DORA regulated IT compliance at holding companies that service local subsidiaries across the EU

When the parent runs the critical ICT and each subsidiary carries the regulatory duty: the compliance–control asymmetry and concentration risk of centralised financial groups, and how to design for both

Abstract

The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, has applied to the EU financial sector since 17 January 2025, and it binds each regulated entity individually: every bank, insurer, payment firm or investment firm must itself manage its ICT risk, report its major incidents, test its resilience and govern its ICT third parties. A common group structure sits awkwardly against that entity principle. A pan-European financial group often places its regulated business in local subsidiaries, one per member state, while a parent or a dedicated group company runs the critical ICT centrally and supplies it to all of them. This paper sets out the two structural problems DORA creates for such a group and offers a design response. The first is a *compliance–control asymmetry*: the duty to comply sits on each subsidiary, which does not control the ICT, while control sits in the holding, which is often not itself a regulated entity and so is reached by DORA only indirectly, as an *ICT intra-group service provider* that the regulation treats like any other third party. The second is *concentration risk*: a single shared core turns what would be independent, diversifiable failures across the group into one correlated, common-mode event that can impair every subsidiary at once and, because each must report to its own national supervisor, surfaces as many simultaneous filings across many member states. We give a minimal model that separates each subsidiary's own failure probability from the group-wide correlated event the shared core creates, and show that centralisation can lower the first while raising the second from a negligible, second-order risk to a first-order one; we read the result against DORA's register of information, concentration-risk and contractual provisions (Articles 28–30), its incident-reporting regime (Articles 17–19), its testing regime (Articles 24–27) and its rule that the management body's responsibility cannot be delegated (Article 5). We close with a target operating model: a group ICT risk framework run as a shared service but visible to and challengeable by each subsidiary's board, intragroup contracts written as if to an external vendor, a consolidated register, one incident taxonomy feeding many regulatory filings, and pooled testing of the shared core. This is practitioner-facing analysis for groups implementing DORA, not legal advice.

Keywords: DORA; Digital Operational Resilience Act; Regulation (EU) 2022/2554; ICT third-party risk; intra-group ICT service provider; operational resilience; concentration risk; common-mode failure; financial groups; register of information; incident reporting; threat-led penetration testing; critical or important functions; EU financial regulation

1. Introduction

A large financial group that operates across the European Union rarely operates as one legal entity. It operates as a parent and a fan of subsidiaries, typically one regulated company per member state, each holding its own licence, each answering to its own national supervisor, each shaped by the local rules on top of the common European ones. The reason is partly historical, partly regulatory and partly commercial: licences are national, supervisors are national, and a local entity with a local name and a local balance sheet is easier to authorise, to supervise and to sell through. What the group does centralise, almost always, is the information technology. It is wasteful to build the same core banking platform, the same policy-administration system, the same data centre, the same security operations centre eleven times over, so the group builds them once, in the parent or in a dedicated group IT company, and supplies them to every subsidiary as a shared service. The business is local; the plumbing is central.

The Digital Operational Resilience Act cuts across this arrangement in a way that is easy to miss until it is implemented. DORA, Regulation (EU) 2022/2554, has applied since 17 January 2025, and its basic unit is the individual regulated entity, not the group (DORA, Arts 1–2). Each subsidiary must itself maintain an ICT risk-management framework, classify and report its own major incidents, test its own resilience, keep its own register of ICT third parties and govern them under its own board (DORA, Arts 5–30). The regulation does not care that the subsidiary did not build the platform it runs on and cannot change it; the duty is the subsidiary's regardless. And when the group turns to the entity that did build the platform, the parent, it finds that DORA has already named the relationship: a group company that supplies ICT to the regulated entities of its own group is an *ICT intra-group service provider*, and DORA treats it, for almost every purpose, as a third party (DORA, Art 3(20)).

Two problems follow, and they are the subject of this paper. The first is a mismatch between where the duty sits and where the control sits. DORA puts the duty on the subsidiary and leaves the control with the holding, and the holding, if it is not itself a regulated financial entity, is outside the regulation's direct reach, touched only through the contracts and the oversight its subsidiaries are obliged to impose on it. We call this the compliance–control asymmetry, and Section 3.1 anatomises it. The second is that centralising the ICT concentrates the risk. A shared core is a single point whose failure is not one subsidiary's problem but every subsidiary's problem at once, a correlated, common-

mode event rather than an independent, diversifiable one, and because each affected subsidiary must report to its own supervisor, one technical failure becomes a fan of simultaneous regulatory filings across the Union. Section 3.2 sets this out and Section 4 models it.

The contribution is a diagnosis and a design, not a legal commentary. We state the two structural problems plainly, give a small quantitative model of the concentration one so that a group can see how its degree of centralisation trades per-entity reliability against group-wide correlated risk (Section 4), and work through what DORA's main obligations, the register and contracts (Section 5), incident reporting (Section 6), testing (Section 7) and governance (Section 8), require of a centralised group in particular. Section 9 proposes a target operating model that satisfies the regulation while keeping the efficiency that made the group centralise in the first place. Sections 10 to 12 answer objections, state limits and conclude. The question throughout is: **how does a group comply, entity by entity, with a regulation that assumes each entity controls its own ICT, when in fact one shared core controls them all?**

2. What DORA requires, and of whom

2.1. The five pillars

DORA organises the operational resilience of a financial entity into five areas, and it is worth stating them once because the group problem touches all five. The first is *ICT risk management* (Chapter II, Arts 5–16): a governance and control framework, owned by the management body, covering identification, protection, detection, response and recovery, with a lighter simplified framework available to certain smaller entities (Art 16). The second is *ICT-related incident management and reporting* (Chapter III, Arts 17–23): a process to detect and handle incidents, a harmonised classification of their severity (Art 18), and an obligation to report major incidents to the competent authority on a fixed timetable of initial, intermediate and final reports (Art 19). The third is *digital operational resilience testing* (Chapter IV, Arts 24–27): a programme of regular testing for every entity, and advanced threat-led penetration testing (TLPT) at least every three years for those the authorities single out as significant (Arts 26–27). The fourth is the *management of ICT third-party risk* (Chapter V, Arts 28–44), which is where the group structure bites hardest, and which we treat at length below. The fifth is *information-sharing* on cyber threats (Chapter VI, Art 45), which is voluntary and need not detain us here.

2.2. The entity principle

The feature of DORA that governs everything in this paper is that its obligations attach to the individual authorised entity. A banking group is not authorised; its bank subsidiaries are. DORA's scope provision lists the kinds of financial entity it binds, and each is an entity that holds a licence (Art 2). The consequence is that compliance is assessed, and enforced, one entity at a time, by that entity's own competent authority. There is no group licence to comply on behalf of the subsidiaries, and no single European supervisor to whom the group as a whole answers for its resilience. The register of information is the one place the group dimension is explicit: an entity must keep it not only at its own level but, where it is part of a group, at sub-consolidated and consolidated levels too (Art 28(3)), so that a consolidating entity assembles a group-wide view. But the duty to comply, to govern, to report and to test remains the individual subsidiary's, and cannot be discharged by pointing upward to the parent.

2.3. Intragroup ICT is third-party ICT

The second feature that governs this paper is DORA's treatment of ICT supplied from within the group. It would be natural to assume that services a subsidiary receives from its own parent are internal, and outside the third-party regime that DORA aims at external vendors. DORA closes that assumption off. It defines an *ICT intra-group service provider* as an undertaking that is part of the group and provides ICT services predominantly to entities of the same group (Art 3(20)), and it brings such a provider inside the third-party rules: the receiving subsidiary must record the arrangement in its register (Art 28(3)), govern it under a written contract carrying the mandatory provisions (Art 30), assess the concentration it creates (Art 29), and hold exit arrangements for it where it supports a critical or important function (Art 28(8)). The intragroup nature of the relationship is something to be recorded, not a reason for exemption. In short, when the parent supplies the platform, DORA reads the parent as a third-party provider and the subsidiary as its customer, with all the obligations that a customer of an external cloud or software vendor would carry. A group that treats the relationship as a purely internal matter, governed by a service catalogue and an intercompany recharge rather than a DORA-compliant contract, is not compliant.

3. The centralised-holding pattern

Figure 1 draws the pattern this paper is about. A holding or group IT company runs the critical ICT core and supplies it to several regulated subsidiaries, each in its own member state and each supervised by its own national competent authority. The arrows of service run downward from the core; the arrows of supervision and incident reporting run from each subsidiary to its own authority. The two problems of the Introduction are visible in the picture: the thing that binds the group together, the core, is supplied by an entity that the regulators reach only indirectly, and a failure at the top of the diagram propagates to every branch at once while the reporting fragments across every authority at the bottom.

3.1. The compliance–control asymmetry

In a textbook entity, the firm that bears the DORA duty also runs the systems, so the duty and the levers to discharge it are in the same hands. The centralised group pulls them apart. The subsidiary bears the duty, because it is the authorised entity, but it does not run the core, cannot patch it, cannot choose its architecture, cannot set its recovery objectives and cannot, on its own, test it. The holding runs the core and holds all those levers, but it bears no direct DORA duty if it is not itself an authorised financial entity, which a pure IT or holding company usually is not. The

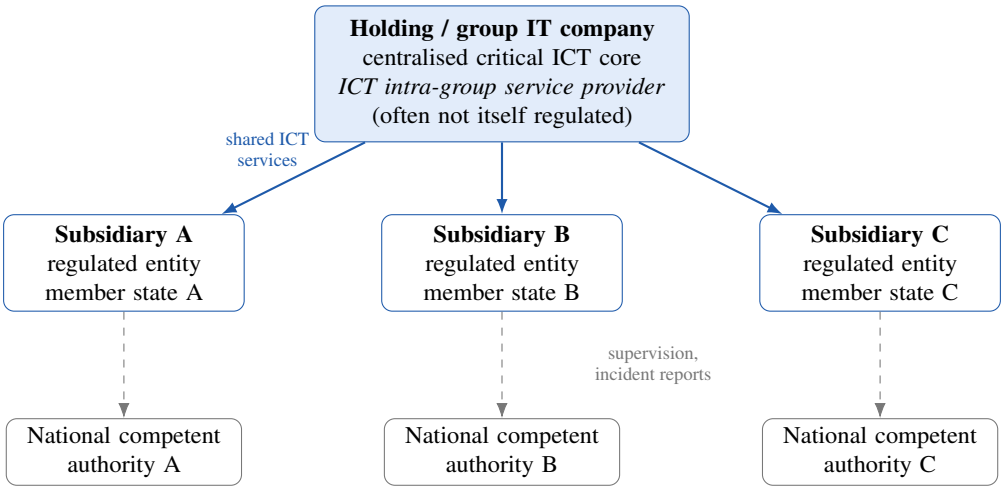


Figure 1. The centralised-holding pattern. A group IT company supplies the critical ICT core to regulated subsidiaries in several member states. Service flows down from the core (solid); supervision and incident reporting flow from each subsidiary up to its own national competent authority (dashed). The DORA duty sits on the subsidiaries; control of the ICT sits in the holding; a core failure reaches every subsidiary at once and is reported to every authority separately.

regulation anticipates exactly this and routes around it: it reaches the holding through the subsidiary, by requiring the subsidiary to impose, by contract, the access, audit, cooperation, incident-notification, testing and exit rights that let the subsidiary discharge a duty over systems it does not own (Art 30). The subsidiary's compliance therefore depends on its contractual power over its own parent, which is an unusual and uncomfortable thing to have to exercise.

The asymmetry has a sharp practical edge. A subsidiary's board is told by DORA that it is ultimately responsible for the entity's ICT risk and cannot delegate that responsibility (Art 5(2)); yet the board's real influence over the core that carries most of that risk runs through a group function that reports to the parent, not to it. If the board simply trusts the centre, it has delegated in substance what it may not delegate in law. If it tries to exercise genuine oversight, it needs information, assurance and rights that a casual intragroup relationship does not provide. The design response, developed in Section 9, is to give the relationship the formality it would have with an external vendor precisely so that the subsidiary's board can see into and challenge the core, and to build the group framework so that each board's oversight is a real input rather than a courtesy.

3.2. Concentration risk

The second problem is that the shared core is a concentration. DORA names concentration risk directly and requires each entity to assess it before contracting and to keep it under review, explicitly including the risk from intragroup arrangements and from providers that are hard to substitute (Art 29). In a centralised group the concentration is near-total: one core, one security operations centre, one set of recovery arrangements, serving every regulated entity in the group. The efficiency case for this is exactly its danger. The same single platform that is cheaper to build and easier to secure once is also a single point whose failure is shared by all who depend on it. Where a federated group of subsidiaries each running its own ICT would suffer failures one at a time, independently, a centralised group suffers them together, because the failures have a common cause.

This is the distinction between independent and common-mode failure that the safety and systemic-risk literatures have long insisted on (Perrow, 1999; Leveson, 2011; ESRB, 2022). Independent failures diversify: the chance that many fall at once is the product of small probabilities, and vanishingly small. Common-mode failures do not diversify: when the shared cause fails, everything downstream of it fails together, and the group's resilience is bounded by the resilience of its weakest shared component, not improved by the number of entities spreading the load. Concentrating the ICT does not spread the risk across the subsidiaries; it couples the subsidiaries to a single risk. The next section makes the point precise.

4. A minimal model of correlated group risk

The model is a sketch, meant to make the mechanism explicit and to let a group reason about its own degree of centralisation, not a calibrated risk estimate. It separates the failure a subsidiary suffers on its own from the failure the whole group suffers together, and shows how centralisation moves risk from the first kind to the second.

4.1. Per-entity impairment

Consider a group of n regulated subsidiaries. A share c of them, which we will treat as the probability that any given subsidiary depends on the holding's shared core for a critical or important function, are *wired* to the core; call c the *centralisation ratio*. In a given period the shared core suffers a critical disruption with probability p_0. This is a common-mode event: when it happens, every wired subsidiary is impaired at the same moment, for the same reason. Independently of the core, each subsidiary's own local ICT fails in the period with probability q. A wired subsidiary is therefore impaired when either the core or its own local ICT fails,

$$u = 1 - (1 - p_0)(1 - q), \tag{1}$$

Equation 1. A wired subsidiary is impaired when either the shared core or its own local ICT fails.

which is the figure a single subsidiary's board sees when it looks at its own incident record. The centralisation that wires the subsidiary to a well-run core tends to lower q, because a professional shared platform is usually run better than a small local one, so u can fall as the group centralises. Looked at one entity at a time, centralisation improves resilience, and this is the honest half of the efficiency case.

4.2. From independent to correlated

The group does not experience its risk one entity at a time. What matters to the group, and to the regulators, is the chance that several subsidiaries are impaired *at the same time*, because that is the event that is systemic, cross-border and simultaneously reportable. Without a shared core, the only way two subsidiaries fall together is if two of them happen to fail locally in the same period, a coincidence of independent events whose probability is of order q^2, that is, second-order small. With a shared core, a single core disruption takes down every wired subsidiary at once, so the probability of a simultaneous, multi-entity event is of the order of the core's own failure probability,

$$P_{\text{corr}}(\geq 2) = p_0\big[\,1-(1-c)^n - nc(1-c)^{n-1}\,\big], \qquad (2)$$

Equation 2. A shared core makes a simultaneous, multi-entity incident a first-order event in the core's own failure probability.

where the bracket is the probability that at least two of the n subsidiaries are wired, so that a core failure impairs at least two at once. The point is not the exact form but the order: centralisation converts the probability of a group-wide event from second-order in a small local probability to first-order in the core's probability. A core that fails only rarely is still, as a source of simultaneous multi-entity failure, far more dangerous than the sum of the subsidiaries' independent risks, because its failures are shared rather than spread. Figure 2 draws this probability against the centralisation ratio for the two architectures: a federated group, each subsidiary on its own ICT, holds it flat near zero, while a centralised group's climbs away from that baseline as more of the group is wired to the shared core.

4.3. The regulatory-load multiplier

There is a second consequence of the common-mode event that is specific to DORA and to the group structure, and it concerns not resilience but reporting. Because each subsidiary is a separate regulated entity answering to its own competent authority (Section 2.2), a single core failure does not generate one incident report; it generates one from every subsidiary it impairs, each to a different authority, each on that authority's clock, possibly in that authority's language. The expected number of simultaneous major-incident reports triggered by one core disruption is just the expected number of wired subsidiaries,

$$E[R \mid \text{core fails}] = nc, \qquad (3)$$

Equation 3. One core failure triggers, in expectation, nc parallel major-incident reports, one per impaired subsidiary to its own supervisor.

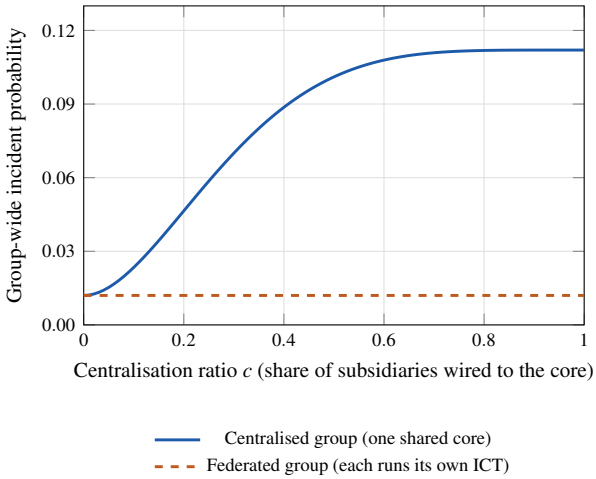


Figure 2. Concentration and the group-wide incident. The probability that two or more subsidiaries suffer a critical incident at the same time, a cross-border event each affected entity must report to its own supervisor, in a single period. A federated group, where each subsidiary runs its own ICT, holds this near zero, because a joint failure would need an independent coincidence, a second-order event. As a group wires more of its critical functions to one shared core, the same probability climbs, because a single core failure impairs every dependent subsidiary at once, a first-order event. The gap between the lines is the concentration premium the shared core adds. Curves illustrative.

so a group of a dozen subsidiaries fully wired to a shared core turns a single technical event into a dozen parallel regulatory filings in a dozen jurisdictions, inside DORA's initial-report deadline, all describing the same root cause. This regulatory-load multiplier is invisible in any one subsidiary's planning and becomes visible only at the group level, which is precisely the level DORA does not make a single entity responsible for. It is the strongest practical argument for the group-level coordination that Section 9 builds.

5. The register, concentration and contracts

DORA's third-party chapter gives the centralised group three instruments it must use, and each of them, applied honestly, surfaces the problems above rather than hiding them.

The *register of information* (Art 28(3)) is an inventory of every contractual arrangement for ICT services, kept to a standard template set by implementing technical standards (ITS 2024/2956) and distinguishing the arrangements that support critical or important functions from those that do not. For a centralised group the register is where the intragroup dependency becomes undeniable: every subsidiary's register lists the holding as a provider of its critical services, and the consolidated register the group must assemble (Art 28(3)) shows, on a single page, that one provider sits behind the critical functions of the entire group. A group that fills the register in properly has documented its own concentration; a group tempted to leave the intragroup arrangement out, on the theory that it is internal, both breaches the register obligation and blinds itself to the very

risk the register exists to show. Table 1 sets out the three levels at which the register is kept and what each is for.

The *concentration-risk assessment* (Art 29) then asks the question the register poses: what happens if this provider fails or must be replaced? For an external provider the answer is a substitution analysis; for the intragroup core it is harder, because the core is usually not substitutable at all on any reasonable horizon, having been built once for the whole group. DORA does not forbid concentration, but it requires the entity to see it and to weigh it, and a centralised group's honest answer, that the core is a single point of failure for the group and effectively irreplaceable in the short term, is itself the finding that should drive the resilience investment and the exit planning the regulation also requires (Art 28(8)).

The *contractual arrangements* (Art 30) are the mechanism by which the subsidiary acquires power over a core it does not own. DORA prescribes a floor of provisions for every arrangement and a longer list for arrangements supporting critical or important functions: full service-level descriptions, locations of service and data, access, inspection and audit rights, obligations to assist on incidents, cooperation with the authorities, rights to monitor, conditions on subcontracting (now detailed by RTS 2025/532) and documented exit strategies (Arts 28(8), 30(2)–(3)). The intragroup setting does not relax any of this. The design instruction, developed below, is to write the intragroup contract as though the counterparty were an external vendor at arm's length, because that is the only way the subsidiary's board gets, on paper, the rights the asymmetry otherwise denies it.

6. One incident, many regulators

The incident-reporting regime is where the regulatory-load multiplier of Section 4 becomes an operational problem. DORA requires an entity to classify an ICT-related incident against harmonised criteria, and, if it is major, to notify its competent authority with an initial report on a short deadline, then an intermediate report as the picture firms up, then a final report with root cause (Arts 18–19). The classification criteria, the thresholds and the templates are harmonised across the Union by Level 2 rules, which is a help; but the reports still go to each entity's own authority, and the clock starts for each entity when that entity becomes aware.

For a centralised group a single core failure is, simultaneously, a major incident for every subsidiary it impairs. Each subsidiary must classify it, each must decide whether it crosses the major threshold, and each must file, to its own authority, within the deadline. If the subsidiaries classify independently and draft independently, the group produces a scatter of reports that describe the same event inconsistently, arrive at different times, and expose the group to the obvious supervisory question of why its entities disagree about what happened to their shared system. The failure mode is not under-reporting but incoherent over-reporting. The remedy is not to centralise the reporting, which DORA does not allow, since the obligation is each entity's, but to centralise the *facts*: one incident taxonomy, one root-cause determination and one clock run from the group security operations centre, feeding a consistent core of fact into each subsidiary's own filing, which each subsidiary's own responsible function then owns, signs and submits to its own authority. The group supplies the truth; each entity supplies the filing. Section 9 makes this concrete.

7. Testing a shared core

DORA's testing regime has two tiers, and the group structure complicates both. The basic tier requires every entity to run a programme of resilience tests, proportionate to its size and risk (Art 24–25). The advanced tier requires threat-led penetration testing, roughly every three years, for those entities the authorities identify as significant enough to warrant it (Arts 26–27). In a centralised group the object worth testing is largely the shared core, because that is where the critical systems and the concentration are; but the obligation to test sits on the subsidiaries, which do not run the core.

Testing the same shared core separately for each subsidiary would be wasteful and, worse, risky, since repeated live red-teaming of a production platform that serves the whole group multiplies the chance that a test itself causes an incident. DORA anticipates shared providers and allows, under conditions, testing to be pooled or conducted jointly where several entities rely on the same ICT provider or belong to the same group and share systems, so that one properly governed test of the shared core can satisfy the participating entities (Arts 26–27 and the TLPT technical standards). Pooling does not dissolve the individual obligation: each participating subsidiary must still be a party to the arrangement, must still ensure the test covers its own critical functions, and must still act on the findings. But it lets the group test the thing that actually matters, the core, once and well, rather than many times and badly. The design implication is that the group should plan testing from the core outward, scope each subsidiary's critical functions into the shared test, and hold the contractual rights (Art 30) that let a subsidiary require its provider, here its own parent, to participate.

8. Accountability that cannot be delegated upward

The thread running through every section is DORA's insistence that the management body of each entity bears the ultimate responsibility for that entity's ICT risk, and that this responsibility cannot be contracted or delegated away (Art 5). In a centralised group this is the provision most in tension with the operating reality, because the reality is that the subsidiaries have delegated the ICT, in substance, to the group. DORA does not forbid the group from running the ICT centrally; what it forbids is the subsidiary board treating that arrangement as a reason to stop being responsible. The board must retain enough understanding of the core it depends on, enough information about how it is run and how it is failing, and enough contractual and governance power to challenge and, in extremis, to act, that its statutory responsibility is real rather than nominal.

This cuts against a natural and usually well-meant centralising instinct, which is to spare the subsidiary boards the

Table 1. The register of information at three levels (Art 28(3)). A centralised group must keep the register not only entity by entity but consolidated, and it is the consolidated level that reveals the group's dependence on a single shared core.

Level	What it records	What it reveals in a centralised group
Entity	Each subsidiary's own contractual arrangements for ICT services, including the intragroup supply of the shared core	That the subsidiary depends on the holding for its critical or important functions, and cannot comply on its own
Sub-consolidated	The arrangements of a sub-group, where the group has intermediate holding structures	Shared dependencies within a regional or sectoral sub-group, and intermediate points of concentration
Consolidated	All arrangements across the group, assembled by the consolidating entity	That one intragroup provider sits behind the critical functions of every regulated entity in the group: the concentration, on a single page

technical detail and let the experts at the centre handle it. DORA requires the opposite: that each subsidiary board be equipped and obliged to govern a risk it has outsourced to its own parent. The practical consequences are a reporting line from the group ICT function into each subsidiary board, not only into the parent; board-level ICT-risk literacy at every subsidiary, not only at the centre; and a group framework designed so that each board's oversight is a genuine control point. A group that builds the shared core but leaves the subsidiary boards uninformed has created the compliance–control asymmetry in its most dangerous form, where the people who are responsible in law are the least able in fact to exercise the responsibility.

9. A target operating model for the group

The design that answers the two problems is not to decentralise the ICT, which would throw away the efficiency and, by the model of Section 4, might not even improve group resilience once the shared core is well run. It is to keep the central core and wrap it in the structure DORA requires, so that the duty and the control are reconnected by governance and contract rather than by ownership. Five moves follow from the analysis.

Run one group ICT risk framework, visible to every board. Build the ICT risk-management framework once, at the group, to the standard DORA and its RTS require (Art 6; RTS 2024/1774), but wire its reporting into each subsidiary's management body and not only into the parent's, so that each board governs the shared risk with real information. The framework is central; the accountability stays distributed, as the regulation demands.

Contract with the parent as if it were a vendor. Give every intragroup supply of a critical or important function a written contract carrying the full Article 30 provisions, access and audit rights, incident-assistance and cooperation duties, subcontracting conditions and a documented exit strategy, exactly as a subsidiary would impose on an external cloud provider. The formality is not bureaucratic overhead; it is the instrument that converts the subsidiary's paper responsibility into real power over the core.

Keep a consolidated register and read it as a risk map. Maintain the register at entity, sub-consolidated and consolidated levels (Art 28(3)) and treat the consolidated view not as a filing chore but as the group's map of its own concentration, the input to the concentration-risk assessment (Art 29) and to the resilience investment that follows from it.

Centralise the facts of an incident, distribute the filing. Run one incident taxonomy, one root-cause process and one clock from the group security operations centre, and feed a single, consistent account of any core incident into each affected subsidiary's own reporting, which that subsidiary owns and files with its own authority (Arts 18–19). The group supplies one truth; each entity meets its own obligation.

Test the core once, for all who depend on it. Plan resilience and threat-led testing from the shared core outward, using DORA's provisions for pooled and group testing (Arts 26–27) so that the thing that carries the concentration is tested properly and rarely rather than repeatedly and thinly, with each subsidiary's critical functions scoped in and each subsidiary acting on the findings.

None of these undoes centralisation; each reconnects a duty DORA placed on the subsidiary to a control the group placed in the holding. Together they let a group keep the platform it built once and still give each regulated entity, and each national supervisor, the governed, contracted, documented and tested relationship the regulation requires.

10. Objections and replies

The parent is not a regulated entity, so DORA does not apply to it. Directly, no; through its subsidiaries, entirely. DORA reaches the holding as an ICT intra-group service provider by obliging each subsidiary to govern, contract with and oversee it (Arts 3(20), 30). A group that reads the parent's lack of a licence as freedom from DORA has mistaken the route of the obligation for its absence, and will find the obligation waiting in every subsidiary's register, contract and audit.

Centralising ICT improves resilience, so concentration is a feature, not a risk. Both are true, which is the point of Section 4. A well-run shared core lowers each subsidiary's own, independent failure probability; it simultaneously raises the probability of a single correlated event that impairs the whole group at once. DORA's concentration provisions (Art 29) exist precisely because the second effect is real and is invisible from inside any one entity. The design task is to capture the first benefit while seeing, pricing and mitigating the second, not to deny that the trade-off exists.

Writing a full Article 30 contract between a parent and

its own subsidiary is legalistic theatre. It would be, if the contract's only purpose were to satisfy a checklist. Its real purpose is to give the subsidiary's board, which is responsible in law for a core it does not own, enforceable rights to information, audit, assistance and exit over that core. Without them the board's statutory responsibility (Art 5) is nominal. The formality is the mechanism that makes the responsibility exercisable, and the intragroup setting, where the counterparty is a sister entity with the same ultimate owner, is exactly where informal arrangements tend to leave those rights unwritten.

Pooled testing lets the group off the individual testing hook. It does not. Pooling (Arts 26–27) is a way to test the shared core efficiently and safely, not a way to discharge an entity's obligation by pointing at someone else's test. Each participating subsidiary remains individually obliged to ensure its own critical functions are in scope and to act on the findings; the pool concerns how the test is run, not whose duty it is.

11. Limitations

This is practitioner-facing analysis, and its limits should be stated plainly. It is not legal advice; the controlling text is the Regulation and its Level 2 acts, read with the guidance of the European Supervisory Authorities and each relevant national competent authority, and a group's own counsel must map the general structure here to its specific entities, licences and member states. The article references are to DORA as it stood in early 2025, with the delegated and implementing acts then adopted; the detail of the technical standards, and supervisory practice under them, will continue to develop. The model of Section 4 is a sketch whose quantities are defined clearly enough to measure but whose functional forms and illustrative values are chosen to make the mechanism visible, not estimated from a group's data; a group should populate c, p_0 and q from its own architecture and incident history before drawing any conclusion from the curves. The paper also treats the common and clean case of a single central core and a clear parent–subsidiary split; real groups have several cores, partial centralisation, intermediate holdings, shared external providers behind the intragroup one, and functions that are critical in one member state and not in another, each of which complicates the picture without changing its two basic problems.

12. Conclusion

A pan-European financial group that runs its critical ICT from the centre and its regulated business from the edges has built the most sensible structure for efficiency and the most awkward one for DORA. The regulation binds each subsidiary individually, assumes each controls its own ICT, and finds instead that one shared core, supplied by a parent the regulation reaches only at second hand, controls them all. Two problems follow: the duty to comply sits where the control does not, and centralising the ICT concentrates the group's risk into a single correlated point whose failure impairs every subsidiary at once and is reported to every supervisor separately. We have set both out, modelled the second to show that centralisation trades a lower per-entity failure probability for a higher group-wide correlated one, and read the result against DORA's register, concentration, contract, incident, testing and governance provisions.

The answer is not to abandon the central core but to govern it as DORA requires: one group framework visible to every board, intragroup contracts written as if to an external vendor, a consolidated register read as a concentration map, one set of incident facts distributed into many filings, and the shared core tested once for all who depend on it. Each move reconnects a duty the regulation placed on the subsidiary to a control the group placed in the holding, so that the thing the group built once can be run compliantly by every entity that depends on it. The deeper lesson is the one DORA was written to teach: that operational resilience is not a property of a platform but of the arrangements around it, and that in a group those arrangements, not the ownership chart, are what decide whether a single point of efficiency is also a single point of failure.

Appendix A. The model in full

The model of Section 4 uses four quantities, all of which a group can estimate from its own architecture and incident history. The centralisation ratio c is the share of the group's regulated subsidiaries whose critical or important functions depend on the shared core; a group can read it from the consolidated register (Art 28(3)) by counting, of its subsidiaries, how many list the intragroup core behind a critical function. The core-failure probability p_0 is the probability that the shared core suffers a disruption severe enough to impair a dependent subsidiary's critical function in a chosen period; it is estimated from the core's own incident record, not from any one subsidiary's. The local-failure probability q is the corresponding probability for a subsidiary's own, non-shared ICT. The count n is the number of regulated subsidiaries.

The independent baseline is the comparison that makes the concentration visible. If there were no shared core, each subsidiary failing independently with probability q, the probability that at least two subsidiaries were impaired in the same period would be $1-(1-q)^n-nq(1-q)^{n-1}$, which for small q is approximately $\binom{n}{2}q^2$, a second-order quantity. With the shared core, the leading term of the same probability is p_0 times the chance that at least two subsidiaries are wired, a first-order quantity in p_0. The ratio of the two is the factor by which centralisation raises the group's exposure to simultaneous, multi-entity events, and it is large whenever p_0 is not much smaller than q^2, which it almost never is. This is the formal content of the claim that concentration couples the subsidiaries to a single risk rather than spreading the risk across them.

Two pitfalls deserve note. The first is estimating p_0 from a single subsidiary's experience of the core, which understates it, because a given subsidiary sees only the core incidents that happened to impair it; p_0 must be read from the core's own record across all dependents. The second is treating c as fixed when it is a decision: the group chooses, function by function, how much to wire to the core, and the model's value is in showing the cost, in correlated group-wide risk, of each increment of that choice, so that the

choice is made with the trade-off of Figure 2 in view rather than on efficiency grounds alone.

Appendix B. An intragroup contractual-provisions checklist

The checklist below collects the Article 30 provisions a subsidiary should secure in its contract for the intragroup supply of a critical or important function. It is not a substitute for the Regulation or for legal advice; it is a working list for the design conversation between a group's central IT function and its subsidiary boards. Each provision is one the subsidiary needs in order to discharge, over a core it does not own, a duty DORA places on it; the intragroup setting is where each is most often left implicit and should instead be written down.

Table 2. Intragroup contractual provisions for a critical or important function (Art 30). Each is a right the subsidiary needs over the shared core it depends on but does not control.

Provision	Why the subsidiary needs it
Service levels and locations	To know what it is relying on and where its data and processing sit
Access, inspection and audit	To verify the core's controls itself, as its board's responsibility requires
Incident assistance and notification	To learn of a core incident in time to meet its own reporting deadline
Cooperation with authorities	To let its supervisor reach the core through it
Subcontracting conditions	To see and control what the core itself depends on (RTS 2025/532)
Exit strategy	To have a documented, tested plan should the arrangement end (Art 28(8))

References

[1] European Union (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act). *Official Journal of the European Union*, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[2] European Commission (2024). Commission Delegated Regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes and policies and the simplified ICT risk management framework. *Official Journal of the European Union*, L series. https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj

[3] European Commission (2024). Commission Delegated Regulation (EU) 2024/1773 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards on the policy on contractual arrangements on the use of ICT services supporting critical or important functions. *Official Journal of the European Union*, L series. https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj

[4] European Commission (2024). Commission Delegated Regulation (EU) 2024/1502 supplementing Regulation (EU) 2022/2554 with regard to criteria for the designation of ICT third-party service providers as critical for financial entities. *Official Journal of the European Union*, L series. https://eur-lex.europa.eu/eli/reg_del/2024/1502/oj

[5] European Commission (2024). Commission Implementing Regulation (EU) 2024/2956 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 with regard to the standard templates for the register of information. *Official Journal of the European Union*, L series. https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

[6] European Commission (2025). Commission Delegated Regulation (EU) 2025/532 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the elements a financial entity must determine and assess when subcontracting ICT services supporting critical or important functions. *Official Journal of the European Union*, L series. https://eur-lex.europa.eu/eli/reg_del/2025/532/oj

[7] European Supervisory Authorities (EBA, EIOPA and ESMA) (2024). *Final report on draft regulatory technical standards on subcontracting under Article 30(5) of Regulation (EU) 2022/2554* (JC 2024 53). Joint Committee of the European Supervisory Authorities. https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024_53_Final_report_DORA_RTS_on_subcontracting.pdf

[8] Basel Committee on Banking Supervision (2021). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm

[9] Financial Stability Board (2019). *Third-party dependencies in cloud services: Considerations on financial stability implications*. https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/

[10] Financial Stability Board (2023). *Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities*. https://www.fsb.org/2023/12/enhancing-third-party-risk-management-and-oversight-a-toolkit/

[11] European Systemic Risk Board (2022). *Mitigating systemic cyber risk*. European Systemic Risk Board. https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemicCyberRisk220127~b6655fa027.en.pdf

[12] European Banking Authority (2019). *Guidelines on outsourcing arrangements* (EBA/GL/2019/02). https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

[13] European Union Agency for Cybersecurity (ENISA) (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[14] Perrow, C. (1999). *Normal accidents: Living with high-risk technologies* (Updated ed.). Princeton University Press. ISBN 978-0-691-00412-9.

[15] Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press. ISBN 978-0-262-01662-9.

[16] Kaufman, G. G., & Scott, K. E. (2003). What is systemic risk, and do bank regulators retard or contribute to it? *The Independent Review*, 7(3), 371–391. https://www.independent.org/pdf/tir/tir_07_3_scott.pdf