R00

DORA SNI Documentation & Implementation Suite — Architecture and Traceability Report

ARCHITECTURE REPORT — VERSION 1.1

ENTITY	[ENTITY LEGAL NAME]
OWNER	[ROLE / FUNCTION]
APPROVER	[BOARD / MANAGEMENT BODY / EXECUTIVE]
VERSION	[1.1]
EFFECTIVE DATE	[DD MONTH YYYY]
NEXT REVIEW	[DD MONTH YYYY]

TEMPLATE STATUS

Complete and validate every yellow-bracketed field. Delete drafting notes before approval. Technical controls, inventories, provider facts, tests and audit conclusions must not be assumed or invented.

Document control and approval

Field	Controlled value
Document ID	R00
Document title	DORA SNI Documentation & Implementation Suite — Architecture and Traceability Report
Owner	[DORA Programme Owner / Legal]
Approval authority	Management body for entity-specific adoption
Version	[1.1]
Effective date	[DD MONTH YYYY]
Review cycle	At least annually and on legal, classification or material operating-model change
Classification	Confidential — Internal

Approval record

Approver	Capacity	Decision	Date
[NAME]	[ROLE]	Approved / conditional	[DATE]
[NAME]	[ROLE]	Approved / conditional	[DATE]

Version history

Version	Date	Change	Author
0.1	[DATE]	Initial template tailoring	[NAME]
1.0	[DATE]	First approved version	[NAME]
1.1	23 July 2026	D06 Annexes A–E added; 206 broken references remediated; 19 authority-only records remapped to R00 Appendix A; supporting workbooks, evidence mapping and site library updated.	[NAME]

Executive conclusion

> **WHAT THIS SUITE IS**
> A reusable, conservative but proportionate template architecture for a small and non-interconnected investment firm. It is not a compliance certificate and does not substitute for client facts, technical implementation, testing, provider remediation or independent assurance.

The suite separates document readiness from operational implementation and evidence. D01–D14 form a single control system: D01 governs; D02, D05, D06, D08, D09, D12 and D13 establish policies/procedures/programmes; D03, D04, D07, D10 and D14 hold structured records; D11 holds provider-level analysis and contractual/exit evidence.

1. Scope and assumptions

Assumption	Position
Entity	Icelandic investment firm within DORA scope and meeting the SNI criteria in Article 12(1) IFR.
Framework	Article 16 simplified ICT risk management framework; DORA Articles 5–15 are excluded.
Microenterprise	Not assumed. Record separately because SNI and DORA microenterprise are different tests.
Operating model	Small, SaaS/cloud-dependent firm with no material proprietary software development; optional development controls retained.
Client assets/payments	No assumption; conditional modules and fact-finding fields retained.
TLPT	No designation assumed; monitoring and activation checklist retained.
Language / branding	English, neutral reusable internal templates.
Readiness standard	Conservative licensing readiness, with proportional implementation and explicit validation flags.

2. Icelandic legal baseline

DORA has force of law in Iceland under Act No. 78/2025 from 1 January 2026. The Central Bank of Iceland is the competent authority and Rules No. 310/2026 incorporate the relevant incident, ICT-risk, third-party/subcontracting and TLPT Level 2 measures. The Central Bank's public guidance identifies its reporting portal, advance-notification expectation and the register-of-information submission architecture.

> **IMPORTANT CORRECTION**
> RTS 2024/1773 is incorporated in Iceland, but its formal policy content is tied to DORA Article 28(2), which expressly excludes Article 16(1) SNI entities. Direct duties under Articles 28(1), 28(3)–(8), 29 and 30 remain applicable; D09 therefore retains proportionate lifecycle controls without asserting that the RTS 2024/1773 policy is mandatory.

3. Document architecture

ID	Deliverable	Function
D01	Governance & simplified ICT-risk framework	Board governance, proportionality, risk tolerance, methodology, reporting, review.
D02	Information security & ICT operations	Consolidated security/operations policy rather than proliferating standalone policies.
D03	ICT risk register	Risk scoring, treatment, acceptance, monitoring and decisions.
D04	Functions, assets & dependencies	Criticality, inventories, providers, data flows and interdependencies.
D05	Continuity, response & recovery	BIA, RTO/RPO, scenarios, backup, restoration and return to normal.
D06	Incident management & reporting	Detection, escalation, DORA classification, Central Bank runbook and learning, with mandatory Annex A classification tool, mandatory Annex B reporting pack, conditional Annex C, context-only Annex D and optional Annex E.
D07	Incident register	Operational incident, threshold, reporting and corrective-action record.
D08	Resilience testing	Annual programme, test scripts, reports, remediation and conditional TLPT activation.
D09	ICT third-party risk	Proportionate provider lifecycle, notifications, monitoring and exit governance.

ID	Deliverable	Function
D10	Register of information	All 14 ITS templates and 98 field definitions.
D11	Provider compliance pack	Criticality, due diligence, Article 30 matrix, concentration, subcontracting and exit.
D12	Training programme	Board, staff and role-based training, assessment and records.
D13	Audit & framework review	Risk-based assurance and searchable Article 41 review report.
D14	Control evidence register	Requirement/control-to-evidence index, currency and reviewer status.

4. Control and evidence model

1. Legal requirement — exact paragraph/point and applicability conclusion.
2. Control objective — the outcome that must be achieved.
3. Controlled deliverable — primary and supporting D01–D14 location.
4. Operational record — risk, asset, incident, provider, test or approval record.
5. Evidence — current objective proof that the control operated.
6. Assurance — review, test, audit or framework-review conclusion.

A document may be approved while the underlying control remains unimplemented. The suite therefore uses separate readiness concepts: legal coverage, document readiness, control implementation, evidence currency and testing/assurance.

5. Governance and approval model

Approval level	Deliverables / decisions
Management body	D01; material risk tolerance; D02/D05/D06/D08/D09 as determined by governance; high/critical risk; material exceptions; Article 41 report; material provider/exit decisions.
Management / executive	Operational procedures, annual plans, provider onboarding within delegated tolerance, routine remediation and training programme.
Control functions	Independent challenge, monitoring, classification/report review and assurance input.
Operational owners	Maintain inventories, controls, registers, evidence and action completion.
Internal audit / independent assurance	Risk-based audit and verified follow-up; no management substitution.

6. Dependency and implementation order

Phase	Outcome
1. Classify and scope	Confirm SNI, microenterprise, services, client-assets/payments, group and TLPT position.
2. Map reality	Populate D04 and initial D10; identify critical functions, systems, data, providers and dependencies.
3. Assess risk	Populate D03; define tolerance, treatments and accepted assumptions.
4. Establish controls	Tailor/approve D01, D02, D05, D06, D08, D09 and D12.

Phase	Outcome
5. Remediate providers	Complete D11 packs, Article 30 gaps, subcontracting, concentration, exit and notifications.
6. Prove operation	Perform training, access review, restore test, tabletop, security testing and evidence capture in D14.
7. Assure and approve	Complete D13 readiness review, close/accept high-risk gaps and integrate into licence materials.

7. Readiness gates

Gate	Minimum suite state
Before application	Applicability fixed; D01/D02/D03/D04/D05/D06/D09/D10 materially complete; critical provider risks identified; action plan credible.
Before authorisation	Principal documents approved; incident portal/forms ready; material contracts remediated or decided; initial training and key tests performed; evidence indexed.
Before launch	Critical controls operational; access/backup/monitoring/recovery verified; owners and escalation live; unresolved high risk approved with containment.
BAU	Registers current; incidents reported; testing/training/audit/review calendar operated; provider and legal changes monitored; evidence refreshed.

8. Responsibility split

Party	Primary responsibility
Management body	Ultimate accountability, approval, challenge, resources and risk decisions.
Management	Implementation, ownership, escalation and operational resilience.
Legal counsel	Regulatory mapping, governance, contracts, licensing narrative and legal change.
Compliance / risk	Monitoring, challenge, reporting oversight, traceability and risk escalation.
ICT provider / cyber adviser	Technical architecture, configuration, monitoring, testing, recovery and evidence validation.
Internal audit / independent reviewer	Independent risk-based assurance and follow-up.
Vendors	Contracted services, controls, reporting, cooperation, audit evidence and exit support.

9. Client fact-finding and technical validation

- licence permissions, client money/instruments and payment-service interfaces;
- headcount, revenue/balance sheet and DORA microenterprise test;
- governance, group structure, control functions and outsourcing model;
- business functions, products, clients, transaction flows and criticality;
- systems, devices, data, interfaces, locations and recovery architecture;
- providers, contracts, subcontractors, assurance and data locations;
- access administration, patching, logging, monitoring, backup and incident support;

- application, authorisation and launch dates.

10. Limitations and safe use

- Do not mark a control implemented because a policy states it.
- Do not populate tests, incidents, audit findings, RTO/RPO or provider facts with invented results.
- Do not assume SNI equals DORA microenterprise.
- Do not rely on provider certificates without scope/currency/relevance review.
- Do not treat an Article 30 gap as cured merely because bespoke negotiation is unavailable.
- Revalidate law and Central Bank channels before client use.

Official source register

Source	Official URL
DORA	https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
Simplified ICT-risk RTS 2024/1774	https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/eng
Incident classification RTS 2024/1772	https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj/eng
Incident content/timing RTS 2025/301	https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng
Incident forms ITS 2025/302	https://eur-lex.europa.eu/eli/reg_impl/2025/302/oj/eng
Register ITS 2024/2956	https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/eng
Subcontracting RTS 2025/532	https://eur-lex.europa.eu/eli/reg_del/2025/532/oj/eng
Icelandic Act No. 78/2025	https://www.althingi.is/lagas/nuna/2025078.html
Central Bank Rules No. 310/2026	https://island.is/stjornartidindi/nr/87da1483-6a2a-412a-9021-30b9a817ad51
Central Bank DORA guidance	https://sedlabanki.is/fjarmalaeftirlit/stafraenn-vidnamsthrottur-a-fjarmalamarkadi-dora/

10. D06 annex remediation release

Version 1.1 establishes one controlled annex convention throughout D06. Annex A is the mandatory classification and escalation tool; Annex B is the mandatory regulatory reporting pack and submission runbook; Annex C is conditional on payment-service relevance; Annex D is context only; and Annex E is optional for Article 45 information-sharing participation.

The 206-record remediation log records every former broken reference, its new primary and supporting location, evidence expectation, reason and validation result. No requirement was deleted. The 19 provisions imposing duties only on authorities are mapped primarily to this report's Appendix A, not represented as firm-side controls.

Appendix A — Master regulatory requirements and traceability schedule

The schedule contains all 612 controlled requirement records considered in the suite, including applicable, conditional, optional, SNI-carved-out and authority-only provisions. Version 1.1 resolves all 206 former D06 annex references: 187 remain mapped to substantive D06 annexes, while 19 authority-only/context records are mapped primarily to R00 Appendix A with D06 Annex D as supporting context. The accompanying workbook is the controlling sortable version and contains the unabridged fields.

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
IS-CBI-ADV	CBI_GUIDE Advance notification	Applicable	The authority expects advance notification of planned ICT arrangements supporting critical or important functions, when a function becomes critical or important, and relevant chang	D09 — Section 7 — Regulatory notifications	Notification decision, form and submission evidence
IS-CBI-INC	CBI_GUIDE Major incident reporting	Applicable	Major ICT-related incidents must be reported through the Financial Supervisory Authority electronic portal using the current templates; significant cyber threats may be notified vo	D06 — Section 8 — Central Bank reporting runbook	Portal access test, reporting contacts and submission record
IS-CBI-ROI	CBI_GUIDE Register of information	Applicable	The authority may request the complete register covering all ICT contractual arrangements; it is submitted through the supervisory reporting system and should follow the 2024/2956	D10 — Instructions and all prescribed worksheets	Validated register and submission readiness evidence
DORA-A16-P1	DORA Article 16(1)	Applicable	Articles 5 to 15 of this Regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutio	D01 — Sections 4–8 — Simplified ICT risk management framework	Controlled document, approval and implementation evidence
DORA-A16-P1-2	DORA Article 16(1)	Applicable	Without prejudice to the first subparagraph, the entities listed in the first subparagraph shall:	D01 — Sections 4–8 — Simplified ICT risk management framework	Controlled document, approval and implementation evidence
DORA-A16-P1-A	DORA Article 16(1)(a)	Applicable	put in place and maintain a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of	D01 — Sections 4–8 — Simplified ICT risk management framework	Controlled document, approval and implementation evidence
DORA-A16-P1-B	DORA Article 16(1)(b)	Applicable	continuously monitor the security and functioning of all ICT systems;	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P1-C	DORA Article 16(1)(c)	Applicable	minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activitie	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P1-D	DORA Article 16(1)(d)	Applicable	allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled;	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P1-E	DORA Article 16(1)(e)	Applicable	identify key dependencies on ICT third-party service providers;	D04 — Providers and Dependencies worksheets	Controlled document, approval and implementation evidence
DORA-A16-P1-F	DORA Article 16(1)(f)	Applicable	ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration mea	D05 — Sections 4–10 — Continuity, response and recovery	Controlled document, approval and implementation evidence
DORA-A16-P1-G	DORA Article 16(1)(g)	Applicable	test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c);	D08 — Sections 3–8 — Risk-based testing programme	Controlled document, approval and implementation evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A16-P1-H	DORA Article 16(1)(h)	Applicable	implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process a	D12 — Sections 3–7 — Training and lessons learned	Controlled document, approval and implementation evidence
DORA-A16-P2	DORA Article 16(2)	Applicable	The ICT risk management framework referred to in paragraph 1, second subparagraph, point (a), shall be documented and reviewed periodically and upon the occurrence of major ICT-rel	D13 — Part B — Simplified framework review report	Controlled document, approval and implementation evidence
DORA-A16-P3	DORA Article 16(3)	Applicable	The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards in order to:	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A16-P3-13	DORA Article 16(3)	Applicable	When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale an	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A16-P3-14	DORA Article 16(3)	Applicable	The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A16-P3-15	DORA Article 16(3)	Applicable	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A16-P3-A	DORA Article 16(3)(a)	Applicable	specify further the elements to be included in the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a);	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A16-P3-B	DORA Article 16(3)(b)	Applicable	specify further the elements in relation to systems, protocols and tools to minimise the impact of ICT risk referred to in paragraph 1, second subparagraph, point (c), with a view	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P3-C	DORA Article 16(3)(c)	Applicable	specify further the components of the ICT business continuity plans referred to in paragraph 1, second subparagraph, point (f);	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P3-D	DORA Article 16(3)(d)	Applicable	specify further the rules on the testing of business continuity plans and ensure the effectiveness of the controls referred to in paragraph 1, second subparagraph, point (g) and en	D02 — Sections 8–12 — Operations, monitoring and system security	Controlled document, approval and implementation evidence
DORA-A16-P3-E	DORA Article 16(3)(e)	Applicable	specify further the content and format of the report on the review of the ICT risk management framework referred to in paragraph 2.	D04 — Providers and Dependencies worksheets	Controlled document, approval and implementation evidence
DORA-A17-P1	DORA Article 17(1)	Applicable	Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P2	DORA Article 17(2)	Applicable	Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consist	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3	DORA Article 17(3)	Applicable	The ICT-related incident management process referred to in paragraph 1 shall:	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3-A	DORA Article 17(3)(a)	Applicable	put in place early warning indicators;	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3-B	DORA Article 17(3)(b)	Applicable	establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the service	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A17-P3-C	DORA Article 17(3)(c)	Applicable	assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3-D	DORA Article 17(3)(d)	Applicable	set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, includi	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3-E	DORA Article 17(3)(e)	Applicable	ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents, explaining the i	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A17-P3-F	DORA Article 17(3)(f)	Applicable	establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.	D06 — Sections 4–5 — Incident process, roles and escalation	Incident records, escalation evidence and post-incident record
DORA-A18-P1	DORA Article 18(1)	Applicable	Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-A	DORA Article 18(1)(a)	Applicable	the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whet	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-B	DORA Article 18(1)(b)	Applicable	the duration of the ICT-related incident, including the service downtime;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-C	DORA Article 18(1)(c)	Applicable	the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-D	DORA Article 18(1)(d)	Applicable	the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-E	DORA Article 18(1)(e)	Applicable	the criticality of the services affected, including the financial entity's transactions and operations;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P1-F	DORA Article 18(1)(f)	Applicable	the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P2	DORA Article 18(2)	Applicable	Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, numbe	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P3	DORA Article 18(3)	Applicable	The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards further specifying the following:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P3-A	DORA Article 18(3)(a)	Applicable	the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents or, as applicable, major operational or security payment-related i	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A18-P3-B	DORA Article 18(3)(b)	Applicable	the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payme	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P3-C	DORA Article 18(3)(c)	Applicable	the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P4	DORA Article 18(4)	Applicable	When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2), a	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P4-14	DORA Article 18(4)	Applicable	The ESAs shall submit those common draft regulatory technical standards to the Commission by 17 January 2024.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A18-P4-15	DORA Article 18(4)	Applicable	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 in accordance with Articles 10 to 14 of	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
DORA-A19-P1	DORA Article 19(1)	Applicable	Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article.	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P1-2	DORA Article 19(1)	Applicable	Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46, Member States shall designate a single competent authori	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P1-3	DORA Article 19(1)	Applicable	Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall report major ICT-related incidents to the relevant national co	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P1-4	DORA Article 19(1)	Applicable	For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, the initial notification and reports referred	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P1-5	DORA Article 19(1)	Applicable	The initial notification and reports referred to in paragraph 4 shall include all information necessary for the competent authority to determine the significance of the major ICT-r	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P1-6	DORA Article 19(1)	Applicable	Without prejudice to the reporting pursuant to the first subparagraph by the financial entity to the relevant competent authority, Member States may additionally determine that som	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P2	DORA Article 19(2)	Applicable	Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial sys	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P2-8	DORA Article 19(2)	Applicable	Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, may, on a voluntary basis, notify significant cyber threats to relev	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P2-9	DORA Article 19(2)	Applicable	Member States may determine that those financial entities that on a voluntary basis notify in accordance with the first subparagraph may also transmit that notification to the CSIR	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A19-P3	DORA Article 19(3)	Applicable	Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it,	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P3-11	DORA Article 19(3)	Applicable	In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures whi	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P4	DORA Article 19(4)	Applicable	Financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit the following to the relevant compete	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P4-A	DORA Article 19(4)(a)	Applicable	an initial notification;	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P4-B	DORA Article 19(4)(b)	Applicable	an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the majo	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P4-C	DORA Article 19(4)(c)	Applicable	a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are ava	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P5	DORA Article 19(5)	Optional	Financial entities may outsource, in accordance with Union and national sectoral law, the reporting obligations under this Article to a third-party service provider. In case of suc	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6	DORA Article 19(6)	Applicable	Upon receipt of the initial notification and of each report referred to in paragraph 4, the competent authority shall, in a timely manner, provide details of the major ICT-related	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6-A	DORA Article 19(6)(a)	Applicable	EBA, ESMA or EIOPA;	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6-B	DORA Article 19(6)(b)	Applicable	the ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d);	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6-C	DORA Article 19(6)(c)	Applicable	the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6-D	DORA Article 19(6)(d)	Applicable	the resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regul	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P6-E	DORA Article 19(6)(e)	Applicable	other relevant public authorities under national law.	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P7	DORA Article 19(7)	Applicable	Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record
DORA-A19-P8	DORA Article 19(8)	Applicable	The notification to be done by ESMA pursuant to paragraph 7 of this Article shall be without prejudice to the responsibility of the competent authority to urgently transmit the det	D06 — Sections 7–9 — Regulatory and client reporting runbook	Portal submission, report forms and reporting decision record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A20-Part_20	DORA Article 20(art_20)	No direct entity obligation	The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop:	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A20-Part_20-2	DORA Article 20(art_20)	No direct entity obligation	The ESAs shall submit the common draft regulatory technical standards referred to in the first paragraph, point (a), and the common draft implementing technical standards referred	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A20-Part_20-3	DORA Article 20(art_20)	No direct entity obligation	Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in the first paragraph, point (a), in accordanc	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A20-Part_20-4	DORA Article 20(art_20)	No direct entity obligation	Power is conferred on the Commission to adopt the common implementing technical standards referred to in the first paragraph, point (b), in accordance with Article 15 of Regulation	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A20-Part_20-A	DORA Article 20(art_20)(a)	No direct entity obligation	common draft regulatory technical standards in order to: (i) establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Arti	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A20-Part_20-B	DORA Article 20(art_20)(b)	No direct entity obligation	common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and t	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P1	DORA Article 21(1)	No direct entity obligation	The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident repo	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2	DORA Article 21(2)	No direct entity obligation	The joint report referred to in paragraph 1 shall comprise at least the following elements:	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-A	DORA Article 21(2)(a)	No direct entity obligation	prerequisites for the establishment of a single EU Hub;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-B	DORA Article 21(2)(b)	No direct entity obligation	benefits, limitations and risks, including risks associated with the high concentration of sensitive information;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-C	DORA Article 21(2)(c)	No direct entity obligation	the necessary capability to ensure interoperability with regard to other relevant reporting schemes;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-D	DORA Article 21(2)(d)	No direct entity obligation	elements of operational management;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-E	DORA Article 21(2)(e)	No direct entity obligation	conditions of membership;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P2-F	DORA Article 21(2)(f)	No direct entity obligation	technical arrangements for financial entities and national competent authorities to access the single EU Hub;	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A21-P2-G	DORA Article 21(2)(g)	No direct entity obligation	a preliminary assessment of financial costs incurred by setting-up the operational platform supporting the single EU Hub, including the requisite expertise.	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A21-P3	DORA Article 21(3)	No direct entity obligation	The ESAs shall submit the report referred to in paragraph 1 to the European Parliament, to the Council and to the Commission by 17 January 2025.	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A22-P1	DORA Article 22(1)	No direct entity obligation	Without prejudice to the technical input, advice or remedies and subsequent follow-up which may be provided, where applicable, in accordance with national law, by the CSIRTs under	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A22-P2	DORA Article 22(2)	No direct entity obligation	The ESAs shall, through the Joint Committee, on an anonymised and aggregated basis, report yearly on major ICT-related incidents, the details of which shall be provided by competen	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A22-P2-3	DORA Article 22(2)	No direct entity obligation	The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.	R00 — Appendix A — Authority-only and regulatory-context schedule	No standalone entity evidence required; retain legal-source and applicability rationale
DORA-A23-Part_23	DORA Article 23(art_23)	Conditional	The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, whe	D06 — Annex C — Conditional Payment-Service Incident Interface	Payment-service applicability decision and, if relevant, sectoral reporting interface record
DORA-A24-P1	DORA Article 24(1)	Applicable	For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly im	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A24-P2	DORA Article 24(2)	Applicable	The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 an	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A24-P3	DORA Article 24(3)	Applicable	When conducting the digital operational resilience testing programme referred to in paragraph 1 of this Article, financial entities, other than microenterprises, shall follow a ris	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A24-P4	DORA Article 24(4)	Applicable	Financial entities, other than microenterprises, shall ensure that tests are undertaken by independent parties, whether internal or external. Where tests are undertaken by an inter	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A24-P5	DORA Article 24(5)	Applicable	Financial entities, other than microenterprises, shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the te	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A24-P6	DORA Article 24(6)	Applicable	Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or impo	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A25-P1	DORA Article 25(1)	Applicable	The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropri	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A25-P2	DORA Article 25(2)	Applicable	Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrast	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A25-P3	DORA Article 25(3)	Applicable	Microenterprises shall perform the tests referred to in paragraph 1 by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to mai	D08 — Sections 3–8 and Test Catalogue	Approved test plan, scripts, results, remediation and retest evidence
DORA-A26-P1	DORA Article 26(1)	Conditional	Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, thir	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P10	DORA Article 26(10)	Conditional	In the absence of a designation in accordance with paragraph 9 of this Article, and without prejudice to the power to identify the financial entities that are required to perform T	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11	DORA Article 26(11)	Conditional	The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-22	DORA Article 26(11)	Conditional	When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across diff	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-23	DORA Article 26(11)	Conditional	The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-24	DORA Article 26(11)	Conditional	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-A	DORA Article 26(11)(a)	Conditional	the criteria used for the purpose of the application of paragraph 8, second subparagraph;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-B	DORA Article 26(11)(b)	Conditional	the requirements and standards governing the use of internal testers;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-C	DORA Article 26(11)(c)	Conditional	the requirements in relation to: (i) the scope of TLPT referred to in paragraph 2; (ii) the testing methodology and approach to be followed for each specific phase of the testing p	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P11-D	DORA Article 26(11)(d)	Conditional	the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the conte	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P2	DORA Article 26(2)	Conditional	Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P2-3	DORA Article 26(2)	Conditional	Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those suppo	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P2-4	DORA Article 26(2)	Conditional	Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and sh	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P3	DORA Article 26(3)	Conditional	Where ICT third-party service providers are included in the scope of TLPT, the financial entity shall take the necessary measures and safeguards to ensure the participation of such	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A26-P4	DORA Article 26(4)	Conditional	Without prejudice to paragraph 2, first and second subparagraphs, where the participation of an ICT third-party service provider in the TLPT, referred to in paragraph 3, is reasona	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P4-7	DORA Article 26(4)	Conditional	That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the f	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P4-8	DORA Article 26(4)	Conditional	The number of financial entities participating in the pooled testing shall be duly calibrated taking into account the complexity and types of services involved.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P5	DORA Article 26(5)	Conditional	Financial entities shall, with the cooperation of ICT third-party service providers and other parties involved, including the testers but excluding the competent authorities, apply	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P6	DORA Article 26(6)	Conditional	At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers shall provide to the authority, de	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P7	DORA Article 26(7)	Conditional	Authorities shall provide financial entities with an attestation confirming that the test was performed in accordance with the requirements as evidenced in the documentation in ord	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P7-12	DORA Article 26(7)	Conditional	Without prejudice to such attestation, financial entities shall remain at all times fully responsible for the impact of the tests referred to in paragraph 4.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8	DORA Article 26(8)	Conditional	Financial entities shall contract testers for the purposes of undertaking TLPT in accordance with Article 27. When financial entities use internal testers for the purposes of under	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8-14	DORA Article 26(8)	Conditional	Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall only use external testers in accordance with Article 2	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8-15	DORA Article 26(8)	Conditional	Competent authorities shall identify financial entities that are required to perform TLPT taking into account the criteria set out in Article 4(2), based on an assessment of the fo	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8-A	DORA Article 26(8)(a)	Conditional	impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8-B	DORA Article 26(8)(b)	Conditional	possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P8-C	DORA Article 26(8)(c)	Conditional	specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A26-P9	DORA Article 26(9)	Conditional	Member States may designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level and shall entrust	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P1	DORA Article 27(1)	Conditional	Financial entities shall only use testers for the carrying out of TLPT, that:	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A27-P1-A	DORA Article 27(1)(a)	Conditional	are of the highest suitability and reputability;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P1-B	DORA Article 27(1)(b)	Conditional	possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P1-C	DORA Article 27(1)(c)	Conditional	are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P1-D	DORA Article 27(1)(d)	Conditional	provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the fin	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P1-E	DORA Article 27(1)(e)	Conditional	are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P2	DORA Article 27(2)	Conditional	When using internal testers, financial entities shall ensure that, in addition to the requirements in paragraph 1, the following conditions are met:	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P2-A	DORA Article 27(2)(a)	Conditional	such use has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P2-B	DORA Article 27(2)(b)	Conditional	the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P2-C	DORA Article 27(2)(c)	Conditional	the threat intelligence provider is external to the financial entity.	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A27-P3	DORA Article 27(3)	Conditional	Financial entities shall ensure that contracts concluded with external testers require a sound management of the TLPT results and that any data processing thereof, including any ge	D08 — Appendix C — TLPT activation checklist	Designation record or documented non-designation monitoring
DORA-A28-P1	DORA Article 28(1)	Applicable	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1), and in accordan	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P1-A	DORA Article 28(1)(a)	Applicable	financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compli	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P1-B	DORA Article 28(1)(b)	Applicable	financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account: (i) the nature, scale, complexity and	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P10	DORA Article 28(10)	Applicable	The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2 in relati	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A28-P10-35	DORA Article 28(10)	Applicable	When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale an	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A28-P10-36	DORA Article 28(10)	Applicable	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A28-P2	DORA Article 28(2)	Not applicable — SNI carve-out	As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, shall ado	D09 — Section 2 — Proportionate internal procedure (voluntary architecture)	Controlled document, approval and implementation evidence
DORA-A28-P3	DORA Article 28(3)	Applicable	As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of informa	D10 — All prescribed ITS worksheets	Complete and validated register of information
DORA-A28-P3-6	DORA Article 28(3)	Applicable	The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or im	D10 — All prescribed ITS worksheets	Complete and validated register of information
DORA-A28-P3-7	DORA Article 28(3)	Applicable	Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service	D10 — All prescribed ITS worksheets	Complete and validated register of information
DORA-A28-P3-8	DORA Article 28(3)	Applicable	Financial entities shall make available to the competent authority, upon its request, the full register of information or, as requested, specified sections thereof, along with any	D10 — All prescribed ITS worksheets	Complete and validated register of information
DORA-A28-P3-9	DORA Article 28(3)	Applicable	Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important fun	D10 — All prescribed ITS worksheets	Complete and validated register of information
DORA-A28-P4	DORA Article 28(4)	Applicable	Before entering into a contractual arrangement on the use of ICT services, financial entities shall:	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P4-A	DORA Article 28(4)(a)	Applicable	assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P4-B	DORA Article 28(4)(b)	Applicable	assess if supervisory conditions for contracting are met;	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P4-C	DORA Article 28(4)(c)	Applicable	identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT con	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P4-D	DORA Article 28(4)(d)	Applicable	undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P4-E	DORA Article 28(4)(e)	Applicable	identify and assess conflicts of interest that the contractual arrangement may cause.	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P5	DORA Article 28(5)	Applicable	Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contr	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P6	DORA Article 28(6)	Applicable	In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the freq	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A28-P6-18	DORA Article 28(6)	Applicable	Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P7	DORA Article 28(7)	Applicable	Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P7-A	DORA Article 28(7)(a)	Applicable	significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P7-B	DORA Article 28(7)(b)	Applicable	circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arr	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P7-C	DORA Article 28(7)(c)	Applicable	ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integr	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P7-D	DORA Article 28(7)(d)	Applicable	where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arr	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8	DORA Article 28(8)	Applicable	For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerg	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-25	DORA Article 28(8)	Applicable	Financial entities shall ensure that they are able to exit contractual arrangements without:	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-26	DORA Article 28(8)	Applicable	Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-27	DORA Article 28(8)	Applicable	Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-pa	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-28	DORA Article 28(8)	Applicable	Financial entities shall have appropriate contingency measures in place to maintain business continuity in the event of the circumstances referred to in the first subparagraph.	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-A	DORA Article 28(8)(a)	Applicable	disruption to their business activities,	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-B	DORA Article 28(8)(b)	Applicable	limiting compliance with regulatory requirements,	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P8-C	DORA Article 28(8)(c)	Applicable	detriment to the continuity and quality of services provided to clients.	D09 — Sections 3–10 — Lifecycle management	Provider assessment, approvals, monitoring, contract and exit evidence
DORA-A28-P9	DORA Article 28(9)	Applicable	The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information refe	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence
DORA-A28-P9-33	DORA Article 28(9)	Applicable	Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2	D01 — Section 2 — Legal and regulatory basis	Controlled document, approval and implementation evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A29-P1	DORA Article 29(1)	Applicable	When performing the identification and assessment of risks referred to in Article 28(4), point (c), financial entities shall also take into account whether the envisaged conclusion	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P1-2	DORA Article 29(1)	Applicable	Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envis	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P1-A	DORA Article 29(1)(a)	Applicable	contracting an ICT third-party service provider that is not easily substitutable; or	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P1-B	DORA Article 29(1)(b)	Applicable	having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service prov	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P2	DORA Article 29(2)	Applicable	Where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further su	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P2-6	DORA Article 29(2)	Applicable	Where contractual arrangements concern ICT services supporting critical or important functions, financial entities shall duly consider the insolvency law provisions that would appl	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P2-7	DORA Article 29(2)	Applicable	Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third c	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A29-P2-8	DORA Article 29(2)	Applicable	Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how	D11 — Part D — Concentration and substitutability assessment	Provider and portfolio concentration assessment
DORA-A30-P1	DORA Article 30(1)	Applicable	The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include th	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2	DORA Article 30(2)	Applicable	The contractual arrangements on the use of ICT services shall include at least the following elements:	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-A	DORA Article 30(2)(a)	Applicable	a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service suppo	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-B	DORA Article 30(2)(b)	Applicable	the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-C	DORA Article 30(2)(c)	Applicable	provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-D	DORA Article 30(2)(d)	Applicable	provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-E	DORA Article 30(2)(e)	Applicable	service level descriptions, including updates and revisions thereof;	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A30-P2-F	DORA Article 30(2)(f)	Applicable	the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante , when an ICT in	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-G	DORA Article 30(2)(g)	Applicable	the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons a	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-H	DORA Article 30(2)(h)	Applicable	termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resoluti	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P2-I	DORA Article 30(2)(i)	Applicable	the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training i	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3	DORA Article 30(3)	Applicable	The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least t	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-13	DORA Article 30(3)	Applicable	By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access,	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-A	DORA Article 30(3)(a)	Applicable	full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow eff	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-B	DORA Article 30(3)(b)	Applicable	notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impac	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-C	DORA Article 30(3)(c)	Applicable	requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide a	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-D	DORA Article 30(3)(d)	Applicable	the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-E	DORA Article 30(3)(e)	Applicable	the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following: (i) unrestricted rights of access, inspection and audit	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P3-F	DORA Article 30(3)(f)	Applicable	exit strategies, in particular the establishment of a mandatory adequate transition period: (i) during which the ICT third-party service provider will continue providing the respec	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P4	DORA Article 30(4)	Applicable	When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public autho	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P5	DORA Article 30(5)	Applicable	The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial e	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
DORA-A30-P5-22	DORA Article 30(5)	Applicable	When developing those draft regulatory technical standards, the ESAs shall take into consideration the size and overall risk profile of the financial entity, and the nature, scale	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P5-23	DORA Article 30(5)	Applicable	The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A30-P5-24	DORA Article 30(5)	Applicable	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles	D11 — Part C and Contract Matrix — Mandatory contractual provisions	Executed contract, addendum or approved remediation/risk decision
DORA-A04-P1	DORA Article 4(1)	Applicable	Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, a	D01 — Section 3 — Scope, applicability and proportionality	Recorded proportionality assessment and periodic review
DORA-A04-P2	DORA Article 4(2)	Applicable	In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and	D01 — Section 3 — Scope, applicability and proportionality	Recorded proportionality assessment and periodic review
DORA-A04-P3	DORA Article 4(3)	Applicable	The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework	D01 — Section 3 — Scope, applicability and proportionality	Recorded proportionality assessment and periodic review
DORA-A45-P1	DORA Article 45(1)	Optional	Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber securit	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
DORA-A45-P1-A	DORA Article 45(1)(a)	Optional	aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threa	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
DORA-A45-P1-B	DORA Article 45(1)(b)	Optional	takes places within trusted communities of financial entities;	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
DORA-A45-P1-C	DORA Article 45(1)(c)	Optional	is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full r	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
DORA-A45-P2	DORA Article 45(2)	Optional	For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on t	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
DORA-A45-P3	DORA Article 45(3)	Optional	Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership	D06 — Annex E — Optional Information-Sharing Decision Record	Approved information-sharing decision record, participation terms and competent-authority notification evidence
IS-ACT78-S1	IS_ACT78 Section 1	Applicable	DORA has force of law in Iceland with EEA adaptations under JCD No. 40/2025. The Act entered into force on 1 January 2026.	D01 — Section 2 — Icelandic legal basis	Applicability memorandum and legal-source register
IS-ACT78-S3	IS_ACT78 Section 3	Applicable	The Central Bank of Iceland is the competent authority and the Financial Supervisory Authority supervises compliance.	D01 — Section 2 and Section 9 — Authority and reporting interface	Current authority contacts and reporting-channel evidence
IS-ACT78-S4	IS_ACT78 Section 4	Applicable	The Financial Supervisory Authority may require remediation within an appropriate period where requirements are not met.	D13 — Part C — Findings and remediation tracker	Supervisory action log and closure evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
IS-ACT78-S5	IS_ACT78 Section 5	Applicable	Administrative fines may be imposed for breaches of the specified DORA obligations, including Articles 16–19, 24–30.	D01 — Section 2 — Legal basis and consequences	Board and staff training record
IS-R310-A2	IS_RULE310 Article 2	Applicable	The incorporated Level 2 measures govern ICT incident management/reporting, ICT-risk management, third-party use and, conditionally, TLPT.	D01 — Section 2 — Applicable Level 2 measures	Controlled legal-source register and periodic change review
ITS2956-B0101	ITS2956 Annex I — Template B_01.01	Applicable	Maintain the prescribed data fields for template B_01.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_01.01	Populated and validated template worksheet
ITS2956-B0102	ITS2956 Annex I — Template B_01.02	Applicable	Maintain the prescribed data fields for template B_01.02 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_01.02	Populated and validated template worksheet
ITS2956-B0103	ITS2956 Annex I — Template B_01.03	Applicable	Maintain the prescribed data fields for template B_01.03 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_01.03	Populated and validated template worksheet
ITS2956-B0201	ITS2956 Annex I — Template B_02.01	Applicable	Maintain the prescribed data fields for template B_02.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_02.01	Populated and validated template worksheet
ITS2956-B0202	ITS2956 Annex I — Template B_02.02	Applicable	Maintain the prescribed data fields for template B_02.02 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_02.02	Populated and validated template worksheet
ITS2956-B0203	ITS2956 Annex I — Template B_02.03	Applicable	Maintain the prescribed data fields for template B_02.03 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_02.03	Populated and validated template worksheet
ITS2956-B0301	ITS2956 Annex I — Template B_03.01	Applicable	Maintain the prescribed data fields for template B_03.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_03.01	Populated and validated template worksheet
ITS2956-B0302	ITS2956 Annex I — Template B_03.02	Applicable	Maintain the prescribed data fields for template B_03.02 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_03.02	Populated and validated template worksheet
ITS2956-B0303	ITS2956 Annex I — Template B_03.03	Applicable	Maintain the prescribed data fields for template B_03.03 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_03.03	Populated and validated template worksheet
ITS2956-B0401	ITS2956 Annex I — Template B_04.01	Applicable	Maintain the prescribed data fields for template B_04.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_04.01	Populated and validated template worksheet
ITS2956-B0501	ITS2956 Annex I — Template B_05.01	Applicable	Maintain the prescribed data fields for template B_05.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_05.01	Populated and validated template worksheet
ITS2956-B0502	ITS2956 Annex I — Template B_05.02	Applicable	Maintain the prescribed data fields for template B_05.02 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_05.02	Populated and validated template worksheet

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
ITS2956-B0601	ITS2956 Annex I — Template B_06.01	Applicable	Maintain the prescribed data fields for template B_06.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_06.01	Populated and validated template worksheet
ITS2956-B0701	ITS2956 Annex I — Template B_07.01	Applicable	Maintain the prescribed data fields for template B_07.01 in accordance with the column-level instructions and mandatory/conditional status in Annex II.	D10 — Worksheet B_07.01	Populated and validated template worksheet
ITS2956-A02-Part_2	ITS2956 Article 2(art_2)	Applicable	Financial entities shall assign a rank to each ICT third-party service provider. The rank shall be any natural number higher or equal to '1' where the lower the natural number assi	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A02-Part_2-2	ITS2956 Article 2(art_2)	Applicable	The rank of the direct ICT third-party service provider in the ICT service supply chain shall always be '1'.	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A02-Part_2-3	ITS2956 Article 2(art_2)	Applicable	The rank of the subcontractor in the ICT service supply chain shall always be higher than '1'.	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P1	ITS2956 Article 3(1)	Applicable	Financial entities shall use the templates set out in Annex I to IV to maintain and update the register of information in accordance with Article 28(3) of Regulation (EU) 2022/2554	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P2	ITS2956 Article 3(2)	Applicable	Financial entities shall ensure that the templates referred to in paragraph 1 include all of the following:	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P2-A	ITS2956 Article 3(2)(a)	Applicable	the relevant information in relation to all the ICT services provided by direct ICT third-party providers;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P2-B	ITS2956 Article 3(2)(b)	Applicable	information on all subcontractors that effectively underpin ICT services supporting critical or important functions or material parts thereof.	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P3	ITS2956 Article 3(3)	Applicable	Financial entities shall ensure that the information contained in the templates referred to in paragraph 1 is accurate and consistent. Financial entities shall review the informati	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P3-6	ITS2956 Article 3(3)	Applicable	In case of groups, financial entities responsible for maintaining and updating the register of information at sub-consolidated and consolidated level shall ensure that information	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4	ITS2956 Article 3(4)	Applicable	Financial entities shall ensure that the information contained in the templates referred to in paragraph 1 adhere to the following principles of data quality:	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4-A	ITS2956 Article 3(4)(a)	Applicable	accuracy;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4-B	ITS2956 Article 3(4)(b)	Applicable	completeness;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4-C	ITS2956 Article 3(4)(c)	Applicable	consistency;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4-D	ITS2956 Article 3(4)(d)	Applicable	integrity;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P4-E	ITS2956 Article 3(4)(e)	Applicable	uniformity;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
ITS2956-A03-P4-F	ITS2956 Article 3(4)(f)	Applicable	validity.	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P5	ITS2956 Article 3(5)	Applicable	Financial entities shall use a valid and active legal entity identifier (LEI) or the European Unique Identifier referred to in Article 16 of Directive (EU) 2017/1132 ('EUID'), and	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A03-P6	ITS2956 Article 3(6)	Applicable	Where an ICT service provided by a direct ICT third-party service provider is supporting a critical or important function of the financial entities, financial entities shall ensure	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A04-P1	ITS2956 Article 4(1)	Applicable	Unless otherwise specified in the instructions, each template composing the register of information shall be a table with a predefined number of columns and an indefinite number of	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A04-P2	ITS2956 Article 4(2)	Applicable	Financial entities shall complete each data element with a single value. Where more than one value is valid for a specific data element, financial entities shall add an additional	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A04-P3	ITS2956 Article 4(3)	Applicable	Financial entities shall complete all data elements in the register of information at entity level, sub-consolidated and consolidated level, as applicable.	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1	ITS2956 Article 5(1)	Applicable	Financial entities shall include in the register of information, in accordance with the instructions set out in Annex I, the following information:	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-A	ITS2956 Article 5(1)(a)	Applicable	general information on the financial entity maintaining and updating the register of information at entity, sub-consolidated and consolidated level, respectively, as specified in t	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-B	ITS2956 Article 5(1)(b)	Applicable	general information on the entities in the consolidation as specified in template B_01.02 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-C	ITS2956 Article 5(1)(c)	Applicable	identification of the branches of financial entities located outside the home country listed in template B_01.02, where applicable, as specified in template B_01.03 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-D	ITS2956 Article 5(1)(d)	Applicable	general information on the contractual arrangements as specified in template B_02.01 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-E	ITS2956 Article 5(1)(e)	Applicable	specific information on the contractual arrangements as specified in template B_02.02 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-F	ITS2956 Article 5(1)(f)	Applicable	information on the links between intra-group contractual arrangements and contractual arrangements with ICT third-party service providers which are not part of the group using the	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-G	ITS2956 Article 5(1)(g)	Applicable	information on the entities signing the contractual arrangements with the direct ICT third-party service providers for receiving ICT services or on behalf of the entities using the	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-H	ITS2956 Article 5(1)(h)	Applicable	identification of the ICT third-party service providers signing the contractual arrangements for providing ICT services as specified in template B_03.02 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
ITS2956-A05-P1-I	ITS2956 Article 5(1)(i)	Applicable	identification of the entities signing the contractual arrangements for providing ICT services to other entities in the consolidation as specified in template B_03.03 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-J	ITS2956 Article 5(1)(j)	Applicable	information on the entities making use of the ICT services provided by the ICT third-party service providers as specified in template B_04.01 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-K	ITS2956 Article 5(1)(k)	Applicable	information on the direct ICT third-party service providers and subcontractors, as specified in template B_05.01 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-L	ITS2956 Article 5(1)(l)	Applicable	information on the ICT service supply chain, as specified in template B_05.02 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-M	ITS2956 Article 5(1)(m)	Applicable	information on the identification of functions as specified in template B_06.01 of Annex I;	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-N	ITS2956 Article 5(1)(n)	Applicable	information on the assessment of the ICT services provided by ICT third-party service providers supporting a critical or important function or material parts thereof as specified i	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P1-O	ITS2956 Article 5(1)(o)	Applicable	information on the terminology used by financial entities and the terms included in the closed lists and classification systems used when filling in the templates as specified in t	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A05-P2	ITS2956 Article 5(2)	Applicable	Where relevant for their risk management or contract management purposes, financial entities may include into the register of information additional information in the format that	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A06-P1	ITS2956 Article 6(1)	Applicable	In the case of groups, the parent undertakings shall take into account the relevant sectorial Union legislation when determining which entities to be included in the register of in	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS2956-A06-P2	ITS2956 Article 6(2)	Applicable	A register of information maintained and updated at sub-consolidated and consolidated levels shall include all financial entities and ICT intra-group service providers, which are p	D10 — Prescribed ITS worksheet and Instructions sheet	Complete, internally consistent and export-ready register of information
ITS302-A01-P1	ITS302 Article 1(1)	Applicable	Financial entities shall use the template laid down in Annex I to submit the initial notification, the intermediate report, and the final report referred to in Article 19(4) of Reg	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P1-A	ITS302 Article 1(1)(a)	Applicable	financial entities that submit an initial notification shall complete the data fields of the template which correspond to the information to be provided in accordance with Article	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P1-B	ITS302 Article 1(1)(b)	Applicable	financial entities that submit an intermediate report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 3	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P1-C	ITS302 Article 1(1)(c)	Applicable	financial entities that submit a final report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 4 of Dele	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P2	ITS302 Article 1(2)	Applicable	Financial entities shall ensure that the information contained in the initial notification, and in the intermediate and final report, is complete and accurate.	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
ITS302-A01-P3	ITS302 Article 1(3)	Applicable	Financial entities shall provide estimated values based on other available data and information, to the extent possible, where accurate data are not available at the time of report	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P4	ITS302 Article 1(4)	Applicable	When submitting an intermediate or final report, financial entities shall use the template laid down in Annex I to submit all required information and update, where applicable, the	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A01-P5	ITS302 Article 1(5)	Applicable	Financial entities shall follow the data glossary and instructions set out in Annex II when completing the template laid down in Annex I.	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A02-Part_2	ITS302 Article 2(art_2)	Applicable	Financial entities may combine the submission of the initial notification, the intermediate report, and the final report to provide two or all of those at the same time, where regu	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A03-Part_3	ITS302 Article 3(art_3)	Applicable	Financial entities that provide information on non-major recurring ICT-related incidents that cumulatively meet the conditions for one major ICT-related incident as set out in Arti	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A04-P1	ITS302 Article 4(1)	Applicable	Financial entities shall use secure electronic channels as made available by their competent authority to submit the initial notification and the intermediate and final reports.	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A04-P2	ITS302 Article 4(2)	Applicable	Financial entities that are unable to use the secure electronic channels as made available by their competent authority shall inform their competent authority about a major ICT-rel	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A05-Part_5	ITS302 Article 5(art_5)	Applicable	Where after further assessment, the financial entity concludes that the ICT-related incident previously reported as major, at no time fulfilled the classification criteria and thre	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A06-P1	ITS302 Article 6(1)	Applicable	Financial entities that have outsourced the obligation to report major ICT-related incidents in accordance with Article 19(5) of Regulation (EU) 2022/2554 shall inform their compet	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A06-P2	ITS302 Article 6(2)	Applicable	Financial entities shall provide the competent authority with the name, contact details, and identification code of the third-party that will submit the major ICT-related incident	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A06-P3	ITS302 Article 6(3)	Applicable	Financial entities shall inform their competent authority as soon as they no longer outsource their reporting obligations as referred to in Article 19(5) of Regulation (EU) 2022/25	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P1	ITS302 Article 7(1)	Applicable	A third-party service provider to whom reporting obligations have been outsourced as referred to in Article 19(5) of Regulation (EU) 2022/2554 may use the template set out in Annex	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P1-A	ITS302 Article 7(1)(a)	Applicable	the major ICT-related incident to be reported originates from or is being caused by a third-party ICT service provider;	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P1-B	ITS302 Article 7(1)(b)	Applicable	that third-party service provider provides the relevant ICT service to more than one financial entity, or to a group;	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
ITS302-A07-P1-C	ITS302 Article 7(1)(c)	Applicable	the ICT-related incident is classified as major by each financial entity covered in the aggregated notification or report;	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P1-D	ITS302 Article 7(1)(d)	Applicable	the major ICT-related incident affects financial entities within a single Member State and the aggregated report relates to financial entities which are supervised by the same comp	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P1-E	ITS302 Article 7(1)(e)	Applicable	competent authorities have explicitly permitted this type of financial entities to aggregate their reporting.	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P2	ITS302 Article 7(2)	Applicable	Paragraph 1 shall not apply to credit institutions that are considered to be of significant relevance as referred to in Article 2 point (16) of Regulation (EU) No 468/2014 of the E	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A07-P3	ITS302 Article 7(3)	Applicable	Where competent authorities require information on the individual impact of the major ICT-related incident on a single financial entity, upon request of the competent authority, th	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A08-P1	ITS302 Article 8(1)	Optional	Financial entities that notify significant cyber threats to competent authorities in accordance with Article 19(2) of Regulation (EU) 2022/2554 shall use the template laid down in	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
ITS302-A08-P2	ITS302 Article 8(2)	Optional	Financial entities shall ensure that the information contained in the notification of significant cyber threats is complete and accurate.	D06 — Section 8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS1190-A10	RTS1190 Article 10	Conditional — TLPT designation	Following the approval of the scope specification document by the TLPT authority, the threat intelligence provider shall analyse generic and sector-specific threat intelligence rel	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A11	RTS1190 Article 11	Conditional — TLPT designation	Following approval of the targeted threat intelligence report by the TLPT authority, the testers shall prepare the red team test plan that shall contain the information set out in	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A12	RTS1190 Article 12	Conditional — TLPT designation	Following the end of the active red team testing phase, the control team lead shall inform the blue team that a TLPT took place. Within 4 weeks from the end of the active red team	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A13	RTS1190 Article 13	Conditional — TLPT designation	Within 8 weeks from the notification referred to in Article 12(7) of this Regulation, the financial entity shall provide the remediation plans and the documentation referred to in	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A14	RTS1190 Article 14	Conditional — TLPT designation	The attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall contain the information set out in Annex VIII. Where several TLPT authorities have been involved in	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A15	RTS1190 Article 15	Conditional — TLPT designation	Financial entities shall establish all of the following arrangements for the use of internal testers: The policy referred to in point (a) shall: the establishment and implementatio	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A16	RTS1190 Article 16	Conditional — TLPT designation	For the purposes of conducting a TLPT in relation to a financial entity providing services in more than one Member State, including through a branch, its TLPT authority shall: The	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1190-A02	RTS1190 Article 2	Conditional — TLPT designation	TLPT authorities shall assess whether any financial entity is required to perform TLPT, taking into account the impact of those financial entities, their systemic character and the	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A03	RTS1190 Article 3	Conditional — TLPT designation	A TLPT authority shall assign the responsibility for coordinating TLPT-related activities to a TCT. A TCT shall be composed of test managers that are assigned to oversee an individ	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A04	RTS1190 Article 4	Conditional — TLPT designation	Financial entities shall appoint a control team lead which shall be responsible for the day-to-day management of the TLPT and the decisions and actions of the control team. Financi	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A05	RTS1190 Article 5	Conditional — TLPT designation	During the preparation phase referred to in Article 9, the control team shall assess the risks associated with the testing of live production systems of critical or important funct	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A06	RTS1190 Article 6	Conditional — TLPT designation	In the case of a joint TLPT or a pooled TLPT, the control team of each financial entity shall conduct its own risk assessment and establish its own risk management measures. The co	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A07	RTS1190 Article 7	Conditional — TLPT designation	The control team shall take measures to manage the risks relating to the TLPT and shall in particular ensure that, for each TLPT: the threat intelligence provider and external test	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A08	RTS1190 Article 8	Conditional — TLPT designation	Unless otherwise decided by the lead TLPT authority, where several financial entities, identified in accordance with Article 16(2) or (4), are involved in a pooled or joint TLPT, e	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1190-A09	RTS1190 Article 9	Conditional — TLPT designation	A financial entity identified pursuant to Article 26, paragraph 8, third subparagraph of Regulation (EU) 2022/2554 shall initiate a TLPT following a notification from the TLPT auth	D08 — Appendix C — TLPT activation checklist	Designation monitoring; if activated, a separate TLPT project file
RTS1772-A01-P1	RTS1772 Article 1(1)	Applicable	The number of clients affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, shall reflect the number of all affected clients, whether n	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A01-P2	RTS1772 Article 1(2)	Applicable	The number of financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554 shall reflect the number of all affected fina	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A01-P3	RTS1772 Article 1(3)	Applicable	In relation to the relevance of clients and financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A01-P4	RTS1772 Article 1(4)	Applicable	In relation to the amount or number of transactions affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial entity shall ta	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A01-P5	RTS1772 Article 1(5)	Applicable	Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estim	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A10-Part_10	RTS1772 Article 10(art_10)	Applicable	For the purposes of Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be considered significant where all of the following conditions are fulfilled:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A10-Part_10-2	RTS1772 Article 10(art_10)	Applicable	Where, depending on the type of cyber threat and available information, the financial entity concludes that the materiality thresholds set out in Article 9(2), (3), (5) and (6) cou	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A10-Part_10-A	RTS1772 Article 10(art_10)(a)	Applicable	the cyber threat, if materialised, could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third-part	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A10-Part_10-B	RTS1772 Article 10(art_10)(b)	Applicable	the cyber threat has a high probability of materialisation at the financial entity or at other financial entities, taking into account at least the following elements: (i) applicab	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A10-Part_10-C	RTS1772 Article 10(art_10)(c)	Applicable	the cyber threat could, if materialised, meet any of the following: (i) the criterion regarding criticality of services set out in Article 18(1), point (e), of Regulation (EU) 2022	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A11-Part_11	RTS1772 Article 11(art_11)	Applicable	The assessment of whether the major incident is relevant for competent authorities in other Member States as referred to in Article 19(7) of Regulation (EU) 2022/2554 shall be base	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A11-Part_11-A	RTS1772 Article 11(art_11)(a)	Applicable	clients or financial counterparts;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A11-Part_11-B	RTS1772 Article 11(art_11)(b)	Applicable	a branch of the financial entity or another financial entity within the group;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A11-Part_11-C	RTS1772 Article 11(art_11)(c)	Applicable	a financial market infrastructure or a third-party provider which may affect financial entities to which they provide services.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A12-Part_12	RTS1772 Article 12(art_12)	Applicable	The details of major incidents to be submitted by competent authorities to other competent authorities in accordance with Article 19(6) of Regulation (EU) 2022/2554 and the notific	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A02-P1	RTS1772 Article 2(1)	Applicable	For the purposes of determining the reputational impact of the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, financial entities shall consider	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A02-P1-A	RTS1772 Article 2(1)(a)	Applicable	the incident has been reflected in the media;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A02-P1-B	RTS1772 Article 2(1)(b)	Applicable	the incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A02-P1-C	RTS1772 Article 2(1)(c)	Applicable	the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A02-P1-D	RTS1772 Article 2(1)(d)	Applicable	the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the incident.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A02-P2	RTS1772 Article 2(2)	Applicable	When assessing the reputational impact of the incident, financial entities shall take into account the level of visibility that the incident has gained or is likely to gain in rela	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A03-P1	RTS1772 Article 3(1)	Applicable	Financial entities shall measure the duration of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the incident occurs until the	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A03-P1-2	RTS1772 Article 3(1)	Applicable	Where financial entities are unable to determine the moment when the incident occurred, they shall measure the duration of the incident from the moment it was detected. Where finan	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A03-P1-3	RTS1772 Article 3(1)	Applicable	Where financial entities do not yet know when the incident will be resolved or are unable to verify records in logs or other data sources, they shall apply estimates.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A03-P2	RTS1772 Article 3(2)	Applicable	Financial entities shall measure the service downtime of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the service is fully	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A03-P2-5	RTS1772 Article 3(2)	Applicable	Where financial entities are unable to determine the moment when the service downtime started, they shall measure the service downtime from the moment it was detected.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A04-Part_4	RTS1772 Article 4(art_4)	Applicable	For the purpose of determining the geographical spread with regard to the areas affected by the incident as referred to in Article 18(1), point (c), of Regulation (EU) 2022/2554, f	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A04-Part_4-A	RTS1772 Article 4(art_4)(a)	Applicable	clients and financial counterparts in other Member States;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A04-Part_4-B	RTS1772 Article 4(art_4)(b)	Applicable	branches or other financial entities within the group carrying out activities in other Member States;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A04-Part_4-C	RTS1772 Article 4(art_4)(c)	Applicable	financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services, to the extent such information	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A05-Part_5	RTS1772 Article 5(art_5)	Applicable	For the purpose of determining the data losses that the incident entails as referred to in Article 18(1), point (d), of Regulation (EU) 2022/2554, financial entities shall take int	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A05-Part_5-A	RTS1772 Article 5(art_5)(a)	Applicable	in relation to the availability of data, whether the incident has rendered the data on demand by the financial entity, its clients or its counterparts temporarily or permanently in	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A05-Part_5-B	RTS1772 Article 5(art_5)(b)	Applicable	in relation to the authenticity of data, whether the incident has compromised the trustworthiness of the source of data;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A05-Part_5-C	RTS1772 Article 5(art_5)(c)	Applicable	in relation to the integrity of data, whether the incident has resulted in non-authorised modification of data that has rendered it inaccurate or incomplete;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A05-Part_5-D	RTS1772 Article 5(art_5)(d)	Applicable	in relation to the confidentiality of data, whether the incident has resulted in data having been accessed by or disclosed to an unauthorised party or system.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A06-Part_6	RTS1772 Article 6(art_6)	Applicable	For the purpose of determining the criticality of the services affected as referred to in Article 18(1), point (e), of Regulation (EU) 2022/2554, financial entities shall assess wh	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A06-Part_6-A	RTS1772 Article 6(art_6)(a)	Applicable	affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A06-Part_6-B	RTS1772 Article 6(art_6)(b)	Applicable	affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A06-Part_6-C	RTS1772 Article 6(art_6)(c)	Applicable	constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1	RTS1772 Article 7(1)	Applicable	For the purpose of determining the economic impact of the incident as referred to in Article 18(1), point (f), of Regulation (EU) 2022/2554, financial entities shall, without accou	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-A	RTS1772 Article 7(1)(a)	Applicable	expropriated funds or financial assets for which they are liable, including assets lost to theft;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-B	RTS1772 Article 7(1)(b)	Applicable	costs for replacement or relocation of software, hardware or infrastructure;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-C	RTS1772 Article 7(1)(c)	Applicable	staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-D	RTS1772 Article 7(1)(d)	Applicable	fees due to non-compliance with contractual obligations;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-E	RTS1772 Article 7(1)(e)	Applicable	costs for redress and compensation to customers;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-F	RTS1772 Article 7(1)(f)	Applicable	losses due to forgone revenues;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-G	RTS1772 Article 7(1)(g)	Applicable	costs associated with internal and external communication;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P1-H	RTS1772 Article 7(1)(h)	Applicable	advisory costs, including costs associated with legal counselling, forensic services and remediation services.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A07-P2	RTS1772 Article 7(2)	Applicable	Costs and losses referred to in paragraph 1 shall not include costs that are necessary for the day-to-day operation of the business, in particular the following:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P2-A	RTS1772 Article 7(2)(a)	Applicable	costs for general maintenance of infrastructure, equipment, hardware and software, and costs for keeping skills of staff up to date;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P2-B	RTS1772 Article 7(2)(b)	Applicable	internal or external costs to enhance the business after the incident, including upgrades, improvements and risk assessment initiatives;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P2-C	RTS1772 Article 7(2)(c)	Applicable	insurance premiums.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P3	RTS1772 Article 7(3)	Applicable	Financial entities shall calculate the amounts of costs and losses based on data available at the time of reporting. Where the actual amounts of costs and losses cannot be determin	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A07-P4	RTS1772 Article 7(4)	Applicable	When assessing the economic impact of the incident, financial entities shall sum up the costs and losses referred to in paragraph 1.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P1	RTS1772 Article 8(1)	Applicable	An incident shall be considered a major incident for the purposes of Article 19(1) of Regulation (EU) 2022/2554 where it has affected critical services as referred to in Article 6	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P1-A	RTS1772 Article 8(1)(a)	Applicable	the materiality threshold referred to in Article 9(5), point (b), is met;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P1-B	RTS1772 Article 8(1)(b)	Applicable	two or more of the other materiality thresholds referred to in Articles 9(1) to (6) are met.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P2	RTS1772 Article 8(2)	Applicable	Recurring incidents that individually are not considered a major incident in accordance with paragraph 1 shall be considered as one major incident where they meet all of the follow	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P2-5	RTS1772 Article 8(2)	Applicable	Financial entities shall assess the existence of recurring incidents on a monthly basis.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P2-6	RTS1772 Article 8(2)	Applicable	This paragraph does not apply to microenterprises and to financial entities listed in Article 16(1) of Regulation (EU) 2022/2554.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P2-A	RTS1772 Article 8(2)(a)	Applicable	they have occurred at least twice within 6 months;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A08-P2-B	RTS1772 Article 8(2)(b)	Applicable	they have the same apparent root cause as referred to in Article 20, first subparagraph, point (b) of Regulation (EU) 2022/2554;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A08-P2-C	RTS1772 Article 8(2)(c)	Applicable	they collectively fulfil the criteria for being considered a major incident set out in paragraph 1.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1	RTS1772 Article 9(1)	Applicable	The materiality threshold for the criterion 'clients, financial counterparts and transactions' is met where any of the following conditions are fulfilled:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-2	RTS1772 Article 9(1)	Applicable	Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estim	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-A	RTS1772 Article 9(1)(a)	Applicable	the number of affected clients is higher than 10 % of all clients using the affected service;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-B	RTS1772 Article 9(1)(b)	Applicable	the number of affected clients using the affected service is higher than 100 000;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-C	RTS1772 Article 9(1)(c)	Applicable	the number of affected financial counterparts is higher than 30 % of all financial counterparts carrying out activities related to the provision of the affected service;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-D	RTS1772 Article 9(1)(d)	Applicable	the number of affected transactions is higher than 10 % of the daily average number of transactions carried out by the financial entity related to the affected service;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-E	RTS1772 Article 9(1)(e)	Applicable	the amount of affected transactions is higher than 10 % of the daily average value of transactions carried out by the financial entity related to the affected service;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P1-F	RTS1772 Article 9(1)(f)	Applicable	clients or financial counterparts which have been identified as relevant in accordance with Article 1(3) have been affected.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P2	RTS1772 Article 9(2)	Applicable	The materiality threshold for the criterion 'reputational impact' is met where any of the conditions set out in Article 2, points (a) to (d), are fulfilled.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P3	RTS1772 Article 9(3)	Applicable	The materiality threshold for the criterion 'duration and service downtime' is met where any of the following conditions are fulfilled:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P3-A	RTS1772 Article 9(3)(a)	Applicable	the duration of the incident is longer than 24 hours;	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P3-B	RTS1772 Article 9(3)(b)	Applicable	the service downtime is longer than 2 hours for ICT services that support critical or important functions.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P4	RTS1772 Article 9(4)	Applicable	The materiality threshold for the criterion 'geographical spread' is met where the incident has an impact in two or more Member States in accordance with Article 4.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1772-A09-P5	RTS1772 Article 9(5)	Applicable	The materiality threshold for the criterion 'data losses' is met where any of the following conditions are fulfilled:	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P5-A	RTS1772 Article 9(5)(a)	Applicable	any impact as referred to in Article 5 on the availability, authenticity, integrity or confidentiality of data has or will have an adverse impact on the implementation of the busin	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P5-B	RTS1772 Article 9(5)(b)	Applicable	any successful, malicious and unauthorised access not covered by point (a) occurs to network and information systems, where such access may result in data losses.	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1772-A09-P6	RTS1772 Article 9(6)	Applicable	The materiality threshold for the criterion 'economic impact' is met where the costs and losses incurred by the financial entity due to the incident have exceeded or are likely to	D06 — Section 6 and Annex A — ICT Incident Classification and Escalation Tool	Completed Annex A classification worksheet, threshold evidence, decision approval and reassessment record
RTS1773-A01	RTS1773 Article 1	Not applicable — SNI carve-out	The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'policy') shall take into account the size and t	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A10	RTS1773 Article 10	Not applicable — SNI carve-out	The policy shall contain requirements for a documented exit plan for each contractual arrangement and for the periodic review and testing of the documented exit plan. When establis	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A02	RTS1773 Article 2	Not applicable — SNI carve-out	Where this Regulation applies on a sub-consolidated or consolidated basis, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial s	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A03	RTS1773 Article 3	Not applicable — SNI carve-out	The management body shall review the policy at least once a year and update it where necessary. Changes made to the policy shall be implemented in a timely manner and as soon as it	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A04	RTS1773 Article 4	Not applicable — SNI carve-out	The policy shall specify the requirements, including the rules, the responsibilities and the processes, for each main phase of the lifecycle of the contractual arrangement, coverin	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A05	RTS1773 Article 5	Not applicable — SNI carve-out	The policy shall require that the business needs of the financial entity are defined before a contractual arrangement is concluded. The policy shall require that a risk assessment	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A06	RTS1773 Article 6	Not applicable — SNI carve-out	The policy shall set out an appropriate and proportionate process for selecting and assessing the prospective ICT third-party service providers taking into account whether or not t	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A07	RTS1773 Article 7	Not applicable — SNI carve-out	The policy shall specify the appropriate measures to identify, prevent and manage actual or potential conflicts of interest arising from the use of ICT third-party service provider	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A08	RTS1773 Article 8	Not applicable — SNI carve-out	The policy shall specify that the relevant contractual arrangement are to be in written form and are to include all the elements referred to in Article 30(2) and (3) of Regulation	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30
RTS1773-A09	RTS1773 Article 9	Not applicable — SNI carve-out	The policy shall require that the contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, the performance of ICT third party service provi	D09 — Sections 2–10 — Proportionate lifecycle procedure	Proportionate provider-lifecycle evidence under directly applicable DORA Articles 28–30

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A28-P1	RTS1774 Article 28(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall have in place an internal governance and control framework that ensures an effective and prud	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2	RTS1774 Article 28(2)	Applicable	The financial entities referred to in paragraph 1 shall, as part of their simplified ICT risk management framework, ensure that their management body:	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-A	RTS1774 Article 28(2)(a)	Applicable	bears the overall responsibility for ensuring that the simplified ICT risk management framework allows for the achievement of the financial entity's business strategy in accordance	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-B	RTS1774 Article 28(2)(b)	Applicable	sets clear roles and responsibilities for all ICT-related tasks;	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-C	RTS1774 Article 28(2)(c)	Applicable	sets out information security objectives and ICT requirements;	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-D	RTS1774 Article 28(2)(d)	Applicable	approves, oversees, and periodically reviews: (i) the classification of information assets of the financial entity as referred to in Article 30(1) of this Regulation, the list of m	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-E	RTS1774 Article 28(2)(e)	Applicable	allocates and reviews at least once a year the budget necessary to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, includin	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-F	RTS1774 Article 28(2)(f)	Applicable	specifies and implements the policies and measures included in Chapters I, II and III of this Title to identify, assess and manage the ICT risk the financial entity is exposed to;	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-G	RTS1774 Article 28(2)(g)	Applicable	identifies and implements procedures, ICT protocols, and tools that are necessary to protect all information assets and ICT assets;	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-H	RTS1774 Article 28(2)(h)	Applicable	ensures that the staff of the financial entity is kept up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the fin	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P2-I	RTS1774 Article 28(2)(i)	Applicable	establishes reporting arrangements, including the frequency, form, and content of reporting to the management body on the information security and digital operational resilience.	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P3	RTS1774 Article 28(3)	Applicable	The financial entities referred to in paragraph 1 may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requ	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P4	RTS1774 Article 28(4)	Applicable	The financial entities referred to in paragraph 1 shall ensure an appropriate segregation and the independence of control functions and internal audit functions.	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P5	RTS1774 Article 28(5)	Applicable	The financial entities referred to in paragraph 1 shall ensure that their simplified ICT risk management framework is subject to an internal audit by auditors, in line with the fin	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence
RTS1774-A28-P6	RTS1774 Article 28(6)	Applicable	Based on the outcome of the audit referred to in paragraph 5, the financial entities referred to in paragraph 1 shall ensure the timely verification and remediation of critical ICT	D01 — Section 5 and 9–11 — Governance, reporting, resources and assurance	Board minutes, RACI, reports, budget and assurance evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A29-P1	RTS1774 Article 29(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document, and implement an information security policy in the context of the simplif	D02 — Sections 2–17 — Information security policy and measures	Policy approval and control evidence
RTS1774-A29-P2	RTS1774 Article 29(2)	Applicable	Based on their information security policy referred to in paragraph 1, the financial entities referred to in paragraph 1 shall establish and implement ICT security measures to miti	D02 — Sections 2–17 — Information security policy and measures	Policy approval and control evidence
RTS1774-A29-P2-3	RTS1774 Article 29(2)	Applicable	The ICT security measures shall include all of the measures referred to in Articles 30 to 38.	D02 — Sections 2–17 — Information security policy and measures	Policy approval and control evidence
RTS1774-A30-P1	RTS1774 Article 30(1)	Applicable	As part of the simplified ICT risk management framework referred to in Article 16(1), point (a), of Regulation (EU) 2022/2554, the financial entities referred to in paragraph 1 of	D04 — Functions, Assets, Providers and Dependencies worksheets	Current inventories and classifications
RTS1774-A30-P2	RTS1774 Article 30(2)	Applicable	The financial entities referred to in paragraph 1 shall identify all critical or important functions supported by ICT third-party service providers.	D04 — Functions, Assets, Providers and Dependencies worksheets	Current inventories and classifications
RTS1774-A31-P1	RTS1774 Article 31(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall include in their simplified ICT risk management framework all of the following:	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P1-A	RTS1774 Article 31(1)(a)	Applicable	a determination of the risk tolerance levels for ICT risk, in accordance with the risk appetite of the financial entity;	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P1-B	RTS1774 Article 31(1)(b)	Applicable	the identification and assessment of the ICT risks to which the financial entity is exposed;	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P1-C	RTS1774 Article 31(1)(c)	Applicable	the specification of mitigation strategies at least for the ICT risks that are not within the risk tolerance levels of the financial entity;	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P1-D	RTS1774 Article 31(1)(d)	Applicable	the monitoring of the effectiveness of the mitigation strategies referred to in point (c);	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P1-E	RTS1774 Article 31(1)(e)	Applicable	the identification and assessment of any ICT and information security risks resulting from any major change in ICT system or ICT services, processes, or procedures, and from ICT se	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P2	RTS1774 Article 31(2)	Applicable	The financial entities referred to in paragraph 1 shall carry out and document the ICT risk assessment periodically commensurate to the financial entities' ICT risk profile.	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P3	RTS1774 Article 31(3)	Applicable	The financial entities referred to in paragraph 1 shall continuously monitor threats and vulnerabilities that are relevant to their critical or important functions, and information	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A31-P4	RTS1774 Article 31(4)	Applicable	The financial entities referred to in paragraph 1 shall set out alert thresholds and criteria to trigger and initiate ICT-related incident response processes.	D03 — Risk Methodology and Risk Register worksheets	Risk records and accepted treatment decisions
RTS1774-A32-P1	RTS1774 Article 32(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify and implement physical security measures designed on the basis of the threat landsca	D02 — Section 7 — Physical and environmental security	Physical-security evidence
RTS1774-A32-P2	RTS1774 Article 32(2)	Applicable	The measures referred to in paragraph 1 shall protect the premises of financial entities and, where applicable, data centres of financial entities where ICT assets and information	D02 — Section 7 — Physical and environmental security	Physical-security evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A32-P3	RTS1774 Article 32(3)	Applicable	The protection from environmental threats and hazards shall be commensurate with the importance of the premises concerned and, where applicable, the data centres and the criticalit	D02 — Section 7 — Physical and environmental security	Physical-security evidence
RTS1774-A33-Part_33	RTS1774 Article 33(art_33)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document, and implement procedures for the control of logical and physical access an	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-2	RTS1774 Article 33(art_33)	Applicable	For the purposes of point (c), the financial entity shall assign privileged, emergency, and administrator access on a need-to-use or an ad-hoc basis for all ICT systems, and shall	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-3	RTS1774 Article 33(art_33)	Applicable	For the purposes of point (d), financial entities shall use strong authentication methods that are based on leading practices for remote access to the financial entities' network,	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-A	RTS1774 Article 33(art_33)(a)	Applicable	access rights to information assets, ICT assets, and their supported functions, and to critical locations of operation of the financial entity, are managed on a need-to-know, need-	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-B	RTS1774 Article 33(art_33)(b)	Applicable	user accountability, which ensures that users can be identified for the actions performed in the ICT systems;	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-C	RTS1774 Article 33(art_33)(c)	Applicable	account management procedures to grant, change, or revoke access rights for user and generic accounts, including generic administrator accounts;	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-D	RTS1774 Article 33(art_33)(d)	Applicable	authentication methods that are commensurate to the classification referred to in Article 30(1) and to the overall risk profile of ICT assets, and which are based on leading practi	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A33-Part_33-E	RTS1774 Article 33(art_33)(e)	Applicable	access rights are periodically reviewed and are withdrawn when no longer required.	D02 — Sections 5–6 — Identity, access and privileged access	Access records and reviews
RTS1774-A34-Part_34	RTS1774 Article 34(art_34)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall, as part of their systems, protocols, and tools, and for all ICT assets:	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-2	RTS1774 Article 34(art_34)	Applicable	For the purposes of point (f), financial entities shall align the level of detail of the logs with their purpose and usage of the ICT asset producing those logs.	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-A	RTS1774 Article 34(art_34)(a)	Applicable	monitor and manage the lifecycle of all ICT assets;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-B	RTS1774 Article 34(art_34)(b)	Applicable	monitor whether the ICT assets are supported by ICT third-party service providers of financial entities, where applicable;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-C	RTS1774 Article 34(art_34)(c)	Applicable	identify capacity requirements of their ICT assets and measures to maintain and improve the availability and efficiency of ICT systems and prevent ICT capacity shortages before the	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-D	RTS1774 Article 34(art_34)(d)	Applicable	perform automated vulnerability scanning and assessments of ICT assets commensurate to their classification as referred to in Article 30(1) and to the overall risk profile of the I	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A34-Part_34-E	RTS1774 Article 34(art_34)(e)	Applicable	manage the risks related to outdated, unsupported, or legacy ICT assets;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-F	RTS1774 Article 34(art_34)(f)	Applicable	log events related to logical and physical access control, ICT operations, including system and network traffic activities, and ICT change management;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-G	RTS1774 Article 34(art_34)(g)	Applicable	identify and implement measures to monitor and analyse information on anomalous activities and behaviour for critical or important ICT operations;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-H	RTS1774 Article 34(art_34)(h)	Applicable	implement measures to monitor relevant and up-to-date information about cyber threats;	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A34-Part_34-I	RTS1774 Article 34(art_34)(i)	Applicable	implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware, and check for	D02 — Sections 8–10 — ICT operations, vulnerabilities, patching and logging	Operations, patching and log evidence
RTS1774-A35-Part_35	RTS1774 Article 35(art_35)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall, as part of their systems, protocols, and tools, develop and implement safeguards that ensure	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-A	RTS1774 Article 35(art_35)(a)	Applicable	the identification and implementation of measures to protect data in use, in transit, and at rest;	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-B	RTS1774 Article 35(art_35)(b)	Applicable	the identification and implementation of security measures regarding the use of software, data storage media, systems and endpoint devices that transfer and store data of the finan	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-C	RTS1774 Article 35(art_35)(c)	Applicable	the identification and implementation of measures to prevent and detect unauthorised connections to the financial entity's network, and to secure the network traffic between the fi	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-D	RTS1774 Article 35(art_35)(d)	Applicable	the identification and implementation of measures that ensure the availability, authenticity, integrity, and confidentiality of data during network transmissions;	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-E	RTS1774 Article 35(art_35)(e)	Applicable	a process to securely delete data on premises, or that are stored externally, that the financial entity no longer needs to collect or store;	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-F	RTS1774 Article 35(art_35)(f)	Applicable	a process to securely dispose of, or decommission, data storage devices on premises, or data storage devices that are stored externally, that contain confidential information;	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A35-Part_35-G	RTS1774 Article 35(art_35)(g)	Applicable	the identification and implementation of measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the financial entity's ability to car	D02 — Sections 11–12 — Data, system, network and endpoint security	Configuration and security evidence
RTS1774-A36-P1	RTS1774 Article 36(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall establish and implement an ICT security testing plan to validate the effectiveness of their I	D08 — Sections 3–8 — ICT security testing	Test plans, reports and remediation
RTS1774-A36-P2	RTS1774 Article 36(2)	Applicable	The financial entities referred to in paragraph 1 shall review, asses and test ICT security measures, taking into consideration the overall risk profile of the ICT assets of the fi	D08 — Sections 3–8 — ICT security testing	Test plans, reports and remediation

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A36-P3	RTS1774 Article 36(3)	Applicable	The financial entities referred to in paragraph 1 shall monitor and evaluate the results of the security tests and update their security measures accordingly without undue delay in	D08 — Sections 3–8 — ICT security testing	Test plans, reports and remediation
RTS1774-A37-Part_37	RTS1774 Article 37(art_37)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall design and implement, where appropriate, a procedure governing the acquisition, development,	D02 — Section 14 — ICT acquisition, development and maintenance	Acquisition and supplier-assurance records
RTS1774-A37-Part_37-A	RTS1774 Article 37(art_37)(a)	Applicable	ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements, including information security requirements, are clea	D02 — Section 14 — ICT acquisition, development and maintenance	Acquisition and supplier-assurance records
RTS1774-A37-Part_37-B	RTS1774 Article 37(art_37)(b)	Applicable	ensure the testing and approval of ICT systems prior to their first use and before introducing changes to the production environment;	D02 — Section 14 — ICT acquisition, development and maintenance	Acquisition and supplier-assurance records
RTS1774-A37-Part_37-C	RTS1774 Article 37(art_37)(c)	Applicable	identify measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environmen	D02 — Section 14 — ICT acquisition, development and maintenance	Acquisition and supplier-assurance records
RTS1774-A38-P1	RTS1774 Article 38(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document, and implement an ICT project management procedure and shall specify the ro	D02 — Section 15 — Project and change management	Project/change approvals and test evidence
RTS1774-A38-P2	RTS1774 Article 38(2)	Applicable	The financial entities referred to in paragraph 1 shall develop, document, and implement an ICT change management procedure to ensure that all changes to ICT systems are recorded,	D02 — Section 15 — Project and change management	Project/change approvals and test evidence
RTS1774-A39-P1	RTS1774 Article 39(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop their ICT business continuity plans considering the results of the analysis of their	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2	RTS1774 Article 39(2)	Applicable	The ICT business continuity plans referred to in paragraph 1 shall:	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-3	RTS1774 Article 39(2)	Applicable	For the purposes of point (f), the measures referred to in that point shall provide for the mitigation of failures of critical third-party providers.	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-A	RTS1774 Article 39(2)(a)	Applicable	be approved by the management body of the financial entity;	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-B	RTS1774 Article 39(2)(b)	Applicable	be documented and readily accessible in the event of an emergency or crisis;	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-C	RTS1774 Article 39(2)(c)	Applicable	allocate sufficient resources for their execution;	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-D	RTS1774 Article 39(2)(d)	Applicable	establish planned recovery levels and timeframes for the recovery and resumption of functions and key internal and external dependencies, including ICT third-party service provider	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-E	RTS1774 Article 39(2)(e)	Applicable	identify the conditions that may prompt the activation of the ICT business continuity plans and what actions are to be taken to ensure the availability, continuity, and recovery of	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-F	RTS1774 Article 39(2)(f)	Applicable	identify the restoration and recovery measures for critical or important business functions, supporting processes, information assets, and their interdependencies to avoid adverse	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A39-P2-G	RTS1774 Article 39(2)(g)	Applicable	identify backup procedures and measures that specify the scope of the data that are subject to the backup, and the minimum frequency of the backup, based on the criticality of the	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-H	RTS1774 Article 39(2)(h)	Applicable	consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics, or unforeseen circumstances;	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-I	RTS1774 Article 39(2)(i)	Applicable	specify the internal and external communication arrangements, including escalation plans;	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A39-P2-J	RTS1774 Article 39(2)(j)	Applicable	be updated in line with lessons learned from incidents, tests, new risks, and threats identified, changed recovery objectives, major changes to the financial entity's organisation,	D05 — Sections 4–10 — ICT business continuity components	Approved and actionable continuity/recovery plan
RTS1774-A40-P1	RTS1774 Article 40(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall test their business continuity plans referred to in Article 39 of this Regulation, including	D08 — Section 5 and continuity test scripts	Continuity test reports and remediation
RTS1774-A40-P2	RTS1774 Article 40(2)	Applicable	The testing of business continuity plans referred to in paragraph 1 shall demonstrate that the financial entities referred to in that paragraph are able to sustain the viability of	D08 — Section 5 and continuity test scripts	Continuity test reports and remediation
RTS1774-A40-P3	RTS1774 Article 40(3)	Applicable	The financial entities referred to in paragraph 1 shall document the results of the testing of business continuity plans and any identified deficiencies resulting from that testing	D08 — Section 5 and continuity test scripts	Continuity test reports and remediation
RTS1774-A41-P1	RTS1774 Article 41(1)	Applicable	The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall submit the report on the review of the ICT risk management framework referred to in paragraph	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2	RTS1774 Article 41(2)	Applicable	The report referred to in paragraph 1 shall contain all of the following information:	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-A	RTS1774 Article 41(2)(a)	Applicable	an introductory section providing: (i) a description of the context of the report in terms of the nature, scale, and complexity of the financial entity's services, activities, and	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-B	RTS1774 Article 41(2)(b)	Applicable	where applicable, the date of the approval of the report by the management body of the financial entity;	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-C	RTS1774 Article 41(2)(c)	Applicable	a description of the reasons for the review, including: (i) where the review has been initiated following supervisory instructions, evidence of such instructions; (ii) where the re	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-D	RTS1774 Article 41(2)(d)	Applicable	the start and end date of the review period;	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-E	RTS1774 Article 41(2)(e)	Applicable	the person responsible for the review;	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-F	RTS1774 Article 41(2)(f)	Applicable	a summary of findings, and a self-assessment of the severity of the weaknesses, deficiencies, and gaps identified in ICT risk management framework for the review period, including	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS1774-A41-P2-G	RTS1774 Article 41(2)(g)	Applicable	remedying measures identified to address weaknesses, deficiencies, and gaps in the simplified ICT risk management framework, and the expected date for implementing those measures,	D13 — Part B — Article 41 review report template	Approved review report and action plan

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS1774-A41-P2-H	RTS1774 Article 41(2)(h)	Applicable	overall conclusions on the review of the simplified ICT risk management framework, including any further planned developments.	D13 — Part B — Article 41 review report template	Approved review report and action plan
RTS301-A01-Part_1	RTS301 Article 1(art_1)	Applicable	Financial entities shall include in the initial notification, the intermediate report, and the final report, as referred to in Article 19(4) of Regulation (EU) 2022/2554, the follo	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-A	RTS301 Article 1(art_1)(a)	Applicable	the type of submission (initial notification, intermediate report, or final report);	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-B	RTS301 Article 1(art_1)(b)	Applicable	the name of the financial entity, its LEI code, and the type of financial entity, as referred to in Article 2(1) of Regulation (EU) 2022/2554;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-C	RTS301 Article 1(art_1)(c)	Applicable	the name and identification code of the entity that submits the initial notification, or intermediate or final report, for the financial entity;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-D	RTS301 Article 1(art_1)(d)	Applicable	where applicable, the names and LEI codes of all financial entities covered in the aggregated initial notification or intermediate or final report;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-E	RTS301 Article 1(art_1)(e)	Applicable	the contact details of the persons responsible for communicating with the competent authority on the major ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-F	RTS301 Article 1(art_1)(f)	Applicable	where applicable, the identification of the parent undertaking of the group to which the financial entity belongs;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A01-Part_1-G	RTS301 Article 1(art_1)(g)	Applicable	where there is monetary impact, the currency the amounts are based on.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2	RTS301 Article 2(art_2)	Applicable	Initial notifications as referred to in Article 19(4), point (a), of Regulation (EU) 2022/2554 shall contain at least all of the following specific information:	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-A	RTS301 Article 2(art_2)(a)	Applicable	the incident reference code assigned by the financial entity;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-B	RTS301 Article 2(art_2)(b)	Applicable	the date of detection, time of detection, and classification of the incident pursuant to Article 8 of Commission Delegated Regulation (EU) 2024/1772 (7) ;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-C	RTS301 Article 2(art_2)(c)	Applicable	a description of the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-D	RTS301 Article 2(art_2)(d)	Applicable	the criteria, laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772, on the basis of which the financial entity classified the ICT-related incident as major;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS301-A02-Part_2-E	RTS301 Article 2(art_2)(e)	Applicable	the Members States that are impacted by the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-F	RTS301 Article 2(art_2)(f)	Applicable	information on how the ICT-related incident was discovered;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-G	RTS301 Article 2(art_2)(g)	Applicable	where available, information about the origin of the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-H	RTS301 Article 2(art_2)(h)	Applicable	information about whether the financial entity has activated a business continuity plan;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-I	RTS301 Article 2(art_2)(i)	Applicable	where applicable, information about the reclassification of the ICT-related incident from major to non-major;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A02-Part_2-J	RTS301 Article 2(art_2)(j)	Applicable	where available, any other relevant information.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3	RTS301 Article 3(art_3)	Applicable	Intermediate reports as referred to in Article 19(4), point (b), of Regulation (EU) 2022/2554 shall contain at least all of the following specific information:	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-A	RTS301 Article 3(art_3)(a)	Applicable	where applicable, the incident reference code provided by the competent authority;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-B	RTS301 Article 3(art_3)(b)	Applicable	the date and time of occurrence of the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-C	RTS301 Article 3(art_3)(c)	Applicable	where applicable, the date and time when the financial entity has recovered its regular activities;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-D	RTS301 Article 3(art_3)(d)	Applicable	information about how the criteria laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772 have been fulfilled, on the basis of which the financial entity classified th	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-E	RTS301 Article 3(art_3)(e)	Applicable	the type of ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-F	RTS301 Article 3(art_3)(f)	Applicable	where applicable, the threats and techniques used by the threat actor;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-G	RTS301 Article 3(art_3)(g)	Applicable	affected functional areas and business processes;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS301-A03-Part_3-H	RTS301 Article 3(art_3)(h)	Applicable	affected infrastructure components supporting business processes;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-I	RTS301 Article 3(art_3)(i)	Applicable	impact on the financial interest of clients;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-J	RTS301 Article 3(art_3)(j)	Applicable	information about reporting about the ICT-related incident to other authorities;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-K	RTS301 Article 3(art_3)(k)	Applicable	temporary actions or measures taken or planned to be taken by the financial entity to recover from the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A03-Part_3-L	RTS301 Article 3(art_3)(l)	Applicable	where applicable, information on indicators of compromise.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4	RTS301 Article 4(art_4)	Applicable	Final reports as referred to in Article 19(4), point (c), of Regulation (EU) 2022/2554 shall contain all of the following specific information:	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-A	RTS301 Article 4(art_4)(a)	Applicable	information about the root causes of the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-B	RTS301 Article 4(art_4)(b)	Applicable	dates and times when the ICT-related incident was resolved and the root cause(s) addressed;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-C	RTS301 Article 4(art_4)(c)	Applicable	information on the resolution of the ICT-related incident;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-D	RTS301 Article 4(art_4)(d)	Applicable	where applicable, information relevant for resolution authorities;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-E	RTS301 Article 4(art_4)(e)	Applicable	information about direct and indirect costs and losses stemming from the ICT-related incident and information about financial recoveries;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A04-Part_4-F	RTS301 Article 4(art_4)(f)	Applicable	where applicable, information about recurring ICT-related incidents.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P1	RTS301 Article 5(1)	Applicable	Financial entities shall submit the initial notification and the intermediate and final reports as referred to in Article 19(4), points (a), (b) and (c), of Regulation (EU) 2022/25	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P1-A	RTS301 Article 5(1)(a)	Applicable	for the initial report: as early as possible, but in any case, within four hours from the classification of the ICT-related incident as a major ICT-related incident and no later th	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS301-A05-P1-B	RTS301 Article 5(1)(b)	Applicable	for the intermediate report: at the latest within 72 hours from the submission of the initial notification, even where the status or the handling of the incident have not changed a	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P1-C	RTS301 Article 5(1)(c)	Applicable	for the final report: no later than one month after either the submission of the intermediate report, or, where applicable, after the latest updated intermediate report.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P2	RTS301 Article 5(2)	Applicable	Where the financial entity has not classified an ICT-related incident as major within 24 hours from the moment the financial entity has become aware of the ITC-related incident but	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P3	RTS301 Article 5(3)	Applicable	Financial entities that are unable to submit the initial notification, intermediate report, or final report within the time limits set out in paragraph 1, shall inform the competen	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P4	RTS301 Article 5(4)	Applicable	Where the time limit for the submission of an initial notification, intermediate report, or a final report falls on a weekend day or a bank holiday in the Member State of the repor	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P5	RTS301 Article 5(5)	Applicable	Paragraph 4 shall not apply for the submission of an initial notification or an intermediate report by credit institutions, central counterparties, operators of trading venues, and	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A05-P6	RTS301 Article 5(6)	Applicable	Competent authorities may decide that paragraph 4 shall not apply for the submission of an initial notification or an intermediate report by financial entities, other than those re	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6	RTS301 Article 6(art_6)	Optional	The content of the voluntary notification in relation to significant cyber threats as referred to in Article 19(2) of Regulation (EU) 2022/2554 shall cover all of the following:	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-A	RTS301 Article 6(art_6)(a)	Optional	general information about the notifying financial entity as set out in Article 1;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-B	RTS301 Article 6(art_6)(b)	Optional	the date and time of detection of the significant cyber threat and any other relevant timestamps related to the significant cyber threat;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-C	RTS301 Article 6(art_6)(c)	Optional	a description of the significant cyber threat;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-D	RTS301 Article 6(art_6)(d)	Optional	information about the potential impact of the significant cyber threat on the financial entity, its clients, or financial counterparts;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-E	RTS301 Article 6(art_6)(e)	Optional	the classification criteria that would have triggered a major incident report laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772 if the cyber threat had materialis	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-F	RTS301 Article 6(art_6)(f)	Optional	information about the status of the significant cyber threat and any changes in the threat activity;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS301-A06-Part_6-G	RTS301 Article 6(art_6)(g)	Optional	where applicable, a description of the actions taken by the financial entity to prevent the materialisation of the significant cyber threats;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-H	RTS301 Article 6(art_6)(h)	Optional	information about any notification of the significant cyber threat to other financial entities or authorities;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-I	RTS301 Article 6(art_6)(i)	Optional	where applicable, information on indicators of compromise;	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS301-A06-Part_6-J	RTS301 Article 6(art_6)(j)	Optional	where available, any other relevant information.	D06 — Sections 7–8 and Annex B — Regulatory Reporting Pack and Submission Runbook	Completed reporting schedules, reviewed submission, portal receipt, acknowledgement and follow-up record
RTS532-A01-Part_1	RTS532 Article 1(art_1)	Applicable	Financial entities shall take into account their size and their overall risk profile and the nature, scale, and elements of increased or reduced complexity of their services, activ	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-A	RTS532 Article 1(art_1)(a)	Applicable	the type of ICT services that support critical or important functions covered by the contractual arrangement between the financial entity and the ICT third-party service provider;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-B	RTS532 Article 1(art_1)(b)	Applicable	the type of ICT services covered by the contractual arrangement between the ICT-third party service provider and its subcontractors;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-C	RTS532 Article 1(art_1)(c)	Applicable	the location of the ICT subcontractor providing ICT services that support critical or important functions or a material part thereof, or of its parent company;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-D	RTS532 Article 1(art_1)(d)	Applicable	the length and complexity of the chain of subcontractors providing ICT services that support critical or important functions or material parts thereof used by the ICT third-party s	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-E	RTS532 Article 1(art_1)(e)	Applicable	the nature of the data shared with the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-F	RTS532 Article 1(art_1)(f)	Applicable	whether the ICT services that support critical or important functions or material parts thereof are provided by subcontractors, located within a Member State or in a third country,	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-G	RTS532 Article 1(art_1)(g)	Applicable	whether the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof are part of the same group as the financial entity to w	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-H	RTS532 Article 1(art_1)(h)	Applicable	whether the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof are authorised, registered or subject to supervision or	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-I	RTS532 Article 1(art_1)(i)	Applicable	whether the ICT third-party service providers that support critical or important functions or material parts thereof are authorised, registered or subject to supervision or oversig	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS532-A01-Part_1-J	RTS532 Article 1(art_1)(j)	Applicable	whether the provision of ICT services supporting critical or important functions or material parts thereof is concentrated to a single subcontractor of an ICT third-party service p	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-K	RTS532 Article 1(art_1)(k)	Applicable	whether the subcontracting of ICT services that support critical or important functions or material parts would impact the transferability of those ICT services to another ICT thir	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A01-Part_1-L	RTS532 Article 1(art_1)(l)	Applicable	the potential impact of disruptions on the continuity and availability of the ICT services that support critical or important functions or material parts thereof provided by the IC	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A02-Part_2	RTS532 Article 2(art_2)	Conditional	Where this Regulation applies on a sub-consolidated or consolidated basis, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial s	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1	RTS532 Article 3(1)	Applicable	A financial entity shall, before entering into a contractual arrangement with an ICT third-party service provider, decide whether that ICT third-party service provider may subcontr	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-A	RTS532 Article 3(1)(a)	Applicable	the due diligence processes on the ICT third-party service provider ensure that it is able to select and assess the operational and financial abilities of potential ICT subcontract	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-B	RTS532 Article 3(1)(b)	Applicable	the ICT third-party service provider is able to identify all subcontractors that provide ICT services that support critical or important functions or material parts thereof, to not	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-C	RTS532 Article 3(1)(c)	Applicable	the ICT third-party service provider ensures that the contractual arrangements with the subcontractors that provide ICT services that support critical or important functions or mat	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-D	RTS532 Article 3(1)(d)	Applicable	the subcontractor grants the financial entity and competent and resolution authorities the same contractual rights of access and inspection as those granted by the ICT third-party	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-E	RTS532 Article 3(1)(e)	Applicable	without prejudice to the financial entity's final responsibility to comply with its legal and regulatory obligations, the ICT third-party service provider itself has sufficient abi	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-F	RTS532 Article 3(1)(f)	Applicable	the financial entity has sufficient abilities, expertise, and adequate financial, human and technical resources to monitor the ICT risks relating to the service supporting critical	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-G	RTS532 Article 3(1)(g)	Applicable	the financial entity has assessed the impact on the financial entity's digital operational resilience and financial soundness of a possible failure of a subcontractor that provides	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-H	RTS532 Article 3(1)(h)	Applicable	the financial entity has assessed the risks associated with the location of the potential subcontractors in relation to the ICT services that support critical or important function	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P1-I	RTS532 Article 3(1)(i)	Applicable	the financial entity has assessed the ICT concentration risks at entity level in accordance with Article 29 of Regulation (EU) 2022/2554;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS532-A03-P1-J	RTS532 Article 3(1)(j)	Applicable	the financial entity has assessed whether there are any obstacles to the exercise of audit, inspection and access rights by the competent authorities, resolution authorities, or th	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P2	RTS532 Article 3(2)	Applicable	Financial entities that use ICT third-party service providers that subcontract ICT services that support critical or important functions or material parts thereof shall periodicall	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A03-P3	RTS532 Article 3(3)	Applicable	Reliance on the results of the risk assessment carried out by their ICT third-party service providers on their subcontractors in complying with the obligations set out in this arti	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1	RTS532 Article 4(1)	Applicable	The contractual arrangement concluded between the financial entity and the ICT third-party service provider shall identify which ICT services that support critical or important fun	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-A	RTS532 Article 4(1)(a)	Applicable	that the ICT third-party service provider is responsible for the provision of the services provided by the subcontractors;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-B	RTS532 Article 4(1)(b)	Applicable	that the ICT third-party service provider is required to monitor all subcontracted ICT services that support critical or important functions or material parts thereof to ensure tha	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-C	RTS532 Article 4(1)(c)	Applicable	the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity regarding subcontractors that provide ICT services that support critic	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-D	RTS532 Article 4(1)(d)	Applicable	that the ICT third-party service provider is to assess all risks associated with the location of the current or potential subcontractors that provide ICT service that support criti	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-E	RTS532 Article 4(1)(e)	Applicable	the location of data processed or stored by the subcontractor, where relevant;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-F	RTS532 Article 4(1)(f)	Applicable	that the ICT third-party service provider is to specify in its contract with its subcontractors the monitoring and reporting obligations of that subcontractor towards the ICT third	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-G	RTS532 Article 4(1)(g)	Applicable	that the ICT third-party service provider is to ensure the continuity of the ICT services that support critical or important functions throughout the chain of subcontractors in cas	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-H	RTS532 Article 4(1)(h)	Applicable	that the contractual arrangement between the ICT third-party service provider and its subcontractors contains the requirements on business contingency plans referred to in Article	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-I	RTS532 Article 4(1)(i)	Applicable	that the contractual arrangement between the ICT third-party service provider and its subcontractors specifies the ICT security standards and any additional security requirements r	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-J	RTS532 Article 4(1)(j)	Applicable	that the subcontractor is to grant to the financial entity and relevant competent and resolution authorities the same rights of access, inspection, and audit as those referred to i	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS532-A04-P1-K	RTS532 Article 4(1)(k)	Applicable	that the ICT third-party service provider is to notify the financial entity of any material change to subcontracting arrangements;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P1-L	RTS532 Article 4(1)(l)	Applicable	that the financial entity has the right to terminate the contract with the ICT third-party service provider when the conditions laid down in either Article 6 of this Regulation or	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A04-P2	RTS532 Article 4(2)	Applicable	Changes relative to contractual agreements between the financial entity and ICT third-party service providers that provide an ICT service supporting critical or important functions	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P1	RTS532 Article 5(1)	Applicable	The contractual arrangement shall provide that the ICT third-party service provider shall inform the financial entity about any intended material changes to its subcontracting arra	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P1-A	RTS532 Article 5(1)(a)	Applicable	the impact on the risks it is or might be exposed to;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P1-B	RTS532 Article 5(1)(b)	Applicable	whether such material changes might affect the ability of the ICT third-party service provider to meet its contractual obligations vis-a-vis the financial entity.	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P2	RTS532 Article 5(2)	Applicable	The contractual arrangement shall contain a reasonable notice period by which the financial entity is to approve or object to the changes.	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P3	RTS532 Article 5(3)	Applicable	The ICT third-party service provider shall only implement the material changes to its subcontracting arrangements after the financial entity has either approved or not objected to	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P4	RTS532 Article 5(4)	Applicable	Where the financial entity is of the opinion that the material changes referred to in paragraph 1 exceed the financial entity's risk tolerance, the financial entity shall, before t	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P4-A	RTS532 Article 5(4)(a)	Applicable	inform the ICT third-party service provider thereof;	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A05-P4-B	RTS532 Article 5(4)(b)	Applicable	object to the changes and request modifications to those changes before they are implemented.	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A06-Part_6	RTS532 Article 6(art_6)	Applicable	The financial entity shall have the right to provide in the contractual arrangement with the ICT third-party service provider that the contractual arrangement is to terminate in ea	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A06-Part_6-A	RTS532 Article 6(art_6)(a)	Applicable	the financial entity has objected to material changes to the subcontracting arrangements supporting critical or important functions and requested for modifications to those arrange	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record
RTS532-A06-Part_6-B	RTS532 Article 6(art_6)(b)	Applicable	the ICT third-party service provider has implemented material changes to subcontracting arrangements supporting critical or important functions or material parts thereof before the	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record

Requirement ID	Legal reference	Applicability	Requirement	Primary deliverable / exact location	Required evidence
RTS532-A06-Part_6-C	RTS532 Article 6(art_6)(c)	Applicable	the ICT third-party service provider subcontracts an ICT service that supports a critical or important function or material part thereof not explicitly permitted to be subcontracte	D11 — Part E — Subcontracting assessment and contract controls	Subcontractor due diligence, supply-chain mapping, notices and termination/exit record

Appendix B — Applicability conclusions requiring confirmation

ID	Reference	Status	Rationale / open point
DORA-A19-P5	DORA Article 19(5)	Optional	Voluntary notification of significant cyber threats.
DORA-A20-Part_20	DORA Article 20(art_20)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A20-Part_20-2	DORA Article 20(art_20)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A20-Part_20-3	DORA Article 20(art_20)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A20-Part_20-4	DORA Article 20(art_20)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A20-Part_20-A	DORA Article 20(art_20)(a)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A20-Part_20-B	DORA Article 20(art_20)(b)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P1	DORA Article 21(1)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2	DORA Article 21(2)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-A	DORA Article 21(2)(a)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-B	DORA Article 21(2)(b)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-C	DORA Article 21(2)(c)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-D	DORA Article 21(2)(d)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-E	DORA Article 21(2)(e)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-F	DORA Article 21(2)(f)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P2-G	DORA Article 21(2)(g)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A21-P3	DORA Article 21(3)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A22-P1	DORA Article 22(1)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A22-P2	DORA Article 22(2)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.
DORA-A22-P2-3	DORA Article 22(2)	No direct entity obligation	Provision primarily directs the ESAs or competent authorities; reflected only as context.

ID	Reference	Status	Rationale / open point
DORA-A23-Part_23	DORA Article 23(art_23)	Conditional	Relevant only to operational or security payment-related incidents where the firm provides payment services. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P1	DORA Article 26(1)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P10	DORA Article 26(10)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11	DORA Article 26(11)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-22	DORA Article 26(11)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-23	DORA Article 26(11)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-24	DORA Article 26(11)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-A	DORA Article 26(11)(a)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-B	DORA Article 26(11)(b)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-C	DORA Article 26(11)(c)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P11-D	DORA Article 26(11)(d)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P2	DORA Article 26(2)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P2-3	DORA Article 26(2)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P2-4	DORA Article 26(2)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P3	DORA Article 26(3)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P4	DORA Article 26(4)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P4-7	DORA Article 26(4)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P4-8	DORA Article 26(4)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.

ID	Reference	Status	Rationale / open point
DORA-A26-P5	DORA Article 26(5)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P6	DORA Article 26(6)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P7	DORA Article 26(7)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P7-12	DORA Article 26(7)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8	DORA Article 26(8)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8-14	DORA Article 26(8)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8-15	DORA Article 26(8)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8-A	DORA Article 26(8)(a)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8-B	DORA Article 26(8)(b)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P8-C	DORA Article 26(8)(c)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A26-P9	DORA Article 26(9)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1	DORA Article 27(1)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1-A	DORA Article 27(1)(a)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1-B	DORA Article 27(1)(b)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1-C	DORA Article 27(1)(c)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1-D	DORA Article 27(1)(d)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P1-E	DORA Article 27(1)(e)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P2	DORA Article 27(2)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.

ID	Reference	Status	Rationale / open point
DORA-A27-P2-A	DORA Article 27(2)(a)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P2-B	DORA Article 27(2)(b)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P2-C	DORA Article 27(2)(c)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A27-P3	DORA Article 27(3)	Conditional	Applies only if the firm is identified or otherwise required to perform TLPT; designation is not assumed for an SNI firm. Confirm entity facts and operating model; tailor implementation and evidence.
DORA-A28-P2	DORA Article 28(2)	Not applicable — SNI carve-out	Article 28(2) expressly excludes entities referred to in Article 16(1), first subparagraph, from the formal strategy/policy requirement.
DORA-A45-P1	DORA Article 45(1)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
DORA-A45-P1-A	DORA Article 45(1)(a)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
DORA-A45-P1-B	DORA Article 45(1)(b)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
DORA-A45-P1-C	DORA Article 45(1)(c)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
DORA-A45-P2	DORA Article 45(2)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
DORA-A45-P3	DORA Article 45(3)	Optional	Participation in cyber-threat information-sharing arrangements is voluntary, subject to conditions and notification.
ITS302-A08-P1	ITS302 Article 8(1)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
ITS302-A08-P2	ITS302 Article 8(2)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS1190-A10	RTS1190 Article 10	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A11	RTS1190 Article 11	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A12	RTS1190 Article 12	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A13	RTS1190 Article 13	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A14	RTS1190 Article 14	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A15	RTS1190 Article 15	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A16	RTS1190 Article 16	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A02	RTS1190 Article 2	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A03	RTS1190 Article 3	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A04	RTS1190 Article 4	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A05	RTS1190 Article 5	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A06	RTS1190 Article 6	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.

ID	Reference	Status	Rationale / open point
RTS1190-A07	RTS1190 Article 7	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A08	RTS1190 Article 8	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1190-A09	RTS1190 Article 9	Conditional — TLPT designation	Only activated if the firm is identified or required to perform TLPT. The baseline assumption is that no designation has been made.
RTS1773-A01	RTS1773 Article 1	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A10	RTS1773 Article 10	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A02	RTS1773 Article 2	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A03	RTS1773 Article 3	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A04	RTS1773 Article 4	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A05	RTS1773 Article 5	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A06	RTS1773 Article 6	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A07	RTS1773 Article 7	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A08	RTS1773 Article 8	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS1773-A09	RTS1773 Article 9	Not applicable — SNI carve-out	This RTS specifies the Article 28(2) formal policy requirement, which excludes Article 16(1) SNI entities; analogous controls are retained proportionately in D09 as implementation guidance.
RTS301-A06-Part_6	RTS301 Article 6(art_6)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-A	RTS301 Article 6(art_6)(a)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-B	RTS301 Article 6(art_6)(b)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-C	RTS301 Article 6(art_6)(c)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-D	RTS301 Article 6(art_6)(d)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-E	RTS301 Article 6(art_6)(e)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-F	RTS301 Article 6(art_6)(f)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-G	RTS301 Article 6(art_6)(g)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-H	RTS301 Article 6(art_6)(h)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.

ID	Reference	Status	Rationale / open point
RTS301-A06-Part_6-I	RTS301 Article 6(art_6)(i)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS301-A06-Part_6-J	RTS301 Article 6(art_6)(j)	Optional	Applies only where the firm voluntarily notifies a significant cyber threat.
RTS532-A02-Part_2	RTS532 Article 2(art_2)	Conditional	Group-level application is relevant only where the firm belongs to a group and the arrangement is managed at group level. Confirm entity facts and operating model; tailor implementation and evidence.