RegLens

BANK ONBOARDING READINESS PACKAGE

Hamilton Re Ltd.

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

ISSUED	6 July 2026
SCOPE	2 regulations in scope
CLASSIFICATION	Confidential

EXECUTIVE SUMMARY

Onboarding readiness at a glance

Significant Gaps

Immediate remediation required across multiple principles.

14	29	1	44
GREEN	AMBER	RED	TOTAL ASSESSED

POSTURE

RED

Regulations in scope

BERMUDA-PIPA	Personal Information Protection Act 2016
BMA-OCRM	Operational Cyber Risk Management Code of Conduct

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

AMBER

6 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-B13-Q04 — Does your internal audit function independently assess technology and cyber risk controls at least annually?

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

- 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

AREAS IN PROGRESS

- CTRL-B13-Q02 — Is there a Board-approved technology and cyber risk policy reviewed at least annually?
- CTRL-B13-Q03 — Does your organization have a defined technology risk appetite statement that is actively used in decision-making?
- CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff
- CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

> ACCEPTABLE ANSWER IF ASKED
>
> *Hamilton Re Ltd. has implemented 2 controls in Board & Risk Governance with 4 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-B13-Q04, CTRL-GOV-001. Evidence available on request: policy document, report." 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.*

Information Security Program

AMBER

19 controls mapped

0.4 green · 3.7 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-Q04 — Does your internal audit function independently assess technology and cyber risk controls at least annually?

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

• 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

AREAS IN PROGRESS

• CTRL-B13-Q02 — Is there a Board-approved technology and cyber risk policy reviewed at least annually?

• CTRL-B13-Q03 — Does your organization have a defined technology risk appetite statement that is actively used in decision-making?

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

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

• CTRL-B13-Q05 — Does your organization maintain a current, complete inventory of technology assets, including infrastructure, applications, data stores, endpoints, and cloud resources where applicable?

• CTRL-B13-Q06 — Are cloud assets (VMs, storage, databases, APIs) tagged and classified by business criticality and data sensitivity?

• CTRL-B13-Q07 — Does your cloud architecture follow documented, approved reference architectures aligned to security and resilience requirements?

• CTRL-B13-Q09 — Are security and compliance requirements (including B-13 controls) embedded into your SDLC / change management process?

• CTRL-B13-Q10 — Do you have documented Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical technology systems?

• CTRL-B13-Q11 — Has your organization conducted a full disaster recovery test for cloud workloads in the past 12 months?

• CTRL-B13-Q22 — Do you have a documented Business Continuity Plan covering failure scenarios for critical technology service providers and infrastructure dependencies (including cloud provider outages)?

• CTRL-B13-Q14 — Does your organization conduct formal cyber risk assessments of technology environments at least annually?

• CTRL-B13-Q15 — Do you have continuous monitoring in place to identify vulnerabilities and misconfigurations across cloud environments?

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

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

• CTRL-B13-Q19 — Are security testing practices, such as static application security testing (SAST), dynamic application security testing (DAST), penetration testing, or equivalent testing methods, integrated into application development and change processes?

• CTRL-B13-Q20 — Do you have a centralized SIEM or equivalent capability providing real-time detection of security events across applicable technology environments?

> ACCEPTABLE ANSWER IF ASKED
>
> *Hamilton Re Ltd. has implemented 2 controls in Information Security Program with 17 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-B13-Q04, CTRL-GOV-001. Evidence available on request: policy document, report." 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.*

Access Control & Identity

AMBER

2 controls mapped

0 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.

AREAS IN PROGRESS

• CTRL-B13-Q17 — Is Role-Based Access Control (RBAC) enforced using least-privilege principles across all cloud environments?

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

> ACCEPTABLE ANSWER IF ASKED
>
> *Hamilton Re Ltd. has implemented 0 controls in Access Control & Identity with 2 additional controls under active development. 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.*

Data Protection & Encryption

AMBER

21 controls mapped

2.1 green · 4.7 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-005 — Personal Information Retention and Disposal

Evidence: Documented retention schedule for personal information categories

• CTRL-PRIV-007 — Data Subject Access and Correction Rights

Evidence: Documented access/correction request procedure

• CTRL-PRIV-008 — Privacy Complaints Handling

Evidence: Complaints procedure document (publicly available)

• CTRL-PRIV-009 — Personal Information Breach Response

Evidence: Incident register

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

Evidence: Transfer impact assessment template

• 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

• CTRL-PRIV-016 — Personal Information Accuracy

Evidence: Data quality and accuracy policy aligned with applicable privacy legislation

AREAS IN PROGRESS

• CTRL-B13-Q12 — Is sensitive financial and customer data classified, and are controls applied based on classification (encryption, access controls, residency)?

• CTRL-B13-Q13 — Do you have documented data residency controls ensuring regulated data stays within required geographic boundaries?

• CTRL-B13-Q14 — Does your organization conduct formal cyber risk assessments of technology environments at least annually?

• CTRL-B13-Q15 — Do you have continuous monitoring in place to identify vulnerabilities and misconfigurations across cloud environments?

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

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

• CTRL-B13-Q19 — Are security testing practices, such as static application security testing (SAST), dynamic application security testing (DAST), penetration testing, or equivalent testing methods, integrated into application development and change processes?

• CTRL-B13-Q20 — Do you have a centralized SIEM or equivalent capability providing real-time detection of security events across applicable technology environments?

• CTRL-PRIV-001 — Privacy Program Accountability

• CTRL-PRIV-002 — Personal Information Collection Purpose Identification

• CTRL-PRIV-003 — Personal Information Consent Management

• CTRL-PRIV-004 — Personal Information Data Minimisation

• CTRL-PRIV-006 — Privacy Policy Transparency

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

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Hamilton Re Ltd. has implemented 7 controls in Data Protection & Encryption with 14 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-PRIV-005, CTRL-PRIV-007, CTRL-PRIV-008. Evidence available on request: policy document, audit log." 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.*

Privacy Program

AMBER

13 controls mapped

4.9 green · **4.2 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-PRIV-005 — Personal Information Retention and Disposal

Evidence: Documented retention schedule for personal information categories

• CTRL-PRIV-007 — Data Subject Access and Correction Rights

Evidence: Documented access/correction request procedure

• CTRL-PRIV-008 — Privacy Complaints Handling

Evidence: Complaints procedure document (publicly available)

• CTRL-PRIV-009 — Personal Information Breach Response

Evidence: Incident register

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

Evidence: Transfer impact assessment template

• 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

• CTRL-PRIV-016 — Personal Information Accuracy

Evidence: Data quality and accuracy policy aligned with applicable privacy legislation

AREAS IN PROGRESS

• CTRL-PRIV-001 — Privacy Program Accountability

• CTRL-PRIV-002 — Personal Information Collection Purpose Identification

• CTRL-PRIV-003 — Personal Information Consent Management

• CTRL-PRIV-004 — Personal Information Data Minimisation

• CTRL-PRIV-006 — Privacy Policy Transparency

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

ACCEPTABLE ANSWER IF ASKED

Hamilton Re Ltd. has documented and operating controls across Privacy Program. For each question in this category, the typical response is: "Yes — CTRL-PRIV-005, CTRL-PRIV-007, CTRL-PRIV-008. Evidence available on request: policy document, audit log." Specific controls in this category: Personal Information Retention and Disposal, Data Subject Access and Correction Rights, Privacy Complaints Handling. Verify accuracy with internal compliance counsel before sending.

Cyber Threat Management

AMBER

6 controls mapped

0 green · **3.6 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.

AREAS IN PROGRESS

• CTRL-B13-Q14 — Does your organization conduct formal cyber risk assessments of technology environments at least annually?

• CTRL-B13-Q15 — Do you have continuous monitoring in place to identify vulnerabilities and misconfigurations across cloud environments?

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

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

• CTRL-B13-Q19 — Are security testing practices, such as static application security testing (SAST), dynamic application security testing (DAST), penetration testing, or equivalent testing methods, integrated into application development and change processes?

• CTRL-B13-Q20 — Do you have a centralized SIEM or equivalent capability providing real-time detection of security events across applicable technology environments?

ACCEPTABLE ANSWER IF ASKED

Hamilton Re Ltd. has implemented 0 controls in Cyber Threat Management with 6 additional controls under active development. 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.

Incident Response

RED

3 controls mapped

0 green · 2 amber · 1 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.

AREAS IN PROGRESS

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

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

ACKNOWLEDGED GAPS

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

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Hamilton Re Ltd. is actively building out Incident Response controls. Currently implementing 2 controls with documented project plans; scoping 1 additional control for remediation. We can share our implementation and remediation plans upon request. Verify accuracy with internal compliance counsel before sending.*

Business Continuity & Resilience

AMBER

8 controls mapped

0.7 green · 2.1 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

AREAS IN PROGRESS

• CTRL-B13-Q05 — Does your organization maintain a current, complete inventory of technology assets, including infrastructure, applications, data stores, endpoints, and cloud resources where applicable?

• CTRL-B13-Q06 — Are cloud assets (VMs, storage, databases, APIs) tagged and classified by business criticality and data sensitivity?

• CTRL-B13-Q07 — Does your cloud architecture follow documented, approved reference architectures aligned to security and resilience requirements?

• CTRL-B13-Q09 — Are security and compliance requirements (including B-13 controls) embedded into your SDLC / change management process?

• CTRL-B13-Q10 — Do you have documented Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical technology systems?

• CTRL-B13-Q11 — Has your organization conducted a full disaster recovery test for cloud workloads in the past 12 months?

• CTRL-B13-Q22 — Do you have a documented Business Continuity Plan covering failure scenarios for critical technology service providers and infrastructure dependencies (including cloud provider outages)?

> ACCEPTABLE ANSWER IF ASKED
>
> *Hamilton Re Ltd. has implemented 1 control in Business Continuity & Resilience with 7 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-EXIT-001. Evidence available on request: policy document, test report." 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.*

Operational Resilience

AMBER

7 controls mapped

0 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.

AREAS IN PROGRESS

• CTRL-B13-Q05 — Does your organization maintain a current, complete inventory of technology assets, including infrastructure, applications, data stores, endpoints, and cloud resources where applicable?

• CTRL-B13-Q06 — Are cloud assets (VMs, storage, databases, APIs) tagged and classified by business criticality and data sensitivity?

• CTRL-B13-Q07 — Does your cloud architecture follow documented, approved reference architectures aligned to security and resilience requirements?

• CTRL-B13-Q09 — Are security and compliance requirements (including B-13 controls) embedded into your SDLC / change management process?

• CTRL-B13-Q10 — Do you have documented Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical technology systems?

• CTRL-B13-Q11 — Has your organization conducted a full disaster recovery test for cloud workloads in the past 12 months?

• CTRL-B13-Q22 — Do you have a documented Business Continuity Plan covering failure scenarios for critical technology service providers and infrastructure dependencies (including cloud provider outages)?

ACCEPTABLE ANSWER IF ASKED

Hamilton Re Ltd. has implemented 0 controls in Operational Resilience with 7 additional controls under active development. 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.

Vendor / Third-Party Risk

GREEN

5 controls mapped

4.3 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-Q08 — Have you assessed and documented concentration risk from reliance on a single critical technology service provider?

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

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

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

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

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

ACCEPTABLE ANSWER IF ASKED

Hamilton Re Ltd. has documented and operating controls across Vendor / Third-Party Risk. For each question in this category, the typical response is: "Yes — CTRL-B13-Q08, CTRL-B13-Q23, CTRL-B13-Q24. Evidence available on request: report, attestation." Specific controls in this category: Have you assessed and documented concentration risk from reliance on a single critical technology service provider?, Do contracts with critical technology service providers include clauses covering data protection, audit rights, incident notification, and exit provisions?, Do you conduct formal risk assessments of critical technology service providers before onboarding and periodically thereafter?. Verify accuracy with internal compliance counsel before sending.

Audit & Compliance

AMBER

6 controls mapped

0.6 green · 1.2 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-B13-Q04 — Does your internal audit function independently assess technology and cyber risk controls at least annually?

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

• 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

AREAS IN PROGRESS

• CTRL-B13-Q02 — Is there a Board-approved technology and cyber risk policy reviewed at least annually?

• CTRL-B13-Q03 — Does your organization have a defined technology risk appetite statement that is actively used in decision-making?

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

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

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Hamilton Re Ltd. has implemented 2 controls in Audit & Compliance with 4 additional controls under active development. For green-status questions, the typical response is: "Yes — CTRL-B13-Q04, CTRL-GOV-001. Evidence available on request: policy document, report." 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.*

CROSS-REGULATION COVERAGE

Answer once, satisfy multiple regulators

Your responses in this assessment satisfy controls across 2 regulations simultaneously. RegLens scored a single set of responses against each applicable regulator's expectations independently.

Regulatory scope of this assessment

BERMUDA-PIPA	Personal Information Protection Act 2016 · 17 controls assessed
BMA-OCRM	Operational Cyber Risk Management Code of Conduct · 29 controls assessed

How responses map across regulations

CONTROL	TITLE	SATISFIES
CTRL-AWARE-001	Mandatory cybersecurity awareness training for all staff	BERMUDA-PIPA · BMA-OCRM
CTRL-B13-Q18	Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?	BERMUDA-PIPA · BMA-OCRM

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.

No Incident Response Plan or not applicable to cloud

RED

Affects: BMA-OCRM

Cloud incidents — misconfigurations, account compromises, CSP outages — follow different patterns than on-premises incidents. A generic or absent IRP leaves your teams improvising during a breach.

Indicative timeline: 8–12 weeks for plan development

Policy exists but was last reviewed over 12 months ago

AMBER

Affects: BMA-OCRM

An outdated policy may not reflect current cloud architecture, threat landscape, or regulatory updates (including the most recent regulatory amendments). Regulatory expectations generally require annual review as a minimum.

Indicative timeline: 3–5 weeks

Risk appetite exists but is rarely referenced in practice

AMBER

Affects: BMA-OCRM

A risk appetite statement that sits on a shelf provides no regulatory protection and no operational value. Supervisory reviews commonly examine how it influenced recent decisions.

Indicative timeline: 2–3 weeks

Do all staff (including contractors and third parties with access) complete formal cybersecurity awareness training on hire and at least annually, with completion tracked and gaps actively followed up?

AMBER

Affects: BMA-OCRM · BERMUDA-PIPA

Training is delivered and completion is tracked, but board and senior-management modules are lighter than staff modules or awareness is not tested (no phishing simulation, no scenario walkthrough).

Indicative timeline: 2–4 weeks

Does your organisation maintain a documented cybersecurity strategy that sets multi-year objectives, target maturity, investment priorities, and key initiatives — distinct from your cyber risk policy and reviewed at least annually?

AMBER

Affects: BMA-OCRM

A strategy more than 12 months old has not been challenged against the changing threat landscape, regulatory updates, or business changes.

Indicative timeline: 4–6 weeks

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