In-Class Exercise: Operational Resilience Business Models

Exercise 1: Structured Debate — "Is Kyndryl an Outsourcer or a Resilience Vendor?"

Format: Split into two teams. Each team prepares arguments for its assigned position, then presents. After both sides speak, the class votes — but first, read the debrief questions.

Team A — "Kyndryl Is an Outsourcer"

Anchoring evidence: Kyndryl spun out of an incumbent infrastructure-services arm, inherited the contracts of that arm, and earns most of its revenue running customer estates that the customer chose not to operate in-house. Its compensation model is per-server, per-environment, per-shift — the classical economics of an IT outsourcer.

	Team A: Kyndryl Is an Outsourcer
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Team B — "Kyndryl Is a Resilience Vendor"

Anchoring evidence: Kyndryl positions itself around mainframe modernisation, recovery-as-a-service, and ICT third-party risk. Its commercial value to a regulated buyer is the named accountable operator who will appear in the supervisor's incident dossier — the exact deliverable a resilience vendor sells.

	Team B: Kyndryl Is a Resilience Vendor
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Debrief Questions

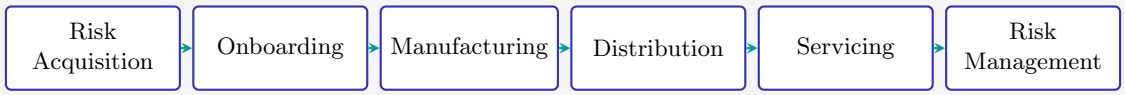
Q1: Does the answer — outsourcer or resilience vendor — matter for how regulators should treat critical-third-party concentration risk? Why or why not?

Q2: Could the answer genuinely be "both"? If so, what does that imply for the usefulness of traditional vendor categories in supervisory frameworks?

Q3: Name another vendor (in any sector) that blurs the boundary between operational delivery and assurance in a similar way. What tensions does the blurring create?

Exercise 2: Value Chain Mapping — the Insurance-and-Risk Stack

Scenario: The corporate risk and insurance value chain breaks into six links. Operational-resilience and risk-management vendors attack individual links with specialised products. Your task: for each link, identify a vendor, describe the friction it removes, and predict the long-term outcome.



Value Chain Link	Vendor Attacking It	Friction Removed	Replaces or Improves?	Incumbent Loses or Adapts?
Risk Acquisition				
Onboarding				
Manufacturing				
Distribution				
Servicing				
Risk Management				

Synthesis Question

Q1: Which link in the resilience value chain is *most vulnerable* to vendor disruption? Which is *most resistant*? Defend your reasoning with reference to switching costs, regulatory barriers, and data advantages.

Facilitator Solutions

Sample answers for instructor reference. These are illustrative; student reasoning may diverge and still be valid.

Exercise 1: Debate Sample Answers

Team A (Kyndryl Is an Outsourcer) — sample arguments

Argument I. Kyndryl's revenue mix is dominated by run-the-environment service contracts inherited from its parent. The economics — per-server, per-shift, per-managed-environment — match the classical outsourcing playbook far more than the subscription-and-evidence model of a resilience vendor. The activity being sold is operational labour, not assurance.

Argument II. The customer base is concentrated in legacy estates that the buyer cannot or will not run in-house. That selection bias means Kyndryl's competitive position is anchored in the buyer's reluctance to staff the work, not in any unique resilience method. Other outsourcers compete for the same contracts on roughly the same dimensions: scope, price, transition risk.

Argument III. The contractual deliverable is operational availability, not regulatory evidence. When a supervisor asks for an attestation, the buyer assembles it from the outsourcer's runbooks, but the assurance product itself remains the buyer's responsibility. A genuine resilience vendor sells the attestation; Kyndryl sells the operations the attestation describes.

Concession. The strongest argument against Team A is that supervisors increasingly treat critical third-party operators as resilience-relevant entities in their own right, which pulls Kyndryl into the assurance perimeter whether it markets itself there or not.

Closing. Even when the regulator pulls a critical operator into the assurance perimeter, the underlying business model remains that of an outsourcer: revenue scales with scope of work, not with the breadth of evidence emitted. Regulatory inclusion changes the supervisory treatment without changing the commercial substance.

Team B (Kyndryl Is a Resilience Vendor) — sample arguments

Argument I. Kyndryl explicitly positions its offering around recovery-as-a-service, mainframe modernisation, and ICT third-party risk — the precise vocabulary the supervisory regime uses to describe operational resilience. The commercial buyer pays for the named accountable operator who will appear in the supervisor's dossier when an incident occurs.

Argument II. The deliverable that drives renewal is documented operational accountability under regulatory tolerance windows. Pure outsourcing does not require recovery-time and recovery-point objectives expressed in supervisory language; resilience contracts do. Kyndryl's reporting commitments are calibrated to that vocabulary, which places the firm inside the resilience category in substance, not just in marketing.

Argument III. The buyer treats Kyndryl's runbooks and recovery exercises as evidence consumable by their second line of defence and external auditors. That changes the asset under management from operational labour to provable preparedness — the same Value Proposition block that anchors a Cyberhaven or a ServiceNow ITM.

Concession. The strongest argument against Team B is that Kyndryl's contracts and revenue model still resemble outsourcing far more than software subscription, and the firm's go-to-market motion remains anchored in legacy-estate transition rather than evidence emission.

Closing. Commercial form is a lagging indicator. The economic substance Kyndryl is selling — a named accountable operator producing supervisor-grade evidence — is the resilience product, even when the contract still looks like an outsourcing master agreement. The category boundary will move in Kyndryl's direction faster than the legacy contract structure can.

Debrief Q1 — Supervisory treatment of concentration risk

Whether Kyndryl is supervised as an outsourcer or as a resilience vendor changes the regulator's instrument set. As an outsourcer, it falls under generic third-party risk-management expectations directed at the buyer. As a critical resilience operator inside a regime such as the EU's ICT-risk framework, it can be designated directly, becoming subject to oversight rights, on-site inspections, and cross-border coordination obligations. The choice matters because concentration risk — many regulated buyers depending on one operator — can only be managed by addressing the operator itself once it crosses a criticality threshold. Treating it solely as an outsourcer leaves the supervisor without the toolkit to address that concentration directly.

Debrief Q2 — "Both" as an answer

The answer can genuinely be "both": Kyndryl operates as an outsourcer in the contractual and revenue sense and as a resilience operator in the regulatory and substantive sense. That duality reveals that traditional vendor categories, inherited from a world where outsourcing was a buy-vs-build choice rather than a critical-path supervisory matter, no longer cleanly capture firms that deliver operational labour and regulator-grade evidence inside the same engagement. If "both" is correct, supervisors and procurement teams need functional rather than institutional categories — focused on the risk a vendor creates and the evidence it emits, not the legacy industry label it carries.

Debrief Q3 — Cross-sector blurring example

Cloud hyperscalers blur the boundary between platform infrastructure and managed-service vendor. Their commercial form is a self-serve platform, but their largest regulated customers consume them as operational delivery partners that produce attestations, audit reports, and incident-response coordination on demand. The tension is acute for supervisors (treat the hyperscaler as a critical third party or as fungible infrastructure?), for buyers (run their own controls or rely on the hyperscaler's?), and for procurement (sign a self-serve agreement or insist on bespoke resilience commitments?). The parallel to Kyndryl is direct: in both cases, the contractual category lags behind the substantive category that the regulator and the buyer increasingly use.

Exercise 2: Value-Chain Mapping Sample Answers

Value Chain Link	Vendor Attacking It	Friction Removed	Replaces or Improves?	Incumbent Loses or Adapts?
Risk Acquisition	Cyberhaven (insider-risk telemetry surface)	Buyer cannot self-discover sensitive data flows across endpoints and clouds	Replaces	Incumbent Loses
Onboarding	Resolver (risk-event intake workflow)	Spreadsheet-and-email coordination of incident capture and follow-up	Improves	Incumbent Adapts
Manufacturing	ServiceNow ITM (control-and-threat catalogue)	Manual mapping between threat intelligence and control inventories	Replaces	Incumbent Adapts
Distribution	Riskonnect (broker-of-record portal)	Manual exposure-data movement between corporate risk teams and brokers	Improves	Incumbent Adapts
Servicing	Kyndryl (managed-resilience operator)	Burden of operating supervised legacy estates with internal staff	Replaces	Incumbent Loses
Risk Management	Specialist chaos-engineering and runbook-as-code vendors	Inability to validate the assumed recovery sequence under realistic failure injections	Improves	Incumbent Adapts

Synthesis Question Sample Answer

The most vulnerable link is **Distribution**. Switching costs at the broker-portal layer are moderate, integration footprints are well-understood, and the buyer can replace the orchestration layer without disturbing either the underwriting carrier upstream or the claims handler downstream. A specialist vendor that owns the broker-of-record portal therefore captures a disproportionate share of the relationship value relative to the substitution cost. The most resistant link is **Risk Management** at the analytics layer. Aggregate-exposure analytics depend on cross-customer telemetry accumulated over many engagements, supervised model validation under regulatory oversight, and integration with core risk and capital systems that carry high switching costs. Regulatory barriers — model-risk governance, auditor sign-off, supervisor familiarity — further entrench incumbents because the compliance investment is non-transferable. A new entrant can improve the interface but will struggle to displace the data moat and supervisory familiarity that underpin this link.

