

Participating entity accreditation application requirements under the *Consumer-Driven Banking Act*

Disclaimer

This guideline is a draft for industry and **public consultation** only. Revisions to the proposed regulations may inform the final version of this guideline.

Contents

Introduction	2
General application information	2
Who can apply for accreditation	2
Where to submit an application	3
What to expect after submitting an application	3
National security review	3
Accreditation application review	4
The Bank's decision	5
If accreditation is approved	5
If accreditation is refused	5
Review and appeal	5
Application and accreditation requirements for prospective participating entities	6
1. Standard accreditation (non-streamlined)	6
2. Streamlined accreditation for registered payment service providers	12
3. Streamlined accreditation for federal and provincial financial institutions	17

Introduction

This supervisory guideline sets out the Bank of Canada's expectations regarding accreditation application requirements and the process to become a participating entity under the *Consumer-Driven Banking Act* (CDBA) and the *Consumer-Driven Banking Regulations* (CDBR). This guideline does not constitute part of the CDBA or CDBR. The CDBA and CDBR take precedence in the event of any inconsistency or conflict with this guideline.

General application information

This section provides a general overview of the application process for accreditation that applies to all pathways of participating entities. Specific application and accreditation requirements for each pathway are addressed later in this document.

Who can apply for accreditation

The following entities and individuals may apply to the Bank for accreditation as a participating entity under the CDBA.

Federal financial institutions

This category includes federal financial institutions that are **not** listed in the Schedule to the CDBA:

- banks listed in Schedule I or II to the *Bank Act* and authorized foreign banks
- companies to which the *Trust and Loan Companies Act* applies
- associations to which the *Cooperative Credit Associations Act* applies
- companies, fraternal benefit societies or foreign companies to which the *Insurance Companies Act* applies

Federal financial institutions may apply for accreditation through a streamlined accreditation pathway. Details on this pathway and its accreditation requirements are available in the [Streamlined accreditation for federal and provincial financial institutions](#) section of this guideline.

Provincial financial institutions

This category includes:

- cooperative credit societies, savings and credit unions or caisses populaires that are regulated by a provincial Act
- provincial Crown corporations that offer deposit-taking services
- insurance companies that are regulated by a provincial Act

Provincial financial institutions may apply for accreditation through a streamlined accreditation pathway. Details on this pathway and its accreditation requirements are available in the [Streamlined accreditation for federal and provincial financial institutions](#) section of this guideline.

Registered payment service providers

This category includes payment service providers (PSPs) that are registered as PSPs under the *Retail Payment Activities Act*.

Registered PSPs may also apply for accreditation through a streamlined accreditation pathway.

Details on this pathway and its accreditation requirements are provided in the [Streamlined accreditation for registered payment service providers](#) section of this guideline.

Other entities

This category includes the following types of entities that do not fall within one of the other categories:

- corporations
- trusts
- partnerships
- funds
- unincorporated associations or organizations or federal or provincial Crown corporations

These other entities may apply for accreditation through the standard accreditation pathway.

Details on this pathway and its accreditation requirements are provided in the [Standard accreditation \(non-streamlined\)](#) section of this guideline.

Where to submit an application

Entities or individuals that choose to apply for accreditation under the CDBA must apply through the web application for consumer-driven banking and pay the accreditation fee. Further information on accreditation fees and the accreditation application process is forthcoming.

What to expect after submitting an application

Once it receives an application for accreditation, the Bank will determine whether all necessary information has been submitted.

If the application is complete, the Bank will:

- provide a copy to the Minister of Finance (the Minister) and
- begin its review of the application

As part of that review, the Bank will assess whether the applicant meets the applicable requirements for accreditation under the CDBA and CDBR and will make a decision on the application in accordance with the CDBA.

Request for additional information

The Bank may require additional information at any stage of its review. In such cases, the Bank will request the information in accordance with subsection 15(3), 17(3) or 19(3) of the CDBA, as applicable, and the applicant must provide the requested information within the time frame specified by the Bank.

National security review

After receiving a copy of an accreditation application, the Minister has 60 days to decide whether a national security review is necessary. The Minister may extend this period by one or more 60-day periods if necessary.

The Bank cannot accredit an applicant while the Minister is deciding whether to conduct a national security review. If the Minister decides to conduct a national security review, the Bank cannot accredit the applicant until the review has been completed and the Minister has notified the Bank of the outcome.

If the Minister decides to conduct a review, the Minister will inform the Bank, and the Bank will notify the applicant.

After deciding to review the application, the Minister must complete the review within **180 days** but may extend that period by one or more 180-day periods if necessary.

Request for additional information

As part of the national security review, the Minister may request additional information about the applicant or its planned activities under the Act. The applicant must provide the requested information to the Bank within **30 days beginning on the day after the applicant receives the request**. The Bank will then provide the information to the Minister as soon as feasible.

After the review

Following the review, the Minister will either:

- issue a directive to refuse accreditation or
- notify the Bank of their decision to not issue such a directive

If the Minister decides not to issue a directive, the Bank will notify the applicant. This notification does not mean the entity has been accredited. The Bank must still complete its review of the application before making a decision about accreditation.

If the Minister issues a directive to refuse accreditation for any reason set out in section 51 of the CDBA, the Bank must refuse accreditation and notify the applicant in writing as soon as feasible. The applicant may request a review of the directive in accordance with section 53 of the CDBA.

Accreditation application review

Submitting an application does not guarantee accreditation. Under the CDBA, the Bank may accredit an applicant if the Bank is satisfied that the applicant meets the applicable requirements of the CDBA and CDBR. The Bank will review each accreditation application to determine whether these requirements are met and whether any other grounds for refusal exist.

The Bank's expectations for these requirements are outlined under each application pathway in the [Application and accreditation requirements for prospective participating entities](#) section of this guideline.

The Bank will refuse accreditation if the applicant does not meet all applicable requirements.

The Bank may also refuse accreditation in other circumstances, including but not limited to where:

- the Bank has received information indicating the applicant would be unable to meet the requirements of the CDBA or CDBR
- information submitted by the applicant indicates that, if accredited, the applicant would not be able to comply with an ongoing requirement under the CDBA or CDBR

In considering these and other circumstances, the Bank will assess whether granting accreditation would be inconsistent with the objects and purpose of the CDBA.

The Bank's decision

If accreditation is approved

Subject to the Minister's national security review process, the Bank will notify the applicant in writing of its decision to accredit as soon as feasible.

The applicant's name and the date of accreditation will be added to the registry, as well as other information prescribed in the CDBA and CDBR.

Once accredited, the participating entity is required to comply with all applicable requirements under the CDBA and CDBR.

- For registered PSPs, this includes continuing to be a registered PSP and meeting the accreditation requirements in subsections 5(1)(a), (d) and (e) of the CDBR.
- For other entities that apply through the standard accreditation pathway, this includes meeting the accreditation requirements in subsections 7(1)(a), (d) and (e) of the CDBR.

If accreditation is refused

As soon as feasible after deciding to refuse an application, the Bank will notify the applicant in writing of the decision and the reasons for it.

Review and appeal

An applicant may request a review of a refusal. The request and written representations must be made within **30 days beginning on the day after the applicant is notified** of the decision to refuse.

The authority to issue a ruling on a review has been delegated by the Governor of the Bank of Canada to the Executive Director of Payments and Regulatory Oversight. The Governor's delegate will consider the request and either accredit the applicant or confirm the refusal within 120 days beginning on the day after the applicant was given the opportunity to make representations. The delegate will then notify the applicant in writing of the decision and the reasons for it as soon as feasible.

If the delegate decides to accredit, the applicant's name and date of accreditation will be added to the registry.

If the applicant does not agree with the delegate's decision, it may appeal the decision to the Federal Court. Further information on the review process is forthcoming.

Application and accreditation requirements for prospective participating entities

This section provides details on the three possible accreditation pathways:

- [standard accreditation \(non-streamlined\)](#)
- [streamlined accreditation for registered payment service providers](#)
- [streamlined accreditation for federal and provincial financial institutions](#)

1. Standard accreditation (non-streamlined)

Entities that are not eligible for a streamlined accreditation pathway may apply through the standard accreditation process under section 19 of the CDBA and sections 6 and 7 of the CDBR.

This pathway generally applies to entities other than federally or provincially regulated financial institutions and registered PSPs. An “entity” is a corporation, trust, partnership, fund, unincorporated association or organization or federal or provincial Crown corporation.

1.1. Application information

Applicants using the standard accreditation pathway must submit a complete application that contains the information specified in subsection 6(1) of the CDBR. This information includes:

- **applicant identification and contact information**, including:
 - legal identity
 - business location
 - key contacts
- **corporate, governance and organizational information** about the applicant, including:
 - organizational structure
 - governance arrangements
 - designated responsible persons
 - other individuals with significant responsibility for consumer-driven banking activities
- **regulatory status and oversight information**, including details about regulatory or supervisory oversight in Canada and participation in consumer-driven banking frameworks in other jurisdictions
- **information pertaining to the applicant's ability to comply with the CDBA and CDBR**, including:
 - security safeguards
 - technical standards
 - consumer dashboards
 - complaint-handling arrangements
 - insurance or guarantees
 - other accreditation requirements
- **operational information**, including anticipated consumer participation and arrangements with the external complaints body
- **national security information**, including details concerning the applicant's:
 - ownership
 - governance
 - affiliations
 - creditors
 - collection, storage, processing and disclosure of personal and financial information

More details about the application process and what information and documentation to submit is forthcoming.

1.2. Accreditation requirements

Under subsection 19(1) of the CDBA, the Bank may accredit an entity applying through the standard accreditation pathway if it is satisfied that the entity meets the requirements in subsection 7(1) of the CDBR. The Bank's supervisory expectations regarding these requirements are described in more detail below.

1.3. Place of business in Canada

- The Bank must be satisfied that the applicant has a place of business in Canada.
- The applicant must provide a declaration that it has a place of business in Canada and the civic address of that place of business.
- The applicant may be considered to have a place of business in Canada if one or more of the following factors are present:
 - The applicant has a physical location in Canada—this includes home offices; the place of business does not have to be a storefront or brick-and-mortar location.
 - The applicant is incorporated in Canada—under either federal or provincial legislation.
 - The applicant has employees, agents or mandataries in Canada.

1.4. Security safeguards

- The Bank must be satisfied that the applicant has obtained—from a sufficiently skilled independent third party—confirmation that the applicant has implemented the security safeguards specified in section 37 of the CDBR.
- The applicant must provide evidence of the independent third party's confirmation.

1.4.1. Sufficiently skilled independent third party

- The Bank considers a sufficiently skilled independent third party to be an individual or organization that is independent of the applicant and is accredited, certified or otherwise recognized by an established industry or professional body to perform cyber security audits, assessments, certifications or assurance engagements.
- The third party should possess the expertise necessary to conduct the assessment and may rely on appropriately qualified personnel to perform specialized aspects of the review.

1.4.2. Acceptable assessments

- A sufficiently skilled third party's assessment should demonstrate how the applicant has addressed each of the security safeguard requirements outlined in section 37 of the CDBR. The assessment should consist of one or more of the following:
 - Assessments conducted directly against the security safeguard requirements set out in section 37 of the CDBR.
 - Audits, certifications, assurance reports or other independent assessments conducted for other purposes that assess cyber security controls relevant to the security safeguard requirements outlined in section 37 of the CDBR. For example, International Organization for Standardization 27001 certifications, System and Organization Controls reports, and assessments based on the National Institute of Standards and Technology Cybersecurity Framework may provide evidence supporting an applicant's implementation of certain security safeguards.

- Assessments conducted against other cyber security standards or frameworks. In such cases, the independent third party should demonstrate why the assessment provides an appropriate basis for confirming that the applicant has implemented the security safeguards in section 37 of the CDBR.

1.4.3. Independent third-party confirmation

The Bank expects the independent third party's confirmation to be based on an assessment completed within the 12 months before the application was submitted.

For each security safeguard requirement in section 37 of the CDBR, the independent third party's confirmation should:

- identify the standard, framework or assessment methodology used
- describe the scope of the assessment
- identify any material limitations, exclusions or qualifications to the assessment
- confirm whether, in the third party's opinion, the applicant has implemented the requirement in section 37 of the CDBR
- explain, where applicable, the basis for the third party's conclusion that an assessment conducted against a standard or framework other than an assessment directly against the requirements in section 37 provides a sufficient basis for that confirmation

1.5. Technical standard

- The Bank must be satisfied that the applicant complies with the technical standard referred to in section 125 of the CDBA.
- The applicant must provide evidence of its compliance with the technical standard.

Note: At the time this draft guideline was prepared, the Minister of Finance had not yet designated a Technical Standards Body. The Bank will provide additional guidance on its supervisory expectations for compliance with the technical standard once a Technical Standards Body has been designated.

1.6. Insurance or comparable guarantee

- The Bank must be satisfied that the applicant holds insurance or a guarantee sufficient to cover the applicant's risks in relation to its management of data under the consumer-driven banking framework.
- Applicants must provide evidence that they hold such insurance or guarantee.

1.6.1. Sufficiency of insurance or comparable guarantee

- The Bank expects applicants to have professional indemnity insurance and cyber insurance, or one or more comparable guarantees that provide equivalent protection. Examples of coverage include:
 - professional indemnity insurance, which may provide protection for:
 - acts, errors or omissions relating to provision of consumer-driven banking services
 - failure to comply with contractual obligations
 - regulatory costs and fines
 - cyber insurance, which may provide protection for:

- cyber incidents, cyber extortion and terrorism
 - business interruption losses
 - data and system recovery costs
 - incident response expenses
 - violations of privacy or information security law
 - consumer redress
- The insurance or guarantee should not contain exclusions for privacy or data-related incidents or for claims or losses arising from the applicant's consumer-driven banking activities.
- Coverage limits may vary based on the applicant's risk profile. The Bank expects the applicant to develop a methodology for determining the amount of insurance or guarantee required to cover the risks arising from the applicant's management of data under the consumer-driven banking framework. When developing this methodology, applicants may consider factors such as:
 - the nature and sensitivity of the data collected, used, retained or shared
 - the volume of consumer data managed by the applicant
 - the nature, scale and complexity of the applicant's consumer-driven banking activities
 - the potential financial impact of privacy, cyber security, operational or other data-related incidents
 - any other factors that could reasonably affect the applicant's risk exposure
- Applicants are expected to document the methodology used to determine the amount of insurance or guarantee coverage and review it periodically. The purpose of this review is to ensure that coverage remains sufficient to address the risks arising from the applicant's management of data under the consumer-driven banking framework.
- Where an applicant relies on a combination of insurance and guarantee(s), the combined coverage should be sufficient to cover the risks arising from the applicant's management of data under the consumer-driven banking framework.

1.6.2. Evidence of insurance or comparable guarantee

- As evidence of the insurance or guarantee, the applicant should provide:
 - a copy of the insurance or guarantee issued by the insurer or guarantor and
 - a written statement explaining why the insurance or guarantee is sufficient to cover the risks related to the applicant's management of data under the consumer-driven banking framework, including relevant factors such as the nature, sensitivity and volume of data that the applicant expects to collect, use or share under the framework

1.7. Integrity and character of individuals with significant responsibility for consumer-driven banking activities

- The Bank must be satisfied that the applicant has implemented a policy to regularly assess the integrity and good character of all individuals who will have significant responsibility for the applicant's consumer-driven banking activities (the Integrity and Good Character Policy).
- The Integrity and Good Character Policy must set out that individuals with significant responsibility for the applicant's consumer-driven banking activities must report to the applicant any change in circumstance that may affect an assessment of their integrity and good character.
- Applicants must provide:

- a description of the Integrity and Good Character Policy
- the name, title and brief job description of each individual who will have significant responsibility for the applicant's consumer-driven banking activities
- an attestation that those individuals have been assessed in accordance with that policy
- The Bank also expects the Integrity and Good Character Policy to:
 - establish a documented process for assessing the integrity and good character of individuals with significant responsibility for the applicant's consumer-driven banking activities
 - establish processes for regularly reassessing individuals who have previously been assessed
 - set out the frequency of reassessment and any events that would trigger a reassessment, such as a change in role or responsibilities
 - describe the steps involved in conducting reassessments and explain any material differences between the reassessment process and the initial assessment
 - require that records be maintained of assessments, reassessments and decisions made under the Policy
- The Bank also expects that the Integrity and Good Character Policy, and any material amendments to it, be approved by the applicant's senior management with decision-making or executive authority.

1.7.1. Individuals with significant responsibility for consumer-driven banking activities

- Individuals with significant responsibility for the applicant's consumer-driven banking activities will generally include:
 - any individual designated under section 80 of the CDBA to be responsible for the security safeguards that the applicant implements with respect to the sharing of consumer data under the CDBA
 - any officer or employee designated under subsection 105(1)(b) of the CDBA to be responsible for implementing the applicant's complaint-handling procedures
 - senior executives with significant responsibility for the applicant's consumer-driven banking activities, which may include the chief executive officer/executive director, chief financial officer, chief legal officer, chief technology officer, chief risk officer or equivalent positions
 - members of the board of directors
- It is understood that an individual may perform more than one listed function in an entity. When an individual performs more than one listed function, each function must be identified.

1.7.2 Indicators of integrity and good character

The Bank expects the Integrity and Good Character Policy to identify factors that will be considered when assessing the integrity and good character of individuals with significant responsibility for the applicant's consumer-driven banking activities.

At a minimum, the applicant should consider the following factors. Where these factors exist, the applicant should assess and document whether they affect the individual's suitability to hold significant responsibility for the applicant's consumer-driven banking activities.

Criminal history

Evidence, such as a criminal record check, indicating whether the individual:

- has a criminal record involving serious offenses in Canada or another jurisdiction or
- is subject to ongoing legal proceedings relating to serious offenses

Professional disciplinary history

Evidence, such as a certification or accreditation of good standing from a professional association or regulatory body based on that association's or body's bylaws or code of professional or personal conduct. If any disciplinary findings or sanctions have been issued by the association or body in respect of an individual, consideration may be given to steps taken, or lack thereof, to remedy the issue, and to the professional association's or regulatory body's response to those steps.

Regulatory or government investigations

Whether the individual is the subject of an investigation relating to alleged misconduct, wrongdoing or non-compliance by a government authority, law enforcement agency or regulatory body in Canada or another jurisdiction.

Insolvency and bankruptcy history

Any history of insolvency or bankruptcy involving the individual or an entity for which the individual had significant responsibility.

2. Streamlined accreditation for registered payment service providers

Registered PSPs may apply for accreditation through a streamlined accreditation process under section 17 of the CDBA and sections 4 and 5 of the CDBR.

This pathway is available to PSPs registered under the *Retail Payment Activities Act*.

2.1. Application information

Registered PSP applicants must submit a complete application that contains the information in subsection 4(1) of the CDBR. This information includes:

- **applicant identification and contact information**, including:
 - legal identity
 - business location
 - key contacts
- **corporate, governance and organizational information about the applicant**, including:
 - organizational structure
 - governance arrangements
 - designated responsible persons
 - other individuals with significant responsibility for consumer-driven banking activities
- **regulatory status and oversight information**, including details about participation in consumer-driven banking frameworks in other jurisdictions
- **information demonstrating the applicant's ability to comply with the CDBA and CDBR**, including evidence and descriptions relating to security safeguards, technical standards, insurance or guarantees, and other accreditation requirements
- **consumer-driven banking operational information**, including arrangements with the external complaints body
- **national security information**, including details concerning the applicant's:
 - ownership
 - governance
 - affiliations
 - creditors
 - collection, storage, processing and disclosure of personal and financial information

More information about the application process and what information and documentation to submit is forthcoming.

2.2. Accreditation requirements

Under subsection 17(1) of the CDBA, the Bank may accredit a registered PSP applying through the streamlined accreditation pathway if the Bank is satisfied that the registered PSP meets the requirements in subsection 5(1) of the CDBR. The Bank's supervisory expectations respecting these requirements are described in more detail below.

2.3. Place of business in Canada

- The Bank must be satisfied that the applicant has a place of business in Canada.

- The applicant must provide a declaration that it has a place of business in Canada and the civic address of that place of business
- The applicant may be considered to have a place of business in Canada if one or more of the following factors are present:
 - The applicant has a physical location in Canada—this includes home offices; it does not have to be a storefront or brick-and-mortar location.
 - The applicant is incorporated in Canada—under either federal or provincial legislation.
 - The applicant has employees, agents or mandataries in Canada.

2.4. Security safeguards

- The Bank must be satisfied that the applicant has obtained—from a sufficiently skilled independent third party—confirmation that the applicant has implemented the security safeguards specified in section 37 of the CDBR.
- The applicant must provide evidence of the independent third party's confirmation.

2.4.1. Sufficiently skilled independent third party

- The Bank considers a sufficiently skilled independent third party to be an individual or organization that is independent of the applicant and is accredited, certified or otherwise recognized by an established industry or professional body to perform cyber security audits, assessments, certifications or assurance engagements. The third party should possess the expertise necessary to conduct the assessment and may rely on appropriately qualified personnel to perform specialized aspects of the review.

2.4.2. Acceptable assessments

- A sufficiently skilled third party's assessment should demonstrate how the applicant has addressed each of the security safeguard requirements outlined in section 37 of the CDBR. The assessment should consist of one or more of the following:
 - Assessments conducted directly against the security safeguard requirements set out in section 37 of the CDBR.
 - Audits, certifications, assurance reports or other independent assessments conducted for other purposes that assess cyber security controls relevant to the security safeguard requirements in section 37 of the CDBR. For example, International Organization for Standardization 27001 certifications, System and Organization Controls reports, and assessments based on the National Institute of Standards and Technology Cybersecurity Framework may provide evidence supporting an applicant's implementation of certain security safeguards.
 - Assessments conducted against other cyber security standards or frameworks. In such cases, the independent third party should demonstrate why the assessment provides an appropriate basis for confirming that the applicant has implemented the security safeguards in section 37 of the CDBR.

2.4.3. Independent third-party confirmation

The Bank expects the independent third party's confirmation to be based on an assessment completed within the 12 months before the application was submitted.

For each security safeguard requirement in section 37 of the CDBR, the independent third party's confirmation should:

- identify the standard, framework or assessment methodology used
- describe the scope of the assessment
- identify any material limitations, exclusions or qualifications to the assessment
- confirm whether, in the third party's opinion, the applicant has implemented the requirement in section 37 of the CDBR
- explain, where applicable, the basis for the third party's conclusion that an assessment conducted against a standard or framework other than against the requirements in section 37 provides a sufficient basis for that confirmation

2.5. Technical standard

- The Bank must be satisfied that the applicant is in compliance with the technical standard referred to in section 125 of the CDBA.
- The applicant must provide evidence of its compliance with the technical standard.

Note: At the time this draft guideline was prepared, the Minister of Finance had not yet designated a Technical Standards Body. The Bank will provide additional guidance on its supervisory expectations for compliance with the technical standard once a Technical Standards Body has been designated.

2.6. Insurance or comparable guarantee

- The Bank must be satisfied that the applicant holds insurance or a guarantee sufficient to cover the applicant's risks in relation to its management of data under the consumer-driven banking framework.
- Applicants must provide evidence that they hold such insurance or guarantee.

2.6.1. Sufficiency of insurance or comparable guarantee

- The Bank expects applicants to have professional indemnity insurance and cyber insurance, or one or more comparable guarantees that provide equivalent protection. Examples of coverage include:
 - professional indemnity insurance, which may provide protection for:
 - acts, errors or omissions relating to provision of consumer-driven banking services
 - failure to comply with contractual obligations
 - regulatory costs and fines
 - cyber insurance, which may provide protection for:
 - cyber incidents, cyber extortion and terrorism
 - business interruption losses
 - data and system recovery costs

- incident response expenses
 - violations of privacy or information security law
 - consumer redress
- The insurance or guarantee should not contain exclusions for privacy or data-related incidents or for claims or losses arising from the applicant's consumer-driven banking activities.
- Coverage limits may vary based on the applicant's risk profile. The Bank expects the applicant to develop a methodology for determining the amount of insurance or guarantee required to cover the risks arising from the applicant's management of data under the consumer-driven banking framework. When developing this methodology, applicants may consider factors such as:
 - the nature and sensitivity of the data collected, used, retained or shared
 - the volume of consumer data managed by the applicant
 - the nature, scale and complexity of the applicant's consumer-driven banking activities
 - the potential financial impact of privacy, cyber security, operational or other data-related incidents
 - any other factors that could reasonably affect the applicant's risk exposure
- Applicants are expected to document the methodology used to determine the amount of insurance or guarantee coverage and review it periodically. The purpose of this review is to ensure that coverage remains sufficient to address the risks arising from the applicant's management of data under the consumer-driven banking framework.
- Where an applicant relies on a combination of insurance and guarantee(s), the combined coverage should be sufficient to cover the risks arising from the applicant's management of data under the consumer-driven banking framework.

2.6.2. Evidence of insurance or comparable guarantee

As evidence of insurance sufficiency, the applicant should provide:

- a copy of the insurance or guarantee issued by the insurer or guarantor and
- a written statement explaining why the insurance or guarantee is sufficient to cover the risks related to the applicant's management of data under the consumer-driven banking framework, including relevant factors such as the nature, sensitivity and volume of data that the applicant expects to collect, use or share under the framework.

2.7. Integrity and character of individuals with significant responsibility for consumer-driven banking activities

2.7.1. If the applicant is an individual

- The Bank must be satisfied that the individual is of good character.
- The applicant must provide an attestation of good character and evidence that supports the attestation.

Further information on integrity and good character attestations is forthcoming.

2.7.2. If the applicant is an entity

- If the registered PSP is an entity, the Bank must be satisfied that the applicant has implemented a policy to regularly assess the integrity and good character of all individuals who will have significant

responsibility for the applicant's consumer-driven banking activities (the Integrity and Good Character Policy).

- The Integrity and Good Character Policy must set out that individuals with significant responsibility for the applicant's consumer-driven banking activities must report to the applicant any change in circumstance that may affect an assessment of their integrity and good character.
- Applicants must provide:
 - a description of the Integrity and Good Character Policy
 - the name, title and brief job description of each individual who will have significant responsibility for the applicant's consumer-driven banking activities
 - an attestation that those individuals have been assessed in accordance with that policy
- The Bank expects the Integrity and Good Character Policy to:
 - establish a documented process for assessing the integrity and good character of individuals with significant responsibility for the applicant's consumer-driven banking activities
 - establish processes for regularly reassessing individuals who have previously been assessed
 - set out the frequency of reassessments and any events that would trigger a reassessment, such as a change in role or responsibilities
 - describe the steps involved in conducting reassessments and explain any material differences between the reassessment process and the initial assessment
 - require that records be maintained of assessments, reassessments and decisions made under the Policy
- The Bank also expects that the Integrity and Good Character Policy, and any material amendments to it, be approved by the applicant's senior management with decision-making or executive authority.

2.7.3. Individuals with significant responsibility for consumer-driven banking activities

- Individuals with significant responsibility for the applicant's consumer-driven banking activities will generally include:
 - any individual designated under section 80 of the CDBA to be responsible for the security safeguards that the applicant implements with respect to the sharing of consumer data under the CDBA
 - any officer or employee designated under paragraph 105(1)(b) of the CDBA to be responsible for implementing the applicant's complaint-handling procedures
 - senior executives with significant responsibility for the applicant's consumer-driven banking activities, which may include the chief executive officer/executive director, chief financial officer, chief legal officer, chief technology officer, chief risk officer or equivalent positions
 - members of the board of directors
- It is understood that an individual may perform more than one listed function in an entity. When an individual performs more than one listed function, each function must be identified.

2.7.4. Indicators of integrity and good character

The Bank expects the Integrity and Character Policy to identify factors that will be considered when assessing the integrity and good character of individuals with significant responsibility for the applicant's consumer-driven banking activities.

At a minimum, the applicant should consider the following factors. Where these factors exist, the applicant should assess and document whether they affect the individual's suitability to hold significant responsibility for the applicant's consumer-driven banking activities.

Criminal history

Evidence, such as a criminal record check, indicating whether the individual:

- has a criminal record involving serious offenses in Canada or another jurisdiction or
- is subject to ongoing legal proceedings relating to serious offenses

Professional disciplinary history

Evidence, such as a certification or accreditation of good standing from a professional association or regulatory body based on that association's or body's bylaws or code of professional or personal conduct. If any disciplinary findings or sanctions have been issued by the association or body in respect of an individual, consideration may be given to steps taken, or lack thereof, to remedy the issue, and to the professional association's or regulatory body's response to those steps.

Regulatory or government investigations

Whether the individual is the subject of an investigation relating to alleged misconduct, wrongdoing or non-compliance by a government authority, law enforcement agency or regulatory body in Canada or another jurisdiction.

Insolvency and bankruptcy history

Any history of insolvency or bankruptcy involving the individual or an entity for which the individual had significant responsibility. Where such matters exist, the applicant should assess and document whether they affect the individual's suitability to hold significant responsibility for the applicant's consumer-driven banking activities.

3. Streamlined accreditation for federal and provincial financial institutions

Federal financial institutions and provincial financial institutions may apply for accreditation through the streamlined accreditation process under section 15 of the CDBA and section 3 of the CDBR.

This pathway applies to federal and provincial financial institutions as defined in the CDBA. These include:

- banks
- authorized foreign banks
- trust and loan companies
- cooperative credit associations
- credit unions
- caisses populaires
- insurance companies
- certain provincial Crown corporations that offer deposit-taking services

3.1. Application information

Federal or provincial financial institutions must submit a complete application that contains the information in subsection 3(1) of the CDBR. This information includes:

- **applicant identification and contact information**, including details about the applicant's:
 - legal identity
 - business location
 - key contacts
- **corporate, governance and organizational information**, including details about the applicant's:
 - organizational structure
 - governance arrangements
 - designated responsible persons
 - other individuals with significant responsibility for consumer-driven banking activities
- **regulatory status and oversight information**, including details about regulatory or supervisory oversight in Canada and participation in consumer-driven banking frameworks in other jurisdictions
- **information demonstrating the applicant's ability to comply with the CDBA and CDBR**, including evidence and descriptions relating to security safeguards and technical standards
- **national security information**, including details concerning the applicant's:
 - ownership
 - governance
 - affiliations
 - creditors
 - collection, storage, processing and disclosure of personal and financial information

More information about the application process and what information and documentation to submit is forthcoming.

3.2. Accreditation requirements

The Bank may accredit a federal or provincial financial institution applying through the streamlined accreditation pathway if the Bank is satisfied that the applicant is in compliance with the technical standard referred to in subsection 125(1) of the CDBA and the security safeguards set out in section 37 of the CDBR.

3.2.1. Technical standard

- The applicant must provide evidence of its compliance with the technical standard referred to in section 125 of the CDBA.

Note: At the time this draft guideline was prepared, the Minister of Finance had not yet designated a Technical Standards Body. The Bank will provide additional guidance on its supervisory expectations for compliance with the technical standard once a Technical Standards Body has been designated.

3.2.2. Security safeguards

- The applicant must provide a declaration that it is in compliance with the security safeguards referred to in section 37 of the CDBR.

- The Bank expects the declaration to be made by the senior officer or employee designated under section 80 of the CDBA as responsible for the security safeguards governing the applicant's sharing of consumer data.
- This declaration should be dated no more than 90 days before the application is submitted.