

GOVERNANCE DOCS

EU Digital Operational Resilience Act

Gap Assessment Report

EU Digital Operational Resilience Act (Regulation (EU) 2022/2554)

Baltic Payments Institution (sample)

ICT risk management, incident reporting, resilience testing and third-party risk for the payment services business.

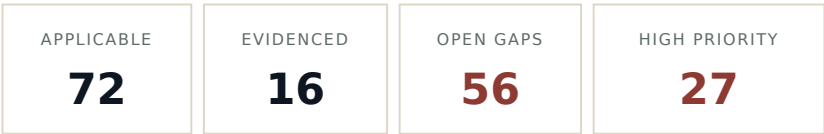
ASSESSED	25 September 2026
EDITION	Regulation (EU) 2022/2554, applying since 17 January 2025
IN SCOPE	78 requirements, 72 applicable
PROFILE	Banking and financial services · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

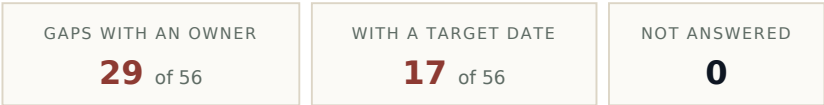
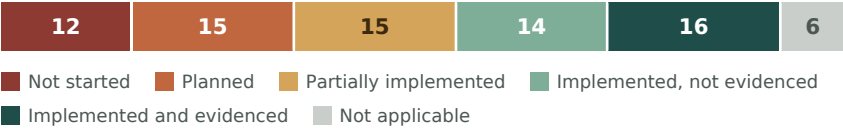
- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Baltic Payments Institution (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Baltic Payments Institution (sample) stands against DORA



STATUS OF EVERY REQUIREMENT



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 52.4% against DORA across 72 applicable controls. 16 of them are implemented and evidenced.
- Most open gaps: Third-party risk: principles, with 7 at 39%. Strongest area: Third-party risk: contracts at 85%.
- 14 controls are operating but not evidenced. Collecting their records alone lifts the score to 57.3% (+4.9 points), the cheapest gain available.
- 27 gaps are high priority (not started or only planned); 4 of them are in Scope and proportionality.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 4 high-priority gaps in Scope and proportionality	HR Manager	DORA Scope & Applicability Assessment Procedure
2	MEDIUM	Adopt and tailor the DORA Scope & Applicability Assessment Procedure, which closes 3 open gaps	To assign	DORA Scope & Applicability Assessment Procedure
3	LOW	Evidence the 14 controls that already operate (+4.9 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

Your readiness score is 52.4%, and you should prioritize formalizing scope and baseline protection controls across the organization.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment shows an overall readiness score of 52.4%, placing us at level 2 of 4, defined as Developing. Our primary operational exposure stems from 56 open gaps, including 27 high-priority items in protection, incident management, and third-party risk. Only 17 gaps have assigned target dates today. To protect operations and address audit findings, management requires board approval for the risk management strategy, clear accountability across business units, and resources to implement planned security controls.

WHERE YOU STAND

The self-assessment places the organization at a readiness score of 52.4%, which corresponds to the Developing level, or level 2 of 4. This status indicates that the programme is under way, with material gaps an auditor would find. Out of 72 applicable requirements, there are 56 open gaps, and 27 of those are high priority. Furthermore, only 29 gaps currently have an assigned owner, and only 17 have a recorded target date. While 16 requirements are implemented and evidenced, 12 requirements have not been started.

WHAT IT MEANS FOR THE ORGANIZATION

Operational capabilities exist in pockets, but formal governance and evidence are inconsistent across operational areas. While Third-party risk: contracts scores 85% and Response and recovery reaches 75%, core baseline areas remain underdeveloped. Protection and prevention stands at 29.2%, Scope and proportionality is at 33.3%, and Threat-led penetration testing sits at 25%. Evidencing what already runs would lift the score to 57.3%, but substantial risk remains unaddressed because 15 requirements remain planned and 15 are only partially implemented without complete operating procedures.

WHERE TO FOCUS FIRST

You should focus first on defining operational scope and closing high-priority gaps in technical safeguards and incident procedures. Clarifying entity scope and microenterprise status establishes proper baseline rules. Next, you must address Protection and prevention by establishing formal controls for network segmentation, access, and change management. Finally, assign formal owners and completion dates to all 56 open gaps. Progressing planned controls into live operations can raise the score to 83.3%, while completing partially implemented items brings the score to 67.7%.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Define operational scope and applicability boundaries SP.1 Entity type in scope · SP.3 Microenterprise determination · SP.2 Exclusions considered	Operating without formal entity scoping risks misapplying legal requirements and misallocating security resources. Establishing clear applicability ensures the organization implements the exact controls mandated for its operational profile.	Review the organizational profile against the DORA Scope & Applicability Assessment Procedure.	DORA Scope & Applicability Assessment Procedure DORA Toolkit - 100+ Comprehensive Templates	30 DAYS
2 Establish baseline protection and prevention controls 9.4b Network and segmentation · 9.4e Change and patch management · 9.4c Access management	Protection and prevention has an overall score of 29.2% with 6 open gaps. Weak network segmentation and uncontrolled changes leave systems vulnerable to preventable technical disruptions.	Draft the Network Security & Segmentation Standard to define boundary defenses across internal environments.	Network Security & Segmentation Standard DORA Toolkit - 100+ Comprehensive Templates	60 DAYS
3 Standardize incident classification and reporting mechanics 17.3 Early warning and roles · 18.1b Major incident determination · 19.weekend Deadline mechanics	Incident management and classification scored 45.8%, with critical gaps in early warning and major incident determination. Delayed incident identification prevents timely operational recovery and regulatory escalation.	Implement the Major Incident Determination Decision Tree & Threshold Guide for operational response teams.	Major Incident Determination Decision Tree & Threshold Guide DORA Toolkit - 100+ Comprehensive Templates	60 DAYS
4 Formalize third-party risk principles and diligence 28.3b Register reported to the authority · 28.4 Pre-contractual due diligence · 28.8 Exit strategies	Third-party risk: principles sits at 39.3% with 7 open gaps. Failing to execute pre-contractual due diligence or maintain register reporting exposes the firm to severe vendor failures.	Initiate pre-contractual due diligence assessments for all critical third-party service providers.	Pre-Contractual Due Diligence Procedure DORA Toolkit - 100+ Comprehensive Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS - Complete the DORA Scope & Applicability Assessment Procedure to define entity boundaries. - Assign named owners and target completion dates for all 56 open gaps. - Gather and log existing operational evidence to lift the baseline score to 57.3%.	DAYS 31 TO 60 - Draft and publish the Network Security & Segmentation Standard across technical environments. - Implement the Major Incident Determination Decision Tree & Threshold Guide for incident triage. - Adopt procedures for patch management, change management, and access controls.	DAYS 61 TO 90 - Roll out the Pre-Contractual Due Diligence Procedure for all critical vendor relationships. - Establish the register reporting process and formal exit strategies for third-party providers. - Document the annual testing programme and action remediation tracker for system resilience.
--	---	---

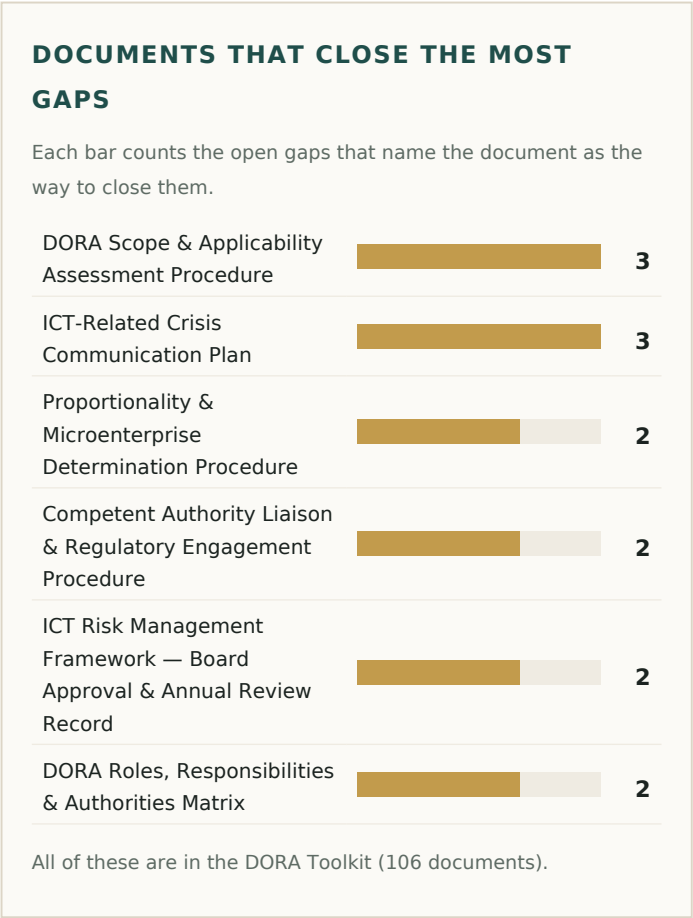
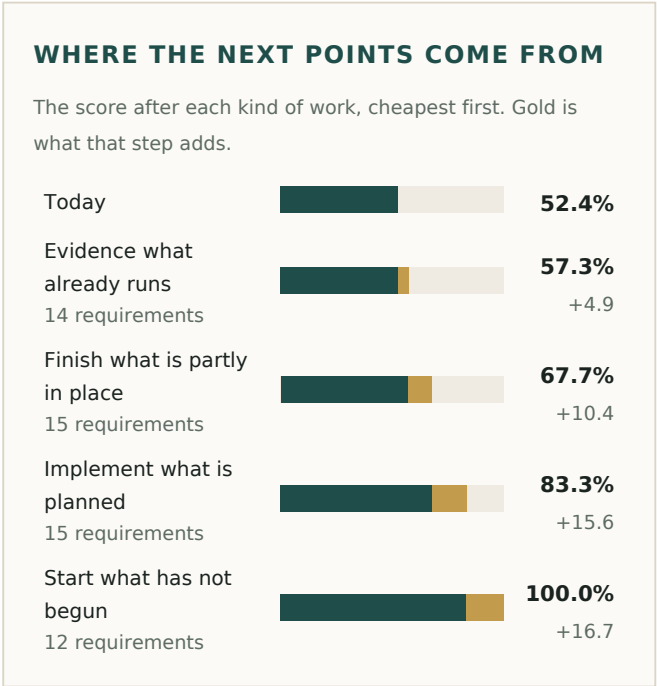
Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and proportionality	2 2 2	33%	4 0 2
Governance and organisation	2 1 2	60%	2 1 0
ICT risk management framework	2 1 3 1	71%	2 0 1
Protection and prevention	2 2 1 1 1	29%	4 1 1
Detection	2 1	67%	0 2 0
Response and recovery	1 2 2 1	75%	1 0 2
Learning and communication	2 1 1	33%	2 1 0
Incident management and classification	2 2 1 1	46%	2 2 1
Incident reporting	2 2 1 2	61%	2 2 1
Resilience testing	1 3 1	50%	1 3 0
Threat-led penetration testing	2 2 1	25%	4 0 1
Third-party risk: principles	3 1 3 1	39%	3 1 3
Third-party risk: contracts	1 1 3	85%	0 1 1
Oversight and information sharing	1 1 1 1	75%	0 1 1

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

Where the next points come from



Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 12

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
SP.1	Entity type in scope	Scope and proportionality	To assign	DORA Scope & Applicability Assessment Procedure
SP.3	Microenterprise determination	Scope and proportionality	To assign	Proportionality & Microenterprise Determination Procedure
9.4b	Network and segmentation	Protection and prevention	To assign	Network Security & Segmentation Standard
9.4e	Change and patch management	Protection and prevention	HR Manager 26 Nov 2026	ICT Change Management Procedure · Patch & Vulnerability Management Procedure
17.3	Early warning and roles	Incident management and classification	Risk Manager 29 Oct 2026	ICT-Related Incident Management Procedure
18.1b	Major incident determination	Incident management and classification	IT Manager 7 Jan 2027	Major Incident Determination Decision Tree & Threshold Guide
24.5	Remediation of findings	Resilience testing	Compliance Lead	Test Inventory, Schedule & Remediation Tracker · Remediation & Action Tracker
26.1	TLPT applicability	Threat-led penetration testing	To assign	TLPT Policy & Scoping Specification
26.4	Threat intelligence for TLPT	Threat-led penetration testing	Compliance Lead 12 Nov 2026	TLPT Threat Intelligence Requirements Procedure
28.3b	Register reported to the authority	Third-party risk: principles	To assign	Register of Information — Completion & Maintenance Procedure · Competent Authority Liaison & Regulatory Engagement Procedure
28.4	Pre-contractual due diligence	Third-party risk: principles	To assign	Pre-Contractual Due Diligence Procedure · ICT Service Criticality Assessment Procedure
28.8	Exit strategies	Third-party risk: principles	Compliance Lead	Exit Strategy & Substitutability Policy · Exit Plan Template — Critical ICT Service

HIGH **Planned · 15**

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SP.2	Exclusions considered	Scope and proportionality	HR Manager	DORA Scope & Applicability Assessment Procedure
SP.4	Simplified framework eligibility	Scope and proportionality	Compliance Lead 7 Jan 2027	Simplified ICT Risk Management Framework (Article 16) · Proportionality & Microenterprise Determination Procedure
5.2a	Approving the framework and strategy	Governance and organisation	Operations Manager 12 Nov 2026	ICT Risk Management Framework — Board Approval & Annual Review Record · Digital Operational Resilience Strategy
5.2b	Roles and responsibilities	Governance and organisation	IT Manager	DORA Roles, Responsibilities & Authorities Matrix
6.8	Risk assessment methodology	ICT risk management framework	To assign	ICT Risk Assessment Methodology & Procedure · ICT Risk Register
8.1	Identification of ICT assets	ICT risk management framework	HR Manager 29 Oct 2026	ICT Asset Identification & Classification Procedure · ICT Asset Inventory & Criticality Register
9.4c	Access management	Protection and prevention	IT Manager	Identity & Access Management Policy
9.4d	Cryptography and key management	Protection and prevention	Risk Manager 10 Dec 2026	Cryptography & Key Management Policy
12.1	Backup policies and procedures	Response and recovery	To assign	Backup, Restoration & Recovery Procedure
13.1	Post-incident learning	Learning and communication	HR Manager 4 Feb 2027	Learning & Evolving Procedure · Root Cause Analysis Procedure
14.3	Communication to staff and stakeholders	Learning and communication	Risk Manager 24 Dec 2026	ICT-Related Crisis Communication Plan · DORA Roles, Responsibilities & Authorities Matrix
19.weekend	Deadline mechanics	Incident reporting	To assign	Incident Reporting Timeline & Deadline Tracker
23	Payment-related incidents	Incident reporting	HR Manager 29 Oct 2026	Payment-Related Operational or Security Incident Procedure
26.6	Red team and control team	Threat-led penetration testing	To assign	TLPT Red Team & Control Team Engagement Procedure

27	Tester requirements	Threat-led penetration testing	IT Manager 26 Nov 2026	Tester Selection & Independence Criteria · TLPT Closure, Attestation & Remediation Procedure
----	---------------------	--------------------------------	---------------------------	--

MEDIUM Partially implemented · 15

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
5.2c	Budget and resources	Governance and organisation	Operations Manager	Management Body Responsibilities & Accountability Statement · DORA Compliance Policy Statement
9.4a	Information security policy	Protection and prevention	Operations Manager	ICT Protection & Prevention Policy · DORA Compliance Policy Statement
10.2	Multiple layers of control	Detection	To assign	ICT Detection & Anomalous Activity Policy · Logging & Monitoring Standard
10.3	Resources for monitoring	Detection	Compliance Lead 4 Feb 2027	Logging & Monitoring Standard
14.1	Crisis communication plans	Learning and communication	To assign	ICT-Related Crisis Communication Plan
18.1	Classification criteria	Incident management and classification	IT Manager	Incident Classification Methodology · Incident Classification Worksheet
17.log	Incident register	Incident management and classification	IT Manager 24 Dec 2026	ICT Incident Register · ICT Incident Log
19.1b	Intermediate report	Incident reporting	To assign	Intermediate Report Template
19.track	Reporting tracker	Incident reporting	Compliance Lead	Major Incident Reporting Tracker
24.1	Testing programme	Resilience testing	Compliance Lead	Digital Operational Resilience Testing Policy · Annual Testing Programme
24.2	Risk-based test planning	Resilience testing	Risk Manager	Test Planning, Scoping & Prioritisation Procedure
25.1	Range of tests	Resilience testing	Risk Manager 26 Nov 2026	Testing of ICT Tools & Systems Standard · Vulnerability Assessment & Scanning Procedure +1 more
28.1	Third-party risk strategy	Third-party risk: principles	Risk Manager 26 Nov 2026	Strategy on ICT Third-Party Risk · ICT Third-Party Risk Management Policy
30.3b	Audit and access rights	Third-party risk: contracts	Compliance Lead 26 Nov 2026	Audit & Access Rights Procedure
31	Critical provider oversight interface	Oversight and information sharing	IT Manager	CTPP Oversight Framework Interface Procedure

LOW Implemented, not evidenced · 14

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SP.5	Group application	Scope and proportionality	To assign	DORA Scope & Applicability Assessment Procedure · DORA Compliance Framework Manual
SP.6	Competent authority	Scope and proportionality	To assign	Competent Authority Liaison & Regulatory Engagement Procedure
6.5	Annual and event-driven review	ICT risk management framework	To assign	ICT Risk Management Framework — Board Approval & Annual Review Record
9.1	Protection and prevention policy	Protection and prevention	To assign	ICT Protection & Prevention Policy
11.1	Response and recovery plans	Response and recovery	To assign	ICT Business Continuity Policy · ICT Response & Recovery Plans
11.6	Crisis management function	Response and recovery	To assign	ICT-Related Crisis Communication Plan · ICT Incident Log
18.2	Significant cyber threats	Incident management and classification	To assign	Significant Cyber Threat Assessment & Voluntary Notification Procedure
19.1c	Final report	Incident reporting	To assign	Final Report Template · Root Cause Analysis Procedure
26.2	TLPT frequency and scope	Threat-led penetration testing	To assign	TLPT Policy & Scoping Specification
28.2	Policy on services supporting critical functions	Third-party risk: principles	To assign	Policy on ICT Services Supporting Critical or Important Functions
28.3a	Register of information maintained	Third-party risk: principles	To assign	Register of Information (multi-sheet, ITS-structured) · Register of Information — Completion & Maintenance Procedure
29.1	Concentration risk	Third-party risk: principles	To assign	ICT Concentration Risk Assessment Procedure
30.3d	Termination rights and triggers	Third-party risk: contracts	To assign	Contract Termination Rights & Triggers Procedure
45.1	Information sharing arrangements	Oversight and information sharing	To assign	Cyber Threat Information & Intelligence Sharing Policy · Information Sharing Arrangement Participation Procedure

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com