RegLens

BANK ONBOARDING READINESS PACKAGE

Awesome Inc

A vendor-facing summary of compliance posture mapped to the categories bank third-party risk teams ask about.

ISSUED	6 July 2026
SCOPE	4 regulations in scope
CLASSIFICATION	Confidential

EXECUTIVE SUMMARY

Onboarding readiness at a glance

Moderate Risk

Several areas require attention. Prioritize amber and red findings.

19	9	0	28
GREEN	AMBER	RED	TOTAL ASSESSED

POSTURE

AMBER

Regulations in scope

OSFI-B-10	Third-Party Risk Management
OSFI-B-13	Technology and Cyber Risk Management
PIPEDA	Personal Information Protection and Electronic Documents Act
QC-LAW-25	Act respecting the protection of personal information in the private sector

CATEGORICAL DETAIL

Readiness by bank-questionnaire category

Each category below aggregates assessed controls that contribute to a standard bank third-party risk questionnaire domain (SIG / CAIQ taxonomy). Counts are weighted by the strength of the control-to- category mapping; a single control may contribute to more than one category. Categories with no assessed controls are omitted. Weighted counts reflect partial-credit contribution where a single control satisfies multiple bank-questionnaire categories; per-control breakdowns below each card use raw counts.

Board & Risk Governance

GREEN

3 controls mapped

1.5 green · **0 amber** · **0 red**

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

- CTRL-GOV-001 — Named senior officer accountable for technology and cyber risk

  Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

- CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff

  Evidence: Training completion report from learning management system showing 100% completion across all in-scope staff

- CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

  Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

> ACCEPTABLE ANSWER IF ASKED
>
> *Awesome Inc has documented and operating controls across Board & Risk Governance. For each question in this category, the typical response is: "Yes — CTRL-GOV-001, CTRL-AWARE-001, CTRL-STRAT-001. Evidence available on request: policy document, report." Specific controls in this category: Named senior officer accountable for technology and cyber risk, Mandatory cybersecurity awareness training for all staff, Documented cybersecurity strategy aligned to business objectives. Verify accuracy with internal compliance counsel before sending.*

Information Security Program

GREEN

5 controls mapped

1.1 green · 0 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-GOV-001 — Named senior officer accountable for technology and cyber risk

Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

• CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff

Evidence: Training completion report from learning management system showing 100% completion across all in-scope staff

• CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

• CTRL-B13-Q16 — Is privileged access to cloud environments managed via a PAM (Privileged Access Management) solution with MFA enforced?

Evidence: IAM policy export showing MFA enforced for all privileged role assignments

• CTRL-B13-Q18 — Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?

Evidence: Configuration screenshots from key management service (AWS KMS, Azure Key Vault, Google Cloud KMS) showing customer-managed or service-managed keys

> ACCEPTABLE ANSWER IF ASKED
>
> *Awesome Inc has documented and operating controls across Information Security Program. For each question in this category, the typical response is: "Yes — CTRL-GOV-001, CTRL-AWARE-001, CTRL-STRAT-001. Evidence available on request: policy document, report." Specific controls in this category: Named senior officer accountable for technology and cyber risk, Mandatory cybersecurity awareness training for all staff, Documented cybersecurity strategy aligned to business objectives. Verify accuracy with internal compliance counsel before sending.*

Access Control & Identity

GREEN

1 control mapped

1 green · 0 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-IAM-001 — MFA enforced for all privileged access

Evidence: IAM policy export showing MFA enforced for all privileged role assignments

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Awesome Inc has documented and operating controls across Access Control & Identity. For each question in this category, the typical response is: "Yes — CTRL-IAM-001. Evidence available on request: config export, screenshot." Specific controls in this category: MFA enforced for all privileged access. Verify accuracy with internal compliance counsel before sending.*

Data Protection & Encryption

AMBER

16 controls mapped

3 green · 1.5 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-B13-Q16 — Is privileged access to cloud environments managed via a PAM (Privileged Access Management) solution with MFA enforced?

Evidence: IAM policy export showing MFA enforced for all privileged role assignments

• CTRL-B13-Q18 — Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?

Evidence: Configuration screenshots from key management service (AWS KMS, Azure Key Vault, Google Cloud KMS) showing customer-managed or service-managed keys

• CTRL-PRIV-003 — Personal Information Consent Management

Evidence: Privacy notice content shown at the point of personal information collection (web form, app, intake document)

• CTRL-PRIV-005 — Personal Information Retention and Disposal

Evidence: Documented retention schedule for personal information categories

• CTRL-PRIV-006 — Privacy Policy Transparency

Evidence: Designated Privacy Officer / Person Responsible appointment letter or board minutes

• CTRL-PRIV-008 — Privacy Complaints Handling

Evidence: Complaints procedure document (publicly available)

• CTRL-PRIV-009 — Personal Information Breach Response

Evidence: Incident register

• CTRL-PRIV-011 — Express Consent for Sensitive Personal Information and Minors

Evidence: Privacy notice content shown at the point of personal information collection (web form, app, intake document)

• CTRL-PRIV-012 — Cross-Border Personal Information Transfer Assessment

Evidence: Transfer impact assessment template

- CTRL-PRIV-013 — Automated Decision-Making Transparency and Explanation

  Evidence: Privacy Impact Assessment (PIA) template and at least one completed PIA for a recent IT project

- CTRL-PRIV-015 — Data Portability and Right to De-Indexing

  Evidence: Documented procedure for handling data subject access, correction, deletion, portability, and de-indexing requests

AREAS IN PROGRESS

- CTRL-PRIV-001 — Privacy Program Accountability
- CTRL-PRIV-002 — Personal Information Collection Purpose Identification
- CTRL-PRIV-004 — Personal Information Data Minimisation
- CTRL-PRIV-007 — Data Subject Access and Correction Rights
- CTRL-PRIV-010 — Privacy Impact Assessment for IT Projects

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Awesome Inc has documented and operating controls across Data Protection & Encryption. For each question in this category, the typical response is: "Yes — CTRL-B13-Q16, CTRL-B13-Q18, CTRL-PRIV-003. Evidence available on request: config export, screenshot." Specific controls in this category: Is privileged access to cloud environments managed via a PAM (Privileged Access Management) solution with MFA enforced?, Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?, Personal Information Consent Management. Verify accuracy with internal compliance counsel before sending.*

Privacy Program

AMBER

14 controls mapped

6.3 green · **3.5 amber** · **0 red**

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

- CTRL-PRIV-003 — Personal Information Consent Management

  Evidence: Privacy notice content shown at the point of personal information collection (web form, app, intake document)

- CTRL-PRIV-005 — Personal Information Retention and Disposal

  Evidence: Documented retention schedule for personal information categories

- CTRL-PRIV-006 — Privacy Policy Transparency

  Evidence: Designated Privacy Officer / Person Responsible appointment letter or board minutes

- CTRL-PRIV-008 — Privacy Complaints Handling

  Evidence: Complaints procedure document (publicly available)

- CTRL-PRIV-009 — Personal Information Breach Response

  Evidence: Incident register

• CTRL-PRIV-011 — Express Consent for Sensitive Personal Information and Minors

Evidence: Privacy notice content shown at the point of personal information collection (web form, app, intake document)

• CTRL-PRIV-012 — Cross-Border Personal Information Transfer Assessment

Evidence: Transfer impact assessment template

• CTRL-PRIV-013 — Automated Decision-Making Transparency and Explanation

Evidence: Privacy Impact Assessment (PIA) template and at least one completed PIA for a recent IT project

• CTRL-PRIV-015 — Data Portability and Right to De-Indexing

Evidence: Documented procedure for handling data subject access, correction, deletion, portability, and de-indexing requests

AREAS IN PROGRESS

• CTRL-PRIV-001 — Privacy Program Accountability
• CTRL-PRIV-002 — Personal Information Collection Purpose Identification
• CTRL-PRIV-004 — Personal Information Data Minimisation
• CTRL-PRIV-007 — Data Subject Access and Correction Rights
• CTRL-PRIV-010 — Privacy Impact Assessment for IT Projects

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Awesome Inc has documented and operating controls across Privacy Program. For each question in this category, the typical response is: "Yes — CTRL-PRIV-003, CTRL-PRIV-005, CTRL-PRIV-006. Evidence available on request: screenshot, audit log." Specific controls in this category: Personal Information Consent Management, Personal Information Retention and Disposal, Privacy Policy Transparency. Verify accuracy with internal compliance counsel before sending.*

Cyber Threat Management

GREEN

2 controls mapped

1.2 green · **0 amber** · **0 red**

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-B13-Q16 — Is privileged access to cloud environments managed via a PAM (Privileged Access Management) solution with MFA enforced?

Evidence: IAM policy export showing MFA enforced for all privileged role assignments

• CTRL-B13-Q18 — Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?

Evidence: Configuration screenshots from key management service (AWS KMS, Azure Key Vault, Google Cloud KMS) showing customer-managed or service-managed keys

ACCEPTABLE ANSWER IF ASKED

Awesome Inc has documented and operating controls across Cyber Threat Management. For each question in this category, the typical response is: "Yes — CTRL-B13-Q16, CTRL-B13-Q18. Evidence available on request: config export, screenshot." Specific controls in this category: Is privileged access to cloud environments managed via a PAM (Privileged Access Management) solution with MFA enforced?, Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?. Verify accuracy with internal compliance counsel before sending.

Incident Response

AMBER

3 controls mapped

1 green · 2 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-IR-REG-001 — Documented procedure for notifying regulators of material cyber incidents

Evidence: Documented regulator notification procedure

AREAS IN PROGRESS

• CTRL-B13-Q21 — Does your organization have a documented Incident Response Plan that explicitly covers critical technology systems and environments?

• CTRL-PRIV-014 — Personal Information Breach Notification to Regulator

ACCEPTABLE ANSWER IF ASKED

Awesome Inc has implemented 1 control in Incident Response with 2 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-IR-REG-001. Evidence available on request: policy document." For amber-status questions, the typical response is: "In implementation — documented project plan in place. Evidence and project plan available on request." Verify accuracy with internal compliance counsel before sending.

Business Continuity & Resilience

GREEN

1 control mapped

0.7 green · 0 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-EXIT-001 — Documented CSP exit strategy

Evidence: Critical CSP exit plan document with trigger conditions, estimated migration timeline, alternative providers, and data portability path

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Awesome Inc has documented and operating controls across Business Continuity & Resilience. For each question in this category, the typical response is: "Yes — CTRL-EXIT-001. Evidence available on request: policy document, test report." Specific controls in this category: Documented CSP exit strategy. Verify accuracy with internal compliance counsel before sending.*

Vendor / Third-Party Risk

AMBER

5 controls mapped

2.3 green · **2 amber** · **0 red**

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

• CTRL-TPRM-001 — Third-Party Concentration and Fourth-Party Risk

Evidence: Vendor concentration analysis identifying critical arrangements with single providers and dependencies on common upstream services

• CTRL-B13-Q24 — Do you conduct formal risk assessments of critical technology service providers before onboarding and periodically thereafter?

Evidence: Completed vendor due diligence questionnaire (DDQ) for the vendor at onboarding

• CTRL-EXIT-001 — Documented CSP exit strategy

Evidence: Critical CSP exit plan document with trigger conditions, estimated migration timeline, alternative providers, and data portability path

AREAS IN PROGRESS

• CTRL-B13-Q23 — Do contracts with critical technology service providers include clauses covering data protection, audit rights, incident notification, and exit provisions?

• CTRL-VENDOR-DD-001 — Cybersecurity due diligence performed on all material non-CSP vendors

ACCEPTABLE ANSWER IF ASKED

Awesome Inc has documented and operating controls across Vendor / Third-Party Risk. For each question in this category, the typical response is: "Yes — CTRL-TPRM-001, CTRL-B13-Q24, CTRL-EXIT-001. Evidence available on request: report, attestation." Specific controls in this category: Third-Party Concentration and Fourth-Party Risk, Do you conduct formal risk assessments of critical technology service providers before onboarding and periodically thereafter?, Documented CSP exit strategy. Verify accuracy with internal compliance counsel before sending.

Audit & Compliance

GREEN

3 controls mapped

0.9 green · 0 amber · 0 red

Controls below may also appear under other categories where they contribute partial coverage. Counts in the card header above reflect this category's weighted contribution.

WHAT WE HAVE IN PLACE

- CTRL-GOV-001 — Named senior officer accountable for technology and cyber risk

  Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

- CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff

  Evidence: Training completion report from learning management system showing 100% completion across all in-scope staff

- CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

  Evidence: Board or executive committee minutes showing formal designation of the accountable officer for technology and cyber risk

ACCEPTABLE ANSWER IF ASKED

Awesome Inc has documented and operating controls across Audit & Compliance. For each question in this category, the typical response is: "Yes — CTRL-GOV-001, CTRL-AWARE-001, CTRL-STRAT-001. Evidence available on request: policy document, report." Specific controls in this category: Named senior officer accountable for technology and cyber risk, Mandatory cybersecurity awareness training for all staff, Documented cybersecurity strategy aligned to business objectives. Verify accuracy with internal compliance counsel before sending.

CROSS-REGULATION COVERAGE

Answer once, satisfy multiple regulators

Your responses in this assessment satisfy controls across 4 regulations simultaneously. RegLens scored a single set of responses against each applicable regulator's expectations independently.

Regulatory scope of this assessment

OSFI-B-10	Third-Party Risk Management · 6 controls assessed
OSFI-B-13	Technology and Cyber Risk Management · 8 controls assessed
PIPEDA	Personal Information Protection and Electronic Documents Act · 13 controls assessed
QC-LAW-25	Act respecting the protection of personal information in the private sector · 17 controls assessed

How responses map across regulations

CONTROL	TITLE	SATISFIES
CTRL-AWARE-001	Mandatory cybersecurity awareness training for all staff	OSFI-B-13 · PIPEDA · QC-LAW-25
CTRL-IAM-001	MFA enforced for all privileged access	OSFI-B-13 · PIPEDA · QC-LAW-25
CTRL-B13-Q18	Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?	PIPEDA · QC-LAW-25
CTRL-EXIT-001	Documented CSP exit strategy	OSFI-B-10 · OSFI-B-13
CTRL-GOV-001	Named senior officer accountable for technology and cyber risk	OSFI-B-10 · OSFI-B-13
CTRL-PRIV-001	Privacy Program Accountability	PIPEDA · QC-LAW-25

CTRL-PRIV-002	Personal Information Collection Purpose Identification	PIPEDA · QC-LAW-25

KEY GAPS

Highest-priority controls to address

The findings below are the controls most likely to be flagged during a bank vendor risk review. Each is shown with the regulations it affects and the indicative remediation timeline RegLens recommends.

IRP documented but not tested within 12 months

AMBER

Affects: OSFI-B-13

An untested IRP has unknown gaps. Teams that have never run through an incident scenario will improvise under pressure — and improvisation during a real incident is costly.

Indicative timeline: 3–5 weeks

Following a personal information breach posing a risk of harm, do you notify the applicable supervisory authority within the timeframe required by applicable legislation, using the prescribed form?

AMBER

Affects: PIPEDA · QC-LAW-25

The notification path to the OPC exists but the PIPEDA s. 10.1 72-hour internal SLA (with 24-hour escalation trigger) and the s. 10.3 register linkage have not been rehearsed.

Indicative timeline: 4–8 weeks

Has your organisation designated an individual responsible for privacy compliance, with documented privacy policies, procedures, governance structures, and staff training for personnel handling personal information?

AMBER

Affects: PIPEDA · QC-LAW-25

A named owner without a documented program leaves the accountability chain unverifiable in a regulatory investigation.

Do you document the purposes for which personal information is collected at or before collection, and communicate those purposes to individuals?

AMBER

Affects: PIPEDA · QC-LAW-25

Purposes are identified in the top-level privacy policy but individual collection points lack contextual notice, which the OPC has found insufficient under Principle 2 when purposes vary by channel.

Do you limit collection of personal information to what is necessary for the identified purposes, avoiding incidental information you don't need?

AMBER

Affects: PIPEDA

Partial minimisation usually means legacy collection points still pull more than the documented purpose requires.

To discuss remediation support, contact your RegLens account team or email **support@reglens.app**.