

Compliance & Evidence Readiness Review

Draft sample output — illustrative example of a professional review of controls, documentation and evidence against defined DORA (Digital Operational Resilience Act) requirements.

Client	Kranitech Analytics Ltd	Framework	DORA
Scope	ICT risk management and ICT third-party risk	Review date	04 September 2026
Material provided	ICT Risk Management Policy, ICT Incident Management Procedure, ICT Third-Party Risk Procedure, ICT Risk Register, Supplier Register	Output	Readiness review + control/evidence mapping

Executive summary

Purpose. Kranitech Analytics Ltd requested a review of how its existing ICT risk management arrangements, documentation and available evidence address the defined DORA requirements within the agreed scope. The review is intended to identify areas where documented arrangements or supporting evidence may not yet provide sufficient coverage.

Review performed. The requirements within scope were considered against the policies, procedures, risk information and supporting material supplied for review. Each requirement was assessed in relation to the relevant control or documented arrangement and the evidence available to support the stated position. Where evidence was incomplete or unclear, this was recorded rather than assumed.

Overall position. The material provides a reasonable foundation for the defined DORA scope, but readiness is reduced by several control and evidence gaps. The main areas requiring attention are ICT risk treatment tracking, incident classification and escalation, testing evidence and the documentation of ICT third-party risk oversight.

Recommended next step. Address the identified gaps, strengthen the supporting evidence and update the affected documentation. The review provides a practical basis for deciding what should be addressed next before relying on the current material as evidence of DORA readiness.

Readiness position

20 requirements reviewed	12 adequately covered	5 partial coverage	3 gaps / missing evidence
------------------------------------	---------------------------------	------------------------------	-------------------------------------

Coverage position

Adequately covered		12
Partial coverage		5
Gap / evidence		3

Key readiness gaps

01 ICT risk treatment tracking

Evidence gap

The ICT risk register records identified risks and owners, but the available material does not consistently demonstrate treatment decisions, target dates and closure status. The documented risk position is therefore stronger than the available evidence of ongoing treatment.

Source: DORA ICT risk management requirement

02 ICT incident classification and escalation

Partial coverage

The incident procedure describes ICT incident handling, but classification criteria, escalation thresholds and responsibilities for significant ICT incidents are not sufficiently clear or consistently evidenced.

Source: DORA ICT-related incident management

03 ICT resilience testing evidence

Evidence gap

Testing activities are referenced in the available documentation, but the supplied evidence does not consistently demonstrate test scope, results, remediation and closure for the defined ICT services.

Source: DORA digital operational resilience testing

04 ICT third-party risk oversight

Control gap

The third-party risk procedure describes supplier assessment, but the material does not clearly demonstrate how ICT third-party risk is monitored throughout the relationship, including material changes and ongoing oversight.

Source: DORA ICT third-party risk management

Practical next steps

High Complete ICT risk treatment evidence

Update the ICT risk register to show treatment decisions, owners, target dates and closure status, with evidence of periodic review.

High Strengthen incident classification and escalation

Define classification criteria, escalation thresholds, responsibilities and notification paths for significant ICT-related incidents.

Medium Formalise resilience testing evidence

Retain evidence of testing scope, outcomes, identified deficiencies, remediation and closure for relevant ICT services.

Medium Strengthen third-party risk oversight

Document ongoing monitoring of ICT third-party risk, including changes in service, risk profile, dependencies and material issues.

Requirement, control & evidence mapping

The extract below illustrates how DORA requirements can be linked to the relevant control or documented arrangement and the evidence available to support the current position.

Ref.	DORA area	Control / arrangement	Evidence considered	Position
RM-01	ICT risk management	ICT Risk Management Policy defines governance, risk ownership and review expectations.	ICT Risk Management Policy; ICT Risk Register.	Partial
RM-02	Risk treatment	ICT Risk Register records risks and owners; treatment status is incomplete for some entries.	ICT Risk Register; treatment evidence incomplete.	Gap
IM-01	ICT incident management	Incident procedure defines handling and escalation of ICT-related incidents.	ICT Incident Management Procedure; incident records not sampled.	Partial
RT-01	Resilience testing	Testing expectations are documented for relevant ICT services.	Testing plan; selected test evidence; remediation evidence incomplete.	Gap
TP-01	ICT third-party risk	Third-party procedure defines assessment and review of ICT providers.	ICT Third-Party Risk Procedure; Supplier Register; ongoing monitoring evidence limited.	Partial
TP-02	Third-party oversight	Supplier Register records key providers and ownership responsibilities.	Supplier Register; review evidence available for sampled providers.	Covered

Overall readiness view

The current material provides a credible documented foundation for the defined DORA scope. Readiness is not yet complete because several requirements lack sufficiently complete evidence or require clearer control definition. Closing the identified gaps would materially improve the ability to demonstrate effective ICT risk management and operational resilience arrangements during a subsequent assurance activity.

Overall position

Further work required

20 requirements reviewed
 12 covered · 5 partial · 3 gaps
 Focus first on risk treatment, incident handling, testing and third-party oversight.

Scope and limitation

This review covers only the defined DORA requirements, scope and documents provided for the engagement. It does not independently verify technical controls, test systems, certify compliance or provide legal/regulatory advice. The readiness view reflects the material available at the time of review.