access to sensitive information, systems, or resources. By conducting these checks, the firm can reduce the likelihood of insider threats, unauthorized access, or other security incidents.
2. Compliance with Regulations and Legal Requirements: Background checks may be required or recommended by industry-specific regulations, legal obligations, or contractual agreements. By asking about the firm's practices, the question seeks to assess compliance with relevant regulations and ensure that appropriate measures are taken to protect sensitive information in accordance with legal requirements.
3. Trust and Reputation: Conducting security background checks on personnel demonstrates the firm's commitment to maintaining a secure environment for the bank and stakeholders. By ensuring that individuals who join the firm undergo a screening process, the firm can instill confidence in its ability to protect sensitive information and maintain the trust of the clients.
4. Protection of Confidential and Sensitive Information: Background checks are conducted to identify any potential risks associated with individuals who may have access to confidential or

sensitive information. By conducting these checks, the firm can assess the trustworthiness, integrity, and reliability of personnel, reducing the risk of information breaches, data leaks, or unauthorized disclosures.

5. Screening Process: The question aims to gather information about the scope of personnel subject to security background checks. By identifying the specific roles, positions, or types of individuals who undergo these checks, the firm may ensure that individuals with elevated privileges or access to critical systems undergo a thorough screening process.
6. Risk Mitigation in Personnel Selection: Background checks contribute to informed decision-making during the hiring or onboarding process. By evaluating the background and qualifications of individuals, the firm may make better-informed decisions regarding personnel selection, thereby minimizing the risk of potential security incidents or misconduct.

### **7.1.13 What controls do you have to prevent unauthorized access to server rooms?**

#### **7.1.13.1 Objective**

To assess access control measures, physical security practices, compliance with regulatory requirements, risk assessment and mitigation efforts, incident response capabilities, employee awareness and training programs, and business continuity strategies.

#### **7.1.13.2 Rationale**

It helps the assessor evaluate the firm's physical security posture and its commitment to protecting critical IT infrastructure and systems housed in server rooms.

#### **7.1.13.3 Practices**

1. Access Control Assessment: The question aims to assess the effectiveness of access controls implemented by the firm to protect server rooms. It seeks to understand whether the firm has established measures to limit and monitor access to server rooms, such as access cards, biometric authentication, key control, security codes, or security personnel. This information helps evaluate the firm's ability to prevent unauthorized individuals from accessing critical IT infrastructure and systems.
2. Physical Security Evaluation: By asking about controls for preventing unauthorized access to server rooms, the assessor can evaluate the firm's physical security practices. This includes assessing the adequacy of physical barriers, such as locked doors, secure entry points, surveillance cameras, or intrusion detection systems. It also encompasses the use of security technologies to detect and deter unauthorized access attempts, such as alarm systems or video monitoring.
3. Compliance and Regulatory Requirements: Depending on the industry or regulatory obligations, there may be specific requirements for securing server rooms and protecting critical IT assets. The question addresses whether the firm has considered these compliance and regulatory requirements and implemented controls accordingly. It helps evaluate the firm's commitment to safeguarding IT infrastructure and meeting legal obligations.
4. Risk Assessment and Mitigation: The question helps identify potential risks associated with unauthorized access to server rooms. By understanding the controls in place, the assessor can evaluate the effectiveness of risk mitigation measures, such as access logs, visitor registration procedures, security audits, or employee training programs. This information allows for assessing the firm's ability to identify vulnerabilities and implement appropriate measures to prevent unauthorized access.

5. Incident Response and Reporting: The question also addresses incident response and reporting capabilities related to unauthorized access to server rooms. By asking about controls, the assessor can assess whether the firm has established procedures to respond to security incidents, such as reporting breaches, conducting investigations, or implementing corrective actions. It helps evaluate the firm's preparedness to address and mitigate the impact of unauthorized access incidents.
6. Employee Awareness and Training: The question indirectly assesses the firm's employee awareness and training programs regarding physical security and access control. Adequate controls require educating employees on the importance of safeguarding server rooms and the proper use of access control mechanisms. The question provides insight into whether the firm has implemented training programs to educate employees on security protocols, access control procedures, and the risks associated with unauthorized access to server rooms.
7. Business Continuity and Disaster Recovery: Server rooms often house critical IT infrastructure and systems that are essential for business operations. By asking about controls to prevent unauthorized access, the assessor can evaluate the firm's business continuity and disaster recovery strategies. It helps assess whether the firm has implemented appropriate controls to protect the availability and integrity of IT systems and ensure the continuity of business operations.

### *7.1.14 For personnel that have access to client information, who is required to sign a confidentiality agreement?*

#### 7.1.14.1 Objective

To maintain confidentiality of information accessible by personnel or external parties.

#### 7.1.14.2 Rationale

It helps the assessor determine whether the firm has documentation in place to maintain the confidentiality of information accessible by personnel or external parties, which is crucial for protecting sensitive data, complying with privacy regulations, gaining a competitive edge, fostering trust, preserving intellectual property, and ensuring the privacy and security of the client's stakeholders.

#### 7.1.14.3 Practices

1. Confidentiality and Data Protection: The question aims to assess the firm's commitment to maintaining the confidentiality and protection of client information. By asking about the requirement of confidentiality agreements, the question seeks to ensure that appropriate measures are in place to safeguard sensitive data and prevent unauthorized disclosure or misuse.
2. Compliance with Legal and Ethical Obligations: Confidentiality agreements are often required to fulfill legal and ethical obligations related to client confidentiality. By inquiring about the firm's practice of requiring personnel to sign such agreements, the question seeks to assess compliance with industry-specific regulations, legal requirements, professional standards, and codes of conduct.
3. Protection of Client Trust and Privilege: Confidentiality agreements play a vital role in establishing and maintaining trust between the firm and its clients. By requiring personnel to sign these agreements, the firm demonstrates its commitment to upholding client privilege and safeguarding sensitive information. The objective of this question is to ensure that appropriate measures are in place to protect client trust and maintain confidentiality.

4. Identification of Personnel with Access to Client Information: By asking about the personnel who are required to sign confidentiality agreements, the question seeks to identify the specific roles or positions within the firm that have access to client information. This information helps in assessing the scope of individuals who handle sensitive data and ensures that appropriate confidentiality measures are applied to relevant personnel.
5. Risk Mitigation: Requiring personnel to sign confidentiality agreements is a risk mitigation strategy that helps prevent unauthorized access, disclosure, or misuse of client information. By asking this question, the question aims to evaluate the firm's efforts to mitigate the risk of data breaches, unauthorized disclosures, or potential conflicts of interest.
6. Legal and Contractual Compliance: In some cases, confidentiality agreements may be a contractual requirement imposed by clients or business partners. By inquiring about the firm's practice, the questionnaire helps assess compliance with contractual obligations and ensures that the firm meets the expectations of clients regarding the protection of their confidential information.

### *7.1.15 Do you have an intrusion detection plan?*

#### 7.1.15.1 Objective

To evaluate the firm's level of preparedness, risk mitigation measures, incident response capabilities, compliance with security standards, continuous monitoring practices, incident identification and reporting procedures, and overall security culture.

#### 7.1.15.2 Rationale

It helps the assessor determine the firm's readiness to detect and respond to potential intrusions, strengthening its security posture and protecting its information assets.

#### 7.1.15.3 Practices

1. Security Preparedness: By inquiring about the presence of an intrusion detection plan, the assessment aims to evaluate the firm's level of preparedness in detecting and responding to security breaches or unauthorized access incidents. It assesses whether the firm has established proactive measures to identify potential intrusions promptly.
2. Risk Mitigation: The question seeks to determine whether the firm has implemented specific detection mechanisms or technologies to identify suspicious activities or intrusion attempts. This helps mitigate the risks associated with unauthorized access, data breaches, or other malicious activities that could compromise the confidentiality, integrity, or availability of sensitive information.
3. Incident Response Capability: Asking about the existence of an intrusion detection plan helps gauge the firm's incident response capabilities. It assesses whether the firm has established processes, tools, and personnel to promptly detect and respond to intrusions, minimizing potential damage and facilitating effective incident management.
4. Compliance with Security Standards: Inquiring about the presence of an intrusion detection plan is also relevant for assessing the firm's compliance with information security standards or regulatory requirements. Many security frameworks and regulations mandate the implementation of intrusion detection systems or processes as part of a firm's security controls.
5. Continuous Monitoring: The question aims to evaluate whether the firm adopts a proactive approach to monitor its information systems for potential intrusions or security incidents. It

- encourages the firm to implement ongoing monitoring practices, rather than relying solely on preventive security measures.
6. Incident Identification and Reporting: By having an intrusion detection plan, the firm can improve its ability to identify security incidents, assess their impact, and report them promptly to the appropriate stakeholders. This contributes to effective incident response and facilitates timely communication and collaboration with relevant parties.
  7. Security Culture and Awareness: The question indirectly assesses the firm's overall security culture and awareness. Having an intrusion detection plan indicates a proactive approach to security, reflecting a firm's commitment to detecting and responding to potential threats. It underscores the importance of a security-conscious mindset among personnel and stakeholders.

### **7.1.16 Do you have an InfoSec threat model for your firm?**

#### **7.1.16.1 Objective**

To assess the firm's level of preparedness and proactive approach towards identifying and managing information security threats.

#### **7.1.16.2 Rationale**

It helps the assessor ensure that the firm is aware of potential threats and resulting risks and has appropriate measures in place to protect the bank's information assets.

#### **7.1.16.3 Practices**

1. Assessment of Risk Management Practices: By inquiring about the presence of an Information Security threat model, the questionnaire aims to assess the firm's approach to identifying, assessing, and managing security risks. A threat model helps in understanding the potential threats and vulnerabilities specific to the firm's information systems and assets.
2. Identification of Security Threats and Vulnerabilities: A threat model enables the firm to identify and document potential security threats and vulnerabilities that could impact its information systems, data, and operations. By asking this question, the questionnaire seeks to determine whether the firm has a structured process in place to identify and analyze security risks.
3. Understanding of Threat Actors and Attack Vectors: A threat model helps in identifying the potential threat actors and the methods they might use to compromise the firm's information security. By having a threat model, the firm gains insights into the different attack vectors that could be exploited by adversaries. The objective of this question is to evaluate the firm's awareness and understanding of potential threat sources and attack vectors.
4. Risk Mitigation and Incident Response Planning: An Information Security threat model serves as a foundation for developing risk mitigation strategies and incident response plans. By asking this question, the assessor aims to assess whether the firm has considered potential threats in its security planning and has implemented measures to mitigate those risks.
5. Compliance with Best Practices and Standards: Having an Information Security threat model aligns with best practices and industry standards in the field of information security. By asking this question, the assessor seeks to determine whether the firm is following recognized practices for threat modeling, which can help demonstrate a commitment to security and compliance with relevant frameworks or standards.
6. Continuous Improvement and Adaptation: Threat modeling is an ongoing process that requires regular updates to account for evolving threats and changes in the firm's systems and

infrastructure. By inquiring about the presence of a threat model, the assessor aims to assess whether the firm has established a framework for continuous improvement and adaptation to address emerging threats and vulnerabilities.

### **7.1.17 What controls do you have for password protection?**

#### **7.1.17.1 Objective**

To assess password security measures, authentication practices, password storage and encryption mechanisms, password management policies, compliance with regulatory requirements, risk assessment and mitigation efforts. It helps the assessor evaluate the firm's commitment to password security and the protection of sensitive information from unauthorized access.

#### **7.1.17.2 Rationale**

It helps the assessor evaluate the firm's commitment to password security and the protection of sensitive information from unauthorized access.

#### **7.1.17.3 Practices**

1. Password Security Assessment: The question aims to assess the effectiveness of password protection controls implemented by the firm. It seeks to understand the measures in place to enforce strong password policies, such as password complexity requirements, minimum length, password expiration, and restrictions on password reuse. This information helps evaluate the firm's ability to protect against unauthorized access due to weak or compromised passwords.
2. Authentication and Access Control: Passwords are commonly used for user authentication and access control purposes. The question addresses whether the firm has controls in place to ensure that only authorized individuals can access systems, applications, or sensitive information. It helps assess the firm's use of passwords as a security mechanism and whether multi-factor authentication or other authentication methods are employed.
3. Password Storage and Encryption: The question also addresses how passwords are stored and protected within the firm's systems. It aims to evaluate whether the firm uses secure password storage mechanisms, such as cryptographic hashing or salting techniques, to prevent unauthorized access to stored passwords. This helps assess the firm's commitment to protecting passwords from potential data breaches or insider threats.
4. Password Management and Policies: The question assesses the existence of password management practices and policies within the firm. It seeks to understand whether the firm has established procedures for password creation, changes, resets, and revocations. It also addresses whether employees receive guidance and training on password best practices, such as not sharing passwords, protecting them from unauthorized disclosure, and promptly reporting any suspected compromises.
5. Compliance and Regulatory Requirements: Depending on the industry or regulatory obligations, there may be specific requirements for password protection and management. The question addresses whether the firm has considered these compliance and regulatory requirements and implemented controls accordingly. It helps evaluate the firm's commitment to safeguarding sensitive information and meeting legal obligations related to password protection.
6. Risk Assessment and Mitigation: The question helps identify potential risks associated with weak or compromised passwords. By understanding the controls in place, the assessor can evaluate the effectiveness of risk mitigation measures, such as password strength meters, account lockouts, or

monitoring for suspicious password-related activities. This information allows for assessing the firm's ability to identify vulnerabilities and implement appropriate measures to protect against password-based attacks.

### **7.1.18 Do you have an incident response plan?**

#### **7.1.18.1 Objective**

To assess the firm's preparedness, detection and reporting capabilities, incident response procedures, roles and responsibilities, communication and coordination practices, and commitment to continuous improvement.

#### **7.1.18.2 Rationale**

It helps the assessor evaluate the firm's ability to effectively respond to security incidents, mitigate their impact, and protect the client's assets and stakeholders.

#### **7.1.18.3 Practices**

1. Incident Preparedness: The question aims to assess the firm's level of preparedness in handling security incidents. An incident response plan outlines the procedures, roles, responsibilities, and actions to be taken in the event of a security incident. By asking this question, the assessor seeks to determine whether the firm has taken proactive measures to establish a structured and documented approach for incident response.
2. Incident Detection and Reporting: The question addresses whether the firm has mechanisms in place to detect and identify security incidents promptly. It also assesses the firm's ability to report incidents to the appropriate parties, such as internal incident response teams, management, regulatory authorities, or law enforcement agencies. This information helps evaluate the firm's capability to initiate a timely response and minimize the potential impact of security incidents.
3. Incident Response Procedures: The question aims to determine whether the firm has documented incident response procedures. An incident response plan typically outlines step-by-step procedures to be followed in the event of an incident, including incident assessment, containment, eradication, recovery, and post-incident analysis. By asking this question, the assessor seeks to understand whether the firm has established a systematic approach to manage incidents effectively.
4. Roles and Responsibilities: The question addresses whether the firm has clearly defined roles and responsibilities for incident response. An incident response plan usually assigns specific roles to individuals or teams, such as incident coordinators, technical experts, legal counsel, or public relations representatives. This information helps assess whether the firm has designated responsible individuals who are accountable for coordinating and executing incident response activities.
5. Communication and Coordination: The question also evaluates whether the firm has established communication and coordination channels for incident response. This includes internal communication among relevant stakeholders and external communication with affected parties, customers, partners, or regulatory bodies. It helps assess the firm's ability to effectively communicate during an incident and coordinate efforts to mitigate the impact and restore normal operations.
6. Continuous Improvement: The question indirectly addresses the firm's commitment to continuous improvement in incident response. Having an incident response plan indicates that

the firm recognizes the importance of learning from past incidents and refining response procedures. It provides an opportunity for the firm to assess and update the plan based on lessons learned, emerging threats, or changes in the business environment.

### **7.1.19 Do you have access to a Computer Security Incident Response Team (CSIRT)?**

#### **7.1.19.1 Objective**

To assess the firm's incident response capabilities, incident detection and response coordination, expertise and technical skills, incident handling procedures, collaboration and communication practices, and commitment to continuous improvement.

#### **7.1.19.2 Rationale**

It helps the assessor evaluate the firm's ability to effectively respond to computer security incidents, mitigate their impact, and protect client assets and stakeholders.

#### **7.1.19.3 Practices**

1. **Incident Response Capability:** The question aims to assess the firm's level of preparedness and capability to respond to computer security incidents. A CSIRT is a specialized group of individuals who are trained and equipped to handle and mitigate security incidents. By asking this question, the assessor seeks to determine whether the firm has access to such a team, indicating a higher level of incident response capability.
2. **Incident Detection and Response Coordination:** The question addresses whether the firm has established a dedicated team or access to external resources for incident detection and response coordination. A CSIRT typically coordinates incident response efforts, assesses the severity and impact of incidents, and directs response actions. This information helps evaluate the firm's ability to effectively detect, respond to, and mitigate computer security incidents.
3. **Expertise and Technical Skills:** The question aims to assess whether the firm has access to individuals or a team with the necessary expertise and technical skills to handle complex security incidents. A CSIRT often consists of individuals who possess specialized knowledge in various areas of information security, incident response, digital forensics, malware analysis, and vulnerability management. This information helps evaluate the firm's ability to address sophisticated and evolving cyber threats.
4. **Incident Handling Procedures:** The question indirectly addresses whether the firm has established incident handling procedures and protocols. A CSIRT typically follows documented procedures for incident assessment, containment, eradication, recovery, and post-incident analysis. This information helps assess whether the firm has a structured approach to handle security incidents effectively.
5. **Collaboration and Communication:** The question also evaluates whether the firm has established channels for collaboration and communication with the CSIRT. Effective incident response often requires coordination among different teams or departments within the firm. This includes sharing information, providing updates, and coordinating response actions. It helps assess the firm's ability to collaborate with the CSIRT and leverage their expertise during incident response activities.
6. **Continuous Improvement:** The question indirectly addresses the firm's commitment to continuous improvement in incident response. Having access to a CSIRT indicates that the firm recognizes the importance of specialized expertise and ongoing enhancements in incident

response capabilities. It provides an opportunity for the firm to learn from past incidents, receive guidance and recommendations from the CSIRT, and refine incident response procedures accordingly.

### **7.1.20 When do you revoke access for terminated personnel (i.e., contractors, lawyers, vendors, non-lawyers)?**

#### **7.1.20.1 Objective**

To assess the firm's access control practices, timeliness of access revocation, process and procedures for access revocation, role-specific considerations, compliance with regulations and legal obligations, and commitment to risk management.

#### **7.1.20.2 Rationale**

It helps the assessor evaluate the firm's ability to maintain a secure environment by promptly revoking access for individuals who are no longer associated with the firm.

#### **7.1.20.3 Practices**

1. Access Control and Security: The question aims to assess the firm's access control practices and their commitment to maintaining a secure environment. Revoking access for terminated personnel helps prevent unauthorized access to sensitive information or systems, reducing the risk of data breaches, insider threats, or misuse of resources. By asking this question, the assessor seeks to understand when and how the firm ensures that terminated personnel no longer have access to organizational resources.
2. Timeliness of Access Revocation: The question addresses the timeframe within which the firm revokes access for terminated personnel. It helps evaluate whether access revocation is performed promptly and efficiently to minimize the potential risks associated with unauthorized access. Timely access revocation reduces the window of opportunity for terminated individuals to misuse their access privileges, intentionally or unintentionally.
3. Process and Procedures: The question aims to assess the existence of established processes and procedures for revoking access when personnel are terminated. It seeks to understand whether the firm has defined steps and protocols in place to initiate and execute access revocation, including communication with relevant stakeholders, such as IT departments or system administrators. This information helps evaluate the firm's level of control and consistency in managing access privileges.
4. Access Revocation for Different Roles: The question specifically mentions various personnel categories, such as contractors, lawyers, vendors, and non-lawyers. By doing so, it addresses the need for role-specific access revocation procedures. Different roles may have different levels of access or different types of systems and resources to which they require access. The question helps assess whether the firm has considered these variations and implemented appropriate procedures for each category.
5. Compliance and Legal Obligations: Depending on industry-specific regulations, contractual agreements, or legal requirements, there may be obligations to revoke access for terminated personnel within specific timeframes. The question aims to determine whether the firm has considered these compliance and legal obligations and incorporated them into their access revocation processes. It helps assess the firm's adherence to relevant regulations and contractual obligations.

6. Risk Management: The question indirectly addresses the firm's commitment to risk management and the prevention of unauthorized access. By revoking access for terminated personnel, the firm reduces the risk of data breaches, unauthorized information disclosure, or misuse of resources. It helps ensure that terminated individuals no longer have the ability to access or manipulate sensitive information or systems.

### **7.1.21 Do you have a records retention plan?**

#### **7.1.21.1 Objective**

To assess the firm's compliance with legal and regulatory requirements, efficient records management practices, documented retention periods, risk management and legal defense considerations, storage and retrieval efficiency, and commitment to continuous improvement.

#### **7.1.21.2 Rationale**

It helps the assessor evaluate the firm's ability to manage records effectively, ensure compliance, and mitigate risks associated with record retention and disposal.

#### **7.1.21.3 Practices**

1. Compliance with Legal and Regulatory Requirements: The question aims to assess whether the firm has considered and addressed the legal and regulatory obligations related to records retention. Different jurisdictions and industries have specific requirements regarding the retention of certain types of records for a specified period. By asking this question, the assessor seeks to determine whether the firm has a plan in place to comply with these obligations.
2. Efficient Records Management: The question addresses whether the firm has established processes and procedures for efficient records management. A records retention plan outlines guidelines and best practices for managing records throughout their lifecycle, including creation, classification, storage, retrieval, and disposal. This information helps evaluate the firm's ability to effectively organize and manage its records.
3. Documented Retention Periods: The question aims to determine whether the firm has documented retention periods for different types of records. A records retention plan typically includes a list of record categories, such as financial records, client information, legal documents, or employee records, along with the recommended retention periods for each category. This information helps assess whether the firm has defined and documented guidelines for retaining records based on their legal, regulatory, or business value.
4. Risk Management and Legal Defense: The question indirectly addresses the firm's commitment to risk management and legal defense. A records retention plan helps mitigate risks associated with the improper disposal of records, potential litigation, or regulatory investigations. By having a plan in place, the firm can demonstrate its commitment to retaining records appropriately, which can be valuable in legal proceedings or regulatory audits.
5. Storage and Retrieval Efficiency: The question also evaluates whether the firm has considered the efficient storage and retrieval of records. A well-designed records retention plan includes guidelines for organizing and indexing records, implementing appropriate storage systems (physical or electronic), and ensuring easy retrieval when needed. This information helps assess the firm's ability to locate and retrieve records efficiently.
6. Continuous Improvement: The question indirectly addresses the firm's commitment to continuous improvement in records management. Having a records retention plan indicates that

the firm recognizes the importance of periodic review and updates to ensure compliance with changing regulations or business requirements. It provides an opportunity for the firm to assess and refine its records management practices over time.

### **7.1.22 What controls do you have to prevent unauthorized access to conference calls?**

#### **7.1.22.1 Objective**

To prevent unauthorized access to conference calls is to assess the firm's access authentication measures, confidentiality and privacy protection, participant management procedures, secure communication channels, monitoring and auditing capabilities, and compliance with policies and regulations.

#### **7.1.22.2 Rationale**

It helps the assessor evaluate the firm's ability to maintain the security and integrity of conference calls, protect sensitive information, and prevent unauthorized access by unauthorized individuals.

#### **7.1.22.3 Practices**

1. Access Authentication: The question aims to determine whether the firm has implemented authentication controls to verify the identity of participants before granting access to conference calls. This can include mechanisms such as unique access codes, PINs, or passwords that are required for participants to join the call. By asking this question, the assessor seeks to evaluate the effectiveness of the firm's access authentication measures.
2. Confidentiality and Privacy: The question addresses the need to protect the confidentiality and privacy of conference call discussions. Unauthorized access to conference calls can lead to the disclosure of sensitive information or discussions intended only for authorized participants. By asking this question, the assessor aims to determine whether the firm has implemented controls to prevent unauthorized individuals from joining or eavesdropping on conference calls.
3. Participant Management: The question indirectly addresses the firm's procedures for managing and controlling the participants in conference calls. It aims to assess whether the firm has processes in place to verify the identity and authorization of participants before granting them access to the call. This helps ensure that only authorized individuals, such as employees or invited guests, can join the conference call.
4. Secure Communication Channels: The question also evaluates whether the firm has implemented secure communication channels for conference calls. This may include the use of encrypted connections or secure communication platforms to protect the confidentiality and integrity of the call. By asking this question, the assessor seeks to determine whether the firm has considered the security of the communication channel itself.
5. Monitoring and Auditing: The question indirectly addresses whether the firm has mechanisms in place to monitor and audit conference calls for security purposes. Monitoring may help detect any unauthorized access attempts or suspicious activities during the call. Auditing may provide a record of participants, call duration, and any security-related incidents. By asking this question, the assessor aims to assess the firm's ability to monitor and maintain the security of conference calls.
6. Compliance with Policies and Regulations: Depending on the industry or organizational requirements, there may be specific policies or regulations that mandate controls for conference call security. The question aims to determine whether the firm has implemented controls in

alignment with such policies or regulations. It helps evaluate the firm's commitment to compliance and adherence to relevant security standards.

### **7.1.23 What controls do you have to prevent unauthorized access to telephone conversations?**

#### **7.1.23.1 Objective**

To assess the firm's access authentication measures, secure communication channels, physical security measures, call monitoring and auditing capabilities, compliance with policies and regulations, and efforts to promote training and awareness.

#### **7.1.23.2 Rationale**

It helps the assessor evaluate the firm's ability to maintain the confidentiality and integrity of telephone conversations, protect sensitive information, and prevent unauthorized access to telephone communication.

#### **7.1.23.3 Practices**

1. Access Authentication: The question aims to determine whether the firm has implemented authentication controls for telephone conversations. It seeks to evaluate whether the firm has measures in place to verify the identity of participants or restrict access to authorized individuals only. This can include features such as unique access codes, PINs, passwords, or other authentication mechanisms required to initiate or participate in telephone conversations.
2. Secure Communication Channels: The question addresses the need to protect the confidentiality and integrity of telephone conversations. It aims to assess whether the firm has implemented secure communication channels, such as encrypted connections or secure telephone systems, to prevent unauthorized interception or eavesdropping on conversations. By asking this question, the assessor seeks to evaluate the effectiveness of the firm's controls in maintaining the privacy of telephone conversations.
3. Physical Security Measures: The question indirectly addresses the physical security measures implemented to prevent unauthorized access to telephone conversations. This may include measures such as securing physical access to telephone devices or systems, ensuring restricted access to areas where telephones are located, or implementing measures to prevent unauthorized tampering with telephone lines or equipment.
4. Call Monitoring and Auditing: The question aims to determine whether the firm has mechanisms in place to monitor and audit telephone conversations for security purposes. Monitoring may help detect any unauthorized access attempts, suspicious activities, or policy violations during phone conversations. Auditing may provide a record of call details, participant information, and any security-related incidents. By asking this question, the assessor seeks to assess the firm's ability to monitor and maintain the security of telephone conversations.
5. Compliance with Policies and Regulations: Depending on the industry or firm requirements, there may be specific policies or regulations that mandate controls for securing telephone conversations. The question aims to determine whether the firm has implemented controls in alignment with such policies or regulations. It helps evaluate the firm's commitment to compliance and adherence to relevant security standards.
6. Training and Awareness: The question indirectly addresses the firm's efforts to educate and raise awareness among employees about the importance of securing telephone conversations. By asking this question, the assessor seeks to evaluate whether the firm provides training or

guidelines to employees on how to handle sensitive information during phone conversations and the importance of preventing unauthorized access.

### **7.1.24 What controls do you have to prevent unauthorized access to fax machines and scanners?**

#### **7.1.24.1 Objective**

To assess the firm's physical security measures, access control mechanisms, monitoring and auditing capabilities, secure transmission practices, user awareness and training efforts, and compliance with policies and regulations.

#### **7.1.24.2 Rationale**

It helps the assessor evaluate the firm's ability to maintain the confidentiality and integrity of faxed or scanned information, protect sensitive data, and prevent unauthorized access to fax machines and scanners.

#### **7.1.24.3 Practices**

1. Physical Security Measures: The question aims to determine whether the firm has implemented physical security measures to prevent unauthorized access to fax machines and scanners. This may include measures such as securing the physical location of the machines, ensuring restricted access to areas where fax machines and scanners are located, or implementing measures to prevent unauthorized use or tampering with the equipment.
2. Access Control: The question addresses the need for access controls to restrict unauthorized use of fax machines and scanners. It aims to assess whether the firm has implemented measures to authenticate and authorize individuals before they can operate the equipment. This may include features such as unique access codes, PINs, or passwords required to use the machines, or physical locks and keys to limit access.
3. Monitoring and Auditing: The question aims to determine whether the firm has mechanisms in place to monitor and audit the use of fax machines and scanners for security purposes. Monitoring may help detect any unauthorized use, misuse, or policy violations related to the equipment. Auditing may provide a record of usage details, user information, and any security-related incidents. By asking this question, the assessor seeks to assess the firm's ability to monitor and maintain the security of fax machines and scanners.
4. Secure Transmission: The question indirectly addresses the firm's measures to ensure the security of transmitted information. It aims to evaluate whether the firm has implemented controls to protect the confidentiality and integrity of the information being sent via fax machines. This may include features such as encryption capabilities for fax transmissions or guidelines for securely handling faxed documents.
5. User Awareness and Training: The question indirectly addresses the firm's efforts to educate and raise awareness among employees about the importance of securing fax machines and scanners. By asking this question, the assessor seeks to evaluate whether the firm provide training or guidelines to employees on how to handle sensitive information when using fax machines and scanners and the importance of preventing unauthorized access.
6. Compliance with Policies and Regulations: Depending on the industry or organizational requirements, there may be specific policies or regulations that mandate controls for securing fax machines and scanners. The question aims to determine whether the firm has implemented

controls in alignment with such policies or regulations. It helps evaluate the firm's commitment to compliance and adherence to relevant security standards.

### **7.1.25 What controls do you have to prevent unauthorized data transfer?**

#### **7.1.25.1 Objective**

To assess the firm's data leakage prevention measures, access controls, network and endpoint security, data loss prevention efforts, encryption and data protection practices, and policy and compliance framework.

#### **7.1.25.2 Rationale**

It helps the assessor evaluate the firm's ability to protect sensitive data from unauthorized transfers, maintain data confidentiality and integrity, and prevent data breaches or unauthorized disclosure of information.

#### **7.1.25.3 Practices**

1. Data Leakage Prevention: The question aims to determine whether the firm has implemented controls to prevent unauthorized transfer of data, both internally and externally. It seeks to evaluate whether the firm has measures in place to detect and prevent unauthorized data transfers that could lead to data breaches, data loss, or unauthorized disclosure of sensitive information.
2. Access Controls: The question addresses the need for access controls to restrict unauthorized data transfer. It aims to assess whether the firm has implemented measures to authenticate and authorize individuals or systems before they can transfer data. This may include features such as user authentication, role-based access controls, encryption, or other mechanisms to ensure that only authorized individuals or systems can initiate data transfers.
3. Network and Endpoint Security: The question indirectly addresses the firm's network and endpoint security measures. It aims to evaluate whether the firm has implemented measures such as firewalls, intrusion detection and prevention systems, or secure configurations on endpoints to prevent unauthorized data transfer. These measures can help protect against external threats and unauthorized access attempts.
4. Data Loss Prevention: The question addresses the firm's efforts to prevent data loss through unauthorized data transfer. It aims to determine whether the firm has implemented data loss prevention (DLP) measures, such as content filtering, data classification, or data monitoring, to identify and prevent unauthorized data transfers. These measures can help detect and block sensitive data from being transferred without proper authorization.
5. Encryption and Data Protection: The question indirectly addresses the firm's use of encryption and data protection mechanisms. It aims to assess whether the firm has implemented encryption for sensitive data during transit or storage, or whether it has employed other data protection techniques to ensure the confidentiality and integrity of the data during transfer. Encryption can provide an additional layer of security to prevent unauthorized access to transferred data.
6. Policy and Compliance: The question also evaluates whether the firm has policies, procedures, or guidelines in place to govern data transfer activities. It aims to determine whether the firm has defined rules and guidelines that employees must follow when transferring data, and whether these policies align with relevant regulatory requirements or industry best practices.

### **7.1.26 What do you do to ensure that your personnel can identify confidential information?**

#### **7.1.26.1 Objective**

To ensure personnel can identify confidential information is to assess the firm's awareness and education programs, data classification practices, policy and guideline framework, training and materials provided to personnel, marking and labeling mechanisms, and ongoing reinforcement efforts.

#### **7.1.26.2 Rationale**

It helps the assessor evaluate the firm's commitment to protecting confidential information, fostering a culture of confidentiality, and ensuring that personnel can effectively identify and handle sensitive information.

#### **7.1.26.3 Practices**

1. Awareness and Education: The question aims to determine whether the firm provides awareness programs or training sessions to personnel regarding the identification of confidential information. It seeks to evaluate whether the firm has implemented measures to educate employees on what constitutes confidential information, its importance, and the potential risks associated with mishandling or unauthorized disclosure.
2. Data Classification: The question indirectly addresses the firm's data classification practices. It aims to assess whether the firm has implemented a data classification scheme or framework that helps personnel identify different levels of confidentiality for information assets. This may include labeling or tagging systems that clearly indicate the sensitivity of information, such as "confidential," "internal use only," or "public."
3. Policy and Guidelines: The question evaluates whether the firm has established policies, procedures, or guidelines that define and explain what constitutes confidential information within the firm. It aims to determine whether the firm provides clear instructions and examples to personnel on how to identify and handle confidential information appropriately.
4. Training and Materials: The question aims to assess whether the firm provide training materials, such as handbooks, guidelines, or reference materials, to personnel to help them identify and handle confidential information. It seeks to evaluate whether the firm equips employees with the necessary knowledge and resources to understand the types of information that should be treated as confidential.
5. Marking and Labeling: The question addresses whether the firm has implemented a system for marking or labeling confidential information. It aims to determine whether the firm uses visual indicators, such as watermarks, headers, footers, or specific document templates, to clearly identify documents or files as confidential. This may help personnel quickly recognize and handle confidential information appropriately.
6. Ongoing Reinforcement: The question evaluates whether the firm has mechanisms in place to reinforce the importance of identifying and protecting confidential information over time. It seeks to determine whether the firm periodically reminds personnel of their responsibilities, provides refresher training, or conducts awareness campaigns to maintain a culture of confidentiality within the firm.

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

**7.1.27.1 Objective**

To assess the firm's recognition of security risks associated with these roles, the provision of specialized security knowledge and training, efforts to mitigate insider threats, adherence to security best practices and procedures, compliance with regulatory requirements, and incident response preparedness.

**7.1.27.2 Rationale**

It helps the assessor evaluate the firm's commitment to security awareness, risk mitigation, and ensuring that personnel with extensive access privileges are equipped with the necessary security knowledge and skills to fulfill their roles securely.

**7.1.27.3 Practices**

1. Awareness of Security Risks: The question aims to determine whether the firm recognizes the elevated security risks associated with personnel who have broad access privileges. It seeks to evaluate whether the firm understands the importance of providing specialized security training to these individuals who have extensive access to sensitive systems, data, or administrative functions.
2. Specialized Security Knowledge: The question addresses the need for personnel with elevated or broad access privileges to possess specialized security knowledge and skills. It aims to assess whether the firm provide training programs tailored to their roles and responsibilities, focusing on security practices, protocols, and procedures specific to their access privileges. This specialized training helps ensure that individuals with extensive access are equipped to handle security-related challenges effectively.
3. Mitigating Insider Threats: The question indirectly addresses the firm's efforts to mitigate insider threats. It aims to evaluate whether the firm recognizes that personnel with elevated or broad access privileges can pose a higher risk for potential insider threats due to their increased access to sensitive information or critical systems. By providing specialized security training, the firm can enhance awareness and understanding of potential risks and help mitigate the insider threat.
4. Best Practices and Procedures: The question evaluates whether the firm imparts best practices and procedures specific to the roles of personnel with elevated or broad access privileges. It aims to determine whether the firm educates these individuals on security measures, such as secure access management, secure system configurations, data protection protocols, incident response procedures, or handling sensitive information. This training helps ensure that personnel understand and follow security best practices in their day-to-day activities.
5. Compliance and Regulatory Requirements: The question indirectly addresses the firm's commitment to compliance and regulatory requirements. It aims to assess whether the firm provides specialized security training to personnel with elevated or broad access privileges to meet the specific security obligations imposed by industry regulations or legal requirements. This training helps ensure compliance with relevant security standards and safeguards sensitive information.
6. Incident Response Preparedness: The question evaluates whether the firm prepares personnel with elevated or broad access privileges for potential security incidents. It aims to determine whether the firm provide training on incident response procedures, including recognizing and reporting security incidents, containment measures, communication protocols, and escalation

procedures. This training helps ensure that personnel are adequately prepared to respond to security incidents effectively.

### **7.1.28 How do you ensure that your personnel are familiar with and trained on your Information security policies and procedures?**

#### **7.1.28.1 Objective**

To assess the firm's efforts in policy communication, training initiatives, accessibility of policies, periodic updates, assessment of understanding, and compliance monitoring.

#### **7.1.28.2 Rationale**

It helps the assessor evaluate the firm's commitment to information security awareness, ensuring personnel have the necessary knowledge to adhere to policies and procedures, and fostering a security-conscious culture throughout the firm.

#### **7.1.28.3 Practices**

1. Policy Familiarity: The question aims to determine whether the firm has established mechanisms to ensure that personnel are familiar with the information security policies. It seeks to evaluate whether the firm has implemented processes to effectively communicate and disseminate the policies to all relevant personnel.
2. Training Programs: The question addresses the firm's training initiatives to ensure personnel are trained on information security policies and procedures. It aims to assess whether the firm provides training programs specifically designed to educate personnel on the content, significance, and application of the policies. This training helps ensure that personnel understand their roles and responsibilities in maintaining information security.
3. Accessibility of Policies: The question evaluates whether the firm provide easy access to information security policies and procedures. It aims to determine whether the policies are readily available to personnel through appropriate channels, such as an intranet, document management systems, or employee portals. This accessibility facilitates personnel's ability to refer to and review the policies as needed.
4. Periodic Training and Updates: The question addresses whether the firm provides regular and periodic training sessions or updates on information security policies and procedures. It aims to assess whether the firm conducts refresher training sessions or communicates updates to personnel whenever there are changes to the policies or procedures. This ensures that personnel stay up to date with the evolving security requirements.
5. Assessment of Understanding: The question indirectly addresses the firm's efforts to assess personnel's understanding of information security policies and procedures. It aims to evaluate whether the firm conducts assessments or quizzes to verify personnel's comprehension of the policies. This assessment helps ensure that personnel have a clear understanding of the policies and can apply them correctly in their daily work.
6. Compliance Monitoring: The question evaluates whether the firm monitors compliance with information security policies and procedures. It aims to determine whether the firm has processes in place to track and monitor personnel's adherence to the policies. This monitoring helps identify any gaps or areas of non-compliance that may require additional training or corrective actions.

### 7.1.29 Technology

During the CRA phase, there are several technical controls that can be assessed to ensure the security of a firm's assets. Some examples of technical controls that are assessed during the cybersecurity assessment include:

1. Firewalls
2. Intrusion detection systems (IDS)
3. Intrusion prevention systems (IPS)
4. Encryption
5. Identification and authentication mechanisms
6. Antivirus and anti-malware software
7. Security information and event management (SIEM)
8. Constrained interfaces
9. Multi-factor user authentication

Technical controls are hardware and software components that protect a system against cyberattacks. They perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred. Technical controls must be organized in such a way that they provide protection for both data at rest (for example, data stored on a hard drive) and data in motion (for example, data moving across a network). A common approach for deploying controls is defense-in-depth, where controls are layered. In such an arrangement, when an attacker breaches one control, there are additional controls in place to prevent further access to the system.

## 7.2 Preferred Accredited Network of Law firms (PANEL) Domain

### 7.2.1 *Does your firm prepare, track and share budgets with us?*

#### 7.2.1.1 Objective

To assess financial transparency, budget planning and management capabilities, collaboration and communication practices, financial accountability, planning and forecasting capabilities, and compliance with financial governance requirements.

#### 7.2.1.2 Rationale

It helps the assessor evaluate the firm's financial practices and ensure transparency and accountability in the relationship between both parties.

#### 7.2.1.3 Practices

1. Financial Transparency: The question aims to determine whether the firm maintains financial transparency with their clients. It seeks to understand whether the firm prepares budgets and shares them with relevant stakeholders. This helps establish an open and transparent financial relationship between the firm and the clients.

2. Budget Planning and Management: By asking about the preparation and tracking of budgets, the question assesses the firm's ability to effectively plan and manage its financial resources. It provides insight into whether the firm has established processes and procedures for budgeting, monitoring expenditures, and making informed financial decisions.
3. Collaboration and Communication: Sharing budgets with clients indicates a collaborative approach to financial management. It demonstrates a willingness to engage in open communication and provide relevant financial information to facilitate decision-making and mutual understanding.
4. Financial Accountability: The question addresses the firm's accountability in managing its financial resources. By tracking budgets and sharing them with clients, the firm demonstrates a commitment to financial responsibility and transparency. It allows for oversight and evaluation of the firm's financial performance and adherence to agreed-upon financial plans.
5. Planning and Forecasting: Budgets serve as tools for planning and forecasting financial activities. By preparing and sharing budgets, the firm provides insight into its financial projections, anticipated expenses, and revenue streams. This information can be valuable for clients in assessing the firm's financial stability, growth potential, and alignment with strategic objectives.
6. Compliance and Governance: The question also addresses compliance and governance aspects. Budget preparation, tracking, and sharing may be required by regulatory or contractual obligations. By asking this question, the assessor can ensure that the firm follows established financial governance practices and meets any specific requirements related to financial reporting and transparency.

### **7.2.2 Does your firm have a formal process for developing value-based pricing or alternative fee arrangements (AFAs)?**

#### **7.2.2.1 Objective**

To gather information about the firm's approach to pricing, assess its consideration of client value and preferences, evaluate the formalization of the pricing process, determine the bank-centricity of the firm, assess financial viability, and evaluate market competitiveness.

#### **7.2.2.2 Rationale**

It helps the assessor understand how the firm adapts its pricing strategies to meet client needs, drive value, and remain competitive in the market.

#### **7.2.2.3 Practices**

1. Value-Based Pricing: The question aims to determine whether the firm employs value-based pricing strategies. It assesses whether the firm considers factors beyond traditional billing models, such as the perceived value of the services provided, bank outcomes, or the economic benefits realized by clients. Value-based pricing aligns the cost of services with the value received by clients.
2. Alternative Fee Arrangements (AFAs): The question addresses whether the firm offers AFAs. AFAs are non-traditional billing structures that go beyond hourly rates and may include fixed fees, contingency fees, success fees, or other arrangements tailored to the specific needs and preferences of clients. This question seeks to determine whether the firm has a formal process for developing and implementing AFAs.

3. Process Formalization: The question evaluates whether the firm has a structured and documented process for developing value-based pricing or AFAs. It aims to assess whether the firm has established guidelines, frameworks, or procedures to guide the pricing decision-making process. A formalized process ensures consistency, transparency, and fairness in determining pricing and fee arrangements.
4. Client-Centric Approach: The question indirectly addresses the firm's bank-centric approach to pricing. It aims to determine whether the firm considers the unique needs, circumstances, and value expectations of individual clients when developing pricing strategies or alternative fee arrangements. This client-centric approach helps foster stronger bank relationships and better aligns pricing with client satisfaction.
5. Financial Viability: The question evaluates whether the firm considers the financial viability and sustainability of value-based pricing or AFAs. It aims to assess whether the firm has mechanisms in place to evaluate the profitability and risk associated with these alternative pricing models. This ensures that pricing decisions align with the firm's financial objectives and sustainability.
6. Market Competitiveness: The question indirectly addresses the firm's competitiveness in the market. It aims to determine whether the firm is responsive to changing market dynamics and bank demands by offering value-based pricing or AFAs. This helps assess the firm's ability to differentiate itself from competitors and attract clients seeking innovative pricing models.

### *7.2.3 Is your firm a customer of Bank or any of our subsidiaries (including any subsidiaries or affiliates)?*

#### 7.2.3.1 Objective

To gather information about the existing business relationship, identify potential conflicts of interest, assess business considerations and risks, evaluate regulatory compliance, and explore ethical considerations.

#### 7.2.3.2 Rationale

It helps the assessor understand the potential implications of the customer relationship and ensures transparency and disclosure regarding any existing financial connections between the firm and the Bank or its subsidiaries.

#### 7.2.3.3 Practices

1. Relationship Identification: The question aims to identify whether there is an existing business relationship between the firm and the Bank or any of its subsidiaries or affiliates. It seeks to gather information about whether the firm has engaged in financial transactions or services with the Bank or its related entities.
2. Potential Conflicts of Interest: The question indirectly addresses the potential for conflicts of interest. It aims to identify if the firm's status as a customer of the Bank or its subsidiaries could create conflicts of interest or compromise the objectivity, impartiality, or independence of the firm's relationship with the Bank.
3. Business Considerations: The question evaluates whether the firm's status as a customer of the bank or its subsidiaries may have implications for business considerations. It seeks to gather information about any financial, operational, or strategic factors that may arise due to the existing customer relationship. This information helps the assessor understand any potential interdependencies or business impacts.

4. Risk Assessment: The question indirectly addresses the risk assessment related to the existing customer relationship. It aims to determine whether the firm has considered the potential risks associated with being a customer of the bank or its subsidiaries, such as financial risks, confidentiality risks, conflicts of interest, or regulatory compliance risks.
5. Regulatory Compliance: The question evaluates the firm's compliance with regulatory requirements and potential conflicts with applicable laws or regulations. It aims to assess whether the firm has disclosed its customer relationship with the Bank or its subsidiaries as required by relevant regulatory bodies.
6. Ethical Considerations: The question addresses ethical considerations related to the customer relationship. It aims to determine whether the firm's relationship with the bank or its subsidiaries aligns with its ethical guidelines, codes of conduct, or professional standards.

### 7.2.4 *How many years has your firm provided legal services to us?*

#### 7.2.4.1 Objective

To gather information about the relationship duration, assess trust and confidence, evaluate experience and expertise, determine stability and reliability, assess relationship satisfaction, and potentially identify competitive advantages.

#### 7.2.4.2 Rationale

It helps the assessor understand the firm's history with the client and provides valuable insights into the nature and effectiveness of their legal services over time.

#### 7.2.4.3 Practices

1. Relationship Duration: The question aims to determine the length of time that the firm has been providing legal services to the client. It helps establish the historical context of the relationship and assess the level of familiarity and experience the firm has with the client.
2. Trust and Confidence: The question indirectly addresses the level of trust and confidence built between the firm and the client over the years. It suggests that a longer duration of providing legal services may indicate a strong and enduring relationship based on trust, satisfaction, and mutual understanding.
3. Experience and Expertise: The question provides insights into the firm's experience and expertise in providing legal services to the client. The number of years may be indicative of the firm's accumulated knowledge, understanding of the client's needs, industry-specific expertise, and ability to navigate the legal landscape over an extended period.
4. Stability and Reliability: The question evaluates the stability and reliability of the firm's legal services. A longer duration of providing services implies a certain level of stability and reliability in terms of delivering consistent and dependable legal support to the client. It suggests that the firm has been able to meet the client's ongoing legal needs over an extended period.
5. Relationship Assessment: The question indirectly assesses the satisfaction and effectiveness of the firm's legal services over the years. By knowing the duration of the relationship, the assessor can evaluate whether the firm's services have met the client's expectations and requirements consistently, leading to a long-lasting partnership.
6. Competitive Advantage: The question indirectly addresses the firm's competitive advantage. A longer duration of providing legal services to the client may imply that the firm has been

successful in meeting the client's legal needs, surpassing competitors, and maintaining a preferred status as their legal service provider.

### **7.2.5 What is our average annual legal spend with you over the last three years?**

#### **7.2.5.1 Objective**

To gather information about the financial impact, evaluate the importance and value of the firm's legal services, assess cost management, facilitate benchmarking, assess relationship stability, and inform contract negotiations.

#### **7.2.5.2 Rationale**

It helps the assessor understand the financial dynamics of the firm's legal services within the context of the bank's overall budget and financial priorities.

#### **7.2.5.3 Practices**

1. Financial Assessment: The question aims to assess the financial impact of the firm's legal services on the client. By knowing the average annual legal spend, the assessor can evaluate the financial resources allocated to legal services and assess the significance of the financial commitment over the specified time frame.
2. Relationship Evaluation: The question indirectly assesses the importance and value of the firm's legal services to the client. The average annual legal spend reflects the client's financial investment in the firm's services, indicating the perceived value, satisfaction, and ongoing need for legal support.
3. Cost Management: The question addresses cost management and budget considerations. By knowing the average annual legal spend over the last three years, the assessor can evaluate whether the client has been able to manage legal costs effectively, control expenses, and align the financial commitment with the expected value or outcomes derived from the legal services.
4. Benchmarking: The question allows for benchmarking and comparison against industry averages or similar firms. The assessor can assess whether the client's average annual legal spend falls within a typical range, providing a reference point for evaluating cost efficiency, resource allocation, and potential cost-saving opportunities.
5. Relationship Stability: The question indirectly addresses the stability and longevity of the relationship between the firm and the client. A consistent or increasing average annual legal spend over the last three years suggests a continued reliance on the firm's services and a stable relationship with ongoing legal needs.
6. Contract Negotiations: The question provides insights into the client's bargaining power during contract negotiations. By knowing the average annual legal spend, the assessor can gauge the client's financial leverage and the potential impact on negotiations, fee structures, or value-added services.

### **7.2.6 To which department(s) did you provide legal services and who are your main contact(s)?**

#### **7.2.6.1 Objective**

To gather information about the service scope, evaluate the relationship, identify key contacts, support relationship management, identify service expansion opportunities, and facilitate account planning.

### **7.2.6.2 Rationale**

It helps the assessor understand the firm's involvement in the client's operations, establish effective communication channels, and align legal services with the specific needs and priorities of each department.

### **7.2.6.3 Practices**

1. Service Scope Identification: The question aims to identify the specific departments within the organization that have utilized the firm's legal services. By knowing which departments have engaged the firm, the assessor can understand the breadth and depth of the legal services provided and the areas of the organization's operations that require legal support.
2. Relationship Evaluation: The question indirectly assesses the strength and depth of the relationship between the firm and the client. By identifying the departments that have sought legal services, the assessor can evaluate the extent to which the firm has been integrated into the organization's operations and decision-making processes.
3. Key Contact Identification: The question aims to identify the main contacts within the departments who have been the primary points of contact for legal service engagements. This information allows the assessor to establish communication channels, understand the roles and responsibilities of the contacts, and assess the level of engagement and collaboration between the firm and the organization's personnel.
4. Relationship Management: The question helps in relationship management by providing insights into the key individuals who have been involved in the legal service engagements. By identifying the main contacts, the assessor can establish and strengthen relationships, understand communication preferences, and ensure effective coordination and collaboration between the firm and the organization's personnel.
5. Service Expansion Opportunities: The question indirectly addresses potential service expansion opportunities. By knowing the departments that have received legal services, the assessor can identify areas within the organization where additional legal support may be required or where the firm can offer additional legal services to address emerging needs or challenges.
6. Account Planning: The question supports account planning and bank relationship strategies. By understanding the specific departments and main contacts, the assessor can develop tailored strategies, allocate resources effectively, and align the firm's legal services with the specific needs and priorities of each department.

## **7.2.7 Does your firm make referrals to us?**

### **7.2.7.1 Objective**

To gather information about referral practices, evaluate the strength of the relationship, identify business development opportunities, assess partnership alignment, understand the referral network, and support relationship development.

### **7.2.7.2 Rationale**

It helps the assessor understand the level of support and contribution from the firm in terms of referring banks or business opportunities to the client, and it provides insights into the potential for ongoing collaboration and partnership.

#### 7.2.7.3 Practices

1. Referral Evaluation: The question aims to evaluate the extent to which the firm has referred organizations or business opportunities to the client. It helps the assessor assess the level of reciprocity in the relationship, indicating whether the firm has actively supported and promoted the client's services by referring potential organizations or business opportunities.
2. Relationship Assessment: The question indirectly assesses the strength and mutual support within the relationship between the firm and the client. If the firm has made referrals, it suggests a willingness to actively contribute to the growth and success of the client by directing potential organizations or business opportunities their way.
3. Business Development Opportunities: The question addresses potential business development opportunities for the client. By knowing whether the firm has made referrals, the assessor can identify potential sources of new organizations or business opportunities that have been referred by the firm. This information can help the client assess the impact of the firm's referrals on their business growth and identify opportunities for further collaboration or partnership.
4. Partnership Alignment: The question helps assess the alignment of values and objectives between the firm and the client. If the firm has made referrals, it indicates a level of confidence and alignment in their relationship, suggesting shared values, mutual support, and a commitment to fostering business opportunities for each other.
5. Referral Network: The question indirectly addresses the existence of a referral network or ecosystem between the firm and the client. By understanding the referral practices, the assessor can assess the potential for ongoing collaboration, cross-referrals, and leveraging each other's networks to expand business opportunities.
6. Relationship Development: The question supports relationship development and future collaboration opportunities. If the firm has not made referrals, it provides an opportunity for the assessor to discuss and explore the potential for mutual referrals, joint marketing efforts, or partnership initiatives to further strengthen the relationship.

#### 7.2.8 *Aside from routine audit reporting, does your firm provide annual or quarterly reporting to us?*

##### 7.2.8.1 Objective

To gather information about reporting practices, assess communication and transparency, support relationship management efforts, monitor performance, evaluate proactive communication practices, and explore opportunities for relationship enhancement.

##### 7.2.8.2 Rationale

It helps the assessor understand the extent to which the firm goes beyond the routine audit reporting in providing additional reports and enables discussions on enhancing reporting practices to meet the client's information needs and foster a strong relationship.

##### 7.2.8.3 Practices

1. Reporting Assessment: The question aims to assess the frequency and nature of reporting provided by the firm to the client. It helps the assessor understand whether the firm goes beyond the routine audit reporting and provides additional reports on an annual or quarterly basis.

2. Communication Evaluation: The question indirectly assesses the level of communication and transparency between the firm and the client. By knowing whether the firm provides annual or quarterly reporting, the assessor can evaluate the extent to which the firm keeps the bank informed about relevant matters, performance, or key metrics beyond the regular audit reporting.
3. Relationship Management: The question supports relationship management efforts by providing insights into the firm's reporting practices. By understanding the frequency and content of the additional reports, the assessor can ensure alignment with the client's information needs, address any gaps in reporting, and explore opportunities for enhanced reporting or customized reporting formats.
4. Performance Monitoring: The question addresses performance monitoring and accountability. If the firm provide annual or quarterly reports, it allows the assessor to assess and monitor the firm's performance, track progress against agreed-upon objectives, and evaluate the outcomes or impact of the firm's services beyond the routine audit reporting.
5. Proactive Communication: The question indirectly assesses the firm's proactive communication practices. If the firm provide additional reports, it suggests a commitment to proactive communication, keeping the client updated on relevant matters, and providing insights or analysis that go beyond the routine audit reporting.
6. Relationship Enhancement: The question provides an opportunity to discuss and explore ways to enhance the reporting relationship between the firm and the client. If the firm does not provide additional reports, the assessor can discuss the possibility of implementing annual or quarterly reporting to further strengthen the relationship, address information needs, and foster transparency and accountability.

### 7.2.9 *Has your firm represented a party adverse to our firm (including any of our subsidiaries or affiliates) in a matter or a dispute at any time within the last 10 years?*

#### 7.2.9.1 Objective

To evaluate potential conflicts of interest, assess the strength of the relationship, consider ethical considerations, evaluate legal risks, ensure trust and confidentiality, promote transparency, and facilitate open communication.

#### 7.2.9.2 Rationale

It helps the assessor identify any potential conflicts or risks that may impact the legal representation and establish a foundation of trust and transparency in the relationship with the law firm.

#### 7.2.9.3 Practices

1. Conflict of Interest Evaluation: The question aims to evaluate whether there are any potential conflicts of interest between the firm's law firm and the client, its subsidiaries, or its affiliates. By knowing whether the law firm has represented an adverse party, the assessor can assess the potential impact on objectivity, confidentiality, or loyalty in the legal representation.
2. Relationship Assessment: The question indirectly assesses the strength and trustworthiness of the relationship between the law firm and the client. By understanding whether the law firm has been involved in representing an opposing party, the assessor can evaluate the potential implications for the existing or future relationship between the law firm and the client.

3. Ethical Considerations: The question addresses ethical considerations in legal representation. It helps the assessor ensure that there are no conflicts of interest that could compromise the legal representation or create potential ethical dilemmas for the law firm.
4. Legal Risk Evaluation: The question supports the evaluation of legal risks and potential challenges. By identifying instances where the law firm has represented an adverse party, the assessor can assess any legal implications or risks that may arise due to conflicts, confidentiality concerns, or adverse relationships.
5. Trust and Confidentiality Assurance: The question aims to ensure trust and confidentiality between the law firm and the client. By understanding the law firm's history of representing adverse parties, the assessor can address any concerns related to confidentiality, attorney-bank privilege, and the assurance that the law firm will prioritize the best interests of the client and maintain strict confidentiality.
6. Relationship Transparency: The question promotes transparency and open communication. By discussing any past representation of adverse parties, the assessor and the law firm can openly address any concerns, discuss potential conflicts, and establish a foundation of transparency and trust in the relationship moving forward.

### ***7.2.10 Would any prior or ongoing engagement prevent your firm from acting for us?***

#### **7.2.10.1 Objective**

To identify and assess potential conflicts of interest, evaluate ethical considerations, assess legal risks, promote transparency, evaluate engagement suitability, and facilitate conflict resolution.

#### **7.2.10.2 Rationale**

It helps the assessor ensure that the law firm is available and capable of providing legal representation without any conflicts or restrictions that could hinder their ability to act in the best interests of this client.

#### **7.2.10.3 Practices**

1. Conflict of Interest Assessment: The question aims to assess whether there are any conflicts of interest that could prevent the law firm from representing this client. By knowing about any prior or ongoing engagements, the assessor can evaluate potential conflicts that may arise from representing this client in a legal matter.
2. Ethical Considerations: The question addresses ethical considerations in legal representation. It helps the assessor ensure that there are no conflicts of interest that could compromise the law firm's ability to provide objective and unbiased legal advice or representation.
3. Legal Risk Evaluation: The question supports the evaluation of legal risks and potential challenges. By identifying any engagements that could prevent the law firm from acting for the bank, the assessor can assess the potential impact on the legal representation, identify potential conflicts or restrictions, and evaluate the need for alternative legal representation.
4. Relationship Transparency: The question promotes transparency and open communication between the law firm and the client. By discussing any prior or ongoing engagements that may pose a conflict, the assessor and the law firm can openly address concerns, discuss potential conflicts, and explore solutions or alternatives to ensure appropriate legal representation.
5. Engagement Evaluation: The question helps evaluate the suitability and feasibility of engaging the law firm for legal services. By understanding any existing engagements that may prevent the law

firm from acting for this client, the assessor can assess whether the law firm is available and able to take on the legal matters effectively.

6. Conflict Resolution: The question provides an opportunity to discuss and explore potential resolutions for conflicts of interest. If there are existing engagements that could prevent the law firm from acting for the client, the assessor and the law firm can discuss potential solutions, such as obtaining waivers or seeking alternative legal representation.

### **7.2.11 How do you manage conflict of interest at your firm?**

#### **7.2.11.1 Objective**

To assess their policies and procedures, evaluate compliance with legal and professional standards, mitigate risks, ensure ethical considerations, protect bank interests, promote transparency, and foster a strong relationship based on trust and shared values.

#### **7.2.11.2 Rationale**

It helps the assessor to gain insights into the law firm's conflict of interest management practices and assess their ability to handle potential conflicts that may arise during the legal representation process.

#### **7.2.11.3 Practices**

1. Policy and Procedure Assessment: The question aims to assess the law firm's formal policies and procedures for managing conflicts of interest. By understanding how the firm manages conflicts, the assessor can evaluate the robustness and effectiveness of their conflict-of-interest management framework.
2. Compliance Evaluation: The question addresses compliance with legal and professional standards. It helps the assessor ensure that the law firm has appropriate mechanisms in place to comply with legal and regulatory requirements related to conflicts of interest.
3. Risk Mitigation: The question supports the evaluation of risk mitigation strategies. By understanding the firm's conflict of interest management practices, the assessor can assess how effectively the firm identifies and mitigates conflicts that could potentially impact the legal representation and the client's interests.
4. Ethical Considerations: The question helps assess the firm's commitment to ethical considerations in legal representation. By learning about their conflict management processes, the assessor can evaluate whether the firm adheres to ethical standards, such as maintaining client confidentiality, avoiding situations of divided loyalty, and ensuring the best interests of the client.
5. Client Protection: The question addresses bank protection and the preservation of confidentiality. It helps the assessor ensure that the law firm has mechanisms in place to protect client's interests and maintain the confidentiality of information.
6. Transparency and Disclosure: The question promotes transparency and disclosure in relationships. By discussing the firm's conflict of interest management practices, the assessor and the law firm can establish a foundation of transparency, trust, and open communication regarding potential conflicts that may arise during the legal representation.
7. Relationship Building: The question provides an opportunity to discuss and understand the law firm's approach to managing conflicts of interest. It helps build a relationship based on mutual understanding, trust, and shared values between the assessor and the law firm.

**7.2.12 Is your firm's management led by a majority of women/minority professionals and individuals?**

**7.2.12.1 Objective**

To assess the firm's diversity and inclusivity, evaluate equal representation in leadership roles, assess organizational culture and values, promote social responsibility, and align with stakeholder expectations.

**7.2.12.2 Rationale**

It helps the assessor to gauge the law firm's commitment to promoting diversity and inclusivity in its leadership positions, fostering an inclusive work environment, and creating opportunities for professional growth and advancement for women and minority professionals.

**7.2.12.3 Practices**

1. Diversity Assessment: The question aims to assess the diversity within the law firm's management team. By understanding the composition of the management team, the assessor can evaluate the extent to which the firm promotes diversity and inclusivity in leadership positions.
2. Inclusivity Evaluation: The question addresses inclusivity in decision-making and leadership roles. It helps the assessor ensure that the law firm provides equal opportunities for women and minority professionals to hold key management positions within the firm.
3. Equal Representation: The question seeks to determine whether the law firm's management team reflects a balanced representation of women and minority professionals. It allows the assessor to assess whether the firm has made efforts to overcome historical disparities and promote equal representation in leadership positions.
4. Organizational Culture: The question provides insights into the law firm's organizational culture and values. By understanding the composition of the management team, the assessor can assess whether the firm values diversity, inclusivity, and equal opportunities for professional growth and advancement.
5. Supplier Diversity: The question may also relate to supplier diversity initiatives. By determining the representation of women and minority professionals in leadership roles, the assessor can assess whether the law firm promotes supplier diversity by engaging and supporting diverse-owned businesses and vendors.
6. Corporate Social Responsibility: The question aligns with corporate social responsibility objectives. It helps the assessor ensure that the law firm actively promotes diversity and inclusivity as part of its commitment to social responsibility, equality, and fairness.
7. Stakeholder Perception: The question addresses the perception of the law firm's commitment to diversity and inclusion. By disclosing the representation within the management team, the law firm demonstrates transparency and openness to stakeholders who value diversity and may prioritize working with firms that promote equal representation.

**7.2.13 Does your firm have an annual internal program for regularly tracking diversity within your firm?**

**7.2.13.1 Objective**

To assess the firm's commitment to diversity and inclusivity, evaluate data collection and analysis practices, measure performance and progress, benchmark against industry standards, promote transparency and accountability, drive continuous improvement, and align with stakeholder expectations.

### **7.2.13.2 Rationale**

It helps the assessor to gauge the law firm's efforts in monitoring diversity, establishing diversity goals, and promoting a diverse and inclusive work environment.

### **7.2.13.3 Practices**

1. Diversity Monitoring: The question aims to assess whether the law firm has a formal program in place to track diversity. By understanding whether the firm monitors diversity metrics regularly, the assessor can evaluate the firm's commitment to diversity and inclusivity.
2. Data Collection and Analysis: The question addresses the law firm's approach to collecting and analyzing diversity-related data. It helps the assessor determine whether the firm has established processes and systems for gathering relevant information on the composition of its workforce, particularly with respect to diversity characteristics such as gender, race, ethnicity, and other protected categories.
3. Performance Evaluation: The question allows for evaluating the effectiveness of the law firm's diversity initiatives. By tracking diversity metrics regularly, the firm can assess its progress over time, identify areas for improvement, and set goals for enhancing diversity and inclusivity within the firm.
4. Benchmarking and Comparison: The question supports benchmarking and comparison with industry standards and best practices. It helps the assessor assess whether the law firm's internal program aligns with recognized diversity tracking methodologies and whether it is comparable to other firms in terms of transparency and accountability in diversity reporting.
5. Transparency and Accountability: The question promotes transparency and accountability in diversity efforts. By having an annual internal program for tracking diversity, the law firm demonstrates its commitment to monitoring progress, identifying disparities, and taking actions to promote diversity and inclusivity within the firm.
6. Continuous Improvement: The question encourages a culture of continuous improvement in diversity initiatives. By regularly tracking diversity, the law firm can identify trends, challenges, and opportunities for enhancing diversity and inclusivity strategies, fostering an environment that values and promotes equal opportunities for all employees.
7. Stakeholder Expectations: The question addresses the expectations of stakeholders, including banks, employees, and the wider community, regarding diversity and inclusion. By tracking diversity within the firm and having an annual program for doing so, the law firm can demonstrate its responsiveness to stakeholder expectations and its commitment to diversity as a core value.

### **7.2.14 Does your firm have any representation goals or targets for diversity?**

#### **7.2.14.1 Objective**

To evaluate the firm's commitment to diversity and inclusion, assess its strategic planning and progress tracking processes, promote equal opportunity, ensure transparency and accountability, enhance employee engagement and retention, benchmark against industry standards, and align with stakeholder expectations.

#### **7.2.14.2 Rationale**

It helps the assessor to understand the firm's proactive measures in promoting diversity representation and creating an inclusive work environment.

### **7.2.14.3 Practices**

1. Diversity Commitment: The question aims to assess the law firm's commitment to promoting diversity and inclusion. By having representation goals or targets, the firm demonstrates its proactive approach towards creating a diverse workforce that reflects the broader community and promotes equal opportunities for individuals from underrepresented groups.
2. Strategic Planning: The question addresses the law firm's strategic planning and goal-setting processes. It helps the assessor understand whether the firm has set measurable objectives related to diversity representation and whether these goals align with the firm's overall business objectives and values.
3. Accountability and Progress Tracking: The question allows for evaluating the firm's accountability and progress in achieving diversity goals. By having specific targets, the firm can track its performance, measure progress over time, and take necessary actions to address any gaps or disparities in diversity representation.
4. Equal Opportunity Promotion: The question supports the promotion of equal opportunity within the law firm. By setting representation goals or targets, the firm actively works towards ensuring fair and inclusive practices in recruitment, hiring, promotion, and retention of employees from diverse backgrounds.
5. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By having representation goals or targets, the law firm can demonstrate its commitment to diversity to clients, stakeholders, and the public. It allows the firm to report on its progress, showcase achievements, and promote transparency in its diversity efforts.
6. Employee Engagement and Retention: The question acknowledges the importance of diversity in fostering employee engagement and retention. By having representation goals or targets, the law firm creates an inclusive work environment that values and supports the diverse perspectives, experiences, and backgrounds of its employees.
7. Benchmarking and Best Practices: The question supports benchmarking against industry standards and best practices. It allows the assessor to assess whether the law firm's representation goals or targets align with recognized diversity initiatives and whether the firm is proactive in adopting strategies to enhance diversity and inclusivity.

### **7.2.15 Does your firm consider the diversity of staffing on bank matters?**

#### **7.2.15.1 Objective**

To assess the firm's commitment to diversity and inclusion, evaluate its responsiveness to client expectations, promote equal opportunity, enhance employee engagement and retention, demonstrate best practices, and foster transparency and accountability in diversity efforts.

#### **7.2.15.2 Rationale**

It helps the assessor to gauge the firm's efforts in providing diverse legal teams and aligning staffing decisions with the goal of inclusivity.

#### **7.2.15.3 Practices**

1. Diversity Consideration: The question aims to assess the law firm's commitment to considering diversity when staffing client matters. By asking this question, the assessor seeks to determine whether the firm actively promotes diversity and inclusivity in its client service delivery.

2. Client Expectations: The question addresses client expectations regarding diversity and inclusivity. It helps the assessor understand whether the law firm aligns its staffing decisions with the client's expectations for diverse legal teams and whether the firm is responsive to bank demands for diverse representation.
3. Equal Opportunity Promotion: The question supports the promotion of equal opportunity and inclusion within the law firm. By considering the diversity of staffing on bank matters, the firm ensures that individuals from underrepresented groups have equal opportunities to participate in high-profile or significant bank engagements.
4. Enhanced Client Relationships: The question recognizes the value of diverse legal teams in building stronger client relationships. By considering diversity in staffing decisions, the law firm can demonstrate its commitment to providing diverse perspectives, experiences, and expertise to clients, potentially fostering stronger connections and understanding.
5. Employee Engagement and Retention: The question acknowledges the importance of diversity in fostering employee engagement and retention. By considering diversity in staffing, the law firm creates opportunities for diverse lawyers to gain valuable experience, contribute to client matters, and enhance their professional growth and satisfaction.
6. Demonstrating Best Practices: The question supports the promotion of best practices in the legal industry. By considering the diversity of staffing, the law firm can showcase its commitment to diversity and inclusivity, potentially serving as a role model for other firms and encouraging industry-wide adoption of diverse staffing practices.
7. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By considering diversity in staffing on bank matters, the law firm can demonstrate its commitment to diversity to clients, stakeholders, and the public. It allows the firm to report on its efforts to provide diverse legal teams and promote transparency in its diversity initiatives.

### **7.2.16 Do the relationship partner(s) assigned to us self-identify as diverse?**

#### **7.2.16.1 Objective**

To assess the firm's commitment to diversity representation at the partner level, evaluate its responsiveness to bank expectations for diverse representation, promote relationship building through diverse perspectives, demonstrate commitment to diversity and inclusion, ensure continuity of diverse representation in bank relationships, and foster transparency and accountability in diversity efforts.

#### **7.2.16.2 Rationale**

It helps the assessor to gauge the law firm's efforts in providing diverse leadership and fostering inclusive bank relationships.

#### **7.2.16.3 Practices**

1. Diversity Representation: The question aims to assess the diversity representation among the relationship partner(s) assigned to the clients' account. By asking this question, the assessor seeks to understand whether the law firm actively promotes diversity at the partner level and ensures diverse representation in client relationship management.
2. Client Expectations: The question addresses client expectations regarding diverse representation among the partner(s) overseeing their legal matters. It helps the assessor understand whether the law firm aligns its staffing decisions with clients' expectations for diverse representation at senior leadership positions.

3. Relationship Building: The question recognizes the importance of diverse perspectives in building strong client relationships. By having diverse relationship partner(s), the law firm can offer a range of viewpoints and experiences that may resonate with the client's goals, values, and challenges.
4. Demonstrating Commitment: The question allows the law firm to showcase its commitment to diversity and inclusion. By having diverse relationship partner(s), the firm demonstrates its proactive efforts to promote diversity at leadership levels and signals its commitment to creating an inclusive and equitable work environment.
5. Relationship Continuity: The question addresses the continuity of diverse representation in the client's relationship management. It helps the assessor understand whether the firm maintains a diverse composition of relationship partner(s) over time and ensures ongoing diversity in client interactions.
6. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By having diverse relationship partner(s), the law firm can demonstrate its commitment to diversity to clients, stakeholders, and the public. It allows the firm to report on its efforts to provide diverse leadership and promote transparency in its diversity initiatives.

### ***7.2.17 Does your firm have internal process improvement initiatives?***

#### **7.2.17.1 Objective**

To assess the firm's focus on operational efficiency, client service enhancement, quality management, cost reduction, innovation and technology adoption, employee engagement and satisfaction, competitive advantage, and external reporting and transparency.

#### **7.2.17.2 Rationale**

It helps the assessor to gauge the law firm's commitment to continuous improvement and its proactive efforts to optimize internal processes and deliver better legal services to its banks.

#### **7.2.17.3 Practices**

1. Operational Efficiency: The question aims to assess the law firm's focus on operational efficiency and continuous improvement. By asking this question, the assessor seeks to determine whether the firm actively identifies and implements initiatives to enhance its internal processes, workflows, and systems.
2. Client Service Enhancement: The question addresses the potential impact of process improvement initiatives on client service. It helps the assessor understand whether the law firm actively seeks to improve its processes to deliver better and more efficient legal services to clients.
3. Quality Management: The question relates to the firm's commitment to quality management. It aims to assess whether the firm has established processes and initiatives to monitor, evaluate, and enhance the quality of its legal work, documentation, and deliverables.
4. Cost Reduction: The question explores the law firm's efforts to reduce costs through process improvement. It seeks to determine whether the firm actively seeks opportunities to streamline its operations, eliminate inefficiencies, and optimize resource utilization to achieve cost savings.
5. Innovation and Technology Adoption: The question may be related to the firm's adoption of innovative technologies and practices. It helps the assessor understand whether the firm embraces technological advancements and innovative approaches to improve its internal processes and drive efficiency gains.

6. Employee Engagement and Satisfaction: The question acknowledges the potential impact of process improvement initiatives on employee engagement and satisfaction. By actively involving employees in identifying process inefficiencies and implementing improvement initiatives, the firm can foster a culture of continuous learning, professional growth, and job satisfaction.
7. Competitive Advantage: The question recognizes the importance of process improvement in maintaining a competitive edge. It allows the assessor to assess whether the law firm proactively seeks to differentiate itself by optimizing its internal operations, which can result in enhanced service delivery, client satisfaction, and market competitiveness.
8. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By having internal process improvement initiatives, the law firm can demonstrate its commitment to efficiency, quality, innovation, and continuous improvement to clients, stakeholders, and the public.

### **7.2.18 Does your firm have bank-facing process improvement initiatives?**

#### **7.2.18.1 Objective**

To assess the firm's focus on client satisfaction, bank-centricity, service delivery efficiency, communication and transparency, technology adoption, bank feedback and continuous improvement, competitive advantage, and external reporting and transparency.

#### **7.2.18.2 Rationale**

It helps the assessor to gauge the law firm's proactive efforts to optimize bank-facing processes and deliver exceptional experiences to its clients.

#### **7.2.18.3 Practices**

1. Client Satisfaction: The question aims to assess the law firm's commitment to enhancing client satisfaction. By asking this question, the assessor seeks to determine whether the firm has specific initiatives in place to improve the processes, workflows, and interactions that directly impact clients.
2. Client-Centric Approach: The question addresses the firm's focus on a client-centric approach to service delivery. It helps the assessor understand whether the firm actively identifies and implements initiatives to streamline and improve client-facing processes, with the aim of delivering a seamless and positive experience for clients.
3. Service Delivery Efficiency: The question explores the firm's efforts to enhance the efficiency of client service delivery. It seeks to determine whether the firm has identified opportunities to optimize its processes, reduce turnaround times, eliminate bottlenecks, and enhance the overall efficiency of client interactions and engagements.
4. Communication and Transparency: The question relates to the firm's initiatives to improve client communication and transparency. It helps the assessor understand whether the firm actively seeks to enhance communication channels, provide timely updates, and ensure transparency in its processes, decisions, and billing practices.
5. Technology Adoption: The question acknowledges the potential impact of technology on client-facing processes. It aims to assess whether the firm leverages technology and digital tools to streamline client interactions, provide self-service options, and improve overall service delivery efficiency.

6. Client Feedback and Continuous Improvement: The question recognizes the importance of client feedback in driving process improvement. It seeks to determine whether the firm actively seeks and incorporates client feedback to identify areas for improvement, refine processes, and enhance the overall client experience.
7. Competitive Advantage: The question addresses the potential role of client-facing process improvement initiatives in gaining a competitive edge. It allows the assessor to assess whether the firm proactively invests in enhancing client-facing processes to differentiate itself in the market and deliver exceptional client experiences.
8. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By having client-facing process improvement initiatives, the law firm can demonstrate its commitment to delivering high-quality, efficient, and client-centric services.

### **7.2.19 Has your firm conducted process improvement initiatives with our bank?**

#### **7.2.19.1 Objective**

To assess the level of collaboration, tailoring of services, incorporation of client feedback, value creation, relationship strengthening, continuous improvement culture, competitive advantage, and external reporting and transparency.

#### **7.2.19.2 Rationale**

It helps the assessor to gauge the law firm's proactive efforts to identify and implement process improvements that specifically benefit clients.

#### **7.2.19.3 Practices**

1. Partnership and Collaboration: The question aims to assess the level of collaboration between the law firm and clients. By asking this question, the assessor seeks to determine whether the law firm has actively engaged with clients to identify and implement process improvement initiatives.
2. Tailored Service Delivery: The question addresses the potential customization of the law firm's services. It helps the assessor understand whether the law firm has proactively identified areas for improvement specific to client needs, processes, and objectives.
3. Client Feedback Incorporation: The question relates to the law firm's responsiveness to client feedback. It seeks to determine whether the firm has actively sought input from clients and incorporated feedback in identifying and implementing process improvement initiatives.
4. Value Creation: The question explores the potential impact of process improvement initiatives on value creation for clients. It aims to assess whether the law firm has taken steps to enhance its service delivery, efficiency, and effectiveness in ways that benefit clients.
5. Relationship Strengthening: The question acknowledges the potential role of process improvement initiatives in strengthening the relationship between the law firm and the client. It helps the assessor understand whether the firm has proactively collaborated with clients to improve mutual understanding, alignment, and operational effectiveness.
6. Continuous Improvement Culture: The question relates to the law firm's commitment to a culture of continuous improvement. It seeks to determine whether the firm actively seeks opportunities to enhance its services, optimize processes, and drive efficiency gains through ongoing collaboration and improvement initiatives with clients.
7. Competitive Advantage: The question addresses the potential role of process improvement initiatives in gaining a competitive edge. It allows the assessor to assess whether the law firm

- proactively engages with clients to identify and implement initiatives that differentiate it in the market and deliver enhanced value.
8. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By having conducted process improvement initiatives with the client, the law firm can demonstrate its commitment to collaborative improvement efforts and its responsiveness to the client's specific needs and expectations.

### **7.2.20 Does your firm share innovation best practices with your banks?**

#### **7.2.20.1 Objective**

To assess the firm's provision of value-added services, thought leadership, collaboration and knowledge sharing, client empowerment, competitive differentiation, trust and long-term relationships, client feedback and improvement, and external reporting and transparency.

#### **7.2.20.2 Rationale**

It helps the assessor to gauge the law firm's proactive efforts to share its innovation expertise and contribute to the success and innovation capabilities of its clients.

#### **7.2.20.3 Practices**

1. Value-added Services: The question aims to assess whether the law firm provides value-added services to clients beyond traditional legal advice. By asking this question, the assessor seeks to determine whether the firm shares its innovation best practices, which can provide clients with insights, strategies, and approaches to enhance their own innovation efforts.
2. Thought Leadership and Expertise: The question addresses the law firm's thought leadership and expertise in the area of innovation. It helps the assessor understand whether the firm has developed innovative practices, processes, or approaches that it can share with clients to support their own innovation journeys.
3. Collaboration and Knowledge Sharing: The question explores the law firm's approach to collaboration and knowledge sharing with clients. It seeks to determine whether the firm actively engages in sharing its innovation best practices, fostering a collaborative relationship with clients and contributing to their success.
4. Client Empowerment: The question recognizes the importance of empowering clients with knowledge and tools for innovation. It aims to assess whether the law firm takes a proactive role in sharing best practices, enabling clients to enhance their innovation capabilities and make informed decisions regarding their legal matters.
5. Competitive Differentiation: The question addresses the potential role of innovation best practices in differentiating the law firm in the market. It allows the assessor to assess whether the firm leverages its innovation expertise as a unique selling point, showcasing its ability to provide added value to clients beyond traditional legal services.
6. Trust and Long-Term Relationships: The question relates to the development of trust and long-term relationships with the client. By sharing innovation best practices, the law firm demonstrates its commitment to the success and growth of the client, fostering trust, and building strong partnerships.
7. Client Feedback and Improvement: The question acknowledges the potential impact of client feedback on the law firm's innovation practices. By sharing best practices with clients, the firm

can gather feedback, refine its approaches, and continuously improve its own innovation capabilities based on real-world experiences and client perspectives.

8. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By sharing innovation best practices with clients, the law firm can demonstrate its commitment to knowledge sharing, transparency, and supporting clients in their own innovation endeavors.

**7.2.21 Does your firm use non-standard technology (such as document automation, machine-learning contract review, e-discovery tools etc.) for delivery of legal services?**

**7.2.21.1 Objective**

To assess the firm's technological innovation, process optimization, client experience and value, competitive advantage, expertise and knowledge base, data security and privacy, continuous improvement and innovation culture, and external reporting and transparency.

**7.2.21.2 Rationale**

It helps the assessor to gauge the law firm's proactive adoption of technology to enhance its service delivery and provide value-added solutions to clients.

**7.2.21.3 Practices**

1. Technological Innovation: The question aims to assess the law firm's adoption of non-standard technology in its legal service delivery. By asking this question, the assessor seeks to determine whether the firm leverages innovative tools and technologies to enhance its efficiency, accuracy, and effectiveness in providing legal services.
2. Process Optimization: The question addresses the potential use of technology to optimize legal processes. It helps the assessor understand whether the firm employs non-standard technology, such as document automation, machine-learning contract review, e-discovery tools, and others, to streamline workflows, reduce manual effort, and improve the overall efficiency of legal service delivery.
3. Client Experience and Value: The question explores the potential impact of non-standard technology on client experience and value. It aims to assess whether the firm utilizes innovative tools to deliver legal services more effectively and efficiently, resulting in enhanced client satisfaction, cost savings, faster turnaround times, and improved outcomes.
4. Competitive Advantage: The question addresses the role of non-standard technology in gaining a competitive edge. It allows the assessor to assess whether the law firm embraces technological advancements to differentiate itself in the market and provide unique value propositions to clients.
5. Expertise and Knowledge Base: The question recognizes the importance of technological proficiency and expertise in the legal profession. It seeks to determine whether the firm possesses the necessary knowledge and capabilities to leverage non-standard technology effectively, keeping pace with evolving industry trends and client expectations.
6. Data Security and Privacy: The question may relate to the firm's approach to data security and privacy when using non-standard technology. It allows the assessor to assess whether the firm has implemented appropriate safeguards and measures to protect client data and ensure compliance with relevant privacy regulations.

7. Continuous Improvement and Innovation Culture: The question acknowledges the potential role of non-standard technology in fostering a culture of continuous improvement and innovation within the law firm. It helps the assessor understand whether the firm actively explores and adopts new technologies, staying at the forefront of industry advancements and driving ongoing improvements in service delivery.
8. External Reporting and Transparency: The question relates to external reporting and transparency initiatives. By utilizing non-standard technology for legal service delivery, the law firm can demonstrate its commitment to leveraging technology for client benefit and showcase its innovative capabilities to clients and external stakeholders.

### ***7.2.22 Does your firm propose improvements to legal documents and strategy on our matters?***

#### **7.2.22.1      Objective**

To assess the firm's value-added services, strategic thinking, expertise and industry knowledge, client collaboration and communication, efficiency and effectiveness, continuous improvement and innovation, client relationship development, and external reporting and transparency.

#### **7.2.22.2      Rationale**

It helps the assessor to gauge the firm's proactive approach to providing comprehensive and high-quality legal services, ensuring that legal documents and strategies are continuously reviewed, refined, and optimized to meet client needs and objectives.

#### **7.2.22.3      Practices**

1. Value-Added Services: The question aims to assess whether the law firm goes beyond the traditional role of legal representation and actively contributes value-added services. By asking this question, the assessor seeks to determine whether the firm proactively identifies opportunities for improving legal documents, such as contracts, agreements, pleadings, or other legal instruments, to ensure clarity, accuracy, and legal effectiveness.
2. Strategic Thinking: The question addresses the law firm's ability to think strategically and provide strategic guidance to clients. It aims to assess whether the firm offers insights and recommendations regarding legal strategies to optimize outcomes and align them with client goals and objectives.
3. Expertise and Industry Knowledge: The question recognizes the importance of expertise and industry knowledge in legal services. It seeks to determine whether the law firm leverages its legal expertise, experience, and understanding of the client's industry to propose improvements in legal documents and strategy, ensuring compliance, mitigating risks, and maximizing advantages.
4. Client Collaboration and Communication: The question highlights the importance of collaboration and communication between the law firm and the client. It aims to assess whether the firm actively engages in discussions and dialogues with the client to identify areas of improvement in legal documents and strategy, fostering a collaborative and client-centric approach.
5. Efficiency and Effectiveness: The question addresses the potential impact of proposed improvements on the efficiency and effectiveness of legal matters. It seeks to understand whether the firm's proactive approach leads to streamlined processes, reduced legal risks, improved outcomes, and overall client satisfaction.
6. Continuous Improvement and Innovation: The question acknowledges the firm's commitment to continuous improvement and innovation. It explores whether the firm actively seeks

opportunities to enhance legal documents and strategy by staying updated with legal developments, incorporating best practices, and leveraging innovative approaches to legal representation.

7. Client Relationship Development: The question relates to the development of a long-term bank relationship. By proposing improvements to legal documents and strategy, the law firm demonstrates its commitment to providing comprehensive and personalized legal services, building trust and loyalty with the client.
8. External Reporting and Transparency: The question also has implications for external reporting and transparency. By actively proposing improvements to legal documents and strategy, the law firm may demonstrate its commitment to quality, legal excellence, and client-centricity to external stakeholders, such as regulators, auditors, or other parties involved in assessing the client's performance.

### **7.2.23 Does your firm hold “voice of client” sessions with us?**

#### **7.2.23.1 Objective**

To evaluate the firm's client-centric approach, feedback collection efforts, bank satisfaction and relationship management, quality improvement initiatives, client engagement and communication, service customization, relationship development and trust building, client retention and loyalty, and continuous engagement and monitoring.

#### **7.2.23.2 Rationale**

It helps the assessor to gauge the firm's commitment to understanding and meeting the client's needs, preferences, and expectations, and to assess the effectiveness of its client feedback mechanisms and processes.

#### **7.2.23.3 Practices**

1. Client-Centric Approach: The question aims to evaluate the law firm's commitment to a client-centric approach. By conducting “voice of client” sessions, the firm demonstrates its interest in understanding the client's perspective, needs, and expectations, and seeks to align its services accordingly.
2. Feedback Collection: The question addresses the firm's efforts to collect feedback from the client on various aspects of their engagement. It seeks to determine whether the firm provides a platform or mechanism for the client to express their opinions, suggestions, concerns, or satisfaction regarding the legal services provided.
3. Client Satisfaction and Relationship Management: The question recognizes the importance of bank satisfaction and relationship management. By holding “voice of client” sessions, the firm aims to assess and improve its performance based on client feedback, strengthen the relationship, and ensure that the client's expectations are being met.
4. Quality Improvement: The question highlights the firm's commitment to continuous improvement and quality enhancement. By actively seeking the client's perspective, the firm can identify areas for improvement in its services, processes, communication, and overall client experience.
5. Client Engagement and Communication: The question addresses the firm's level of engagement and communication with the client. It aims to assess whether the firm proactively initiates

- discussions, meetings, or sessions to gather insights from the client, understand their business objectives, legal requirements, and preferences, and adapt its services accordingly.
- 6. Service Customization: The question acknowledges the importance of tailoring legal services to meet the specific needs and preferences of the client. By conducting “voice of client” sessions, the firm can gather valuable information to customize its services, strategies, and approaches, ensuring a personalized and relevant experience for the client.
  - 7. Relationship Development and Trust Building: The question relates to the development of a strong and long-term client relationship. By holding “voice of client” sessions, the firm demonstrates its commitment to actively listening to the client, valuing their input, and fostering a collaborative and trust-based relationship.
  - 8. Client Retention and Loyalty: The question also has implications for client retention and loyalty. By actively seeking and acting upon client feedback, the firm could address any concerns, enhance the client experience, and increase the likelihood of client satisfaction, loyalty, and future engagements.
  - 9. Continuous Engagement and Monitoring: The question implies an ongoing process of client engagement and monitoring. It assesses whether the firm conducts regular or periodic “voice of client” sessions to ensure that feedback is consistently collected, analyzed, and acted upon.

### **7.2.24 Does your firm hold post-matter reviews with us?**

#### **7.2.24.1 Objective**

To evaluate the firm’s commitment to service evaluation, client satisfaction assessment, identification of strengths and weaknesses, continuous improvement, relationship strengthening, client-centric approach, client retention and loyalty, performance evaluation, and accountability.

#### **7.2.24.2 Rationale**

It helps the assessor to assess the firm’s efforts in gathering client feedback, learning from past experiences, and improving future service delivery based on client insights and expectations.

#### **7.2.24.3 Practices**

- 1. Evaluation of Service Delivery: The question aims to evaluate the law firm’s commitment to evaluating and improving its service delivery. By conducting post-matter reviews, the firm seeks to assess its performance, identify areas of success or improvement, and gather feedback from clients regarding the overall experience and outcomes of the matter.
- 2. Client Satisfaction Assessment: The question addresses the firm’s efforts to assess client satisfaction and gather feedback on the specific legal matter or engagement. It allows the firm to understand the clients’ perspective, expectations, and level of satisfaction with the legal services provided.
- 3. Identification of Strengths and Weaknesses: The question helps in identifying the strengths and weaknesses of the law firm’s performance in the specific matter. By soliciting feedback from clients, the firm can gain insights into the aspects that worked well and those that may require improvement, such as communication, responsiveness, legal strategy, or efficiency.
- 4. Lessons Learned and Knowledge Sharing: The question facilitates knowledge sharing and learning within the law firm. Through post-matter reviews, the firm can capture valuable insights and lessons learned from client perspectives, which can be shared internally to enhance the firm’s collective knowledge and improve future service delivery.

5. Continuous Improvement: The question underscores the importance of continuous improvement and learning from past experiences. By conducting post-matter reviews, the firm may identify opportunities for enhancing its processes, approaches, and bank service, thereby improving the overall quality and value of its legal services.
6. Relationship Strengthening: The question may contribute to strengthening the relationship between the law firm and the client. By actively seeking feedback and engaging in post-matter discussions, the firm demonstrates its commitment to client satisfaction, open communication, and a collaborative approach to addressing client needs.
7. Client-Centric Approach: The question aligns with a client-centric approach to legal services. It demonstrates the firm's willingness to listen, understand, and respond to client feedback, ensuring that their expectations are met, and future engagements are tailored to their specific requirements.
8. Client Retention and Loyalty: The question has implications for client retention and loyalty. By conducting post-matter reviews, the firm shows its commitment to maintaining a strong client relationship beyond the completion of the matter. It allows the firm to address any concerns, address outstanding issues, and further strengthen the client's trust and confidence in the firm's services.
9. Performance Evaluation and Accountability: The question may relate to performance evaluation and accountability within the law firm. By conducting post-matter reviews, the firm establishes a mechanism to assess the performance of its lawyers and teams, providing an opportunity for self-reflection, learning, and accountability.

### **7.2.25 Does your firm use legal process outsourcing (LPO) or alternative legal services providers (ALSP)?**

#### **7.2.25.1 Objective**

To assess the firm's strategies for enhancing efficiency, accessing specialized skills, achieving scalability and flexibility, focusing on core competencies, ensuring quality and expertise, mitigating risks, embracing innovation and technology, delivering value, and adopting industry best practices.

#### **7.2.25.2 Rationale**

It helps the assessor to evaluate the firm's approach to outsourcing, resource allocation, and service optimization to meet client needs effectively and efficiently.

#### **7.2.25.3 Practices**

1. Efficiency and Cost-effectiveness: The question aims to evaluate whether the law firm adopts LPO or ALSP to enhance operational efficiency and reduce costs. By outsourcing certain legal processes or engaging alternative service providers, the firm may leverage specialized expertise, streamlined workflows, and potentially lower labour costs, leading to increased efficiency and cost savings.
2. Access to Specialized Skills: The question addresses the firm's ability to tap into specialized skills or resources that may not be available in-house. LPOs and ALSPs often offer specific expertise, technologies, or industry knowledge that can augment the firm's capabilities and enable them to provide comprehensive and high-quality legal services to clients.
3. Scalability and Flexibility: The question assesses whether the firm leverages LPO or ALSP to scale its operations or adapt to changing workloads. Outsourcing certain tasks or engaging external

- providers can offer scalability and flexibility, allowing the firm to handle fluctuations in workload, meet tight deadlines, or address resource constraints more effectively.
- 4. Focus on Core Competencies: The question examines whether the law firm focuses its internal resources on core legal competencies while outsourcing non-core or repetitive tasks. By utilizing LPO or ALSP, the firm can free up its lawyers' time and energy to focus on strategic legal advice, bank relationships, and other value-added activities, enhancing overall service quality and client satisfaction.
  - 5. Quality and Expertise Assurance: The question seeks to evaluate whether the firm maintains quality standards and ensures expertise in the outsourced or alternative legal services. The firm needs to demonstrate that appropriate due diligence is conducted when engaging LPOs or ALSPs to ensure the quality and reliability of the services provided.
  - 6. Risk Mitigation: The question addresses the firm's risk mitigation strategies when utilizing LPO or ALSP. It allows the assessor to assess whether the firm has implemented measures to safeguard confidentiality, data protection, and compliance with applicable legal and regulatory requirements when outsourcing certain legal processes or engaging external service providers.
  - 7. Innovation and Technology Adoption: The question explores whether the firm embraces innovation and technology through the use of LPO or ALSP. These providers often leverage advanced technologies, automation tools, or AI-driven solutions to enhance efficiency, accuracy, and process optimization. By utilizing such services, the firm can demonstrate a commitment to innovation and staying at the forefront of legal service delivery.
  - 8. Client Value Proposition: The question relates to the firm's client value proposition. By utilizing LPO or ALSP, the firm can offer clients a cost-effective and efficient service delivery model, potentially resulting in more competitive pricing, enhanced turnaround times, and increased overall value for the clients.
  - 9. Industry Best Practices: The question may help identify whether the firm embraces industry best practices and explores emerging trends in legal service delivery. LPOs and ALSPs often bring innovative approaches and methodologies to the table, allowing the firm to benchmark against industry standards and continuously improve its service offerings.

### **7.2.26 Does your firm use alternative internal legal professional sourcing (non-partnership track lawyers; paralegals, etc.)?**

#### **7.2.26.1 Objective**

To assess the firm's strategies for workforce optimization, flexibility, cost-effectiveness, task delegation, service delivery enhancement, professional development, resource allocation, expertise diversity, and career path development.

#### **7.2.26.2 Rationale**

It helps the assessor to evaluate the firm's approach to talent management and resource utilization, ensuring the firm has the right mix of legal professionals to meet client needs efficiently and effectively.

#### **7.2.26.3 Practices**

- 1. Workforce Optimization: The question aims to assess whether the law firm adopts alternative sourcing strategies to optimize its workforce composition and effectively allocate resources. By employing non-partnership track lawyers and paralegals, the firm may streamline its operations,

enhance efficiency, and manage costs more effectively, while still maintaining high-quality legal services.

2. Flexibility and Scalability: The question addresses the firm's ability to scale its workforce based on the fluctuating demand for legal services. By utilizing non-partnership track lawyers and paralegals, the firm can leverage a flexible workforce that can be adjusted as per the changing needs of the clients, cases, or projects.
3. Cost-effectiveness: The question evaluates whether the firm leverages alternative sourcing options to optimize costs. Hiring non-partnership track lawyers or utilizing paralegals can be a cost-effective approach compared to relying solely on partnership-track lawyers for all legal work. This strategy allows the firm to allocate resources appropriately and manage the overall cost structure.
4. Task Delegation and Efficiency: The question assesses the firm's ability to delegate appropriate legal tasks to different roles within the firm. Non-partnership track lawyers and paralegals can handle routine or administrative tasks, allowing partnership-track lawyers to focus on more complex legal matters, strategic advice, and bank management. This delegation of tasks improves overall efficiency and productivity.
5. Enhanced Service Delivery: The question explores whether the firm uses alternative sourcing to enhance its service delivery capabilities. By having a diverse mix of legal professionals, the firm can match the right expertise and skill sets to specific tasks, ensuring optimal client service and efficient resolution of legal matters.
6. Professional Development and Talent Pipeline: The question addresses the firm's commitment to nurturing talent and providing growth opportunities. Utilizing non-partnership track lawyers and paralegals can offer valuable career development paths for legal professionals at various stages of their careers, creating a talent pipeline and promoting internal mobility within the firm.
7. Resource Allocation and Utilization: The question helps assess the firm's ability to allocate and utilize resources effectively. By strategically deploying non-partnership track lawyers and paralegals, the firm can optimize resource allocation based on the complexity and nature of legal work, ensuring that the right resources are assigned to the right tasks.
8. Expertise and Skill Diversity: The question examines whether the firm values and benefits from the diverse expertise and skills that alternative legal professionals bring to the firm. Non-partnership track lawyers and paralegals often possess specialized knowledge or unique skill sets that complement the overall capabilities of the firm, leading to enhanced service offerings and client satisfaction.
9. Career Path and Workforce Engagement: The question addresses the firm's commitment to providing meaningful career paths for legal professionals. It allows the firm to demonstrate its dedication to talent development, engagement, and retention by offering diverse opportunities and recognizing the value of different legal roles within the firm.

### **7.2.27 Does your firm use project managers on our matters? If yes, does your firm charge us for the project managers?**

#### **7.2.27.1      Objective**

To assess the firm's project management capabilities, operational efficiency, cost transparency, value proposition, client collaboration, resource allocation, cost management, and client satisfaction.

### **7.2.27.2 Rationale**

It helps the assessor evaluate the firm's commitment to delivering organized, efficient, and client-focused legal services.

### **7.2.27.3 Practices**

1. Project Management Approach: The question aims to understand whether the law firm employs project management techniques and practices in the execution and delivery of services. Project managers play a crucial role in planning, coordinating, and monitoring the progress of legal projects, ensuring timely and efficient completion.
2. Operational Efficiency: The question addresses the firm's commitment to operational excellence and process improvement. By utilizing project managers, the firm could enhance efficiency, streamline workflows, and optimize resource allocation, leading to improved outcomes and client satisfaction.
3. Cost Transparency: The question seeks to ascertain whether the law firm charges clients for the services of project managers. This information allows clients to have transparency regarding the billing structure and understand any additional costs associated with project management support.
4. Value Proposition: The question helps assess the value proposition offered by the law firm. If project management services are provided without additional charges, it demonstrates the firm's commitment to delivering high-quality legal services with added value, including effective project management.
5. Client Collaboration: The question explores whether the law firm actively collaborates with clients in managing matters. By involving project managers, the firm may facilitate better communication, provide regular updates, and ensure alignment with client objectives throughout the duration of the engagement.
6. Resource Allocation and Utilization: The question assesses how the firm assigns and utilizes resources, including project managers, for client matters. This provides insights into the firm's approach to resource planning, ensuring that appropriate expertise and skills are allocated to each matter for efficient and effective project execution.
7. Cost Management and Control: The question helps banks understand how project management services are factored into the overall cost structure. If there are charges associated with project managers, it allows the client to evaluate the cost-benefit relationship and assess the value of their involvement in managing the matter.
8. Client Engagement and Satisfaction: The question aims to gauge the impact of project managers on client engagement and satisfaction. Effective project management may lead to better coordination, clear communication, and timely delivery of legal services, resulting in enhanced client experience and overall satisfaction.

### **7.2.28 Do you provide free continuing professional development/legal education to us?**

#### **7.2.28.1 Objective**

To evaluate the firm's commitment to client education, value-added services, relationship strengthening, professional development support, thought leadership, client retention, competitive differentiation, and client satisfaction.

**7.2.28.2 Rationale**

It helps the assessor evaluate the firm's efforts to go beyond legal representation and contribute to the knowledge and success of its clients.

**7.2.28.3 Practices**

1. Client Education and Empowerment: The question aims to assess the law firm's commitment to client education and empowerment. By providing free CPD or legal education programs, the firm demonstrates its dedication to keeping clients informed about relevant legal topics, updates, and developments. This helps clients stay knowledgeable and better equipped to make informed decisions related to their legal matters.
2. Value-Added Services: The question explores whether the law firm offers additional value to its clients beyond legal representation. Providing free CPD or legal education programs is a value-added service that enhances the overall client experience and establishes the firm as a trusted resource for legal knowledge and expertise.
3. Relationship Strengthening: By offering free CPD or legal education programs, the law firm aims to strengthen its relationship with clients. These programs provide opportunities for engagement, networking, and knowledge-sharing, fostering a sense of partnership and collaboration between the firm and clients.
4. Professional Development Support: The question addresses whether the law firm supports the ongoing professional development of its clients. By offering free CPD or legal education programs, the firm assists clients in enhancing their professional skills, staying up-to-date with legal trends, and expanding their knowledge base.
5. Thought Leadership and Expertise Showcase: The question seeks to highlight the law firm's thought leadership and expertise. By organizing CPD or legal education programs, the firm demonstrates its in-depth knowledge, subject matter expertise, and ability to deliver informative and engaging educational content to clients.
6. Client Retention and Loyalty: Providing free CPD or legal education programs can contribute to client retention and foster loyalty. Clients appreciate the added value they receive from the firm, creating a stronger bond and incentivizing them to continue their relationship with the firm for future legal needs.
7. Competitive Differentiation: The question helps differentiate the law firm from its competitors. Offering free CPD or legal education programs sets the firm apart by showcasing its commitment to client education, providing a unique selling proposition that may attract new clients and retain existing ones.
8. Client Satisfaction: By providing free CPD or legal education programs, the firm aims to enhance client satisfaction. Clients who participate in these programs have the opportunity to expand their knowledge, gain insights from legal experts, and feel supported in their professional development, leading to increased satisfaction with the firm's services.

**7.2.29 Do you provide clients with secondments of your lawyers?****7.2.29.1 Objective**

To evaluate the firm's commitment to client support, collaboration, knowledge transfer, seamless integration, relationship strengthening, client satisfaction, client retention, and competitive differentiation.

**7.2.29.2 Rationale**

It helps the assessor evaluate the firm's efforts to provide comprehensive and tailored legal services that meet the evolving needs of its clients.

**7.2.29.3 Practices**

1. Client Support and Collaboration: The question aims to assess the law firm's willingness to provide additional support and collaboration opportunities to its clients. By offering secondments, the firm allows its lawyers to work directly with the client's legal team, providing on-site assistance and fostering closer collaboration between the firm and the clients.
2. Knowledge Transfer and Skill Enhancement: Secondments provide an opportunity for knowledge transfer and skill enhancement for both the law firm's lawyers and the client's legal team. Through working closely together on specific projects or cases, lawyers can share expertise, best practices, and industry insights, benefiting both parties and contributing to professional development.
3. Seamless Integration and Understanding: By offering secondments, the law firm facilitates a deeper understanding of the client's business, operations, and legal needs. Lawyers who work on secondment gain firsthand experience of the client's challenges, goals, and internal dynamics, enabling them to provide more tailored and effective legal advice and support.
4. Relationship Strengthening: Secondments can strengthen the relationship between the law firm and the client. By embedding lawyers within the client's legal team, the firm demonstrates a commitment to understanding the client's unique needs and providing personalized services. This can enhance trust, collaboration, and long-term partnership between the firm and the client.
5. Client Satisfaction: The question addresses whether the law firm goes beyond traditional legal services to meet the client's specific requirements. By offering secondments, the firm demonstrates a proactive approach to client satisfaction and a willingness to provide practical and hands-on support that goes beyond traditional attorney-client interactions.
6. Client Retention and Loyalty: Secondments can contribute to client retention and foster loyalty. By offering lawyers on secondment, the law firm provides added value and demonstrates a commitment to the client's success. This can strengthen the client's trust in the firm and increase their likelihood of continuing the relationship for future legal needs.
7. Competitive Differentiation: The question helps differentiate the law firm from its competitors. Offering secondments as an additional service sets the firm apart by showcasing its ability to provide customized support and deep integration with the client's legal team, potentially attracting new clients and retaining existing ones.

**7.2.30 Do you provide clients with opportunities for student(s) to spend a rotation with them?****7.2.30.1 Objective**

To evaluate the firm's commitment to professional development, experiential learning, client engagement, relationship building, talent pipeline development, client satisfaction, and competitive differentiation.

**7.2.30.2 Rationale**

It helps the assessor evaluate the firm's efforts to provide comprehensive and enriching experiences for students while also meeting the needs and expectations of its clients.

**7.2.30.3 Practices**

1. Professional Development: By providing opportunities for students to spend rotations with clients, the law firm aims to enhance the professional development of these students. It allows them to gain practical experience, exposure to real-life legal matters, and the opportunity to work directly with clients. This could help students develop important skills and competencies necessary for their future legal careers.
2. Experiential Learning: The question addresses the firm's commitment to providing experiential learning opportunities to students. By immersing students in the client's legal environment, they gain insights into the client's industry, legal challenges, and business operations. This firsthand experience enhances their understanding of practical legal issues and strengthens their ability to provide relevant and effective legal advice.
3. Client Engagement and Collaboration: Offering student rotations with clients demonstrates the law firm's commitment to client engagement and collaboration. It allows students to work closely with the client's legal team, fostering relationships, and facilitating collaboration. This could contribute to a deeper understanding of client needs, objectives, and expectations.
4. Relationship Building: The question addresses whether the law firm actively invests in relationship building by involving students in client rotations. It demonstrates the firm's commitment to building long-term partnerships with clients by providing opportunities for students to connect and contribute to client legal initiatives. This may help establish strong relationships and trust between the firm, the clients, and future lawyers.
5. Talent Pipeline: By offering student rotations with clients, the law firm helps establish a talent pipeline and build connections with emerging legal professionals. It provides students with exposure to the client's organization, culture, and legal practices, potentially nurturing future employment opportunities. This benefits both the firm and clients by cultivating a pool of talented individuals familiar with the clients' legal needs.
6. Client Satisfaction and Added Value: Offering student rotations as an additional service demonstrates the law firm's commitment to client satisfaction and providing added value. Clients may appreciate the opportunity to contribute to the development of future legal professionals and play an active role in shaping their learning experiences. This may strengthen the client-firm relationship and contribute to long-term client loyalty.
7. Competitive Differentiation: The question helps differentiate the law firm from its competitors by showcasing its commitment to innovative legal education and bank engagement. Providing opportunities for student rotations sets the firm apart by demonstrating its dedication to practical learning and bank integration, potentially attracting new clients and retaining existing ones.

**7.2.31 Do you provide clients with other value-add services?****7.2.31.1 Objective**

To gather information about any supplementary services offered by the firm, assess client satisfaction and retention strategies, evaluate competitive differentiation, measure client engagement and relationship building efforts, explore potential revenue generation opportunities, and determine the firm's client-centric approach.

**7.2.31.2 Rationale**

It helps the assessor understand how the firm goes beyond its core offerings to deliver enhanced value and meet the evolving needs of its clients.

## 7.2.31.3 Practices

1. Identifying Value-Add Services: The question aims to identify any supplementary services provided by the firm that go beyond its primary offerings. It seeks to gather information about value-added services that enhance client experience or provide additional benefits beyond the core services.
2. Client Satisfaction and Retention: The question indirectly addresses the firm's focus on client satisfaction and retention. It aims to evaluate whether the firm recognizes the importance of offering value-add services to enhance client relationships, meet evolving client needs, and retain their business. Value-add services may contribute to client satisfaction, loyalty, and long-term partnerships.
3. Competitive Differentiation: The question evaluates whether the firm differentiates itself from competitors by providing unique value-add services. It aims to assess whether the firm leverages these additional services as a competitive advantage to attract and retain clients in a crowded marketplace. Value-add services may set the firm apart from competitors and position it as a preferred choice for clients.
4. Client Engagement and Relationship Building: The question addresses the firm's efforts to engage with clients and build stronger relationships. It aims to determine whether the firm actively seeks opportunities to offer value-add services that align with client needs, preferences, or strategic goals. Providing such services may foster deeper client engagement and strengthen the overall relationship between the firm and the client.
5. Revenue Generation: The question indirectly addresses the potential for revenue generation through value-add services. It aims to evaluate whether the firm views these additional services as potential sources of revenue beyond its core offerings. Value-add services may create new revenue streams, increase client spend, or lead to cross-selling or upselling opportunities.
6. Client-Centric Approach: The question evaluates whether the firm adopts a client-centric approach by identifying and delivering value-add services. It aims to assess whether the firm actively listens to client feedback, identifies their evolving needs, and develops or acquires services that provide additional value and address those needs.

**8. Glossary, Initialisms and Acronyms**

Term, initialism or acronym	Definition
Botnet	Network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send SPAM messages.
CIRT	Cybersecurity Incident Response Team.
COBIT	A enterprise IT governance and management framework from ISACA.
Critical infrastructure	The processes, systems, facilities, technologies, networks, assets and services essential to the economy.
CSF	Cybersecurity framework.
Cyber-attack	An attempt by hackers or attackers to damage or destroy a computer network or system.
Cyber-incident	Violation of an explicit or implied security policy.
Cyber-physical system	A system of collaborating computational elements controlling physical entities.

## SEAL Methodology: Version 1.2

Cyber-risk	Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its technology.
Cyber-threat	Possibility of a malicious attempt to damage or disrupt a computer network or system. For example, a cyber-threat to a system refers to persons (threat actor or agent) who attempt unauthorized access to a system device and/or network using a data communications pathway.
Cybersecurity	Process of applying security measures to ensure confidentiality, integrity, and availability of data. Cybersecurity attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans.
Cyberspace	The complex environment resulting from the interaction of people, software and services on public networks, such as the Internet, by means of technology devices and networks connected to it, which does not exist in any physical form.
Guidance	Collective term for regulations, laws, policies, standards, methodologies, practices and procedures.
Hijacking	Illegally take over a communication channel and force it to go to a different destination or use it for one's own purposes.
ISACA	An independent, non-profit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems formerly known as Information Systems Audit and Control Association.
IT	Information Technology.
Malware	A program inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity and availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
NIST	National Institute of Standards and Technology.
Phishing	Fraudulent practice of sending emails purporting to be from a reputable company to induce employees to reveal personal or corporate information, such as passwords and credit card numbers.
PII	Personally identifiable information. Sometimes referred to as personal information (PI) or sensitive personal information (SPI).
SPAM	Spam involves nearly identical messages being sent to numerous recipients by e-mail. Clicking on links in spam e-mail may send users to phishing sites or sites that are hosting malware. A.K.A. junk e-mail or unsolicited bulk e-mail (UBE)
Spear-phishing	Targeted phishing.
Spoofing	Situation where one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
Trojan horse	A non-self-replicating program that seems to have a useful purpose, but in reality, has a different, malicious purpose.
UBE	Unsolicited bulk e-mail.
Whaling	Specific form of phishing or spear-phishing targeting senior management in private companies.

Zombie	A program that is installed on a system to cause it to attack other systems.
--------	--

## 9. References

The following guidance provided input into this framework:

1. Canadian Cyber Incident Response Centre (CCIRC), *Cyber Security Technical Advice and Guidance*, Public Services Canada: 2015. Retrieved from <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx>.
2. Center for Internet Security, *Critical Security Controls*, CISSecurity: 2022. Retrieved from <http://www.cisecurity.org/critical-controls.cfm>.
3. Committee of Sponsoring Organizations of the Treadway Commission, *Compliance Risk Management: Applying the COSO ERM Framework*, COSO.org: November 2020. Retrieved from <https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf>.
4. Cybersecurity Nexus, *European Cybersecurity Implementation: Assurance*, ISACA: 2014. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx>.
5. Cybersecurity Nexus, *European Cybersecurity Implementation: Overview*, ISACA: 2014. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx>.
6. Cybersecurity Nexus, *European Cybersecurity Implementation: Resilience*, ISACA: 2014. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx>.
7. Cybersecurity Nexus, *European Cybersecurity Implementation: Risk Guidance*, ISACA: 2014. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx>.
8. Cybersecurity Nexus, *Implementing NIST Cyber-security Framework*, ISACA: 2014. Retrieved from <http://www.isaca.org/Education/COBIT-Education/Pages/Implementing-NIST-Cybersecurity-Framework-Using-COBIT-5.aspx>.
9. Federal Financial Institutions Examination Council, *Cybersecurity Assessment Tool*, FFIEC: May 2017. Retrieved from [https://www.ffiec.gov/pdf/cybersecurity/ffiec\\_cat\\_may\\_2017.pdf](https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf).
10. Federal Financial Institutions Examination Council, *Cybersecurity Resource Guide for Financial Institutions*, FFIEC: October 2018. Retrieved from <https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf>
11. Federation of Law Societies of Canada, *Model Code of Professional Conduct*, FLSC: October 2022. Retrieved from [https://flsc-s3-storage-pub.s3.ca-central-1.amazonaws.com/Model%20Code%20Oct%202022.pdf?rt=MXwxfGNvZGUgb2YgcHJvZmVzc2lvbmFsIGNvZGV8MTY4ODgyODc0MA&rt\\_nonce=024ba842f1](https://flsc-s3-storage-pub.s3.ca-central-1.amazonaws.com/Model%20Code%20Oct%202022.pdf?rt=MXwxfGNvZGUgb2YgcHJvZmVzc2lvbmFsIGNvZGV8MTY4ODgyODc0MA&rt_nonce=024ba842f1).

## SEAL Methodology: Version 1.2

12. Financial Services-Information Sharing and Analysis Center, *FSSCC Automated Cybersecurity Assessment Tool*, FS-ISAC: December 28, 2015, Retrieved from <https://www.fsisac.com/article/fsscc-automated-cybersecurity-assessment-tool>.
13. Information Security Alliance/American National Standards Institute, *The Financial Management of Cyber Risk*, ANSI: 2010. Retrieved from <http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf>.
14. Information Systems Audit and Control Association, *Responding to Targeted Cyberattacks*, ISACA: 2013. Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx>.
15. Information Systems Audit and Control Association, *Transforming Cybersecurity: Using COBIT 5*, ISACA: 2013. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/transforming-cybersecurity-using-cobit-5.aspx>.
16. International Organization for Standardization, *ISO 8000-1:2022, Data Quality -- Part 1: Overview*, ISO: 2022. Retrieved from <https://www.iso.org/standard/81745.html>.
17. International Organization for Standardization, *ISO 9000:2015, Quality management systems – Fundamentals and Vocabulary*, ISO: 2015. Retrieved from <https://www.iso.org/standard/45481.html>.
18. International Organization for Standardization, *ISO/IEC 20000-1:2018, Information Technology -- Service management -- Part 1: Service management system requirements*, ISO: 2018. Retrieved from <https://www.iso.org/standard/70636.html>.
19. International Organization for Standardization, *ISO/IEC 22301:2019, Security and Resilience -- Business continuity management systems -- Requirements*, ISO: 2019. Retrieved from <https://www.iso.org/standard/75106.html>.
20. International Organization for Standardization, *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements*, ISO: 2022. Retrieved from <https://www.iso.org/standard/82875.html>.
21. International Organization for Standardization, *ISO/IEC 27014:2020, Information security, cybersecurity and privacy protection -- Governance of information security*, ISO: 2020. Retrieved from <https://www.iso.org/standard/74046.html>.
22. International Organization for Standardization, *ISO/IEC 27032:2012, Information technology -- Security techniques -- Guidelines for cybersecurity*, ISO: 2012. Retrieved from [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=44375](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375).
23. International Organization for Standardization, *ISO/IEC 31000:2018, Risk management -- Guidelines*, ISO: 2018. Retrieved from <https://www.iso.org/standard/65694.html>.
24. International Organization for Standardization, *ISO/IEC 37001:2016, Anti-bribery management systems -- Requirements with guidance for use*, ISO: 2016. Retrieved from <https://www.iso.org/standard/65034.html>.
25. International Organization for Standardization, *ISO/IEC 37301:2021, Compliance management systems -- Requirements with guidance for use*, ISO: 2021. Retrieved from <https://www.iso.org/standard/75080.html>.
26. International Organization for Standardization, *ISO/IEC 38500:2015, Information technology -- Governance of IT for the firm*, ISO: 2015. Retrieved from [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=62816](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62816).

## **SEAL Methodology: Version 1.2**

27. International Organization for Standardization, *ISO/IEC TR 38502:2017, Information technology -- Governance of IT -- Framework and model*, ISO: 2017. Retrieved from <https://www.iso.org/standard/74358.html>.
28. Law Society of Ontario, *Practice Management Guidelines*, LSO: 2023. Retrieved from <https://lso.ca/lawyers/practice-supports-and-resources/practice-management-guidelines>.
29. Law Society of Ontario, *Rules of Professional Conduct*, LSO: June 28, 2022. Retrieved from <https://lso.ca/about-lso/legislation-rules/rules-of-professional-conduct>.
30. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST: February 12, 2014. Retrieved from <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
31. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST: April 16, 2018. Retrieved from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
32. National Institute of Standards and Technology, *NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing*, NIST: October 2016. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
33. National Institute of Standards and Technology, *NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST: August 2017. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>.
34. National Institute of Standards and Technology, *NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery*, NIST: December 2016. Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>.
35. Office of the Superintendent of Financial Institutions. *Cyber Security Self-Assessment Guidance*, OSFI: August 13, 2021. Retrieved from <http://www.osfi-bsif.gc.ca/Eng/fi-if/iai/Pages/cbrsk.aspx>.
36. Office of the Superintendent of Financial Institutions. *Operational Risk Management Guideline (E-21)*, OSFI: July 2022. Retrieved from <https://www.osfi-bsif.gc.ca/Eng/Docs/e21.pdf>.
37. Office of the Superintendent of Financial Institutions. *Technology and Cyber Risk Management Guideline (B-13)*, OSFI: July 2022. Retrieved from <https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx>.
38. Office of the Superintendent of Financial Institutions. *Third-Party Risk Management Guideline (B-10)*, OSFI: April 2023. Retrieved from [https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10\\_dft\\_2022.aspx](https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10_dft_2022.aspx).
39. Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris: 2015. Retrieved from <http://dx.doi.org/10.1787/9789264245471-en>.