RegLens

BANK ONBOARDING READINESS PACKAGE

Rheinland Payments GmbH

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.

0	0	44	44
GREEN	AMBER	RED	TOTAL ASSESSED

POSTURE

RED

Regulations in scope

DORA	Digital Operational Resilience Act
GDPR	General Data Protection Regulation

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

RED

5 controls mapped

0 green · 0 amber · 2.5 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.

ACKNOWLEDGED GAPS

- 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-GOV-001 — Named senior officer accountable for technology and cyber risk
- CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff
- CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

> ACCEPTABLE ANSWER IF ASKED
>
> *Rheinland Payments GmbH has identified 5 gaps in Board & Risk Governance and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Information Security Program

RED

14 controls mapped

0 green · 0 amber · 3.0 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.

ACKNOWLEDGED GAPS

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

• 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-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-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**
>
> *Rheinland Payments GmbH has identified 14 gaps in Information Security Program and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Access Control & Identity

RED

2 controls mapped

0 green · 0 amber · 2 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.

ACKNOWLEDGED GAPS

• 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**
>
> *Rheinland Payments GmbH has identified 2 gaps in Access Control & Identity and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Data Protection & Encryption

RED

20 controls mapped

0 green · 0 amber · 5.3 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.

ACKNOWLEDGED GAPS

• 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-005 — Personal Information Retention and Disposal

• CTRL-PRIV-006 — Privacy Policy Transparency

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

• CTRL-PRIV-008 — Privacy Complaints Handling

• CTRL-PRIV-009 — Personal Information Breach Response

• CTRL-PRIV-010 — Privacy Impact Assessment for IT Projects

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

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

• CTRL-PRIV-013 — Automated Individual Decision-Making (GDPR Article 22)

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

• CTRL-PRIV-016 — Personal Information Accuracy

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Rheinland Payments GmbH has identified 20 gaps in Data Protection & Encryption and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Privacy Program

RED

15 controls mapped

0 green · 0 amber · 10.5 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.

ACKNOWLEDGED GAPS

• 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-005 — Personal Information Retention and Disposal
• CTRL-PRIV-006 — Privacy Policy Transparency
• CTRL-PRIV-007 — Data Subject Access and Correction Rights
• CTRL-PRIV-008 — Privacy Complaints Handling
• CTRL-PRIV-009 — Personal Information Breach Response
• CTRL-PRIV-010 — Privacy Impact Assessment for IT Projects
• CTRL-PRIV-011 — Express Consent for Sensitive Personal Information and Minors
• CTRL-PRIV-012 — Cross-Border Personal Information Transfer Assessment
• CTRL-PRIV-013 — Automated Individual Decision-Making (GDPR Article 22)
• CTRL-PRIV-015 — Data Portability and Right to De-Indexing
• CTRL-PRIV-016 — Personal Information Accuracy

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Rheinland Payments GmbH has identified 15 gaps in Privacy Program and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Cyber Threat Management

RED

5 controls mapped

0 green · 0 amber · 3 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.

ACKNOWLEDGED GAPS

• 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
>
> *Rheinland Payments GmbH has identified 5 gaps in Cyber Threat Management and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Incident Response

RED

6 controls mapped

0 green · 0 amber · 4.4 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.

ACKNOWLEDGED GAPS

• CTRL-DORA-TLPT-001 — Threat-led penetration testing programme (TLPT)

• CTRL-DORA-INFOSHARE-001 — Cyber threat information sharing arrangements

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

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

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

• CTRL-DORA-IRC-001 — ICT-related incident classification process

> ACCEPTABLE ANSWER IF ASKED
>
> *Rheinland Payments GmbH has identified 6 gaps in Incident Response and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Business Continuity & Resilience

RED

7 controls mapped

0 green · 0 amber · 2.5 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.

ACKNOWLEDGED GAPS

• 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-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-DORA-TLPT-001 — Threat-led penetration testing programme (TLPT)

• CTRL-DORA-INFOSHARE-001 — Cyber threat information sharing arrangements

• CTRL-EXIT-001 — Documented CSP exit strategy

> ACCEPTABLE ANSWER IF ASKED
>
> *Rheinland Payments GmbH has identified 7 gaps in Business Continuity & Resilience and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Operational Resilience

RED

6 controls mapped

0 green · 0 amber · 3 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.

ACKNOWLEDGED GAPS

• 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-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-DORA-TLPT-001 — Threat-led penetration testing programme (TLPT)

• CTRL-DORA-INFOSHARE-001 — Cyber threat information sharing arrangements

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Rheinland Payments GmbH has identified 6 gaps in Operational Resilience and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Vendor / Third-Party Risk

RED

7 controls mapped

0 green · **0 amber** · **6.3 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.

ACKNOWLEDGED GAPS

• CTRL-B13-Q08 — Have you assessed and documented concentration risk from reliance on a single critical technology service provider?

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

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

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

• CTRL-DORA-TPR-001 — Register of ICT third-party arrangements

• CTRL-DORA-SUBC-001 — Sub-contracting controls for critical ICT services

• CTRL-EXIT-001 — Documented CSP exit strategy

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Rheinland Payments GmbH has identified 7 gaps in Vendor / Third-Party Risk and is scoping remediation. A documented remediation plan is in development and can be shared on request. Verify accuracy with internal compliance counsel before sending.*

Audit & Compliance

RED

5 controls mapped

0 green · 0 amber · 1.5 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.

ACKNOWLEDGED GAPS

- 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-GOV-001 — Named senior officer accountable for technology and cyber risk
- CTRL-AWARE-001 — Mandatory cybersecurity awareness training for all staff
- CTRL-STRAT-001 — Documented cybersecurity strategy aligned to business objectives

> **ACCEPTABLE ANSWER IF ASKED**
>
> *Rheinland Payments GmbH has identified 5 gaps in Audit & Compliance and is scoping remediation. A documented remediation plan is in development and can be shared 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

DORA	Digital Operational Resilience Act · 28 controls assessed
GDPR	General Data Protection Regulation · 20 controls assessed

How responses map across regulations

CONTROL	TITLE	SATISFIES
CTRL-AWARE-001	Mandatory cybersecurity awareness training for all staff	DORA · GDPR
CTRL-B13-Q18	Is data encrypted at rest and in transit across applicable technology environments using approved encryption standards?	DORA · GDPR
CTRL-IAM-001	MFA enforced for all privileged access	DORA · GDPR
CTRL-IR-REG-001	Documented procedure for notifying regulators of material cyber incidents	DORA · GDPR

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 formal Board-approved policy exists

RED

Affects: DORA

A Board-approved policy is the foundation of your entire regulatory compliance posture. Without it, all other controls lack governance backing. Regulatory expectations generally require this as a baseline.

Indicative timeline: 6–10 weeks (includes drafting, legal review, Board approval cycle)

No defined technology risk appetite statement

RED

Affects: DORA

Without a risk appetite statement, your institution has no defensible basis for technology risk decisions. The applicable regulation generally expects risk appetite to be defined and actively used — not just documented… (see full assessment for complete rationale)

Indicative timeline: 6–8 weeks

Is a named senior officer formally accountable for technology and cyber risk, with documented authority, board/committee reporting, and a clear escalation path?

RED

Affects: DORA

Without clear accountability for cyber risk, no one owns the outcome when an incident occurs. Regulators expect a named individual at the senior management or board level with explicit responsibility, authority, and… (see full assessment for complete rationale)

Indicative timeline: 2–4 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?

RED

Affects: DORA · GDPR

Controllers and processors subject to the GDPR cannot satisfy Article 32(4)'s requirement to take steps to ensure that any natural person acting under the authority of the controller or processor who has… (see full assessment for complete rationale)

Indicative timeline: 6–10 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?

RED

Affects: DORA

A cyber risk policy specifies what the institution will do; a strategy specifies where it is going. Without a forward-looking strategy, cyber investment is reactive — patching known gaps, responding to incidents… (see full assessment for complete rationale)

Indicative timeline: 8–12 weeks

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