European Sovereign Cloud M&A: Valuing Compliance and Procurement Access

A Rights-Based Framework for Revenue Quality, Switching Costs and Transaction Value

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

European sovereign-cloud providers increasingly compete on a combination of technical service, jurisdictional control, security assurance, operational autonomy and access to regulated or public-sector procurement. The European Commission's Cloud Sovereignty Framework now scores providers across strategic, legal, data and artificial-intelligence, operational, supply-chain, technological, security and environmental objectives. France's SecNumCloud qualification, Germany's BSI C5 attestation framework, the Digital Operational Resilience Act, NIS2, the General Data Protection Regulation and the Data Act create further evidence requirements. These regimes affect demand and diligence, although none turns a supplier's marketing claim into durable revenue by itself.

This paper develops an acquisition and valuation framework for a European sovereign-cloud platform. It tests whether sovereignty credentials create defensible cash flow by tracing each claim through qualification scope, tender eligibility, framework admission, service order, customer acceptance, collection and renewal. It separates general legal compliance, security assurance, procurement access, operational sovereignty, technology dependence and contractual switching friction. The framework also identifies conditions that may weaken value: change-of-control clauses, non-transferable qualifications, subcontractor dependence, foreign-law exposure, customer concentration, cloud-portability obligations and the cost of preserving parallel sovereign operating stacks.

The worked case is wholly hypothetical. It considers the acquisition of a multi-country cloud platform with EUR 214 million of last-twelve-month revenue, EUR 38 million of adjusted EBITDA, EUR 690 million of enterprise value and EUR 210 million of acquisition debt. Of reported revenue, EUR 92 million is linked to public-sector or regulated-customer arrangements. The central case recognises only EUR 61 million as procurement-enabled recurring revenue after testing order status, termination, qualification scope, control change and collection. A market-participant analysis produces a central enterprise-value range of EUR 630 million to EUR 735 million. The figures do not describe an identified company, bidder, lender or transaction.

The paper concludes that sovereignty credentials produce value when they are specific, current, transferable, operationally supported and connected to accepted service and collected cash. Procurement access can widen the addressable market and lower customer acquisition friction. Its value should be recognised through contract cash flow, renewal evidence, credible switching cost and replacement expenditure. A buyer should pay separately for verified revenue, reusable capabilities and scarce rights, while retaining price protection for remediation, dependency and change-of-control risk.

JEL Classification: G34, G32, H57, L86, K23, O33

Keywords: sovereign cloud, European cloud M&A, public procurement, cloud compliance, digital sovereignty, SecNumCloud, BSI C5, DORA, NIS2, Data Act, valuation

1. Define the acquisition perimeter

A sovereign-cloud label can cover a legal entity, a service catalogue, a dedicated region, a joint offering or a managed layer built on another provider. The acquisition perimeter should identify the entities, service instances, infrastructure, software, people, licences, qualifications and customer contracts that transfer to the buyer. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][2][13][20]

The evidence file should begin with corporate structure, asset and service registers, qualification scope, licences, subcontracting, customer contracts, employee mapping and transaction perimeter. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that the buyer values a branded platform while key operating rights, certifications or contracts remain with the seller or a partner. The practical response is to state the unit of account, valuation date, transferred rights, excluded assets, dependencies and permitted use before modelling cash flow. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

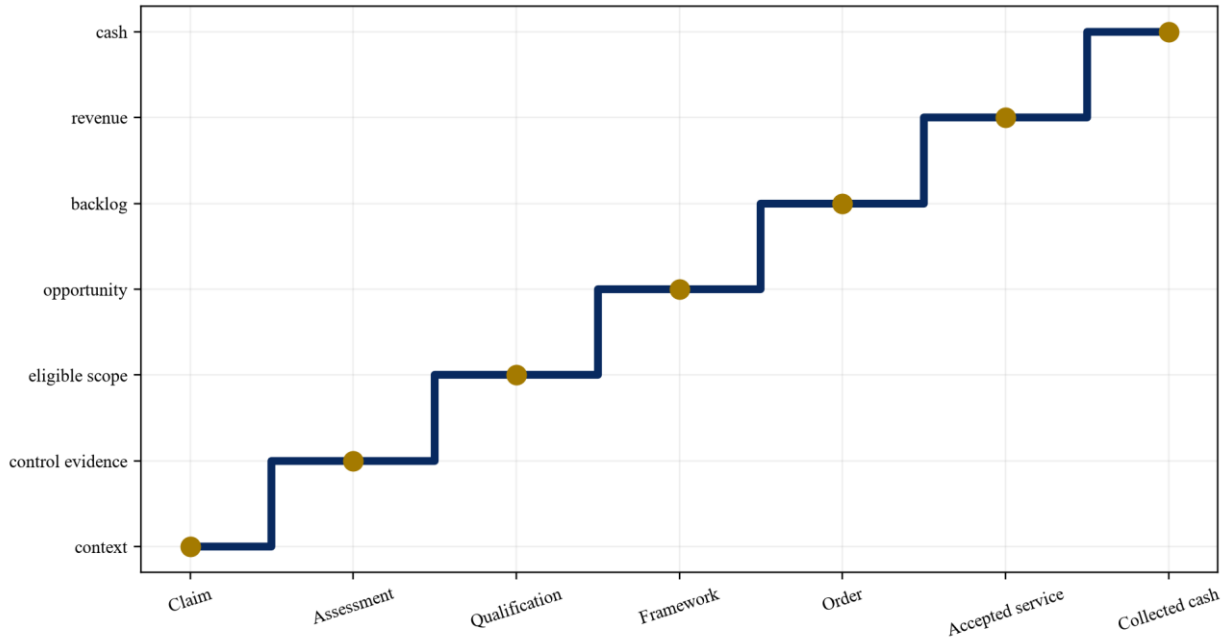
2. Build a sovereignty evidence ladder

Sovereignty is an operating and contractual condition rather than a single certificate. The evidence ladder should move from a provider assertion to assessed controls, qualification, tender eligibility, framework admission, order, accepted service, collection and renewal. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][2][3][4][5]

The evidence file should begin with provider claims, independent assessment, qualification decision, tender documents, framework award, call-off order, acceptance record, invoice, cash receipt and renewal. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that a certification or framework position is treated as equivalent to contracted recurring revenue. The practical response is to assign a permitted valuation use to each evidence stage and prohibit promotion beyond the evidence actually held. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 1. Sovereignty evidence ladder and permitted valuation use



Proposed analytical framework; each stage requires direct supporting evidence.

Table 1. Sovereignty evidence ladder

Stage	Required evidence	Permitted use
provider claim	published statement	market context
assessed control	independent scope and findings	control capability
qualification	valid decision for named service	eligible service scope
framework admission	executed framework position	addressable opportunity
call-off order	binding customer order	backlog
accepted service	acceptance and invoice	recognised revenue test
collected cash	bank receipt and reconciliation	debt-service evidence

Proposed classification; direct records determine treatment.

3. Read the Commission framework as a diligence map

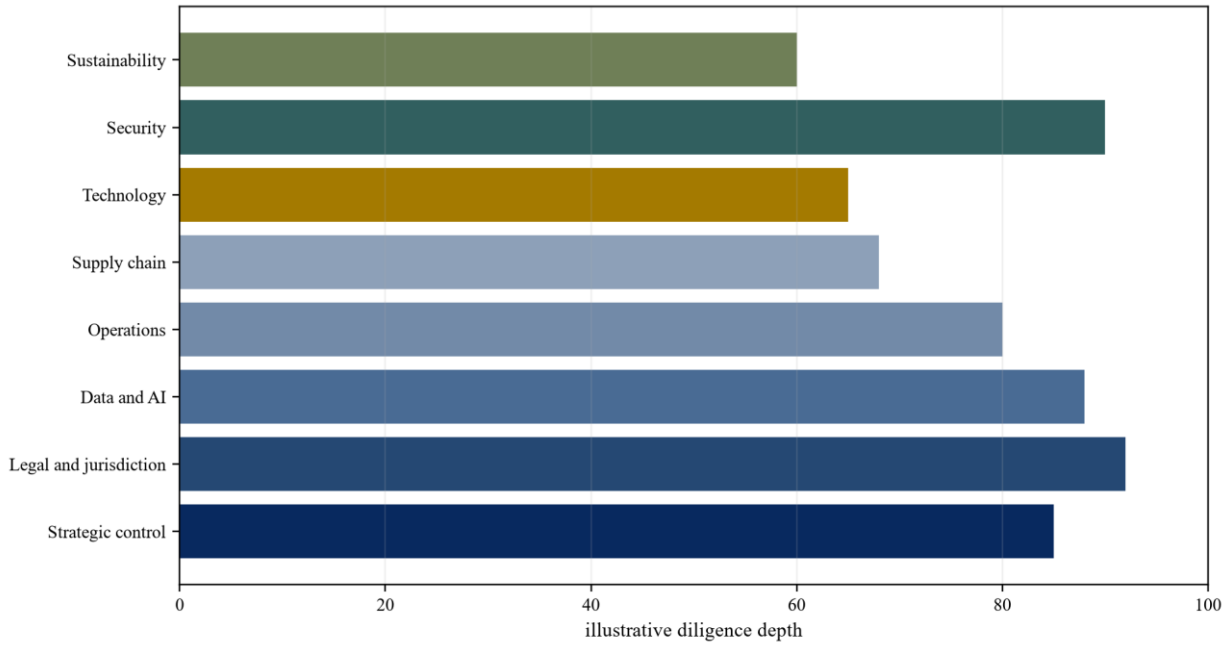
The Commission framework uses two complementary measures and assesses 48 criteria across eight sovereignty objectives. It provides a structured way to test control, jurisdiction, data, operations, supply chain, technology, security and sustainability. A score from one procurement should be reconciled to the target service and acquisition perimeter. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][2]

The evidence file should begin with completed assessment, supporting evidence, tender version, scope, expiry, exceptions and customer-specific scoring. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that a strong sovereignty score is generalised across products, countries and customers that were outside the assessed scope. The practical response is to map every scored criterion to the acquired service, continuing control owner, remediation cost and revenue dependency. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related

qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 2. European sovereign-cloud control layers



Proposed diligence map based on the Commission framework and national requirements.

4. Separate compliance from procurement access

GDPR, NIS2, DORA and the Data Act impose different duties on providers and customers. Compliance can be necessary to sell, yet tender eligibility also depends on procurement terms, financial standing, service scope, security evidence and framework rules. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [6][7][8][9][10]

The evidence file should begin with legal applicability analysis, control matrix, audit reports, procurement criteria, framework rules, exclusion grounds and service evidence. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that the model capitalises regulatory compliance as an exclusive asset even when competitors can meet the same baseline. The practical response is to treat baseline compliance as a cost of market participation and recognise scarcity only where evidence shows differentiated access or economics. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

5. Test national security credentials precisely

SecNumCloud is a qualification for specified cloud services and covers provider, personnel and service requirements. BSI C5 is a controls catalogue supported by independent attestation and is not itself a BSI certification. Scope, version, exceptions and customer requirements determine relevance. The analysis

should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [3][4][5]

The evidence file should begin with qualification certificate, audit opinion, scope statement, control exceptions, surveillance cycle, service architecture and customer tender terms. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that national credentials are described as interchangeable European approval or as applying to every target service. The practical response is to record the credential type, issuer, service scope, jurisdiction, validity, exceptions and renewal obligations separately. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Table 2. Sovereignty-rights matrix

Dimension	Core question	Transaction evidence
jurisdiction	which laws and authorities can compel action?	entity, contracts and legal opinion
data	who can access, move, decrypt or delete?	data map, keys and access logs
operations	who runs and restores the service?	operating model and incident tests
technology	which components can be replaced?	licences, source rights and tests
supply chain	who are the critical subcontractors?	contracts and dependency map
strategic control	who can alter ownership and service?	governance and change-control rights

Proposed diligence; legal and technical evidence governs.

6. Map regulated-customer demand

Financial institutions, health bodies, defence-linked organisations, public administrations and critical infrastructure operators may apply distinct outsourcing, security, data and procurement requirements. Demand quality depends on the actual customer classification and contract. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [7][8][11][12]

The evidence file should begin with customer segment, regulatory status, outsourcing classification, service criticality, approval record, contract, acceptance and payment history. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that sector labels substitute for evidence that the service supports a critical function or meets the customer approval conditions. The practical response is to classify demand by customer obligation, service criticality, approval, term, price, termination and collected cash. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

7. Prove procurement access

A dynamic purchasing system or framework can lower future tender friction, although admission may provide no guaranteed volume. The buyer should distinguish eligibility, selection, framework admission, ranked position, call-off order and accepted delivery. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][2][14][15]

The evidence file should begin with procurement notice, qualification response, evaluation, framework contract, lot, ceiling, call-off order, service acceptance, invoice and collection. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that framework ceiling or addressable market is modelled as backlog. The practical response is to include only executed orders in backlog and value framework access through evidenced win rates, bid costs and renewal behaviour. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Table 3. Procurement and framework tests

Question	Evidence	Valuation treatment
eligible to bid?	qualification and exclusion checks	opportunity only
admitted to framework?	executed lot and scope	pipeline capability
selected for order?	call-off or award	backlog subject to conditions
service accepted?	acceptance record	revenue eligibility
cash collected?	invoice and receipt	cash-flow evidence
access survives acquisition?	consent and continuing conditions	transferable value

Proposed evidence hierarchy; framework terms and orders prevail.

8. Test transferability at change of control

Qualifications, framework positions, licences and customer contracts may require notification, reassessment, consent or continuing ownership conditions after an acquisition. A buyer that changes jurisdiction, control or operating model can lose the very access being acquired. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][3][13][14]

The evidence file should begin with change-of-control clauses, qualification rules, procurement terms, consent requirements, ownership thresholds, security clearances and transaction structure. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that historic credentials are assumed to continue automatically under the buyer ownership and operating model. The practical response is to obtain issuer and customer analysis, conditions precedent, covenant protection and a fallback perimeter before closing. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

9. Distinguish data location from operational sovereignty

European hosting does not by itself establish sovereign control. Administrators, encryption keys, support channels, telemetry, subcontractors, legal compulsion, software updates and incident response can cross borders or depend on non-European actors. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][6][16][17]

The evidence file should begin with data maps, controller and processor roles, key custody, privileged access, support model, logs, subprocessors, transfer assessments and incident procedures. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that server location is presented as complete protection against access, dependency or foreign-law risk. The practical response is to map every control path and test who can access, alter, suspend, decrypt, support and recover the service. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

10. Measure technology autonomy

A target may operate on proprietary hardware, hypervisors, orchestration, security tooling, databases or support controlled by third parties. The Commission framework expressly examines technological sovereignty and supply-chain conditions. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][2][17][18]

The evidence file should begin with software bill of materials, licences, source and escrow rights, support agreements, update authority, interoperability tests and replacement plan. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that European branding is treated as technological independence despite material foreign or single-vendor dependency. The practical response is to score each dependency by criticality, substitutability, transition time, cost, approval and effect on customer commitments. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

11. Price cybersecurity and resilience obligations

NIS2 technical rules cover cloud and data-centre providers, while DORA imposes ICT third-party risk expectations on financial entities and oversight for critical providers. Transaction diligence should identify present control gaps and the cost of sustained evidence. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [7][8][19]

The evidence file should begin with applicability, risk assessments, incident history, control testing, penetration results, resilience tests, remediation, insurance and board reporting. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that the acquisition budget includes a one-off compliance project while recurring assurance and operational resilience costs are omitted. The practical response is to model remediation,

continuing control operation, independent assurance, testing, reporting and customer audit support. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

12. Evaluate cloud portability and switching friction

The Data Act requires contractual support for switching and porting within defined timeframes. Legal portability can reduce contractual lock-in, while application architecture, data gravity, integration, security approval and migration risk may still create economic friction. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [9][16][18]

The evidence file should begin with contract terms, export formats, APIs, egress process, migration tests, dependency map, customer architecture and prior migrations. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that reported retention is attributed to durable lock-in without testing legal switching rights or practical migration ability. The practical response is to separate prohibited lock-in from legitimate switching cost and test retention through renewal, workload growth and successful portability. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

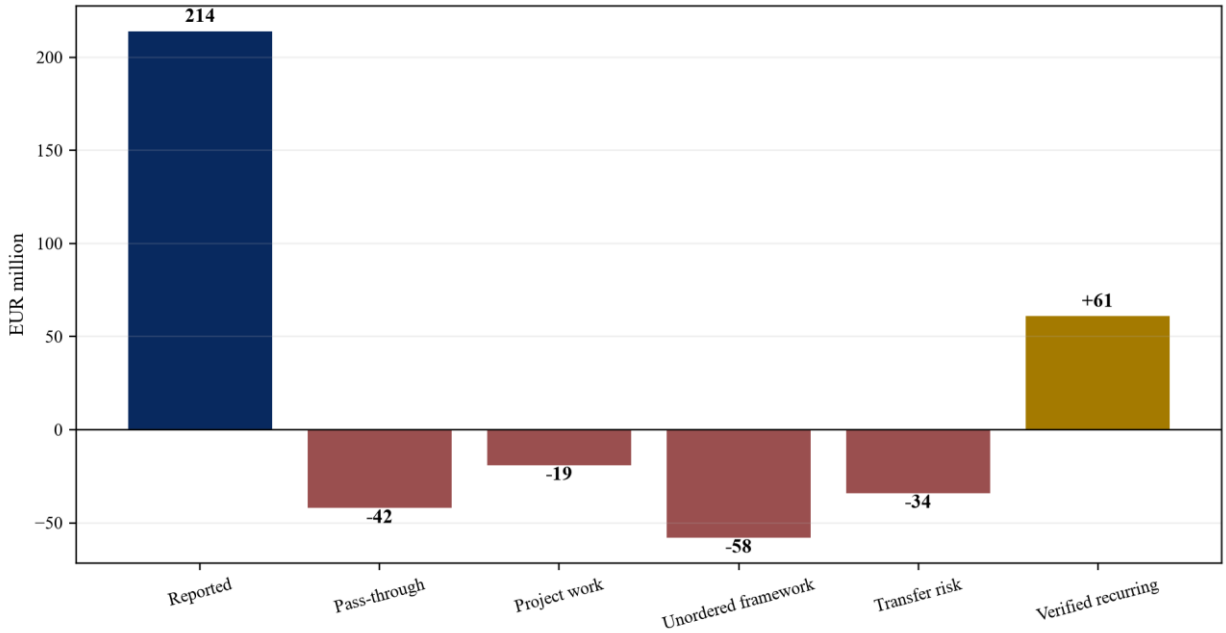
13. Normalise revenue by evidence quality

Reported revenue may include resale, pass-through infrastructure, professional services, minimum commitments, credits, grants and related-party activity. Sovereignty-enabled revenue should be tied to a service whose credential or control materially supported the customer purchase. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [7][11][20]

The evidence file should begin with general ledger, invoice, bank receipt, contract, service order, acceptance, credit note, pass-through cost and credential linkage. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that all public-sector and regulated-customer revenue is described as a sovereignty premium. The practical response is to reconcile revenue to cash, separate recurring and project work, and record the specific right or capability that enabled each sale. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 3. Hypothetical revenue-quality bridge



Wholly hypothetical; EUR million of last-twelve-month revenue.

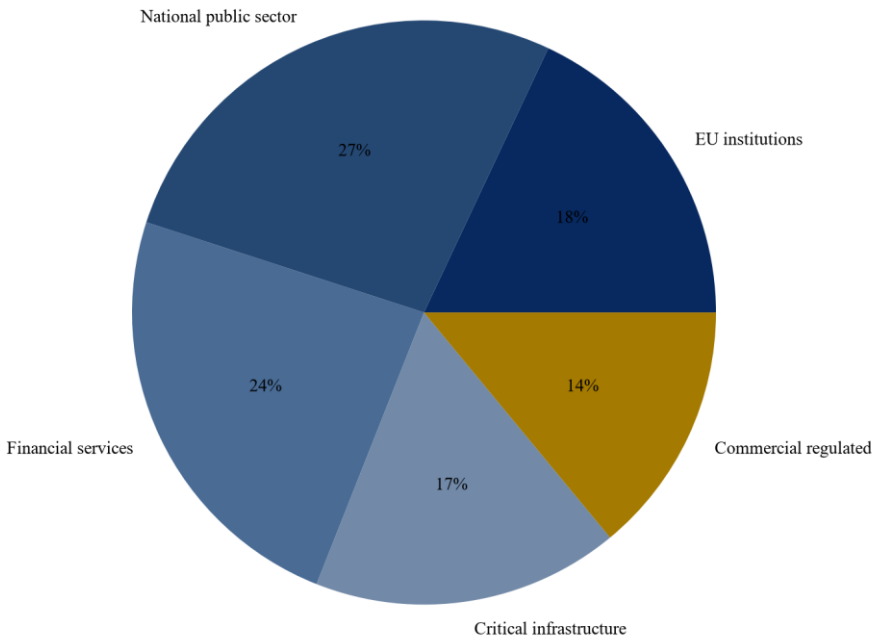
14. Measure renewal and switching evidence

Retention can reflect service quality, procurement inertia, integration, regulated approval effort or temporary lack of alternatives. A buyer should identify the source of renewal and whether the advantage persists after control change. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [9][11][12]

The evidence file should begin with cohort retention, gross and net revenue retention, renewal bids, price changes, lost accounts, migration history, approval lead time and customer interviews. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that historic retention is projected without distinguishing product value from expiring procurement or ownership conditions. The practical response is to build renewal cohorts by contract, customer type, credential dependency, price and migration feasibility. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 4. Hypothetical customer and contract mix



Wholly hypothetical; share of recurring revenue after evidence adjustment.

Table 4. Switching-cost evidence

Source of friction	Evidence	Durability test
data gravity	volume, egress and migration test	portable within required period
integration	interfaces and dependencies	documented replacement path
security approval	customer approval history	repeats after major change
operational knowledge	runbooks and staff	transferable to buyer
procurement cycle	renewal and rebid history	competition at expiry
contract	termination and switching clauses	consistent with Data Act

Proposed analytical framework; contractual and practical portability should be tested together.

15. Identify scarce procurement capabilities

Value may reside in bid teams, cleared personnel, accredited operations, reusable evidence, compliant product design and customer relationships. These capabilities can reduce time and cost for future tenders when they remain with the acquired business. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][3][14][15]

The evidence file should begin with staff roles, clearances, bid library, evaluation scores, win rates, qualification maintenance, customer references and pipeline records. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that a framework name is valued while the people and evidence system that earned it are excluded from the deal. The practical response is to value reusable capability through replacement cost and incremental cash flow, subject to retention and transferability. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

16. Control customer and framework concentration

A few public frameworks or regulated clients can make revenue appear resilient while creating renewal, budget and policy concentration. Framework expiry may also cluster multiple customer decisions. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [2][7][14]

The evidence file should begin with customer and framework revenue, order maturity, budget cycle, renewal calendar, termination, price reset and competitor participation. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that long contracts are assumed to diversify risk even when they depend on one framework, authority or policy. The practical response is to stress correlated renewal and budget events and cap leverage against concentrated or cancellable cash flow. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

17. Map subcontractors and chain outsourcing

Sovereign services can depend on infrastructure, software, network, support and data-processing subcontractors. Financial-sector guidance and DORA place emphasis on chain oversight, audit, location, continuity and exit. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [8][11][12]

The evidence file should begin with subprocessor register, service chain, locations, contracts, audit rights, concentration, incident terms, exit assistance and alternatives. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that the prime provider qualification is assumed to remove material supplier and fourth-party risk. The practical response is to trace every critical service to its ultimate operator and model replacement, consent and continuity requirements. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

18. Separate owned infrastructure from service rights

Enterprise value may combine data-centre assets, leased capacity, cloud equipment, software, managed services and reseller rights. Each has different capital intensity, useful life, margin, security and recoverability. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [20][21][22]

The evidence file should begin with asset register, title, leases, capacity contracts, depreciation, maintenance, licences, customer allocation and security package. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that an EBITDA multiple obscures the amount of replacement capital and third-party infrastructure embedded in earnings. The practical response is to build asset, contract and cash-flow

bridges and value infrastructure, equipment and service capabilities consistently. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Table 5. Financial perimeter

Exposure	Primary value method	Key adjustment
owned data-centre assets	asset and cash flow	replacement capital
leased cloud capacity	contract cash flow	take-or-pay and expiry
software platform	income and relief-from-royalty	dependency and useful life
customer relationships	excess earnings	renewal and concentration
qualification capability	incremental cash or replacement cost	transfer and maintenance
framework access	probability-weighted cash	no guaranteed volume

Proposed classification; final accounting and financing require transaction-specific advice.

19. Model compliance expenditure and technical debt

Qualifications and regulated contracts require continuing personnel, monitoring, audit, remediation, documentation and architecture. Deferred upgrades or unsupported components can create a post-closing cash call and service risk. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [3][4][7][8]

The evidence file should begin with control budget, staffing, audit calendar, vulnerabilities, end-of-support schedule, technical-debt register and remediation estimates. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that adjusted EBITDA removes compliance cost as exceptional even though it is required to preserve access. The practical response is to normalise recurring assurance cost and treat verified catch-up expenditure as debt-like or a price adjustment. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

20. Apply acquisition accounting discipline

IFRS 3 requires recognition and measurement of identifiable assets and liabilities in a business combination. Customer relationships, technology, contracts and other identifiable intangibles require separate analysis, while goodwill remains subject to IAS 36 impairment testing. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [20][21][22][23]

The evidence file should begin with purchase agreement, valuation perimeter, contracts, technology, identifiable rights, tax bases, useful lives and integration plan. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that a commercial sovereignty premium is booked as one intangible without testing identifiability, control and separability. The practical response is to allocate value to supportable identifiable assets and liabilities and document the residual goodwill thesis. Central assumptions should

reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

21. Use market-participant fair value

IFRS 13 defines fair value using an orderly market-participant exit-price perspective. Buyer-only synergies, policy preferences and financing advantages should be separated from transferable target value. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [21][24]

The evidence file should begin with forecast, market evidence, discount rates, comparable transactions, control assumptions, synergies and transaction costs. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that the offer price is justified with acquirer-specific benefits presented as target enterprise value. The practical response is to show standalone market-participant value, buyer synergies, integration cost and risk protection separately. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

22. Value qualifications through cash flow and cost

A qualification can contribute to incremental cash flow, reduced bid cost, shorter approval time or avoided replacement expenditure. The selected method should avoid double counting the same benefit in revenue, margin and intangible value. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [3][4][20][21]

The evidence file should begin with credential-linked revenue, win rates, renewal, price, maintenance cost, replacement timetable, attrition and useful-life evidence. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that a headline premium is added to an EBITDA multiple and also capitalised as an intangible asset. The practical response is to choose a primary cash-flow treatment, use replacement cost as a cross-check and reconcile all value components. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

23. Apply the hypothetical acquisition case

The case tests a multi-country platform whose reported regulated and public-sector revenue requires evidence adjustment. It uses a central purchase price and financing structure to illustrate decision controls rather than forecast an identified deal. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][3][20][21]

The evidence file should begin with the stated hypothetical revenue, margin, contract, qualification, capital expenditure, debt and valuation assumptions. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public

policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that all labelled sovereign revenue is modelled at equal quality and assigned the same multiple. The practical response is to bridge reported revenue to procurement-enabled recurring cash and apply risk to each evidence class. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Table 6. Hypothetical acquisition case

Metric	Central case	Downside or gate
reported LTM revenue	EUR 214m	reconcile to cash
adjusted EBITDA	EUR 38m	EUR 31m after recurring cost
public and regulated revenue	EUR 92m	contract-level test
verified procurement-enabled recurring revenue	EUR 61m	EUR 45m downside
enterprise value	EUR 690m	EUR 630m to EUR 735m range
acquisition debt	EUR 210m	stressed cash-flow cap
remediation reserve	EUR 38m	released against evidence
buyer equity and subordinated capital	EUR 480m	includes fees and reserves

Wholly hypothetical; figures do not describe an identified transaction.

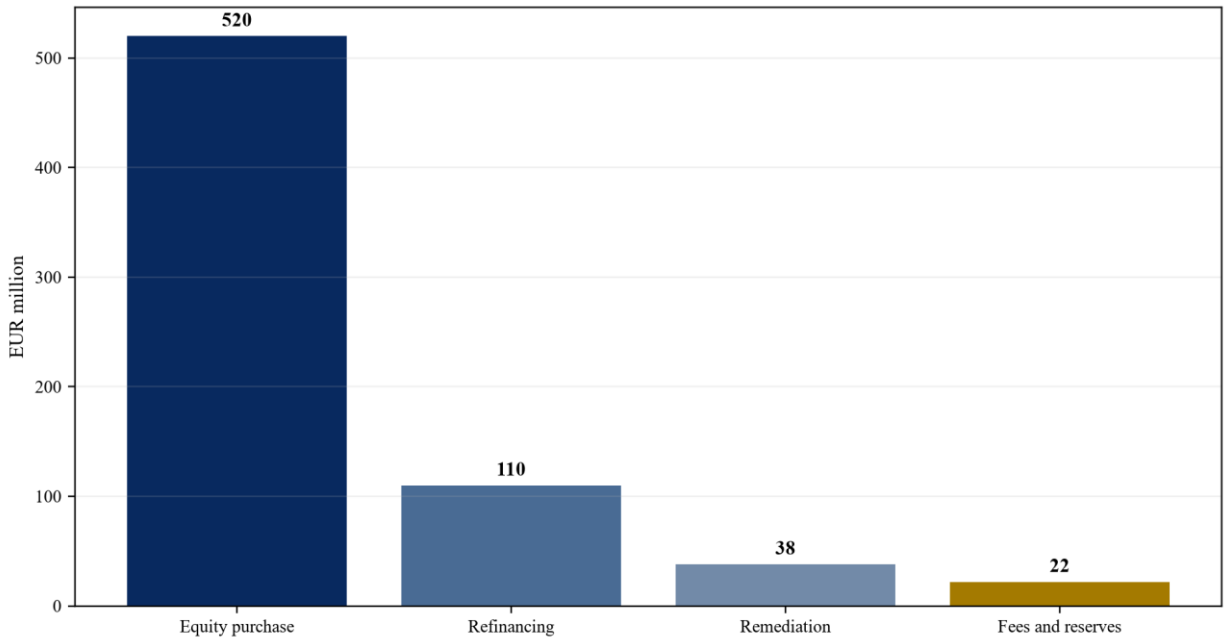
24. Design the acquisition funding stack

Debt capacity should reflect contracted recurring cash, customer concentration, capital expenditure, credential continuity and the cost of post-closing remediation. Acquisition debt should not rely on an unverified sovereignty premium. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [8][20][25]

The evidence file should begin with sources and uses, debt terms, covenant model, contract cash, capital expenditure, remediation, working capital and downside liquidity. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that leverage is sized to headline EBITDA before recurring compliance cost and transfer risk. The practical response is to size debt to stressed cash flow, reserve remediation and make qualification or key-consent loss a reporting and cure event. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 5. Hypothetical acquisition sources and uses



Wholly hypothetical; EUR million.

25. Protect value in transaction documents

The buyer can use conditions precedent, warranties, covenants, indemnities, escrow and earn-out mechanisms to address credential scope, consent, revenue quality, cyber incidents and remediation. Protection should map to evidence and loss. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [3][7][13]

The evidence file should begin with disclosure letter, qualification status, contract consents, control reports, incidents, revenue bridge, remediation plan and insurance. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that broad compliance warranties replace targeted protection for known transfer and control risks. The practical response is to tie each material diligence finding to a closing condition, price term, remedy, owner and verification date. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

26. Plan integration without breaking sovereignty

Centralising operations may reduce cost while changing control, location, personnel, suppliers or technology in ways that affect qualifications and customers. The integration plan should preserve the operating conditions underpinning value. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][3][7][8]

The evidence file should begin with target operating model, regulatory and issuer analysis, customer consents, data flows, access roles, service continuity and phased changes. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that day-one synergy actions invalidate assessed controls or customer approval assumptions. The practical response is to sequence integration through protected service rings, approved changes, evidence refresh and customer communication. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

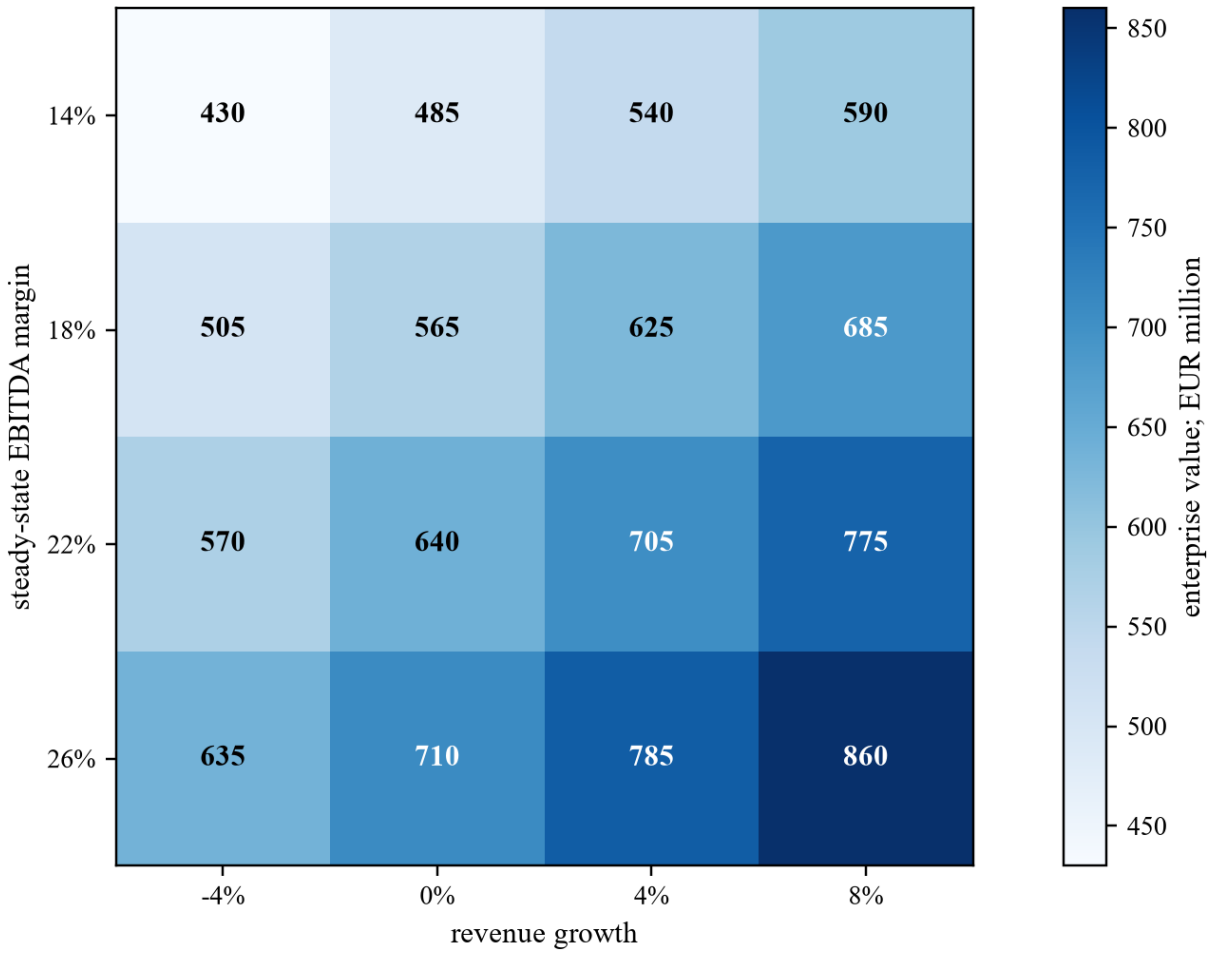
27. Stress exit value and impairment risk

An acquirer should test contract loss, qualification delay, framework expiry, technology replacement, margin compression, higher assurance cost and customer migration. These risks can affect both acquisition value and later goodwill impairment. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [9][21][22][23]

The evidence file should begin with combined downside scenarios, valuation sensitivities, headroom, leading indicators, remediation options and exit routes. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that single-variable sensitivities preserve value even though related regulatory, customer and technology events occur together. The practical response is to run coordinated scenarios and link each trigger to liquidity, covenant, impairment and strategic actions. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Figure 6. Hypothetical enterprise-value sensitivity



Wholly hypothetical; EUR million under combined operating and credential scenarios.

28. Reach the investment decision

Approval should rest on a reconciled chain from sovereignty evidence to transferable contract cash, supported by viable technology, control, people and funding. The decision record should show value recognised, excluded opportunities and retained risks. The analysis should identify the right-holder, the control owner, the economic beneficiary and the party that bears remediation or transition cost. [1][20][21][25]

The evidence file should begin with rights matrix, credential file, contract and cash bridge, customer cohorts, technology dependencies, remediation plan, valuation and financing. Each item should record legal scope, effective date, expiry or review point, relevant service, responsible owner and relationship to customer cash flow. Public policy and market announcements establish context. Transaction value requires transferable rights, customer acceptance and observed performance.

The principal failure is that strategic enthusiasm substitutes for a transaction-specific conclusion on rights, cash, risk and alternatives. The practical response is to approve only the price, leverage and protections supported by verified transferable evidence and executable post-closing controls. Central assumptions should reflect current enforceable arrangements. Downside cases should combine related qualification, customer, technology, cybersecurity, integration, liquidity and change-of-control risks. Material management estimates should be identified in the model and refreshed when source evidence changes.

Table 7. Investment decision record

Decision	Minimum evidence	Possible action
price	cash bridge and transferable rights	bid, resize or withdraw
leverage	stressed recurring cash	lend, condition or reduce
qualification value	scope, transfer and maintenance	recognise or exclude
customer value	orders, acceptance and renewal	include, haircut or defer
remediation	cost, owner and timetable	reserve, covenant or indemnity
integration	preserved control conditions	phase, ring-fence or redesign
exit and impairment	scenarios and triggers	retain, sell, restructure or impair

Proposed governance; each approval retains its legal authority.

Frequently asked questions

Q: Does a sovereign-cloud qualification create guaranteed revenue? A: No. A qualification can establish eligibility or reduce customer diligence. Revenue requires a binding order, accepted service, invoicing and collection. Framework admission without a call-off order remains an opportunity rather than backlog.

Q: How should a buyer value procurement access? A: The buyer should trace access to observed win rates, bid cost, order conversion, renewal, margin and cash. The model should also test transferability after change of control and the cost of maintaining the people, controls and qualifications.

Q: Are SecNumCloud and BSI C5 equivalent? A: No. SecNumCloud is a French qualification for specified cloud services under an ANSSI requirements baseline. BSI C5 is a German controls catalogue supported by independent attestation. Scope, purpose and customer requirements differ.

Q: Does European data hosting establish operational sovereignty? A: Hosting location addresses one element. The buyer also needs evidence on legal compulsion, administrator access, encryption keys, support, software updates, subprocessors, telemetry, incident response and recovery authority.

Q: How does the Data Act affect switching costs? A: The Data Act requires contractual support for switching and porting. Customers may still face practical migration cost from integration, data volume, security approval and operating change. Valuation should distinguish legal lock-in from evidenced economic friction.

Q: Which change-of-control risks matter most? A: The buyer should test customer consent, framework and qualification conditions, ownership or jurisdiction requirements, security clearances, licences, subcontractor rights and whether the buyer's integration plan changes the assessed service.

Q: Can compliance expenditure be added back to EBITDA? A: Recurring expenditure needed to preserve qualifications, security assurance, regulatory compliance and customer approval belongs in normalised earnings. Verified one-off catch-up remediation can be treated separately with a defined budget and timetable.

Q: What should an investment committee require before approval? A: It should require a reconciled sovereignty-rights matrix, credential file, contract-to-cash bridge, customer cohorts, dependency map, remediation plan, financing downside, transaction protections and an integration plan that preserves the conditions supporting value.

References

[1] European Commission, *Cloud Sovereignty Framework; Implementation guidance* (2026). https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en?filename=Cloud+Sovereignty+Framework+-+Implementation+guidance.pdf

[2] European Commission, *Sovereign Cloud Framework explained* (2026). https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

[3] ANSSI, *SecNumCloud requirements baseline v3.2 and qualification references*. https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/comprendre-levaluation-de-securite/qualification-de-produit-et-services/referentiels-qualification/

[4] Bundesamt fuer Sicherheit in der Informationstechnik, *Cloud Computing Compliance Criteria Catalogue C5*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf

[5] BSI, *Frequently asked questions on the minimum standard for external cloud services*. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/FAQ_MST_Externe_Cloud-Dienste/faq_mst_Externe_Cloud-Dienste_node.html

[6] European Union, *General Data Protection Regulation; Regulation (EU) 2016/679*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] European Union, *NIS2 Directive; Directive (EU) 2022/2555*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[8] European Union, *Digital Operational Resilience Act; Regulation (EU) 2022/2554*. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[9] European Union, *Data Act; Regulation (EU) 2023/2854*. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[10] European Commission, *Public procurement legal rules and implementation*. https://single-market-economy.ec.europa.eu/single-market/public-procurement/legal-rules-and-implementation_en

[11] European Banking Authority, *Guidelines on outsourcing arrangements*. https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

[12] European Securities and Markets Authority, *Guidelines on outsourcing to cloud service providers*. https://www.esma.europa.eu/sites/default/files/library/esma50-164-4285_guidelines_on_cloud_outsourcing.pdf

[13] European Union, *Directive 2014/24/EU on public procurement*. https://eur-lex.europa.eu/eli/dir/2014/24/oj

[14] European Commission, *Tender opportunities; Digital Services*. https://commission.europa.eu/funding-and-tenders/find-calls-tender/tender-opportunities-department/tender-opportunities-digital-services_en

[15] Tenders Electronic Daily, *Supplement to the Official Journal of the European Union*. https://ted.europa.eu/en/

[16] European Commission, *Model contractual terms and standard contractual clauses for data and cloud contracts*. https://digital-strategy.ec.europa.eu/en/policies/data-act-model-contractual-terms

[17] European Union Agency for Cybersecurity, *EU cybersecurity certification framework and cloud scheme programme*. https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-framework

[18] National Institute of Standards and Technology, *Cloud Computing Standards Roadmap*. https://www.nist.gov/publications/nist-cloud-computing-standards-roadmap

[19] European Commission, *Commission Implementing Regulation (EU) 2024/2690 under NIS2*. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

[20] IFRS Foundation, *IFRS 3 Business Combinations*. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[21] IFRS Foundation, *IFRS 13 Fair Value Measurement*. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

[22] IFRS Foundation, *IAS 36 Impairment of Assets*. https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/

[23] IFRS Foundation, *IAS 38 Intangible Assets*. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[24] IFRS Foundation, *IFRS 15 Revenue from Contracts with Customers*. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[25] IFRS Foundation, *IFRS 9 Financial Instruments*. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-9-financial-instruments/

[26] European Data Protection Board, *Recommendations on measures that supplement transfer tools*. https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

[27] European Commission, *Standard contractual clauses for international transfers*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[28] OECD, *Digital security risk management*. https://www.oecd.org/en/topics/digital-security.html

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 closure.

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 and leads 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.

https://www.linkedin.com/in/ckadya/

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.