

Working Group Profile

Description of the Working Group

Related Committee	-
Name of the Working Group	N-Tier Data & Supply Chain Network Transparency
Association Contact	Hanno Focken / Michael Hahn

Description / Challenge / Initial Situation:

Regulatory requirements* (UFLPA, EUDR, Battery Regulation, Critical Raw Materials Act, CBAM, due-diligence legislation) and established business practice (directed/named parts, risk and resilience management, geopolitical exposure) increasingly require visibility **beyond the direct business partner**. Today, companies close this gap through manual multi-tier surveys, duplicated questionnaires along the same chain, and proprietary third-party solutions.

Catena-X currently answers the question "*Who is my direct business partner?*". It has no offering for network-level risk management. At the same time, the One-Up/One-Down (1U1D) principle — anchored in contractual relations and antitrust considerations — is one of the constitutive trust principles of the data space.

The Working Group addresses the resulting core question:

How can Catena-X make legitimate need-to-know information about the N-Tier network available and governable, without breaching 1U1D, disclosing business secrets, or centralising data?

Strategic relevance: identity (BPN) plus relationship knowledge is the non-replicable asset of the ecosystem. If Catena-X does not govern this layer, commercial providers will occupy it — without neutrality and without sovereignty guarantees.

Boundary condition agreed across all contributions: transparency ≠ full disclosure. The guiding principle is *Need-to-Know instead of Nice-to-Know*.

**Catena-X supports the consistent and efficient implementation of adopted regulations, but does not contribute to the further expansion or proliferation of regulations.*

Goals:

1. Definition and scope

- Binding definition of "N-Tier data" in Catena-X: distinction between **relationship knowledge** (company/site level), **part-related chain data** (BoM/Industry Core), and **derived indications** (affectedness statements).
- Clear separation between **technical Catena-X capability** and **processual rules of use** (guardrails).

Working Group Profile

2. Need-to-Know model and guardrails

- A legitimacy model that defines *when, who (role), for which purpose, at what granularity and for how long* may access which N-Tier information.
- Codification of the principle **Need-to-Know ≠ Right-to-See**.
- Definition of regulatory disclosure as an **explicit, purpose-bound exception** to 1U1D, limited to legitimated authorities.

3. Use case scoping

- **Reactive / event-driven incident management** — building on the ESS logic: standardised notification of affectedness along the chain.
- **Preventive / proactive risk management** — ad-hoc availability of existing relationship knowledge as a basis for risk assessment (scope and admissibility to be decided, see decision points).
- **Regulatory disclosure** — towards authorities only.
- **Contractual relations** — handling of directed/named parts, where the relationship is known to the contracting parties anyway.

4. Reuse instead of new build

- Assessment and extension of existing assets rather than a new stack: **BPDM**(company twin, master data present — only relationship knowledge missing), **Industry Core** (relationship knowledge at component level), **Traceability**(material and product flow), **ESS / Due Diligence KIT** (event-based search logic, clearing agency concept), **IRS** (traversal of relationships across tiers).
- Assessment of whether the ESS mechanism is usable for risk management, or whether it is too granular for preventive scenarios.
- **SBoM mechanism** to be evaluated if relevant for the target concept.

5. Minimum data set and depth

- Definition of a minimum data set per value-added step: e.g. part number — at least at Tier-1 level, legal company name, BPN/DUNS, address, geo-coordinates, value-added step.
- Principle **"depth only as far as necessary"**: indications (problem yes/no) are preferred over replication of the chain.

6. Architecture option decision

- Comparative assessment of **decentralised** relationship knowledge vs. a **neutral third party / trusted third party** (Catena-X as neutral governor able to flag and forward incidents), including antitrust, liability and sovereignty implications.

7. Deliverable

- A decision-ready framework — including the accompanying communication — for how Catena-X handles N-Tier data, as a basis for standardisation and KIT work.

Standardisation and KIT outlook

Item	Status / Candidate
New standard	To be determined. Candidate: cross-cutting rulebook <i>"N-Tier Data Governance & Need-to-Know Model"</i>

Working Group Profile

	(governance/process standard); target release to be set after the framework decision.
Adaptation of standards	To be determined. Candidates: CX-0125 Traceability (visibility rules), BPDM standards (relationship attributes), Industry Core, ESS/Due Diligence standards, Data Space Operations chapter on Supply Chain Visibility / 1U1D.
New KIT	To be determined. Preference across contributions: extension rather than new KIT — extend ESS / Due Diligence and BPDM.
Adaptation of KITs	To be determined. Candidates: ESS KIT (event-based search for risk management), BPDM KIT (relationship knowledge at company level), IRS-related documentation.

Implementation and alignment with Eclipse Tractus-X and adjacent initiatives is mandatory. For role definitions, see the [Working Model](#).

Rough planning – Milestones / Outcome / Deliverables (e.g., “Date & Activities & Outcome”):

Date	Activity	Outcome
04.09.2026	Feedback from all project group members	Company positions collected
11.09.2026	Draft consolidation by Catena-X e.V.	Consolidated draft
21.09.2026	Alignment of draft with project group	Aligned impulse paper
28.09.2026	Board Meeting	Mandate and scope decision
Following	Launch of the Working Group	Group constituted, lead appointed
Q4 2026	Framework for handling N-Tier data	Decision basis published by year-end 2026
Subsequently	Operationalisation	Standardisation and KIT roadmap, release allocation

Why should I participate?

- The N-Tier layer decides whether Catena-X governs the industry's relationship and identity commons — or whether commercial providers do.
- Direct influence on the guardrails that will apply to your own supply chain data.
- Reduction of duplicated multi-tier surveys by several customers along the same chain.

Working Group Profile

- Foundation for regulatory compliance, resilience and preventive risk management on one shared data basis: **capture once, use many times**.
- Prerequisite for AI-based risk, compliance and procurement agents on trustworthy network data.

What is expected of me?

- Active contribution of company positions, use cases and constraints (not observation).
- Willingness to bring internal legal, procurement, risk and IT perspectives into alignment.
- Contribution to concept work: need-to-know model, minimum data set, guardrails, architecture options.
- Reuse and validation of existing assets (BPDM, Industry Core, ESS, IRS, Traceability)

For more information on the responsibilities of an Working Group, have a look at the [Working Model](#).

Organisation

Selection Framework:

The Expert Group must be balanced across the value chain, because the subject affects every tier asymmetrically.

Requirements for members:

- Proven expertise in at least one of: supply chain risk management, supply chain master data / business partner data, regulatory compliance and due diligence, data sovereignty and data space governance, antitrust and contract law.
- Minimum availability of **10 hours per week**, more is a plus.
- Commitment to regular, active participation and active contribution.
- Agile mindset highly welcome.

We are searching for max. 10-15 members across the industry (suppliers of different sizes and materials, OEM, SME).

- OEMs
- Tier-1 suppliers
- Representatives of further N-Tier levels, including SMEs and material/chemical suppliers
- Experts for data sovereignty, data exchange governance, legal and regulatory requirements
- On demand: experts from existing use cases, in particular ESS / Due Diligence, BPDM, Industry Core, Traceability and Quality
- Operating company perspective

Review group: offered as an extended expert base for feedback, for participants who cannot commit the core time budget. Time commitment: approx. 4 hours per month.

Lead / Co-Lead: sought; approx. 4 additional hours per week for internal and external alignment, meeting preparation and steering. Final composition and lead defined after the application period.

Competence description expert group member

Responsibilities

Working Group Profile

Responsibilities and tasks	• Develop the need-to-know and legitimacy model, including role concept • Define guardrails for use and for relationship-knowledge exploitation • Specify the minimum data set per value-added step • Assess architecture options (decentralised vs. neutral third party) • Map requirements onto existing standards and KITs; propose release allocation • Prepare the year-end 2026 decision basis
-----------------------------------	---

Competencies, knowledge and skills

Management/methodological skills	• Cross-company concept and consensus work; ability to represent a company position and negotiate it • Structured requirements and use case engineering • Ability to bridge legal, commercial and technical language
Specific knowledge and skills	• 1U1D principle and its part-based vs. entity-based interpretation • Catena-X core assets: BPDM, Industry Core, Digital Twin Registry, IRS, ESS/Due Diligence KIT, Traceability • Regulatory landscape: UFLPA, EUDR, Battery Regulation, CRMA, CBAM, CSDDD/LkSG • Antitrust and confidentiality constraints in multi-tier data sharing

Working Group Profile

ANNEX: Current Discussion Results

Consolidated guardrails (agreed across contributions)

1. **Need-to-Know ≠ Right-to-See** — a legitimate information need justifies transmission of the information required for risk control, not automatic disclosure of the underlying company or relationship data.
2. **Depth only as far as necessary**— indications (problem yes/no) are preferred over full replication of the chain.
3. **Voluntariness / opt-in** — use per supplier site and, where applicable, per part, in agreement with the respective contract partner. No automatic data provision.
4. **No commercial use** — the functionality must not serve commercial negotiations; relationship knowledge must not be exploited for the operator's own purposes.
5. **Separation of capability and rules of use** — technical Catena-X capability is defined separately from the processual rules governing it.
6. **Risk management and traceability are kept separate** — risk management is frequently cross-cutting and not part-based.
7. **Regulatory disclosure as an explicit exception** — towards legitimated authorities only, purpose-bound, on the basis of an unambiguous legal obligation. Never towards OEMs, competitors or other market participants.
8. **Sovereignty and secrecy protection remain absolute** — no full supply chain disclosure, no surrender of data ownership, no exposure of business secrets.
9. **Same limits regardless of architecture** — identical sovereignty, access and disclosure boundaries apply to a decentralised and to a third-party model. How decentralisation can be implemented for N-Tier data is to be evaluated.

Decision points — where the contributions genuinely diverge

These are the items the Working Group has to resolve; they should not be smoothed over in the impulse paper.

#	Question	Position A	Position B
1	Level of identity disclosure	Minimum data set per value-added step including legal name, BPN/DUNS, address, geo-coordinates	No disclosure of BPNs, company names, tier levels or concrete supply relationships beyond the direct partner; only affectedness statements

Working Group Profile

2	Preventive risk management in scope?	Yes — ad-hoc, digital, preventive query of supplier relationships as the basis for proactive risk management	No — preventive risk detection and assessment stay with the individual companies; Catena-X focuses on standards, governance and infrastructure
3	Where does relationship knowledge live?	Neutral instance / trusted third party may technically use relationship knowledge without disclosing it	Decentrality must be preserved
4	Organisational model	Use-case-driven Expert Group within the existing structure	Shift from <i>use-case-first</i> to <i>network-twin-first</i> : organisation along a shared capability, with a clear end-to-end owner and a working structure that does not exist in the Association today
5	Target architecture framing	N-Tier as an extension of existing use cases	N-Tier as a step towards the Digital Supply / Value Network Twin as central reference architecture
6	Role definition for access	Not yet defined — who (role) may see and use the information is explicitly open	—