Datarisk
Business Security

Public Intel Edition | April 18, 2026

Consumer-Driven Banking in Canada

Why it matters now, how it is rolling out, what financial institutions should expect, and how to prepare

Purpose: The safety, competitiveness, and resilience of the Canadian financial system depends on the adoption measures related to the latest federal guidance on consumer-driven banking. Globally emerging threats within open banking drive preparedness measures for open banking in Canadian banking, investment and fintech sectors.

Prepared for	Public-facing distribution and stakeholder education
Primary audience	Financial institutions, fintechs, credit unions, advisors, policy teams, and informed consumers
Core message	Canada can use consumer-driven banking to replace risky workarounds with safer, consent-based data sharing while also supporting competition, innovation, and trust. The framework has advanced materially, but it is not yet live and implementation work remains underway.
Status	Implementation stage as of April 2026: the legislative framework has advanced materially, but consumer-driven banking is not yet live in Canada and implementation work remains underway.

Executive Summary: Why Consumer Driven Banking?

Consumer-driven banking, sometimes referred to internationally as open banking, is Canada's emerging framework for secure, consent-based financial data sharing. Consumer-driven banking matters because Canadians are already sharing financial data today, often through insecure workarounds. The federal government has repeatedly pointed to the widespread use of screen scraping, where people hand over online banking credentials to apps or service providers so they can aggregate account data. That creates avoidable security, privacy, operational, and liability risk for customers and institutions alike. A regulated consumer-driven banking regime is meant to replace that workaround with a safer model built on consent, secure data exchange, and common rules.

The case for action is bigger than retail banking convenience. Done well, consumer-driven banking can make it easier for customers and businesses to compare providers, switch to institutions they trust more, and use financial tools that help them budget, borrow, save, reconcile payments, and run operations more efficiently. It can also strengthen the banking system by moving data sharing into a supervised framework with clearer accountability, more consistent controls, and better visibility into who is accessing data and why.

Global experience shows that these reforms can create real benefits when they are implemented with strong governance. In the United Kingdom, Open Banking Limited reported 13.3 million active users as of March 2025. In Australia, the Consumer Data Right is already active in banking and energy and is designed to give consumers and small businesses more choice and control. In Europe, PSD2 opened the market for regulated account-information and payment-initiation services, showing how data access can expand competition while still being tied to authorization, supervision, authentication, and liability rules.
Canada is later to market than several peers, but that delay gives it one important advantage: it can build a more mature regime if it uses the lessons learned elsewhere. Over the past year, the Canadian file has shifted from high-level policy design into implementation architecture. The 2024 Fall Economic Statement filled in major missing elements such as accreditation, privacy, liability, and national security rules. Budget 2025 proposed a revised approach, and Bill C-15 later received Royal Assent, expanding the Bank of Canada's responsibilities to include oversight of the framework for consumer-driven banking. Bill C-15 received Royal Assent on March 26, 2026. Canada has therefore moved beyond the pending-legislation stage, but consumer-driven banking is still not available in Canada and key implementation work remains outstanding.

The urgency of switching to API methods: Unsupervised credential sharing and screen scraping are legacy data collection methods that meet consent and portability requirements but increase the risks related to access control, confidentiality, accountability, cyberfraud along with a false sense of security.

Why Consumer-Driven Banking Is Critically Important in Canada

1. It can help customers move to institutions they trust more

A healthy banking market is not only about product innovation. It is also about switching power. When customers can securely share transaction histories, account data, and related financial information with approved providers, they are better positioned to compare products, verify affordability, switch accounts, manage recurring payments, and choose institutions that offer stronger service, better digital tools, or more trusted relationships. Consumer-driven banking can reduce the friction that keeps people locked into banks or platforms that no longer serve them well.

2. It can make service delivery safer

The federal rationale is explicit: Canada needs a safer alternative to credential sharing. Replacing password-based screen scraping with secure connections, common rules, and auditable consent can improve service delivery for everyone involved. Customers get more clarity. Financial institutions get more predictable control boundaries. Third parties face a more disciplined operating environment. Regulators get a framework they can supervise instead of a market workaround they can only partially see.

3. It can strengthen the overall banking system

Consumer-driven banking is often framed as a customer feature, but it is also a system-safety reform. Standardized access, accreditation, clearer liability allocation, revocation powers, and common security expectations can reduce systemic ambiguity. That does not eliminate risk, but it moves risk into a framework where controls can be designed, tested, and enforced. In a sector that depends on trust, clarity is itself a form of resilience.

4. The benefits go beyond retail banking

Canada's recent framework materials do not limit the policy objective to retail budgeting apps. The government has also emphasized benefits for small and medium-sized businesses. These include more efficient accounting and reconciliation, easier sharing of verified financial records, better integration with payroll and business software, and the potential for faster or more tailored access to credit. For larger institutions, the opportunity extends to treasury services, embedded finance partnerships, digital onboarding, personal financial management, merchant services, and smarter risk decisioning.

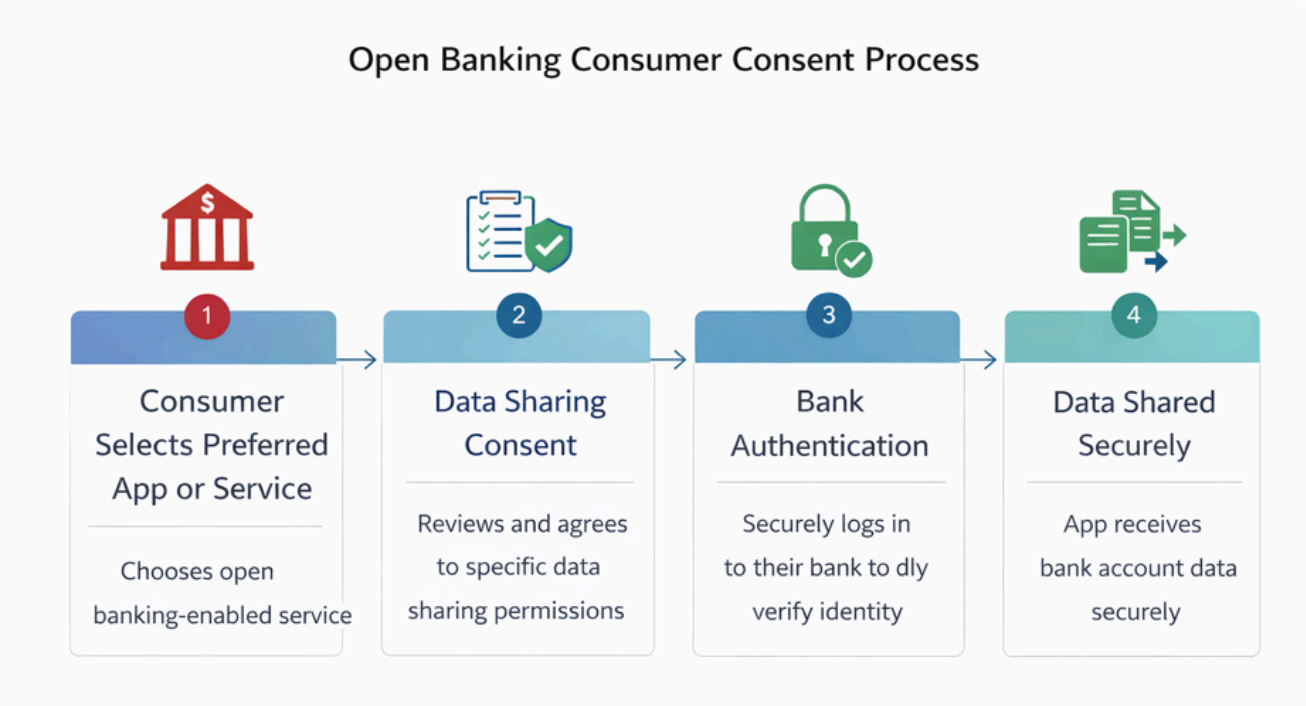
5. The economic case is broader than app convenience

Globally, open banking and adjacent data-sharing reforms have been promoted not only as a consumer rights measure, but also as an economic modernization tool. The UK experience points to sustained user adoption and a growing base for competitive new services. Australia's cross-sector Consumer Data Right shows how secure portability can be treated as economic infrastructure rather than a narrow banking project. Europe's PSD2 regime shows that new services such as payment initiation can change business models, not merely improve data access.

How It Has Rolled Out Globally, and What Canada Can Learn

Jurisdiction	What happened	What Canada can learn
United Kingdom	Open banking moved from regulatory design to scaled market adoption. Open Banking Limited reported 13.3 million active users as of March 2025.	Adoption can become mainstream when standards, supervision, and practical use cases line up.
Australia	Consumer Data Right is active in banking and energy and is framed as a secure consumer data-sharing right for individuals and small businesses.	A broader portability architecture can create spillover benefits beyond banking alone.
European Union	PSD2 opened the door to regulated account-information and payment-initiation services and tied access to authorization, security, and liability rules.	Write access can unlock more value, but only if payments infrastructure and controls are mature.

Canada's framework contemplates a staged path rather than an immediate full-featured launch. The regime is not yet operational, and key implementation details still need to be finalized before launch. Public materials support a phased progression from core supervised data-sharing functionality toward broader participation and, potentially later, more advanced functionality if the legal, technical, and payments infrastructure are ready.



Latest Canadian Developments and Near-Term Outlook

- Budget 2024 formally set out the first federal consumer-driven banking framework and highlighted the need to move Canadians away from screen scraping.
- Bill C-69 received Royal Assent in June 2024 and assigned the FCAC an oversight role under the original model.
- The 2024 Fall Economic Statement added key implementation architecture, including accreditation, common rules, privacy, liability, and national security elements.
- Budget 2025 reframed the rollout, and Bill C-15 later expanded the Bank of Canada's responsibilities to include oversight of the framework for consumer-driven banking.
- Bill C-15 received Royal Assent on March 26, 2026. The focus has therefore shifted from legislative passage to implementation, including regulations, supervisory policies, operational frameworks, accreditation design, technical standards, and launch readiness.

Near-term watch items: draft regulations, accreditation criteria, technical standards, governance choices, Bank of Canada implementation materials, and Payments Canada Real-Time Rail milestones are the signals most likely to shape the real launch path.

Timeline: The Progression of Consumer-Driven Banking in Canada

Date	Milestone	Why it mattered
2018	Federal review begins	The open banking discussion moved from market debate into formal policy examination.
Aug. 2021	Advisory Committee final report	The report recommended a made-in-Canada regime with governance, accreditation, and technical standards.
Mar. 2022	Open banking lead appointed	The federal government moved from conceptual study toward implementation work.
2022-2023	Working groups and policy design	Department of Finance work continued on administration, governance, and rollout planning.
Apr. 2024	Budget 2024 framework released	Canada published its initial framework and clearly

		identified screen scraping as a problem to solve.
Jun. 2024	Bill C-69 receives Royal Assent	The original Consumer-Driven Banking Act structure and FCAC oversight role entered the legislative picture.
Dec. 2024	Fall Economic Statement fills in framework	Major missing implementation pieces, including liability and privacy architecture, were added.
Nov. 2025	Budget 2025 resets rollout	Budget 2025 proposed a revised governance approach, broader scope, and a second-phase discussion. Bill C-15 later gave effect to the Bank of Canada's expanded responsibilities.
Nov. 2025-Mar. 2026	Bill C-15 moves through Parliament	Bill C-15 introduced, passed, and received Royal Assent on March 26, 2026 | The legal framework advanced materially, shifting the focus to implementation and oversight preparation.
2026 onward	Regulations, accreditation, standards, and operational readiness	This is the phase that will determine whether policy intent becomes practical reality.

Challenges, Delays, Risks, and Opportunities

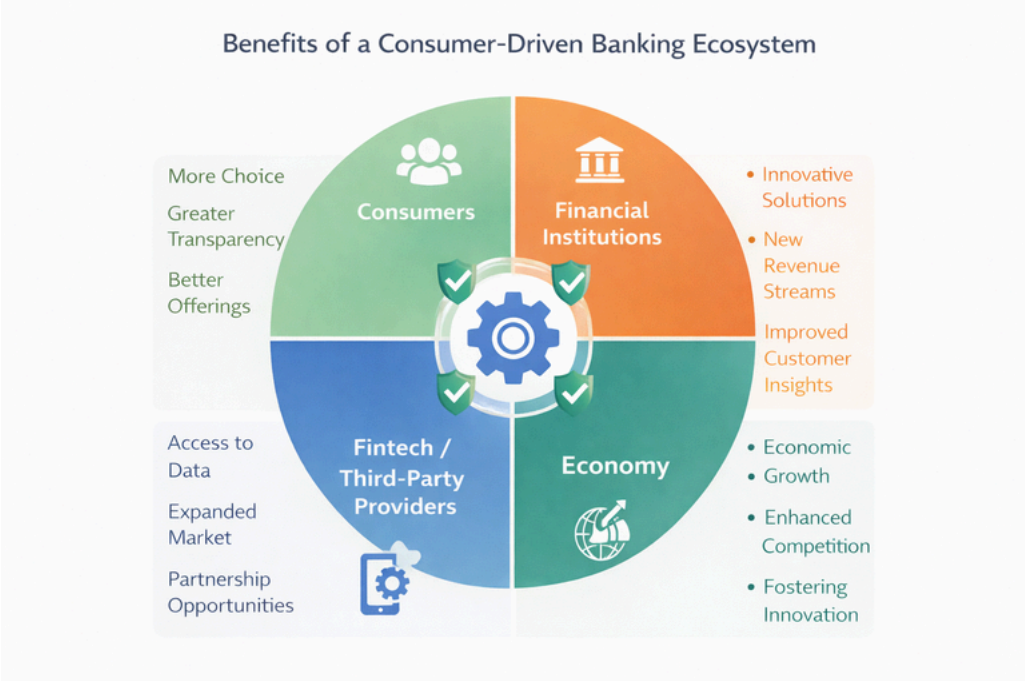
Anticipated delays

- The legal framework has advanced materially, but regulations, operational frameworks, and implementation work remain outstanding.
- Regulations, common rules, technical standards, and accreditation processes still need to be finalized and made operational.
- Provincial and federal coordination may prove complex for some institutions and categories of participants.
- Later-stage functionality appears tied to payments modernization, especially Real-Time Rail readiness.

What has happened, and what has not happened yet

Bill C-15 received Royal Assent on March 26, 2026, and the Bank of Canada now has an expanded mandate that includes oversight of the framework for consumer-driven banking. However, consumer-driven banking is still not available in Canada, and key implementation elements remain outstanding. In addition, several provisions of the original Consumer-Driven Banking Act, including parts dealing with in-scope data and the registry, are not yet in force.

Opportunities



- Safer consumer and business data sharing than existing credential-based workarounds.
- Greater switching power for customers who want to move toward institutions they trust more.
- New products in personal financial management, lending, merchant services, treasury, and embedded finance.
- Better SME experiences in accounting, payroll, cash flow visibility, and financing workflows.
- A stronger basis for trust if customers can see who has access to data, on what terms, and how consent can be revoked.

Major Risks and Clear Threats for Financial Institutions

Consumer-driven banking creates opportunity, but it also changes the risk map. Financial institutions face material threats at each stage: transition, deployment, rollout, and scaled operation. The risk profile is not limited to cyberattack. It also includes customer confusion, partner dependency, legal exposure, resilience failure, governance gaps, and reputational harm.

Phase	Major risk or threat	What it can look like in practice	Preparation priority
Transition	Strategy failure	Senior leaders treat consumer-driven banking as a minor compliance item instead of a cross-functional transformation program.	Assign executive ownership and a formal roadmap.
Transition	Control-mapping gaps	Institutions cannot clearly map which controls apply to data holders, data recipients, support providers, and outsourced functions.	Run legal, security, privacy, and operations mapping early.
Deployment	API and integration weaknesses	Poorly secured interfaces, weak authentication flows, or brittle middleware expand the attack surface and create outages or fraud pathways.	Invest in secure architecture, testing, and monitoring.
Deployment	Consent design failure	Customers do not understand what they are agreeing to, how long access lasts, or how to revoke it.	Build plain-language consent journeys and revocation paths.
Rollout	Third-party concentration risk	A small number of aggregators or platform partners become critical dependencies across multiple institutions.	Perform concentration analysis and contingency planning.
Rollout	Liability disputes	After fraud, service failure, or bad data, parties disagree over who was at fault and which control failed.	Prepare contractual frameworks, evidence trails, and incident playbooks.
Scaled operation	Operational resilience stress	A high-volume ecosystem creates new failure modes, including cascading outages, degraded customer service, and incident-response overload.	Exercise resilience scenarios and recovery playbooks.
Scaled operation	Trust erosion	A publicized failure, breach, or confusing experience undermines customer confidence in the entire regime, not only one institution.	Treat trust, communication, and customer support as core controls.

Threats that deserve special attention

- **Fraud migration risk:** bad actors will look for new weak points as data-sharing patterns and authentication journeys change.

- **Impersonation and social-engineering risk:** a more complex ecosystem can make it easier for criminals to confuse customers about who is asking for access.
- **Data quality and decisioning risk:** if data is incomplete, stale, or poorly interpreted, institutions can make flawed lending, onboarding, or risk decisions.
- **Vendor and supply-chain risk:** consumer-driven banking will likely increase reliance on specialist technology, identity, API, and data-service providers.
- **Reputational spillover:** even if an institution is not at fault, public failures in the ecosystem can reduce willingness to adopt or share data.

Plain-language takeaway: Canada is still in a pre-launch implementation phase, so institutions should plan against the emerging framework without assuming production go-live. The objective is not to eliminate all risk. It is to move to a model where risk is more visible, governable, and recoverable.

Examples and Lessons from Global Experience

The strongest global lesson is that consumer-driven banking succeeds when it is treated as infrastructure, not as a marketing slogan. The UK shows that adoption can grow materially when real services become available under stable governance. Australia shows that portability can be framed as a broader consumer right, not only a banking issue. Europe shows that opening the market to account information and payment initiation can create new services, but only when security and authorization obligations are taken seriously.

The lesson for Canada is straightforward. Customers will not care about legislative elegance if the experience is confusing, slow, or unsafe. Financial institutions will not invest confidently if the rules remain vague. Regulators will not gain trust if accountability is unclear. For that reason, the quality of the rollout will matter as much as the policy decision to proceed.

Key Agencies, Contributions, and Downloadable Resources

Official Canadian resources

Source	Resource	Link
Finance Canada	Budget 2025: Canada's Consumer-Driven Banking Framework	Budget 2025: Canada's Consumer-Driven Banking Framework
Finance Canada	2024 Fall Economic Statement: Canada's Complete Framework for Consumer-Driven Banking	2024 Fall Economic Statement: Canada's Complete Framework for Consumer-Driven Banking
Finance Canada	Budget 2024: Canada's Framework for Consumer-Driven Banking	Bill C-15 status page
Parliament of Canada	Bill C-15, LEGISinfo status page	Open banking, FCAC consumer information

Parliament of Canada	Bill C-15 first-reading text	About our supervisory mandates, Bank of Canada
FCAC	Open banking explainer	Open resource
Payments Canada	Real-Time Rail quarterly update, Q1 2026	Canada's Real-Time Rail Quarterly Update with Jude Pinto: 2026 Q1
Payments Canada	RTR participation guide for payment service providers	RTR: Participation Guide for Payment Service Providers

Global comparator resources

Source	Resource	Link
Open Banking Limited, UK	OBL Impact Report 7, 13.3 million active users as of March 2025	OBL Impact Report 7: open banking delivers real-world impact as adoption accelerates year-on-year
FCA, United Kingdom	Open banking and open finance in the UK	Open Banking and Open Finance in the UK
Australia Consumer Data Right	What is CDR?	CDR GOV AU: What is CDR?
Australia Consumer Data Right	Rollout	CDR GOV AU: Rollout
Australian Treasury	Consumer Data Right policy overview	AU Treasury: Consumer Data Right Policy Overview
European Banking Authority	PSD2 interactive rulebook	EBA: Payment Services Directive 2 (PSD2)

Key agency roles can be summarized this way: Finance Canada remains the policy architect; Parliament established the legislative framework, while implementation now turns more heavily on regulations, oversight design, and operational readiness.

FCAC provides consumer-facing guidance and was central under the original oversight model; the Bank of Canada now has an expanded mandate that includes oversight of the framework for consumer-driven banking, and it has said it is carrying out preparatory work on regulations, supervisory policies, stakeholder engagement, and operational frameworks; and Payments Canada is essential because later-stage functionality is closely linked to the payments infrastructure environment.

What FI Organizations Should Do Now

- Track Bill C-15, related consultations, and implementation papers continuously.
- Decide whether the organization is likely to act primarily as a data holder, data recipient, or both.

- Create a cross-functional program spanning legal, compliance, privacy, security, technology, operations, product, and communications.
- Assess current credential-sharing exposure and identify where existing customer journeys rely on risky workarounds.
- Map control responsibilities for authentication, consent, revocation, incident response, data quality, retention, and complaints handling.
- Review third-party risk processes for aggregators, fintech partners, API providers, and outsourced service providers.
- Build or refresh API security, monitoring, logging, and resilience capabilities.
- Prepare plain-language customer communication for consent and support scenarios.
- Identify priority use cases for retail, small business, commercial, and treasury lines where the regime could create early value.
- Plan for scenario testing, tabletop exercises, and trust-preserving public communication in case the rollout is disrupted.

Decision Support for IT Governance

For boards, technology committees, CIOs, CISOs, procurement leaders, and line-of-business sponsors, consumer-driven banking should be treated as a governance decision as much as a product or compliance project. The implementation challenge is not limited to building APIs. It also involves choosing reliable suppliers, defining accountability, testing controls, preserving resilience, and ensuring that customer trust is not weakened during transition. For federally regulated financial institutions, this work should be aligned to OSFI Guideline B-13 on Technology and Cyber Risk Management, Guideline B-10 on Third-Party Risk Management, Guideline E-21 on Operational Risk Management and Resilience, and OSFI's Integrity and Security Guideline. For Ontario credit unions and other FSRA-regulated entities, it should also align to FSRA's Information Technology Risk Management guidance and incident notification expectations. Where multiple supervisory expectations may apply across affiliates or business lines, institutions should generally adopt the stricter or more operationally robust control design.

Vendor Risk Assessment and Supplier Selection Guidelines

Supplier selection should start with a business service map, not with a sales demonstration. Institutions should first define which customer journeys, datasets, interfaces, and critical operations are in scope, then identify which capabilities must stay in-house and which can be sourced. Vendors should be evaluated not only on feature breadth, but on control maturity, evidence quality, implementation discipline, and their ability to operate under Canadian prudential, privacy, and incident-management expectations.

- Classify each proposed service by criticality: mission-critical, important, or supporting. Use a higher due-diligence threshold where failure could disrupt customer access, payments, consent management, fraud controls, or regulatory reporting.
- Require clear statements of architectural responsibility. A provider should be able to distinguish what it secures, what the institution secures, and where shared-control points exist.
- Assess whether the supplier can support Canadian data, recordkeeping, audit, and incident-response expectations, including regulator engagement where required.
- Evaluate implementation realism. Projects that depend on heavy customization, unclear data mapping, or numerous manual workarounds create hidden operational and security risk.

- Test financial and operational viability. Institutions should understand concentration risk, subcontractor dependence, product roadmap credibility, and exit feasibility before contracting.
- Insist on independent evidence, not marketing assertions. The most useful inputs are current audit reports, control descriptions, penetration-test summaries, secure-development evidence, and resilience test results.

Suggested vendor assessment dimensions

Dimension	What decision-makers should ask	Evidence to request
Governance and accountability	Who owns risk, operations, support, and customer-impact decisions?	RACI model, escalation matrix, committee terms, policy extracts
Security architecture	How are identity, secrets, network controls, encryption, and logging implemented?	Architecture diagrams, key-management description, logging and monitoring standards
Third-party chain	Which subcontractors, cloud providers, and external dependencies are material?	Subprocessor list, dependency map, concentration-risk analysis
Privacy and data handling	What data is collected, retained, transformed, and deleted, and under whose instructions?	Data-flow diagrams, retention schedules, deletion procedures, privacy impact materials
Resilience and recovery	How will the service continue during outage, corruption, or cyber incident?	BCP and DR summaries, recovery testing evidence, service restoration objectives
Secure development	How are code, configurations, and releases governed and tested?	SDLC policy, change-control workflow, vulnerability management evidence
Compliance and auditability	Can the provider support supervisory review and contractual audit rights?	Audit reports, control attestations, sample client reporting packs
Exit and portability	How will data, consents, logs, and configurations be transferred or destroyed at exit?	Exit plan, transition services schedule, data export format specifications

List of services and solutions typically provided by key vendors

Without naming specific firms, institutions will typically encounter suppliers offering some or all of the following services:

- API gateway and developer-portal platforms used to expose account, consent, and service interfaces.
- Consent and authorization services that manage customer permissioning, token flows, revocation, and audit trails.
- Identity, verification, and fraud-control tools used to strengthen onboarding, authentication, and transaction monitoring.
- Data aggregation, normalization, enrichment, and analytics services that transform raw account data into standardized formats or decision inputs.

- Payments enablement and account-to-account initiation capabilities designed for future write-access use cases where permitted.
- Integration, middleware, and workflow orchestration tools connecting core banking, digital channels, CRM, risk engines, and support systems.
- Managed security, SOC, threat-monitoring, and incident-response services supporting 24/7 oversight of exposed services and partner integrations.
- Testing, certification, compliance, and assurance services used to validate APIs, controls, resilience, privacy, and operational readiness.

Key controls and compliance safeguards when engaging solution providers

The contract and control framework should be built before implementation begins. At minimum, institutions should consider the following safeguards:

- A clear service description, control matrix, and shared-responsibility model covering security, privacy, resilience, support, and regulatory engagement.
- Minimum security requirements for identity and access management, privileged-access control, secrets handling, secure configuration, patching, malware protection, encryption, and tamper-evident logging.
- Explicit obligations for vulnerability management, secure coding, penetration testing, remediation timelines, and independent assurance reporting.
- Notification clauses for incidents, control failures, subcontractor changes, significant architecture changes, and legal or regulatory events that could affect service integrity or availability.
- Rights to audit, obtain evidence, review material subcontractors, and receive timely performance, risk, and control reporting.
- Data governance requirements covering permitted use, data minimization, retention, deletion, backup handling, cross-border movement, and customer-consent boundaries.
- Resilience requirements including service restoration objectives, backup and recovery expectations, crisis-management interfaces, failover procedures, and periodic joint exercises.
- Orderly exit provisions for transition support, data extraction, key and credential rotation, evidence retention, and verified destruction where required.

Detailed testing methodology for secure and compliant rollout

A credible testing approach should not wait until code complete. It should begin during design and continue through production readiness and post-launch assurance. The objective is not merely to demonstrate that functions work, but to show that the institution can operate the service safely, recover from disruption, and meet supervisory expectations on technology risk, third-party risk, resilience, and incident handling.

1. Governance and scope definition

Define which legal entities, products, customer segments, channels, datasets, and third parties are in scope. Identify the applicable regulatory perimeter, including whether the institution is primarily responding to OSFI expectations, FSRA expectations, or both. Approve risk appetite, critical operations, target control outcomes, and go-live criteria before build work advances.

2. Architecture and threat assessment

Perform formal design review covering trust boundaries, data flows, interface exposure, authentication paths, consent storage, dependency mapping, and concentration risk. Use threat modeling to test misuse cases such as token theft, API abuse, consent replay, data poisoning, partner compromise, identity fraud, and insider misuse.

3. Control design validation

Validate that preventive, detective, and corrective controls are mapped to identified risks. Review segmentation, encryption, key management, secure build pipelines, vulnerability management, secrets handling, logging, alerting, data retention, and privacy controls. Confirm that shared-control boundaries with vendors are documented and testable.

4. Third-party and supply-chain assurance

Before integration testing, verify supplier control evidence, subcontractor dependencies, support coverage, incident responsibilities, and recovery capabilities. Where services are material, require walk-throughs of control operation and evidence of recent testing rather than relying solely on broad attestations.

5. Functional and integration testing

Test all core workflows end to end: onboarding, consent creation, consent renewal, revocation, API authentication, data retrieval, error handling, exception queues, customer support handoffs, and complaint escalation. Validate that internal records remain consistent across channels and systems.

6. Security testing

Conduct application security testing, API security testing, configuration review, dependency scanning, infrastructure validation, and penetration testing. Test for broken object-level authorization, excessive data exposure, weak rate limiting, replay attacks, session and token misuse, privilege escalation, injection flaws, and insecure error handling. Remediate high-risk findings before production approval.

7. Privacy and consent testing

Confirm that only authorized data is collected and shared, that consent language matches actual data flows, that revocation is effective and timely, and that retention and deletion logic work as intended. Review customer notices, support scripts, and escalation paths for clarity and fairness.

8. Resilience and operational testing

Test backup and recovery, failover, degraded-mode operation, queue backlogs, dependency loss, certificate expiry, cloud-region issues, and operational handoffs during prolonged disruption. Align scenarios to critical operations and disruption tolerances in line with operational resilience expectations.

9. Incident response and regulator notification exercises

Run tabletop and live-response exercises involving technology, fraud, legal, privacy, communications, vendor contacts, and business owners. Test classification thresholds, evidence preservation, executive escalation, customer messaging, and notification workflows. For FRFIs, ensure processes can support OSFI technology and cyber incident reporting expectations. For FSRA-regulated entities, ensure material IT incidents can be assessed and reported in line with FSRA guidance, which generally expects notification within 72 hours or sooner after determining materiality.

10. User acceptance and trust testing

Assess the customer experience, especially consent comprehension, supportability, exception handling, and the ability to explain what data is shared and how to stop sharing. This is particularly important because poor consent design can create both compliance risk and trust erosion even when technical controls are sound.

11. Independent challenge and go-live decision

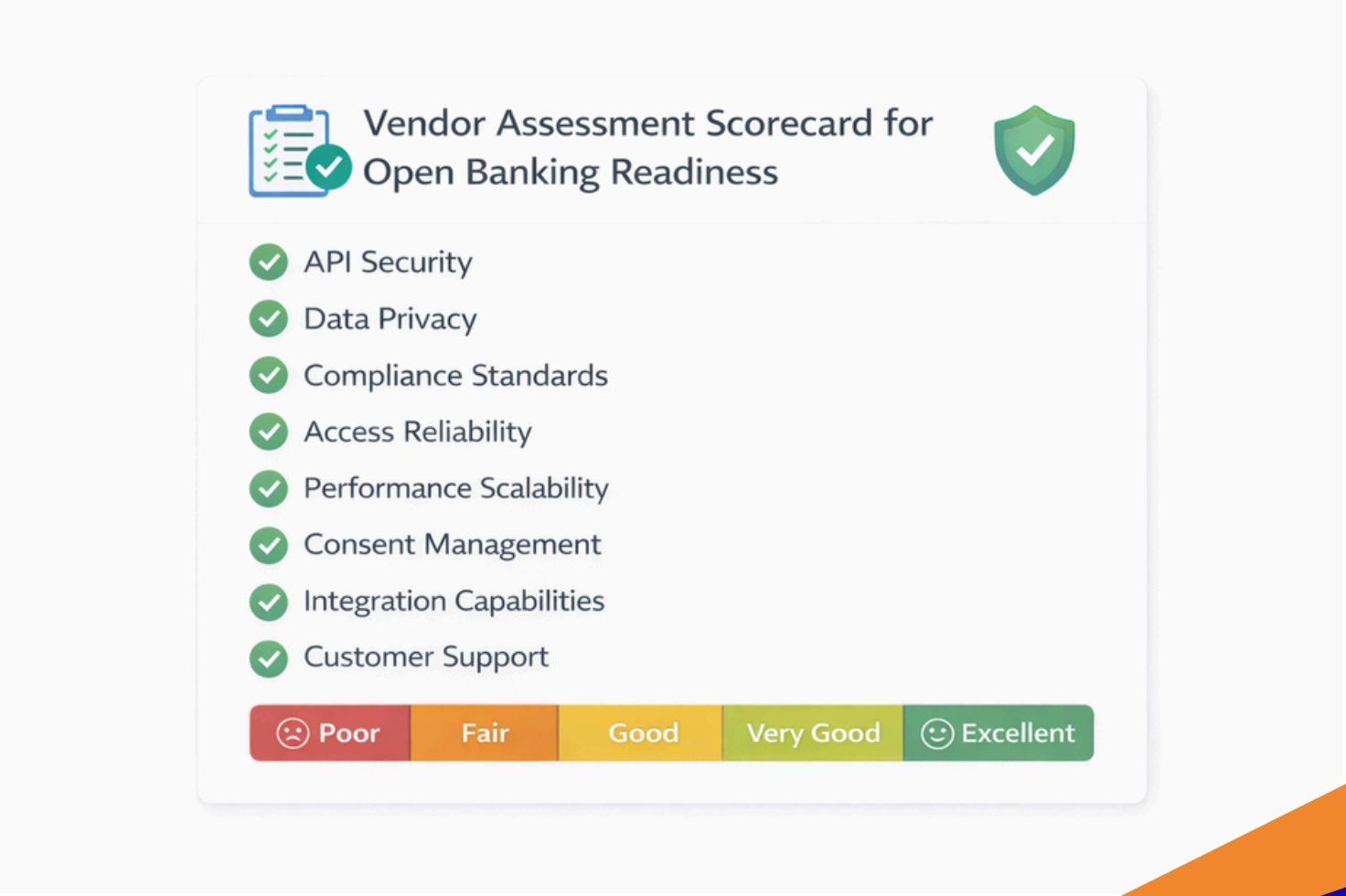
Require independent review by risk, security, compliance, internal audit, or an external assurance function. The final decision should consider open findings, compensating controls, residual risk, vendor readiness, monitoring coverage, and business continuity preparedness, not only project deadlines.

12. Post-launch verification

After go-live, perform heightened monitoring, control sampling, incident trend review, log-quality review, and targeted retesting. Confirm that model drift, control drift, configuration drift, and vendor changes do not quietly erode the security or reliability of the service over time.

Supervisory alignment note

No single testing script will by itself make a consumer-driven banking solution compliant. Institutions should use the methodology above to demonstrate a risk-based, evidence-driven program aligned to published Canadian supervisory expectations. For FRFIs, the most relevant public anchors are OSFI B-13, B-10, E-21, the Integrity and Security Guideline, and OSFI's technology and cyber incident reporting advisory. For Ontario credit unions and other FSRA-regulated entities, the key public anchor is FSRA's IT Risk Management guidance, including its practices for effective IT risk management and material incident notification process. Applicability should be confirmed by legal and regulatory teams based on charter, sector, and corporate structure.



poor consent design can create both compliance risk and trust erosion even when technical controls are sound.

11. Independent challenge and go-live decision
Require independent review by risk, security, compliance, internal audit, or an external assurance function. The final decision should consider open findings, compensating controls, residual risk, vendor readiness, monitoring coverage, and business continuity preparedness, not only project deadlines.

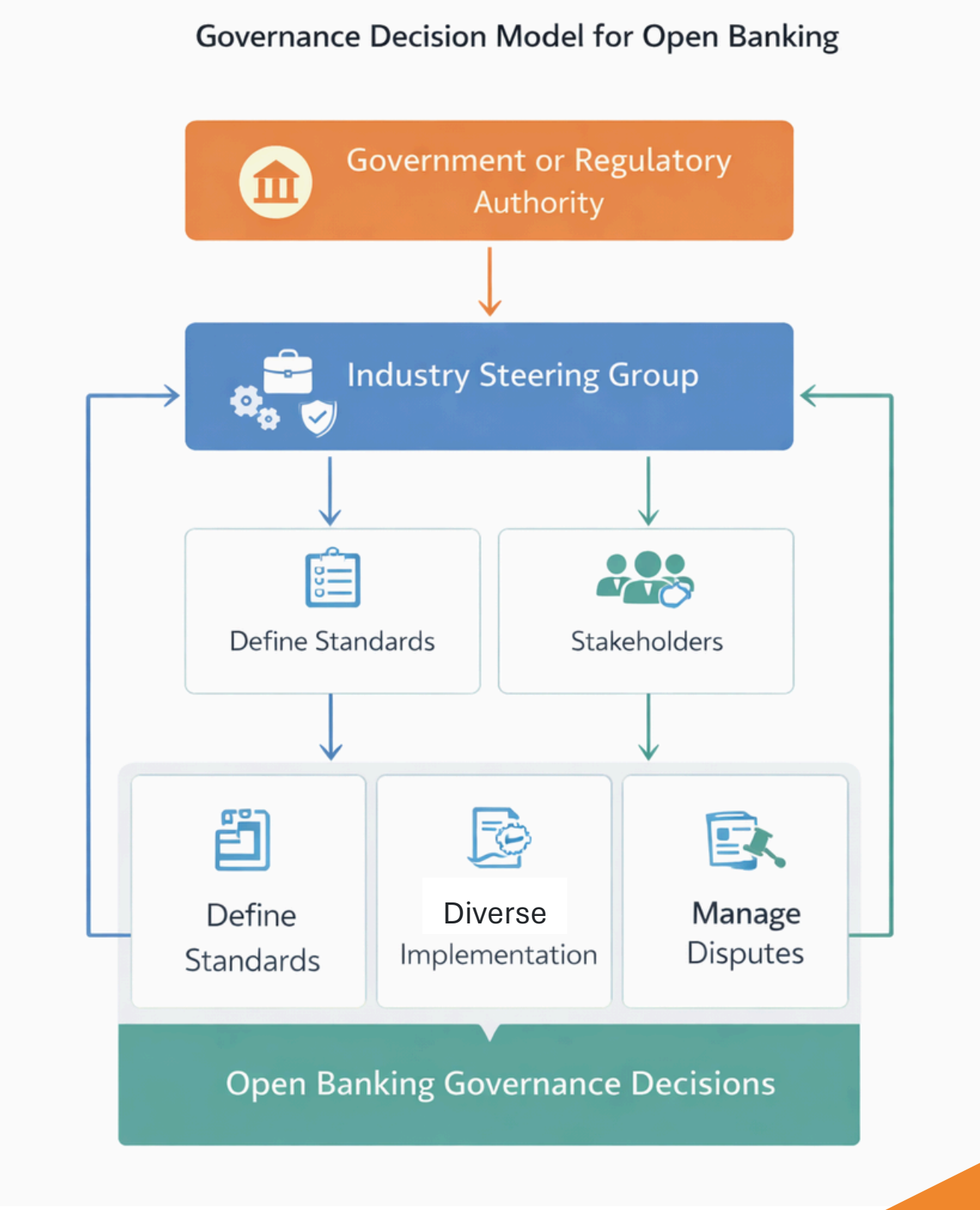
12. Post-launch verification
After go-live, perform heightened monitoring, control sampling, incident trend review, log-quality review, and targeted retesting. Confirm that model drift, control drift, configuration drift, and vendor changes do not quietly erode the security or reliability of the service over time.

Supervisory alignment note
No single testing script will by itself make a consumer-driven banking solution compliant. Institutions should use the methodology above to demonstrate a risk-based, evidence-driven program aligned to published Canadian supervisory expectations. For FRFIs, the most relevant public anchors are OSFI B-13, B-10, E-21, the Integrity and Security Guideline, and OSFI's technology and cyber incident reporting advisory. For Ontario credit unions and other FSRA-regulated entities, the key public anchor is FSRA's IT Risk Management guidance, including its practices for effective IT risk management and material incident notification process. Applicability should be confirmed by legal and regulatory teams based on charter, sector, and corporate structure.

Preparation Checklist

Readiness area	Preliminary Questions
Governance	Who owns the program at the executive and working levels, and how often is progress reviewed?
Legal and compliance	What obligations are likely to apply, and where are the biggest liability and contract gaps?
Privacy and consent	Can the organization explain access, purpose, duration, and revocation in clear language?
Security	Are API, identity, logging, fraud, and monitoring capabilities mature enough for scaled data sharing?
Operations	Can support teams manage complaints, revocations, disputes, and partner incidents at volume?
Third parties	Which critical dependencies would create concentration, resilience, or reputational risk?
Product and customer strategy	Which use cases genuinely improve trust, switching, affordability, or business efficiency?

Resilience	What happens if a partner fails, data quality degrades, or ecosystem trust is damaged by a public incident?



Conclusion and Takeaways

Canada's consumer-driven banking project is about more than letting apps read balances. It is about replacing an unsafe status quo with a supervised data-sharing regime that can give customers more control, make service delivery safer, improve switching and competition, and support a more resilient digital financial system. That promise will only be realized if the rollout is disciplined, understandable, and trusted.

For financial institutions, the main message is simple: this is not a future issue to watch passively. It is a strategic, legal, operational, security, and customer-trust issue that should already be on active planning agendas. The institutions that prepare early will be better positioned not only to comply, but also to compete.

Bibliography and Further Reading

Recent legal and policy analysis

Blake, Cassels & Graydon LLP. "2025 Federal Budget: Financial Sector Highlights." November 6, 2025. https://www.blakes.com/insights/2025-federal-budget-financial-sector-highlights/

McCarthy Tetrault LLP. "Ctrl+Alt+Bank: Canada Reboots Open Banking with Budget 2025." November 7, 2025. https://www.mccarthy.ca/en/insights/blogs/techlex/ctrl-alt-bank-canada-reboots-open-banking-with-budget-2025

McCarthy Tetrault LLP. "Open Banking 2025: Read, Write, and Rewrite the Rules." November 25, 2025. https://www.mccarthy.ca/en/insights/blogs/techlex/open-banking-2025-read-write-and-rewrite-the-rules

McCarthy Tetrault LLP. "Open Banking: New Developments from the 2024 Fall Economic Statement." December 18, 2024. https://www.mccarthy.ca/en/insights/blogs/techlex/open-banking-new-developments-2024-fall-economic-statement

Osler, Hoskin & Harcourt LLP. "Canada's 2026 privacy priorities: data sovereignty, open banking and AI." December 4, 2025. https://www.osler.com/en/insights/reports/2025-legal-outlook/canadas-2026-privacy-priorities-data-sovereignty-open-banking-and-ai/

Torys LLP. "Budget 2025: supporting innovation in financial services." November 2025. https://www.torys.com/en/our-latest-thinking/publications/2025/11/budget-2025-supporting-innovation-in-financial-services

Torys LLP. "Budget 2025: impact on financial consumers." November 2025. https://www.torys.com/en/our-latest-thinking/publications/2025/11/budget-2025-impact-on-financial-consumers

Official Canadian background and implementation materials

Department of Finance Canada. "Budget 2025: Canada's Consumer-Driven Banking Framework." 2025. https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation/budget-2025-canadas-framework-for-consumer-driven-banking.html

Department of Finance Canada. "2024 Fall Economic Statement: Canada's Complete Framework for Consumer-Driven Banking." 2024.
https://www.canada.ca/en/department-finance/news/2024/12/2024- fall-economic-statement-canadas-complete-framework-for-consumer-driven-banking.html

Department of Finance Canada. "Budget 2024: Canada's Framework for Consumer-Driven Banking." 2024.
https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation/budget-2024-canadas-framework-for-consumer-driven-banking.html

Parliament of Canada. "Bill C-15 status page." accessed March 18, 2026.
https://www.parl.ca/legisinfo/en/bill/45-1/c-15

Global comparator materials

Open Banking Limited. "OBL Impact Report 7: open banking delivers real-world impact as adoption accelerates year on year." 2025.
https://www.openbanking.org.uk/insights/obl-impact-report-7-open-banking-delivers-real-world-impact-as-adoption-accelerates-year-on-year/

Financial Conduct Authority. "Open banking and open finance in the UK." 2025.
https://www.fca.org.uk/publication/research-notes/open-banking-open-finance-uk.pdf

Consumer Data Right, Australia. "What is CDR?." accessed March 18, 2026.
https://www.cdr.gov.au/what-is-cdr

FCAC. "Open banking." accessed April 21, 2026.
https://eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/14575

Parliament of Canada. "Government Bill (House of Commons) C-15 (45-1): Royal Assent." accessed April 21, 2026.
https://www.parl.ca/documentviewer/en/45-1/bill/C-15/royal-assent

Bank of Canada. "About our supervisory mandates." accessed April 21, 2026.
https://www.bankofcanada.ca/core-functions/retail-payments-supervision/about-our-supervisory-mandates/

Justice Laws Website. "Consumer-Driven Banking Act." accessed April 21, 2026.
https://www.laws-lois.justice.gc.ca/eng/acts/C-36.75/FullText.html

Parliament of Canada. "C-15 (45-1): LEGISinfo." accessed April 21, 2026.
https://www.parl.ca/legisinfo/en/bill/45-1/c-15