Corrected edition, 11 November 2026. ART-117 editorial and source corrections; methodology and validation status unchanged.

ArtiProof and DORA

The Knowledge Behind Digital Operational Resilience

The system is back.
Can the service resume safely?

Application Whitepaper 1.1.1 EN

11 November 2026

ArtiProof publication series | KopKen VZW

Informative publication. Research-ready; not yet broadly independently validated. The first independent replication remains pending.

AI-assisted drafting and editorial preparation. No independent human peer review is claimed. Publication and method version numbers are separate.

Executive summary

The applications have restarted. The data is available. The recovery plan can be retrieved. But does the institution still possess the knowledge needed to resume the service safely?

This paper proposes a focused ArtiProof application within the EU Digital Operational Resilience Act (DORA): examine the knowledge supporting consequential recovery decisions, supplier transitions and AI-assisted operational work.

DORA has applied since **17 January 2025** to financial entities within its scope. It addresses ICT risk management, incidents, testing and third-party risk, among other subjects. It already includes people, learning, training and capability; ArtiProof is not filling a human dimension missing from the legislation. [1–2]

The proposed contribution is a bounded knowledge-fitness review within existing resilience work. It connects sources, practical understanding and system-generated material to the operational decision that depends on them. A review can confirm a well-supported assessment, qualify it, challenge it or find insufficient evidence. It need not produce another defect to be useful.

The profile remains a proposal for testing. It does not establish DORA compliance, replace regulatory testing or reporting, or guarantee recovery. Its incremental value must be compared with competent DORA implementation and ordinary competent peer review.

1. The system is back. Can the service resume?

Consider a hypothetical payment service recovering from an outage. The platform restarts, but a queue of transactions remains. Some messages may have reached another party before the interruption; others may not have left the institution.

An experienced specialist normally resolves such cases by combining system records, reconciliation results and knowledge of a narrow exception. That specialist is unavailable.

An AI assistant recommends replaying the queue. Its explanation is fluent, but it partly relies on a superseded recovery instruction. The team now needs more than confirmation that the application is running. It must establish which evidence is authoritative, which transaction states remain uncertain and who can authorise the next action.

This scenario illustrates the proposed knowledge question; it is not an incident report, an observed failure or an instruction for a real payments platform. Safe action in an actual service depends on its specific design, records, contracts and authorised recovery procedures.

An ArtiProof-guided review would ask whether the institution can support the relevant reliance decision. Restoring infrastructure and demonstrating the ability to interpret the restored state are related but different observations.

The correct result may be to resume, to operate under a defined restriction, to obtain further verification or to withhold an action. The review should examine the basis for that decision rather than reward speed or caution in isolation.

2. An application inside DORA—not another compliance system

DORA is a binding EU regulation, not a voluntary management model. Its obligations remain the legal baseline. ArtiProof contributes only the optional review practices explicitly identified as proposals here. [1]

The following selective crosswalk concerns the general framework. Entity scope and exemptions under Article 2, proportionality under Article 4 and the simplified framework under Article 16 must be considered before applying it. Articles 5–15 do not apply unchanged to entities covered by Article 16. Relevant secondary legislation and supervisory material must also be checked. [1–2]

Selected legal anchor	Subject already addressed	Proposed ArtiProof question
Articles 5(2), 5(4)	Responsibility and management-body knowledge	Can decision-makers understand and challenge the assumptions behind the selected decision?
Article 8(1), 8(5)	Identification and documentation of functions, assets and dependencies	Which knowledge is needed to interpret and operate the mapped capability?
Articles 11(3), 11(6), 12(6)–(7)	Recovery plans, tests, objectives and reconciliation	Can the team interpret the restored state and support its resumption decision?
Article 13(2), 13(6)	Incident learning and training	Does the evidence demonstrate usable capability, rather than attendance or document completion alone?
Articles 17–19	Incident management, classification and reporting	Can confirmed observations be distinguished from hypotheses and generated summaries?
Articles 24–25	Resilience testing and remediation	What does the existing exercise demonstrate about the selected knowledge dependency?
Articles 28(8), 30(3)(f)	Exit and transition arrangements for relevant services	Will the receiving party retain the understanding needed to use transferred information?

The middle column summarises selected regulatory subjects; the right-hand column contains proposed review questions, not additional legal duties. The crosswalk is not a complete control catalogue or a legal opinion. [1]

3. Follow the knowledge behind the decision

ArtiProof's three knowledge categories describe roles in a selected context. **Source Knowledge** includes an approved instruction, an authoritative record or a specification. **Craft Knowledge** includes practical understanding and professional judgement. **Generated Knowledge** includes system-produced summaries, classifications or recommendations. [5]

In the payment example, a runbook may be authentic yet superseded. A specialist may understand an exception yet rely on an untested assumption. A generated summary may be helpful while omitting a decisive limitation.

The labels do not decide what is true. A generated report can become a source for later work without becoming authoritative, and human expertise does not automatically settle a disputed fact.

The proposed review makes the relationships explicit: the operational capability, the knowledge it requires, the people and systems supplying it, the evidence supporting reliance and the accountable decision.

This relationship can be represented in existing records. It does not require a new enterprise-wide knowledge graph. A candidate Knowledge Matrix or one-page view may help communicate it, but these interfaces remain experimental and must not become another mandatory compliance inventory.

4. Five properties, no compensating score

Integrity asks whether the necessary knowledge is sufficiently complete and protected against inappropriate change or degradation. A technically intact procedure can still omit an important condition.

Provenance asks where the evidence and conclusions came from. A primary transaction record, a human interpretation and a generated summary should not be silently treated as equivalent.

Authority asks what provides a sufficient basis for reliance in this use. The most recent or most confident recommendation is not automatically the approved one.

Understandability asks whether responsible people can interpret the evidence, recognise material uncertainty and appropriately challenge the proposed action.

Resilience asks whether the knowledge-dependent capability survives, or can be recovered, when the usual combination of people, systems and suppliers changes.

These properties remain separately visible. Strong documentation does not cancel a material inability to interpret it. Strong expertise does not erase a serious evidence gap. The profile does not generate an overall DORA-compliance score. [5]

5. Reuse the resilience evidence

Start with the institution's existing runbooks, business-impact analysis, incident records, change history, training evidence, contracts, provider information and exercise results. Before reuse, check the scope, configuration, age, ownership and reliability of each item.

DORA's register of information concerns ICT third-party contractual arrangements. The proposed knowledge view should reference relevant records rather than replace or duplicate the register. The register's standard templates are provided by Implementing Regulation (EU) 2024/2956. [1, 4, 7]

A useful connection might show that the service's recovery decision depends on a particular reconciliation interpretation, who can apply it, which records support it and what an exercise actually demonstrated.

The assessment should distinguish "document exists" from "document supports this conclusion". A past test of a different configuration may be informative without establishing current recovery capability.

Minimum Sufficient Evidence controls the additional ArtiProof review burden. It does not waive statutory recordkeeping, retention, reporting, documentation or testing. Where existing evidence already supports a defensible conclusion, reuse it; do not add administration merely to demonstrate activity.

6. A proposed Knowledge Recovery Challenge

The **Knowledge Recovery Challenge** is a candidate exercise that can be embedded within an appropriately authorised resilience test. It is not a DORA-prescribed test and should not be performed by disrupting a live service merely to demonstrate the method.

First define the capability and the decision being examined. "Recover the service" is too broad unless the expected service level, timing, quality conditions, permitted resources and decision authority are clear.

Next identify a realistic knowledge constraint. The usual expert might be unavailable; the primary knowledge repository might not be reachable; a supplier's support channel might be absent; or an assistant's recommendation might have to be treated as untrusted.

Give a suitably qualified team a synthetic or sanitised scenario with the approved evidence available under those conditions. Observe whether it can locate the appropriate sources, identify an obsolete instruction, explain uncertainty and choose an authorised next action.

Record two things separately: the quality of the decision and achievement of the operational objective. A safe stop may demonstrate good judgement while also revealing that the required service recovery was not achieved. A fast restart may meet a timing objective while failing a material verification condition.

Absence of a demonstration does not automatically prove absence of capability. The appropriate conclusion may be that capability was **not demonstrated under the stated conditions**. Explain the limit rather than convert missing evidence into certainty.

The exercise supplements existing work. It does not replace required technical testing, incident reporting or threat-led penetration testing where applicable. [1–2]

7. Supplier exit must preserve usable understanding

For services supporting critical or important functions, DORA addresses exit strategies and transitions. Delegated Regulation (EU) 2024/1773, Article 10, requires documented exit plans within its scope to be reviewed and tested and to reflect feasible scenarios, reasonable assumptions and schedules compatible with the contractual arrangements. [1, 3]

ArtiProof's proposed question is narrower: **what must the receiving organisation or provider understand to make the transition operationally meaningful?**

A data export might succeed while an important field remains ambiguous. A replacement rule might have the same name but a different practical effect. A handover might transfer instructions without transferring the ability to recognise when an exception applies.

A bounded knowledge-transfer exercise could ask the receiving team to interpret a relevant case using the transferred material, identify uncertainties and demonstrate the required verification or escalation. The result could confirm the existing exit preparation or reveal a specific limitation.

This does not imply that all proprietary knowledge must be disclosed, that every service must be brought in-house or that every supplier must be replaceable instantly. Access and transfer arrangements remain subject to applicable legal, contractual, confidentiality and security constraints. The financial entity's responsibilities are not transferred away merely by using an ICT third-party service. [1]

8. When the AI works but reliance must stop

A system need not be offline to become unsuitable for a particular decision. In the hypothetical recovery example, the assistant remains available but relies on an obsolete instruction.

The proposed exercise should test whether the team can withdraw reliance while preserving the ability to assess the situation. An appropriate route may involve original records, another qualified person, a different tool or a pre-authorised restricted service. Universal manual independence is not the objective.

Generated incident summaries should distinguish confirmed observations, interpretations and unanswered questions. Unsupported inferences should not silently become accepted findings as summaries are copied into subsequent documents.

For reconstruction, prefer observable records of sources, versions, relevant inputs, outputs and transformations. A generated explanation of a model's answer is not automatically evidence of how that answer was produced. This paper does not infer a general DORA obligation to reconstruct model internals or training data.

Withdrawing reliance is an operational action, not automatically a regulatory incident classification. Classification and reporting remain separate decisions under the applicable criteria and deadlines; a knowledge review must not delay them. [1, 4]

9. From a finding to demonstrated learning

Suppose an exercise shows that only the usual specialist can resolve a relevant exception. "Improve documentation" may be a proposed action, but it does not yet explain the problem.

Separate the **finding** from the **causal hypothesis**. Was the instruction incomplete? Was the correct evidence inaccessible? Did the terminology cause confusion? Had the replacement team never practised the task?

Choose an action that addresses the supported cause. Then establish closure through evidence relevant to the capability: for example, a bounded repeat exercise in which another appropriately qualified team uses the revised material and reaches the required decision.

A document update demonstrates that text changed. A relevant repeat exercise may demonstrate more, but only under the tested conditions. Neither warrants a general claim that the institution is resilient or that ArtiProof is validated.

The proposed review can also confirm that an existing lesson has already become usable capability. That is a legitimate finding when supported by positive evidence and meaningful challenge.

10. A defensible conclusion has a visible boundary

Record what was assessed, for which use, in which configuration and period, by whom and with which evidence. Disclose relevant competence, prior involvement, conflicts, evidence restrictions and the actual degree of reviewer separation.

Where DORA requires independent testing and conflict safeguards, those legal conditions still apply; an ArtiProof disclosure is not a substitute for meeting them, including Article 24(4) where applicable. [1]

A reviewer can **confirm**, **qualify**, **challenge** or record **insufficient evidence**. These are bounded knowledge-fitness outcomes, not regulatory grades. Confirmation requires positive support; neither agreement nor the absence of a new defect is sufficient.

Different evidence gaps should remain distinguishable. A record never created differs from one unavailable to the reviewer, withheld or no longer retained. Unknown reasons should remain unknown. A traceable chain establishes something about evidence handling; it does not, on its own, establish the underlying claim.

Specify conditions that would require reconsideration, such as a material source change, supplier transition, different system configuration or loss of a knowledge holder. The resulting conclusion is time-bounded rather than a permanent assurance badge.

Knowledge maps and exercise records may expose sensitive dependencies. Use synthetic or sanitised public examples and controlled access for implementation evidence. Do not publish operational weaknesses or personal information merely to make a methodology demonstration vivid.

11. The comparator must be competent

A credible study must ask whether ArtiProof-guided review adds value to competent existing DORA work and ordinary peer review—not whether it outperforms the absence of review.

Where feasible, compare competent self-assessment, ordinary competent peer review and ArtiProof-guided peer review using matched cases, expertise and evidence access. Control or report review-time differences. Include sound cases, concealed defects and insufficient-evidence cases rather than only failures waiting to be found.

Record warranted confirmation, false confirmation, justified qualification or challenge, correct withholding of judgement, evidence-to-conclusion traceability, clarification work, initial disagreement and gross additional effort. Keep estimated savings separate from observed benefits.

A review may be useful without changing the decision. But if ordinary review reaches equally well-supported conclusions at equal or lower burden, there is no demonstrated ArtiProof-specific advantage in that setting. Preserve that result.

The same applies to overlap with established security, continuity and knowledge-management practices. Existing controls may already answer the question. The profile should reuse that work, not presume a gap.

No empirical outcomes are claimed in this paper. The accompanying recovery protocol is prepared for controlled investigation; no live test, recruitment or independent replication is represented as completed.

12. Keep the interfaces distinct

The ISO 30401 companion addresses a knowledge-management environment. This DORA companion addresses a financial-sector regulatory application. Both use the same ArtiProof knowledge questions without merging their external frameworks or modifying the core.

An institution need not adopt ISO 30401 to consider the DORA application. It need not use ArtiProof to implement DORA. Legal obligations, professional expertise and accountable organisational decisions remain in their existing places.

The profile earns its place only where it improves the basis for reliance enough to justify the additional work.

Conclusion

In the payment example, restarting the platform did not establish what could safely happen next. That required interpretable records, practical understanding, clear authority and an alternative to the unavailable expert or unreliable assistant. ArtiProof proposes a focused review of that knowledge within existing resilience work—not a new compliance system.

Restoring systems matters. So does restoring the ability to use them safely. The proposed ArtiProof application examines the knowledge behind that capability.

Publication boundary and references

This independent ArtiProof publication is informative, not regulatory guidance or a legal opinion. It provides a selective mapping, not a complete legal baseline or a conformity assessment. There is no claim of supervisory endorsement, certification, guaranteed continuity or proven integration benefit.

ArtiProof remains research-ready, not yet broadly independently validated; its first independent replication remains pending. The Knowledge Recovery Challenge and supporting interfaces are candidate practices. Publication version 1.1.1 does not create a new normative method version.

[1] European Parliament and Council. *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. In particular Articles 2, 4–5, 8, 11–13, 16–19, 24–25, 28 and 30. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[2] EIOPA. *Digital Operational Resilience Act (DORA)*. Official overview and catalogue of implementing instruments. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[3] European Commission. *Delegated Regulation (EU) 2024/1773*, Article 10, exit from and termination of contractual arrangements within the policy's scope. https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/eng

[4] FSMA. *The Digital Operational Resilience Act*. Official legislative index, including the register of information and incident-reporting instruments. https://www.fsma.be/en/digital-operational-resilience-act

[5] ArtiProof. Keeping Organisational Knowledge Dependable in the Age of AI. Public Whitepaper 1.2.1 EN in this release. Current methodology: https://artiproof.org/method/

[6] ArtiProof. Current development and validation status. https://artiproof.org/status/

[7] European Commission. Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024, standard templates for the register of information under DORA. Official ELI: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/eng (AP-R-056).

Sources checked: September 2026. The Official Journal text was consulted via IVASS; the secondary-instrument and supervisory review is selective, not an exhaustive legal baseline.