

The Battery's Paper Trail: Passport Data for Manufacturers, Recyclers and Lenders

A commercial-control framework for product identity, lifecycle evidence and financeability

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Background. Battery regulation and market practice are moving from model-level disclosure towards product identity, lifecycle evidence and controlled data access. Objective. This paper develops a commercial-control framework for manufacturers, recyclers and lenders that need battery-passport data to support compliance, operating decisions, transactions and financing. Method. It synthesises the consolidated European Union Batteries Regulation, United Nations Economic Commission for Europe work on cross-border digital product passports, the UN Transparency Protocol and Global Battery Alliance pilot evidence, then applies manufacturing, recycling, credit and transaction-control principles. Findings. A passport is useful only when its identifier, data lineage, access rights, evidence and change history can be reconciled to the physical battery and the relevant commercial contract. Manufacturers must design data ownership into operations; recyclers need safe-access and material-recovery evidence; lenders need defined borrowing-base eligibility, reporting covenants and remedies for data failure. Implications. Passport readiness should be governed as a cross-functional operating programme rather than a standalone software installation. Numerical exhibits are hypothetical decision tools and are not forecasts, valuations, offers or descriptions of a named asset or transaction.

JEL Classification: G21, G31, G32, L62, O33, Q53, Q56

Keywords: battery passport, digital product passport, battery manufacturing, recycling, asset finance, traceability, data assurance, residual value, circular economy, due diligence

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. THE DECISION

The decision is how to convert battery-passport obligations and voluntary traceability initiatives into a reliable commercial-control system. Manufacturers, recyclers and lenders require different views of the same asset. A manufacturer needs product conformity, supplier evidence and field performance. A recycler needs safe handling, chemistry, disassembly and chain-of-custody information. A lender needs evidence that financed inventory, receivables, equipment or project cash flow correspond to identifiable and eligible assets.

A useful passport therefore links a physical battery to controlled records, evidence and accountable owners. It must survive changes in custody, software, corporate ownership and operating status.

2. REGULATORY PERIMETER

Regulation (EU) 2023/1542 requires a battery passport from 18 February 2027 for light means of transport batteries, industrial batteries above 2 kWh and electric-vehicle batteries placed on the market or put into service [1]. Article 77 requires model information and battery-specific information, including information arising from use. Annex XIII divides information by audience and purpose [1].

The perimeter must be tested by battery category, capacity, market-placement event, responsible economic operator and applicable transition. A corporate policy should record the legal interpretation supporting each inclusion or exclusion.

3. FROM DISCLOSURE TO OPERATING EVIDENCE

A static disclosure document can become obsolete as soon as a battery is assembled, used, repaired, repurposed or transferred. The passport concept adds persistent identity, structured data and lifecycle updates. It also creates dependencies between engineering, procurement, sustainability, quality, service, information security and finance.

The operating question is whether each material claim can be traced to an authoritative source and refreshed at the required event. A populated field without evidence, ownership or version history creates apparent completeness while leaving the underlying control untested.

4. BATTERY IDENTITY

Identity begins with the battery model and the individual battery. Article 77 links passport access to a QR code and a unique identifier [1]. Identity design should prevent the same identifier being assigned to multiple assets and should preserve the relationship between cell, module, pack, vehicle or stationary system where relevant.

Controls should cover identifier creation, label printing, commissioning, replacement, rework, scrapping and retirement. A lender or recycler needs to know whether the scanned identity refers to the exact physical unit, its parent system, a model record or a replacement record.

5. ACCESS TIERS

The Regulation distinguishes publicly accessible information, information for authorities and notified bodies, and information available to persons with a legitimate interest for specified purposes [1]. Access is therefore part of the data model rather than a final user-interface setting.

Each field should carry a classification, legal basis, permitted purpose, accountable owner, retention rule and disclosure route. Commercially sensitive composition, dismantling or performance information requires controlled access. Public transparency does not require publication of every underlying supplier document.

6. THE COMMERCIAL-CONTROL SYSTEM

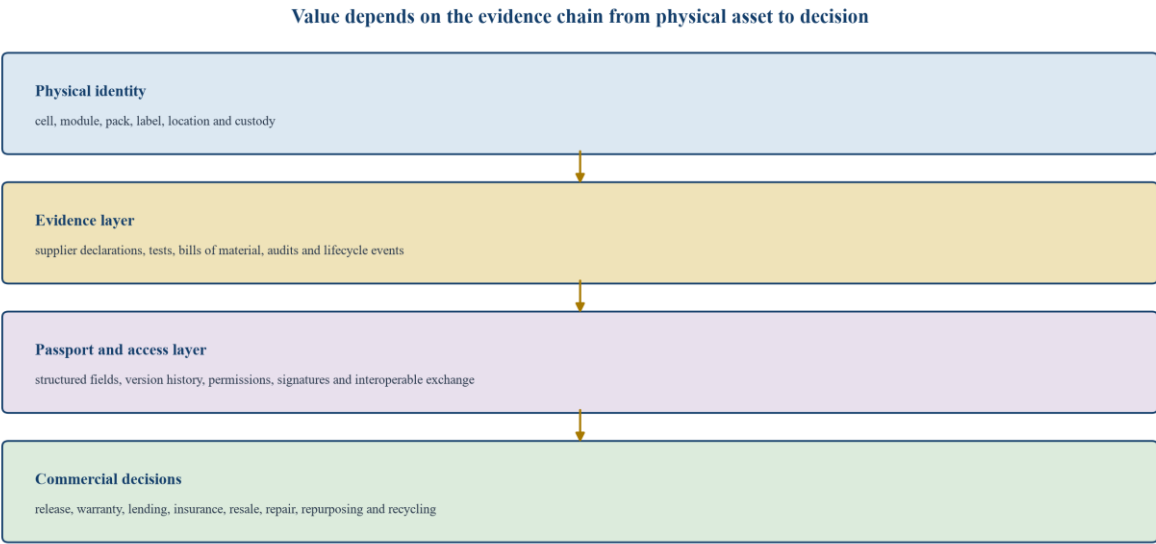


Figure 1. Battery-passport evidence and commercial-control system
Generic operating model; actual legal duties, systems and access rights require jurisdiction-specific confirmation.

7. DATA DOMAINS

Annex XIII covers material composition, chemistry, hazardous substances, critical raw materials, carbon footprint, responsible sourcing, recycled content, technical performance, warranty, conformity and waste information [1]. Restricted fields extend into detailed component composition, spare parts and dismantling information [1].

An implementation team should translate legal fields into governed business objects. The legal label, engineering definition, source system, unit, validation rule and update event may differ. A data dictionary prevents two departments from reporting different meanings under the same field name.

8. CONTROL REGISTER

Table 1. Core data domains and accountable controls

Data domain	Primary operational owner	Evidence	Principal commercial use
Identity and manufacture	Operations and quality	serial record, batch genealogy, release record	conformity, inventory eligibility, warranty
Composition and chemistry	Engineering and procurement	bill of material, supplier declaration, laboratory test	safety, sourcing, recycling route
Carbon and sourcing	Sustainability and procurement	calculation file, chain-of-custody record, audit	compliance, customer tender, financing covenant
Performance and durability	Engineering and service	test report, battery-management-system record	warranty, residual value, repurposing
Repair and dismantling	Service engineering	controlled manual, parts record, event log	safe repair, reuse and recycling
End-of-life recovery	Recycler and compliance	receipt, sorting, treatment and output mass balance	producer responsibility, recovery evidence
Access and change history	Data governance and security	entitlement log, signature, timestamp, version	assurance, dispute resolution, audit

9. MANUFACTURER MASTER DATA

Manufacturers need an authoritative product model that reconciles engineering bills of material, manufacturing bills of material, approved suppliers, plant routings and market variants. The passport should not become a competing product master. It should publish controlled views from designated systems and record the evidence supporting calculated fields.

Variant control matters because chemistry, component supplier, plant, firmware or process changes can alter data. The release process should determine when a change creates a new model record, a revised version or a battery-specific update.

10. SUPPLIER EVIDENCE

Upstream evidence may originate with mines, refiners, active-material producers, cell makers, component suppliers and logistics providers. Contract clauses should define required fields, calculation methods, assurance, update frequency, correction rights, confidentiality and audit access.

Procurement should distinguish a supplier declaration from independently verified evidence. The passport should carry the claim and a link or reference to its support. Missing evidence should trigger a defined exception process, not a silently estimated value.

11. BILL-OF-MATERIAL RECONCILIATION

Composition claims require reconciliation to the actual bill of material and production genealogy. Engineering quantities, purchasing quantities and production consumption can diverge through scrap, substitutions, rework and yield loss.

A defensible process reconciles the approved formula to batch consumption and explains the allocation method for shared process inputs. The passport should not imply unit-level measurement where evidence exists only at model, batch, facility or supplier level.

12. CARBON FOOTPRINT DATA

Carbon-footprint fields combine activity data, energy, material inputs, transport, allocation rules and emissions factors. The calculation boundary, methodology version, data period, facility and supporting study should remain linked to the reported value. Article 7 and Annex XIII connect carbon information to the battery passport [1].

Finance and procurement teams should use the same controlled value when a customer contract, margin adjustment or sustainability-linked covenant references carbon performance. Parallel calculations create reconciliation risk.

13. RESPONSIBLE SOURCING

Responsible-sourcing data depends on policies, risk assessment, supplier engagement, audits and disclosure. Article 52 requires specified operators to make battery due-diligence information available while recognising business confidentiality and competitive concerns [1].

The passport can expose the required result or report reference while underlying evidence remains permissioned. An exception register should capture unavailable origin data, unresolved adverse findings and corrective actions. A binary completed field is inadequate for ongoing supply-chain risk.

14. RECYCLED CONTENT

Recycled-content claims require clear definitions of input, process, allocation and evidence. Purchasing certificates alone may not reconcile to production. The control should connect supplier evidence, incoming material, production consumption and reported product share.

The lender's interest is whether a contractual or regulatory claim can be substantiated and whether failure could interrupt sales. The recycler's interest is whether recovered output is recognised within the relevant accounting and certification framework.

15. PERFORMANCE AND DURABILITY

Performance fields include rated capacity, voltage, power capability, expected lifetime, energy efficiency, resistance and related test conditions [1]. Values should record the test method, temperature, state of charge, sample, manufacturing site and version where material.

The commercial use extends beyond compliance. The same evidence affects product acceptance, warranty provisioning, residual value and repurposing. Users should avoid comparing values produced under different methods or operating conditions.

16. DYNAMIC LIFECYCLE DATA

Battery-specific data may change through use. State of health, charge cycles, temperature exposure, repair and negative events can influence safety and value. The system must identify the source, timestamp, sampling interval, transformation and confidence for dynamic data.

A lender should avoid treating an unverified state-of-health estimate as realised collateral value. A recycler may still use the estimate for routing, subject to inspection and safety controls. The decision rule should match the evidence quality.

17. REPAIR AND REPLACEMENT

Repair can replace modules, electronics or other components and change the relationship between original and current configuration. The event record should identify who performed the work, applicable procedure, installed component identity, tests and release decision.

The passport architecture should preserve the original history and append the authorised event. Overwriting the record removes evidence needed for warranty, product liability, resale and finance.

18. REPURPOSING

Repurposing changes intended use, duty cycle, safety case and revenue model. A vehicle battery entering stationary storage requires testing, grading, configuration and a new operating responsibility. Historical passport data can reduce uncertainty, while it does not replace current inspection and engineering assessment.

Contracts should allocate responsibility for data transfer, testing, new identifiers, warranties and future updates. The original manufacturer may have limited responsibility for the repurposed system.

19. END-OF-LIFE DATA

End-of-life information should support safe removal, transport, storage, disassembly and treatment. Chemistry, residual charge, damage and thermal history can affect routing. The Regulation includes waste-prevention and management information within publicly accessible passport content [1].

Recyclers need information that is timely, accessible and usable at receipt. An unavailable cloud record, damaged label or mismatched identifier requires a safe fallback procedure.

20. RECYCLER INTAKE CONTROL

At intake, the recycler should scan identity, inspect physical condition, record custody, confirm chemistry and route the battery. Exceptions include unreadable identifiers, incomplete records, unauthorised repair, damage and conflicting chemistry indications.

The intake system should preserve both passport evidence and recycler observations. A discrepancy should not be resolved by altering the historical record. It should generate a new event, quarantine decision and investigation.

21. RECOVERY MASS BALANCE

Recovery evidence should reconcile inbound battery mass to reusable components, recovered materials, residues, losses and inventory change. Yield must be reported at the defined process and material boundary. Laboratory recovery does not equal plant output available for sale.

The passport can carry or reference end-of-life outcomes, while the recycler's plant mass balance remains a separate controlled record. Financing decisions should use saleable recovered output after grade, payability, processing charges and working capital.

22. CROSS-BORDER INFORMATION

Battery supply chains and recycling routes cross jurisdictions. UNECE identifies potential conflicts among traceability, data protection, security, confidentiality and national rules for critical raw materials [2]. A global data design therefore needs jurisdictional access rules and contractual transfer mechanisms.

A single public database is not the only architecture. Federated exchange can leave evidence with the responsible party while sharing authorised claims and links. The UN Transparency Protocol describes linked traceability events and structured credentials as a cross-border mechanism [3].

23. INTEROPERABILITY

Article 77 requires open standards, interoperable formats, transfer through an open interoperable data-exchange network, and machine-readable, structured and searchable information [1]. Interoperability should be tested through actual exchange between independent systems.

The test should cover identifier resolution, schema version, units, controlled vocabularies, credentials, attachments, access requests, revocation and correction. Exporting a proprietary report does not establish interoperable lifecycle data.

24. VENDOR CONTINUITY

The passport must remain available if the responsible economic operator ceases activity, subject to the Regulation's requirements [1]. Commercial continuity also matters if a software provider fails, changes terms or withdraws a service.

Contracts should provide data portability, schema documentation, export frequency, escrow or continuity arrangements, service levels, incident handling and termination support. The economic operator remains responsible for the accuracy, completeness and currency of passport information under Article 77 [1].

25. DATA PROVENANCE

Every material field should have a provenance record: source organisation, source system, evidence document, method, period, unit, transformation, approval, timestamp and version. Calculated fields should identify their formula and inputs.

Provenance allows a verifier to follow the claim without reconstructing the entire programme. It also allows a lender to distinguish supplier-reported, manufacturer-tested and independently assured data.

26. ASSURANCE DESIGN

Global Battery Alliance pilot work highlighted the importance of decentralised data custody, digital report signing, data exchange and external verification [4]. The 2024 pilots also found that comprehensive assurance rules for aggregation and exchange still required development and testing [4].

An assurance plan should prioritise fields by legal, safety and financial consequence. Identity, chemistry, carbon, sourcing, performance and recovery claims may justify different procedures and frequencies. Assurance should include the process that creates the data, not only the final value.

27. EVIDENCE HIERARCHY

A practical hierarchy can distinguish direct measurement, controlled system record, verified supplier claim, unverified supplier claim and management estimate. The label should accompany the field in internal decision systems.

Where an estimate is permitted, the method and uncertainty should be explicit. A temporary estimate should have an owner and expiry. Silent substitution of an estimate for missing evidence weakens the entire passport.

28. DATA QUALITY

Data quality can be assessed through completeness, accuracy, timeliness, consistency, uniqueness and validity. A field may be complete and still be wrong. A valid value may be too old for a credit decision.

Quality thresholds should be tied to use. Public information may tolerate a scheduled refresh, while a release or collateral event may require current evidence. Exceptions should be visible to the decision-maker.

29. CYBERSECURITY

The passport creates new attack surfaces through identifiers, application interfaces, supplier exchange and privileged data. Threats include identity cloning, fraudulent claims, unauthorised composition access, ransomware and manipulation of state-of-health data.

Controls should cover authentication, authorisation, least privilege, encryption, key management, signing, logging, vulnerability management, incident response and recovery. Cybersecurity testing should include the physical-to-digital link, because a secure record attached to the wrong battery still fails.

30. PRIVACY AND CONFIDENTIALITY

Battery data can reveal supplier relationships, process know-how, asset use and operating patterns. Access design should disclose only the fields required for the permitted purpose. A lender may need eligibility and exception evidence without receiving proprietary cell recipes.

The programme should document lawful access, purpose limitation, contractual confidentiality, retention and onward-sharing restrictions. The same data may have different treatment across jurisdictions.

31. CHANGE CONTROL

Regulatory requirements, data definitions, schemas, methods and products will change. Each change should have an impact assessment, owner, effective date, migration plan and test evidence.

Historical decisions should remain reproducible. If a carbon method changes, the record should identify which method supported the original customer or credit decision. Recalculation should be distinguishable from restatement.

32. MANUFACTURER ECONOMICS

Passport implementation creates costs in data discovery, supplier engagement, systems integration, assurance, security, governance and operating support. Benefits can arise through faster customer qualification, fewer manual disclosures, stronger warranty control, better recovery planning and improved financing evidence.

Benefits should be measured through defined operational metrics. Compliance alone may justify mandatory spend. Additional value claims require baselines and accountable owners.

33. RECYCLER ECONOMICS

Recyclers can gain from faster chemistry identification, safer routing, better disassembly information, improved feed planning and stronger recovery evidence. Value depends on data availability at intake and compatibility with plant operations.

The recycler should quantify scan success, exception rate, inspection time, sorting accuracy, safety incidents, recovery yield and evidence cycle time. A passport that cannot be consumed by the intake workflow creates limited operating value.

34. LENDER ECONOMICS

Lenders can use passport evidence to improve asset identification, eligibility testing, borrowing-base reporting, technical monitoring and residual-value analysis. The passport does not eliminate technology, market, legal or enforcement risk.

The credit case should state which fields influence a decision and what happens when data is unavailable, inconsistent or disputed. The lender should retain independent rights to inspect, audit and enforce.

35. ILLUSTRATIVE IMPLEMENTATION COST

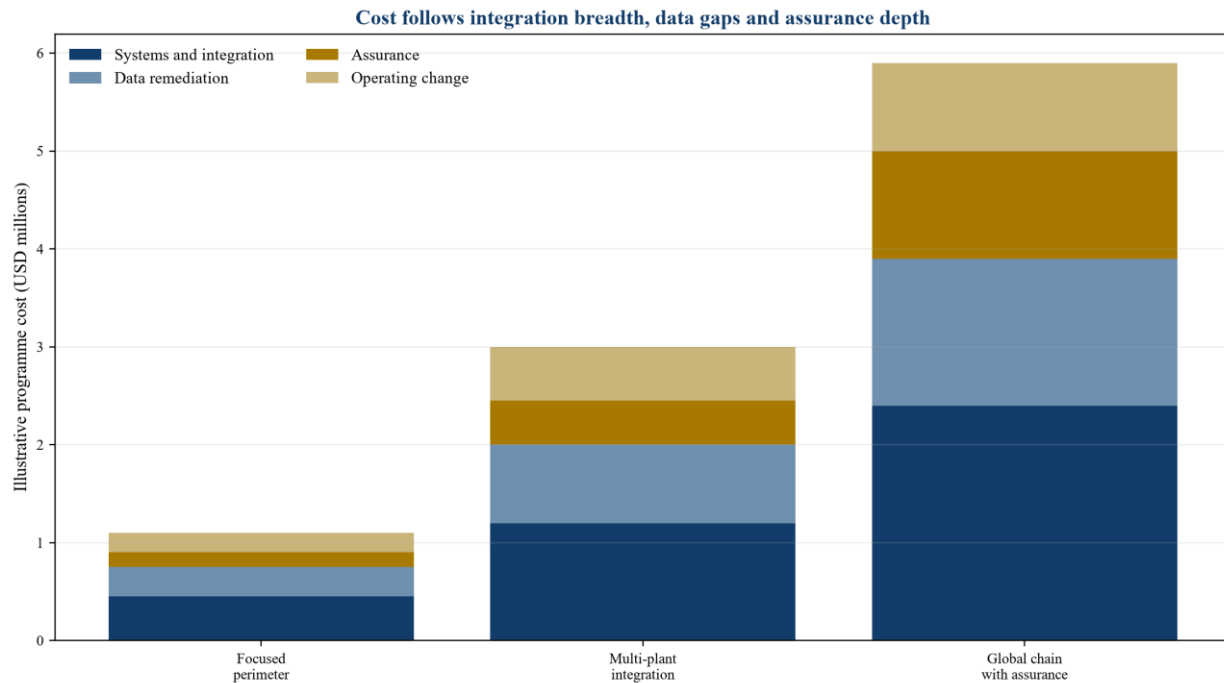


Figure 2. Illustrative implementation-cost sensitivity by complexity and assurance scope
Hypothetical values for decision design only; no actual company cost, quote or forecast is represented.

36. INTERPRETING THE COST CASES

The focused case assumes a limited product perimeter, accessible source data and modest integration. The multi-plant case adds site variation, supplier remediation and lifecycle interfaces. The global case adds jurisdictions, complex supplier chains and broader assurance. All values are illustrative.

Management should replace them with vendor proposals, internal resource plans, data-remediation estimates and contingency. The model should separate one-time implementation from recurring data, hosting, assurance and support.

37. INVENTORY FINANCE

For inventory finance, eligibility can require a valid identifier, recognised model, verified ownership, approved location, conformity status and absence of specified exceptions. The borrowing base should reconcile unit or batch records to warehouse and accounting records.

Duplicate, missing or retired identifiers should be ineligible until resolved. Advance rates should reflect enforceability, liquidity, obsolescence, condition and recovery costs in addition to passport completeness.

38. RECEIVABLES FINANCE

Passport records can support proof that delivered batteries meet contractual specifications, while receivables eligibility still depends on invoice validity, acceptance, dilution, set-off, concentration and debtor credit.

The lender should define which product disputes or data failures create ineligibility. Automated matching can shorten reporting, provided exceptions remain visible and reconciled to the receivables ledger.

39. EQUIPMENT AND FLEET FINANCE

For financed fleets or battery equipment, persistent identity can support asset registers, maintenance, condition monitoring and transfer. The security package should identify how the lender accesses records after default or operator failure.

State-of-health data may inform maintenance and resale, subject to method, calibration and manipulation controls. Valuation should use observed market evidence and inspection, with passport data as one input.

40. MANUFACTURING PROJECT FINANCE

A cell or pack project may depend on qualification, compliant output and customer acceptance. Passport readiness can be included in completion tests where it is necessary for sale. The test should specify systems, data, evidence, interfaces and accepted product.

Debt service should be modelled after ramp-up, warranty, working capital and compliance operating cost. Software installation alone should not satisfy completion.

41. RECYCLING PROJECT FINANCE

A recycling project requires secure feed, permitted operations, proven recovery, saleable products and working capital. Passport data can improve feed visibility and mass-balance evidence. It cannot compensate for unproven process yield or absent offtake.

Completion should test safe intake, chemistry routing, sustained throughput, recovery, product quality, environmental performance and data reporting. Feed without usable passport data should have a defined inspection and pricing route.

42. ACQUISITION DUE DILIGENCE

In an acquisition, the buyer should test regulatory perimeter, product coverage, source systems, supplier rights, data quality, assurance, security, operating continuity and unresolved exceptions. A demonstration environment may not represent production coverage.

The diligence sample should trace selected batteries from physical identity to model data, supplier evidence, manufacturing release and lifecycle events. Findings should influence price, warranty, indemnity, remediation funding and integration planning.

43. CONTRACT ARCHITECTURE

Table 2. Contract provisions for a battery-passport operating model

Interface	Required provisions	Evidence and remedy
Supplier to manufacturer	data fields, methods, update timing, audit, correction, confidentiality	signed evidence, exception notice, replacement or remediation rights
Manufacturer to customer	scope, access, permitted use, warranty boundary, corrections	acceptance record, version history, claim process
Operator to software provider	portability, interoperability, security, service level, continuity, exit	export test, incident log, migration support
Borrower to lender	eligibility, reporting, audit, access after default, data-failure event	borrowing-base certificate, reserve, ineligibility or covenant remedy
Holder to recycler	identity, custody, condition, dangerous-goods information	intake scan, inspection, quarantine and discrepancy record
Recycler to producer or buyer	treatment, recovery, product quality, chain of custody	mass balance, assay, certificate and audit trail

44. REPRESENTATIONS AND WARRANTIES

Representations should address ownership, authority, accuracy of specified fields, lawful access, absence of known manipulation and compliance with agreed methods. They should distinguish current facts from forward-looking performance.

Warranty scope should reflect who created and controlled the data. A manufacturer should not be deemed to guarantee third-party lifecycle records it cannot verify. The contract can require prompt correction and preserve evidence of the prior value.

45. CONDITIONS PRECEDENT

A financing condition precedent may include approved architecture, data dictionary, sample passports, supplier contracts, security testing, business-continuity plan, assurance report and operating procedures. Each deliverable should have an acceptance standard.

Conditions should focus on matters necessary before funding. Later milestones can address expanded supplier coverage or assurance where funding structure and risk permit.

46. REPORTING COVENANTS

Periodic reporting can include coverage, completeness, exceptions, failed scans, stale fields, supplier gaps, cyber incidents, warranty claims, recalls, repair events and recovery outcomes. Metrics should reconcile to the financed perimeter.

The lender should specify delivery timing, certification and access to supporting records. A dashboard without reconciliation to inventory or cash flow is insufficient.

47. DATA-FAILURE REMEDIES

Remedies should be proportionate to consequence. A missing low-risk public field may require correction. Duplicate identity, unsupported conformity or manipulated performance data may require quarantine, ineligibility, reserve, suspension or an event of default if material and uncured.

The agreement should define cure periods, independent review and reinstatement. Automatic default for every technical error can make the control unusable.

48. INSURANCE

Insurers may use identity, condition and event data for underwriting, risk engineering and claims. Coverage and exclusions remain contract-specific. Data access should preserve privilege, confidentiality and claims procedures.

A passport event does not by itself establish causation. Incident investigation should preserve device data, physical evidence, maintenance records and chain of custody.

49. RESIDUAL VALUE

Residual value depends on chemistry, condition, remaining performance, warranty, market demand, removal cost, transport, repurposing suitability and recycling economics. Passport data can reduce information asymmetry where evidence is credible.

The valuation should apply scenario-specific cash flows and observed market references. State of health is one input, and should not be converted mechanically into price.

50. PORTFOLIO MONITORING

At portfolio level, lenders and investors can monitor coverage, exception concentration, ageing, supplier dependency, product changes and adverse events. Aggregation should preserve the ability to drill to the affected asset and evidence.

Trend analysis can identify declining data quality or repeated supplier failure. It should avoid mixing models or methods that are not comparable.

51. ILLUSTRATIVE LENDER FRAMEWORK

Table 3. Illustrative lender eligibility and monitoring scorecard

Dimension	Green	Amber	Red	Illustrative action
Identity	unique and reconciled	temporary location mismatch	duplicate or untraceable	investigate; exclude if unresolved
Conformity evidence	current and complete	minor open document item	unsupported or withdrawn	reserve or exclude
Composition and safety	verified applicable data	supplier evidence pending	conflicting chemistry or safety record	quarantine and technical review
Performance data	method and timestamp controlled	stale within agreed cure	missing, manipulated or incompatible	haircut or exclude from value
Access and continuity	tested lender access and export	remediation scheduled	no effective access or portability	covenant remedy
Lifecycle exceptions	no material unresolved event	repair or incident under review	material unassessed damage or recall	suspend eligibility

52. BORROWING-BASE FORMULA

An illustrative borrowing base can be expressed as eligible units multiplied by the lower of cost and eligible value, then multiplied by an advance rate, less reserves. Eligibility and value should be calculated independently.

The formula should exclude duplicate identities, disputed title, unsupported conformity, prohibited locations and material unresolved incidents. Reserves may address concentration, obsolescence, data quality, recall and enforcement cost. The exact structure requires asset and jurisdiction-specific analysis.

53. STRESS TESTING

Stress cases should combine operational and data events. Examples include supplier evidence failure, delayed regulatory acceptance, cyber outage, mass identifier mismatch, recall, lower recovery yield and reduced resale demand.

The analysis should show liquidity, covenant headroom and remediation time. A data incident can become a cash incident when it stops release, customer acceptance or borrowing-base eligibility.

54. INVESTMENT-COMMITTEE QUESTIONS

The committee should ask which batteries are in scope, who is legally responsible, which fields are decision-critical, where evidence originates, how access survives distress, which exceptions affect revenue and how remediation is funded.

It should also ask whether management has tested physical-to-digital reconciliation at scale. A policy and software demonstration do not establish operating effectiveness.

55. GOVERNANCE

Executive accountability should sit with an owner who can coordinate engineering, operations, procurement, sustainability, legal, security and finance. Data owners remain accountable for their fields. A steering committee should resolve cross-functional exceptions and approve method changes.

Internal audit or an independent assurance function can test design and operation. The first line should retain responsibility for evidence creation and correction.

56. OPERATING METRICS

Core metrics include product coverage, identifier uniqueness, evidence completeness, supplier response, validation failure, stale-field rate, access-response time, correction cycle, scan success, recovery reconciliation and assurance findings.

Metrics should be segmented by product, plant, supplier and market. A high aggregate completeness rate can conceal a critical gap in one financed programme.

57. IMPLEMENTATION ROADMAP

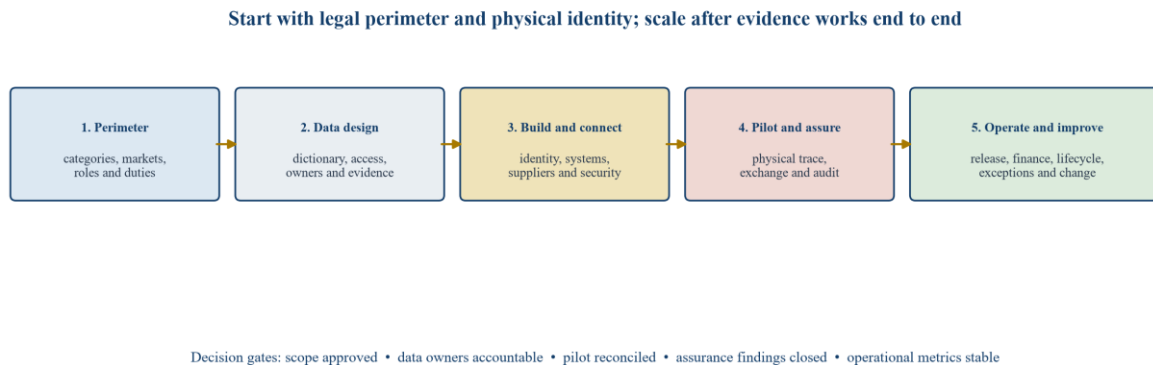


Figure 3. Phased battery-passport implementation roadmap
Generic sequence; regulatory timing and programme duration require organisation-specific confirmation.

58. PHASE ONE: PERIMETER

Map products, markets, capacities, placement events, economic operators and applicable dates. Record legal interpretations and exclusions. Select the first product family based on regulatory relevance, commercial importance and data feasibility.

Create a responsibility map covering manufacturer, importer, authorised representative, supplier, customer, service provider, holder and recycler where applicable.

59. PHASE TWO: DATA DESIGN

Create the data dictionary, evidence register, access matrix, retention schedule and change process. Map each field to source systems and accountable owners. Identify gaps that require supplier action, testing or new operational capture.

Define the physical identifier and relationships among cell, module, pack and system. Approve the method for batch-level and model-level evidence.

60. PHASE THREE: BUILD

Configure identity, integration, validation, credentials, access, logging and user workflows. Update supplier and customer contracts. Establish exception queues and escalation.

Security testing should include interfaces, privileged roles, identifier substitution and recovery. Portability should be demonstrated through an export to an independent environment.

61. PHASE FOUR: PILOT

Select representative batteries, suppliers, plants, markets and lifecycle events. Trace each unit from physical label through source evidence, passport, customer access and correction. Include adverse cases such as damaged labels and missing supplier records.

Independent assurance should test both reported values and the processes that create, aggregate and exchange them. Findings should be closed before scale.

62. PHASE FIVE: OPERATE

Integrate passport controls into product release, procurement, warranty, asset reporting, service and recycling. Monitor coverage and exceptions. Review methods and access rights after regulatory or product change.

Continuity tests should confirm that authorised users can retrieve and export records during a simulated provider outage or corporate transition.

63. FIRST 30 DAYS

Appoint accountable leadership, confirm legal perimeter, select the pilot product, inventory source systems, identify decision-critical fields and establish the issue register. Freeze assumptions that lack verified support.

Engage priority suppliers with exact data and evidence requests. Avoid broad questionnaires that do not map to controlled fields.

64. DAYS 31 TO 60

Complete the data dictionary, physical-identity design, access model and contract requirements. Build the first evidence chain for representative units. Quantify missing data and remediation resources.

Define lender or investor reporting only after the underlying evidence chain is understood. This prevents dashboards from becoming a substitute for control design.

65. DAYS 61 TO 100

Run the pilot through manufacturing release, customer access, repair or simulated lifecycle event and recycler intake. Test correction, revocation, export and recovery. Perform security and assurance reviews.

Approve scale only when critical findings have owners, funding and closure dates. Report remaining limitations explicitly.

66. MANUFACTURER CHECKLIST

Confirm category and market; assign identity; reconcile model and batch; collect supplier evidence; validate composition, carbon and sourcing; control technical performance; configure access; test interoperability; manage change; preserve continuity; report exceptions; and assure critical fields.

The checklist should be embedded in product-launch and change-control gates.

67. RECYCLER CHECKLIST

Confirm legal and safety access; scan and inspect; record custody and condition; route by chemistry and risk; preserve discrepancy evidence; reconcile process mass balance; substantiate recovered output; update lifecycle records where authorised; and maintain fallback procedures.

The recycler should measure whether passport data improves actual intake and recovery decisions.

68. LENDER CHECKLIST

Define financed perimeter; identify passport-dependent eligibility; confirm legal access; test physical identity; review evidence hierarchy; set reporting and audit rights; establish data-failure remedies; stress cash and collateral; test access after distress; and retain independent inspection rights.

The credit memorandum should identify the fields that influence approval, advance rate, reserve or covenant.

69. COMMON FAILURE: SOFTWARE-FIRST PROCUREMENT

Buying a platform before defining scope, data ownership and evidence can automate uncertainty. Integration effort then exposes unresolved definitions and supplier gaps.

Procurement should follow an approved operating model and testable requirements. Vendor demonstrations should use representative customer data and adverse cases.

70. COMMON FAILURE: PUBLIC-FIELD COMPLETENESS

A passport may look complete because public fields are populated while restricted evidence, lifecycle updates or supplier provenance remain weak. Coverage should be assessed by decision use and evidence quality.

Critical exceptions should receive more weight than numerous low-risk completed fields.

71. COMMON FAILURE: ONE-TIME MIGRATION

Initial data loading does not create an operating passport. Product changes, new suppliers, service events and regulatory revisions require continuous updates.

The programme should fund recurring ownership, assurance, support and change control. Otherwise data quality declines after launch.

72. COMMON FAILURE: OVERSTATED RESIDUAL VALUE

Passport data can support condition assessment. It cannot create a liquid secondary market or guarantee sale proceeds. Residual-value models require market evidence, inspection, removal and logistics costs, and scenario analysis.

Credit papers should separate data confidence from market liquidity.

73. COMMON FAILURE: UNCLEAR DISTRESS ACCESS

A lender may rely on data that becomes unavailable when the borrower, manufacturer or software provider fails. Access, export and continuity rights should be documented and tested before funding.

The test should include credentials, encryption keys, schema documentation and ability to interpret exported data.

74. DECISION RULE

Proceed when the regulated perimeter is defined, physical identity works, critical data has accountable owners and evidence, access is controlled, exchange is interoperable, continuity is tested, exceptions have remedies and the economics remain supportable under stress.

Defer scale where identity, evidence or lifecycle ownership remains unresolved. These are operating-control gaps rather than presentation issues.

75. CONCLUSION

Battery passports can become valuable infrastructure for manufacturing, recycling and finance when the record is linked to the physical battery, supported by evidence and governed across its lifecycle. The commercial value arises from better decisions: release, qualification, warranty, lending, repair, repurposing and recovery.

The implementation priority is an auditable evidence chain. Manufacturers should own the operational data model, recyclers should integrate it into safe intake and mass balance, and lenders should translate it into eligibility, reporting and remedies. A well-designed passport strengthens transparency while preserving legitimate access and confidentiality.

76. MINIMUM VIABLE PASSPORT

A minimum viable passport should cover the legally applicable fields, persistent identity, accountable ownership, evidence references, controlled access, version history, correction and continuity. It should operate for a representative product through manufacture, customer access and at least one lifecycle event. Scope should be explicit where fields remain unavailable or methods remain under development.

The minimum should not be defined by the smallest possible user interface. It should be defined by the smallest end-to-end evidence chain that can support a real release, compliance or financing decision. A pilot that displays model data without reconciling a physical unit has not tested the central control.

77. DATA-ROOM DESIGN

A transaction data room should organise evidence by legal perimeter, governance, architecture, field definition, supplier support, operating test, assurance, cybersecurity, continuity and financial impact. Sample records should be anonymised or permissioned where confidentiality requires it.

Reviewers need a route from a reported field to the underlying evidence and approval. Indexing thousands of source documents without the mapping leaves diligence teams to reconstruct lineage. The data room should include unresolved exceptions and management actions, because omission prevents an informed assessment of cost, timing and risk.

78. VALUATION IMPLICATIONS

Passport capability may affect value through avoided interruption, faster qualification, lower manual reporting cost, better warranty control, stronger financing evidence and improved lifecycle recovery. Each pathway requires a measurable operating or cash-flow link. A valuation should avoid applying a general premium merely because a passport platform exists.

The buyer should model required remediation, recurring operating cost and potential commercial benefit separately. A mature evidence chain may reduce uncertainty in specific assumptions. It does not remove market, technology, execution or regulatory risk. Any adjustment should be supported by asset-specific diligence and observable transaction or operating evidence where available.

79. SEPARATION AND INTEGRATION PLANNING

In a carve-out, passport data may depend on shared enterprise systems, supplier contracts, cloud services and security credentials. The separation plan should identify records, interfaces, licences, personnel and transitional services needed to preserve compliance and customer access. Data ownership and export should be agreed before closing.

In an integration, the buyer should preserve traceability while harmonising identifiers, dictionaries and access models. Premature migration can break links between historical evidence and physical units. A controlled mapping should retain legacy identifiers, source provenance and the date at which each system became authoritative.

80. ENFORCEMENT PREPARATION

An enforcement-ready control pack should contain the perimeter decision, responsibility map, data dictionary, source mapping, evidence samples, validation rules, access controls, change records, exception log and assurance results. It should demonstrate how inaccurate or stale information is detected and corrected.

Staff who operate the process should be able to explain the control. Reliance on a small implementation team creates continuity risk. Training, procedures and periodic exercises should cover ordinary updates, supplier failure, security incident, recall, damaged identifier and regulator request.

81. BOARD OVERSIGHT

The board or relevant committee should receive a concise view of regulatory readiness, critical exceptions, supplier concentration, cybersecurity, remediation funding and commercial dependencies. Management should distinguish design completion from operating effectiveness and pilot coverage from full product coverage.

Board approval is most useful at defined gates: scope and accountability, investment case, pilot acceptance, scale decision and material change. Detailed field management remains with accountable executives. Escalation thresholds should capture failures that could stop market access, impair financed assets, create safety exposure or undermine material public claims.

82. PRODUCT-LAUNCH INTEGRATION

New-product introduction should include passport requirements alongside safety, quality, manufacturability, cost and customer qualification. The launch plan should identify data created during design, sourced from suppliers, measured during production and generated after sale. Field ownership should be approved before design freeze.

Launch review should test whether late component substitution, firmware revision or plant transfer changes any published or restricted field. The product should not receive final commercial release when decision-critical passport evidence remains unresolved. A controlled concession can be used only where lawful, documented, time-limited and approved by the accountable function.

83. SUPPLIER-ONBOARDING INTEGRATION

Supplier selection should evaluate data capability as part of technical and commercial qualification. The assessment should cover definitions, source systems, calculation methods, evidence retention, change notification, assurance and secure exchange. The requirement should be proportionate to the component and claim.

Where a smaller supplier lacks mature systems, the buyer can provide templates, guidance and a remediation timetable. The resulting value remains supplier-reported until the agreed validation occurs. Concentration analysis should identify products where one supplier's evidence gap can prevent complete passport records or interrupt customer acceptance.

84. QUALITY-MANAGEMENT INTEGRATION

Quality management should treat passport discrepancies as controlled non-conformities when they affect product identity, conformity, safety or required information. Root-cause analysis should distinguish incorrect physical configuration, incorrect source data, transformation error and publication failure.

Corrective action should address the affected units, the source process and prior disclosures. The passport history should preserve the original value, correction, reason and approver. Product recall or field action remains governed by applicable safety and regulatory procedures. The data-control process should support those procedures through reliable scope identification.

85. TREASURY AND WORKING CAPITAL

Passport readiness can influence working capital if incomplete records delay product release, customer acceptance, invoicing or borrowing-base inclusion. Treasury should model the cash effect of exception volumes and cure time. The model should separate operational delay from permanent ineligibility.

Financing documents may allow a reserve for affected inventory while remediation is underway. The reserve requires clear release tests. Management should monitor whether supplier data delays are creating inventory that is physically complete and economically stranded pending evidence.

86. CUSTOMER TENDERING

Customer tenders increasingly request traceability, carbon, recycled-content and responsible-sourcing information. A governed passport evidence chain can reduce repeated manual responses and inconsistencies across bids. Tender teams should draw from approved data rather than creating separate calculations.

The response should state the reporting period, method, assurance and coverage. Future capability should be described as a planned action with timing and dependency, not as an existing feature. Contract commitments should be reviewed by the functions responsible for providing and maintaining the data.

87. DISPUTE RESOLUTION

Disputes can concern the identity of the battery, accuracy of a field, applicable method, access right, correction or commercial consequence. Contracts should define notice, evidence preservation, technical-expert review and interim treatment of affected assets.

The system should retain signed records, access logs and versions relevant to the disputed decision. A corrected passport does not remove the need to determine which information was available when the contract, release or credit decision occurred. Expert determination may be suitable for technical fields, subject to the governing agreement.

88. PROGRAMME FUNDING

The business case should identify mandatory compliance investment, operating-risk reduction and separately evidenced commercial opportunities. Costs include internal personnel, supplier remediation, integration, security, assurance, licensing, hosting, support and future change.

Funding should follow gated deliverables: approved perimeter, completed data design, working pilot, closed critical findings and scaled operating coverage. Contingency should address supplier gaps and legacy-system complexity. Benefits should have owners, baselines and measurement periods. A general strategic-value statement is insufficient for investment governance.

89. PRACTICAL CLOSING PERSPECTIVE

The strongest battery-passport programme begins with the decisions that depend on the data. Legal teams define the obligation and permitted access. Engineers define the product and performance. Operations connect identity to manufacture. Procurement obtains supplier evidence. Recyclers connect history to safe recovery. Finance translates reliable fields into eligibility, monitoring and remedies.

This shared operating model creates a durable paper trail without relying on paper. Its credibility rests on traceable evidence, clear responsibility and tested continuity. Technology provides the

exchange mechanism. Governance and operating discipline determine whether the record can support a regulator, customer, recycler, lender or investment committee.

REFERENCES

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

LinkedIn: <https://www.linkedin.com/in/ckadya/>

Profile: <https://www.matchpoint-partners.com/team/ck-adya.html>

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.