DOCUMENT 36 · AI THIRD PARTIES AND SUPPLIERS

AI third parties and suppliers

Deciding what to build, buy or partner on, and managing AI suppliers with requirements proportionate to their criticality

Fernando García Varela Version 0.2 (working draft) 19-10-2026 Draft for review

3	4	6	16
requirement levels	classification factors	supplier lifecycle stages	key contractual clauses

IN THIS DOCUMENT

01 Purpose and scope

02 Principles

03 Build, buy or partner

04 Requirement levels N1–N3

05 Supplier lifecycle

06 Key contractual clauses

07 Technological dependency and concentration

08 Embedded AI in software already contracted

09 Supplier register

10 Monitoring and indicators

11 Roles

12 Associated tools and templates

13 Related documents

14 Version control

Legal notice and disclaimer. SEVEN-G is a reference methodological framework provided "as is" and for information purposes only. It does not constitute legal, regulatory, financial or professional advice, nor does it guarantee compliance with any law or standard. References to general regulation (such as the EU AI Act, the GDPR, DORA or NIS2), to technical standards and to regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date. **Each organisation that uses SEVEN-G is solely responsible for identifying the regulation that applies to it, verifying that it is current and certifying its own regulatory compliance**, with the appropriate qualified advice. This methodology is a generic, free aid shared with the community so that nobody has to start from scratch; each person or organisation can and should adapt it to its own use. It must not be inferred that its legally sensitive parts have been reviewed by legal counsel: those reviews, for each company or sector, are the ultimate responsibility of the company, consultant or organisation that uses it. Although every effort is made to keep it up to date, some regulation may have changed without being reflected here. To the fullest extent permitted by law, the author accepts no responsibility whatsoever for the effects of its application in any organisation or for its full applicability. The methodology does not grant certification of any kind. The author accepts no liability for any use made of this content or for any decisions taken on the basis of it. The data, figures, companies and cases in the examples are fictitious or illustrative.

THE ESSENTIALS **Conditional: depends on a trigger**

Trigger: an AI supplier is involved (model, platform or software with AI functions), including AI embedded in software already under contract. The requirement level N1 to N3 decides how much due diligence, which clauses and which exit plan.

Obligation matrix and layered reading (document 94)

01

Purpose and scope

Most of the AI a company uses depends on third parties: general-purpose models consumed as a service, cloud platforms, software with AI features, integrators, data providers and open-source components. This document establishes how the decision to use a third party is made, what is required of it in proportion to its criticality, what the contract must say and how dependency and concentration are monitored.

1.1 Types of third party

Type	Examples	Particular features
Model provider	General-purpose models accessible through an application programming interface; specialised models.	Frequent version changes; use of data; concentration.
Platform	Cloud, data platforms, agent platforms or model deployment platforms.	Architectural dependency; data location.
Software with AI	Business applications with AI features, either contracted specifically or already in place (section 8).	AI arrives through updates; limited control.
Integrator or consultant	Building, integration or operation on behalf of the company.	Knowledge held outside the company; ownership of what is built.
Data provider	Training, enrichment or reference data.	Licences, quality, legal basis.
Open components	Open-weight models, libraries, connectors, tool servers.	No contract: the requirements fall on the company's own verification (SEG-09, AG-13).
Partner or alliance	Joint development, shared exploitation, consortia.	Allocation of intellectual property, data and responsibilities.

1.2 Reference standards

Consulted in September 2026; they must be checked against their current version:

- **Regulation (EU) 2024/1689** (EU AI Act), in particular responsibilities along the value chain (Art. 25), the obligations of deployers (Art. 26) and those of providers of general-purpose AI models (Art. 53). Amended by Regulation (EU) 2026/1744 (Digital Omnibus on AI), published in the Official Journal on 24 July 2026, which postpones the obligations for high-risk systems in Annex III to 2 December 2027 and those in Annex I to 2 August 2028.

- **Regulation (EU) 2022/2554 (DORA)**, Arts. 28 to 30 and their implementing acts: Delegated Regulation (EU) 2024/1773 (policy on contractual arrangements for critical or important functions), Implementing Regulation (EU) 2024/2956 (register of information) and Delegated Regulation (EU) 2025/532 (subcontracting).
- **Regulation (EU) 2016/679 (GDPR)**, Art. 28 (processors) and Chapter V (international transfers).
- **ISO/IEC 42001**, control A.10 of Annex A (third-party and customer relationships).
- **Directive (EU) 2022/2555 (NIS2)** as regards supply chain security, in accordance with its national transposition.

This document does not constitute legal advice. Contractual content must be reviewed with qualified legal counsel. The requirement levels and the obligations described are for guidance only: responsibility for the regulatory classification of third parties and systems and for compliance, including the applicable sector regulation, lies with the organisation (document 93, section 11).

02

Principles

#	Principle	Consequence
1	**Accountability is not outsourced**	The company is answerable to customers, supervisors and the board even if the system belongs to a third party.
2	**Proportionate requirements**	Due diligence, the contract and monitoring depend on the N1–N3 level, not on the contract amount.
3	**Plan the exit before entering**	The exit strategy is designed at selection, not at termination.
4	**The company's data do not train others' models**	Unless there is an express, documented decision.
5	**No model change goes unnoticed**	The supplier reports relevant changes and the company evaluates them.
6	**Concentration is managed at portfolio level**	Dependency on a supplier is measured across all systems, not just one.
7	**AI that arrives through updates is also governed**	AI features in software already contracted are entered in the inventory and assessed.

#	Principle	Consequence
8	**Testing is also using**	No external AI tool is used with company data —not even to test it, research or compare it— without the supplier assessment (P55) proportionate to its N1–N3 level. A test with synthetic or public data does not need it; one with internal, personal or confidential data does.

> **Why it matters.** Many leaks do not happen in production but during a trial: someone uploads a real document to a tool "just to see how it works". Treating a trial as use makes the supplier assessment arrive before the data.

03

Build, buy or partner

3.1 Options

Option	What it means	When it makes sense
Build	In-house development, even if it uses third-party models or components.	Competitive differentiation, unique proprietary data, need for control.
Buy	Off-the-shelf product or service with limited configuration.	Non-differentiating function, mature solution, time-to-market priority.
Adapt	Off-the-shelf product or model with significant fine-tuning, integration or extension.	Mature base with relevant company-specific needs.
Partner	Joint development or exploitation with a third party.	Complementary capabilities or data; risk sharing in Transform bets.

3.2 Decision criteria

Criterion	Favours building	Favours buying	Favours partnering
Differentiation	The capability is a source of competitive advantage.	Standard function in the sector.	An advantage that neither party can achieve alone.

Criterion	Favours building	Favours buying	Favours partnering
Data	Unique and sensitive proprietary data.	The data needed are generic.	Complementary data from both parties.
Internal capability	Team able to build and operate.	No capability and no intention of creating it.	Partial capability.
Time frame	Time frame compatible with development.	Urgency.	Intermediate time frame.
Control and compliance	Need to explain, audit and modify in depth.	The supplier provides verifiable compliance.	Clear contractual allocation of obligations.
Total cost	Lower recurring cost at scale.	Lower initial investment.	Shared investment and risk.
Dependency	Avoid dependency in a critical function.	Acceptable and replaceable dependency.	Balanced mutual dependency.
Intellectual property	Need to own the result.	Not relevant.	Negotiable allocation.

Rules:

1. The decision is documented in the phase 3 feasibility assessment (P10) using the criteria in the table and the three-year total cost according to the categories in document 42, including the **exit cost**.
2. In **Optimise** use cases, buying should be the starting option unless there is a documented reason otherwise. In **Transform**, dependency on a third party for the differentiating capability must be justified to the body that approves the bet.
3. **Building on third-party models does not eliminate dependency**: this document applies to the model provider.
4. If the company substantially modifies a third party's high-risk system, changes its intended purpose or places it on the market under its own name, it may become a **provider** for the purposes of the AI Act (Art. 25(1)), with the corresponding obligations. This consequence is analysed before deciding to adapt.

04

Requirement levels N1–N3

4.1 Classification factors

The level is determined for each relationship between a supplier and a service. The same supplier may have different levels for different services. **The level is the highest resulting from any of the four factors.**

Factor	N1 · Standard	N2 · Enhanced	N3 · Critical
Service criticality	Internal process whose interruption would have an impact of 1–2 (document 33).	Relevant process with impact 3; direct exposure to customers; decisions about people.	Critical or important function (including the DORA definition where applicable); impact 4–5; high-risk system under the AI Act.
Data processed	Public or non-sensitive internal data.	Personal data or confidential information.	Special categories of data, large-scale personal data, trade secrets or critical confidential information.
Autonomy	A0: the supplier's system assists.	A1, or A2 without effects on third parties, money, personal data or production.	A2 or A3 with effects on third parties, money, personal data or production systems.
Substitutability	Replaceable in less than 3 months without relevant cost.	Replaceable in 3 to 12 months or with relevant cost.	More than 12 months, cost above the materiality threshold M, or no alternative.

The substitutability time frames are indicative and are approved in C2 (document 13). The level is determined in phase 3, reviewed at every R6 and upon any change to the service, and recorded in T09.

4.2 Requirements by level

Requirement	N1 · Standard	N2 · Enhanced	N3 · Critical
Due diligence	Basic questionnaire; review of terms of service and privacy terms.	Full questionnaire (4.3; P55); certifications and independent reports; analysis of sub-processors.	Everything in N2, plus financial soundness, continuity, subcontracting chain, references and direct or third-party verification.
Security	Verified data configuration (no training, retention).	Document-based AI security assessment (applicable SEG and AG).	Technical assessment, in-house adversarial testing or recent independent reports; right to test.

Requirement	N1 · Standard	N2 · Enhanced	N3 · Critical
Contract	Standard terms reviewed against clauses 1–4 of section 6.	AI annex and data processing agreement with the clauses marked for N2.	Negotiated contract with all clauses; DORA Art. 30(3) if it supports critical or important functions of a financial entity.
Approval	AI Product Owner with procurement clearance.	AI Sponsor with risk and data protection clearance.	AI Committee with clearance from risk, information security, data protection and legal.
Audit	Not required.	Annual independent reports.	Right of audit and access, directly or through a designated third party.
Monitoring	Annual review.	Half-yearly review and service indicators.	Quarterly review, monthly indicators, relationship governance meeting.
Exit	Guaranteed data export.	Documented exit plan.	Exit plan with an identified alternative and a documented rehearsal or test.
Incidents	According to the supplier's terms, verified.	Notification without undue delay within a time limit compatible with the company's own obligations.	Notification within an agreed maximum time limit (indicatively 24 hours or less from detection) and cooperation in the response and in regulatory notifications.
Register	T09.	T09.	T09 and, if DORA applies, the register of information.

An N3 supplier normally implies **Enterprise** intensity for the use cases that use it (01 §9.2).

4.3 Content of the due diligence questionnaire

1. **Identity and soundness:** group, country, years in operation, financial position, insurance.
2. **Service and model:** models used, proprietary or third-party; versions; policy on changes and version deprecation; model documentation.
3. **Data:** use for training or improvement; retention; location; transfers; encryption; separation between customers; deletion.
4. **Sub-processors and supply chain:** list, location, functions, change policy.
5. **Security:** certifications, penetration testing, vulnerability management, protection against prompt injection, leakage and extraction, agent controls if any.
6. **AI Act compliance:** role of the supplier, classification, technical documentation and instructions for use, logs, human oversight, cooperation on incidents, obligations as a provider of general-purpose AI models where applicable.
7. **Data protection:** status as processor, measures, support for impact assessments and data subject rights.

8. **Intellectual property:** ownership of outputs, training data licences, indemnity.
9. **Continuity:** availability, continuity plans, testing, dependency on third parties.
10. **Incidents:** process, notification time limits, history of relevant incidents.
11. **Exit:** export formats, assistance, time limits, certified deletion.
12. **Ethics and responsible use:** acceptable use policies, bias management, use restrictions.

The full questionnaire is in P55. A **Nonconformant** result in blocks 3 (data), 5 (security) or 7 (data protection) prevents the supplier from being used with production data until it is resolved.

AI security purchasing criteria. At N2 and N3 the company also asks for: ISO/IEC 42001 certification of the service, if any, with its scope; recent independent adversarial testing reports on the AI service; the right to carry out its own tests (N3); access to the input, output and action logs needed for monitoring and incident investigation (52 §11); and the location of processing, including the provider's own filters and monitoring. They are collected in block 5 of P55.

05

Supplier lifecycle

Stage	What is done	Evidence	Owner	SEVEN-G phase
1. Selection	Build, buy or partner decision; requirements; preliminary N level; alternatives compared.	P10; requirements; comparison.	AI Product Owner with procurement.	3
2. Due diligence	Questionnaire and verification according to level; security and data protection assessment; RT-TER risks.	P14; P55; risks in P12.	Procurement, security, data protection, risk.	3
3. Contract	Negotiation with the clauses for the level; approval.	Contract (P56); clause list verified in P14.	Legal and procurement.	3–4
4. Integration	Secure configuration (retention, no training, regions); identities and permissions; logging; testing; exit plan.	P15, P18; exit plan.	AI Technical Owner.	4–5
5. Monitoring	Service indicators, incidents, model changes, sub-processors, periodic reviews, level reassessment.	T09; review minutes (P57 §5); P27.	Relationship manager and AI Operations Owner.	6
6. Exit	Activation of the plan: transition, portability, certified deletion, revocation of access, lessons.	Deletion certificate and closure record (P57 §8–9); P30.	AI Technical Owner and legal.	7

Reassessment triggers: change of model or major version; change of sub-processors or location; S1 or S2 incident attributable to the supplier; change of ownership of the supplier; change of use or autonomy level; new regulatory obligation; deterioration in service indicators; notice of a model's deprecation.

06

Key contractual clauses

Yes = must be included · **Rec.** = recommended · **—** = not required. At N1 many clauses are not negotiable: they are checked in the standard terms and, if missing, the risk is recorded together with who accepts it. At every level, while a **Yes** clause is missing without that risk recorded and accepted by the body corresponding to its level (33 §7), the supplier is not used with production data.

#	Clause	What it must ensure	N1	N2	N3
1	**Use of data for training**	The company's inputs, contexts, outputs and data are not used to train or improve models or for other purposes, unless expressly and specifically authorised.	Yes	Yes	Yes
2	**Confidentiality and data processing**	Confidentiality; data processing agreement in accordance with Art. 28 of the GDPR where personal data are involved; limited retention and deletion.	Yes	Yes	Yes
3	**Location and transfers**	Processing and storage regions; Chapter V GDPR safeguards for international transfers; prior notice of changes.	Yes	Yes	Yes
4	**Security**	Minimum measures, maintained certifications, vulnerability management, protection against AI-specific threats.	Yes	Yes	Yes
5	**Sub-processors**	Up-to-date list; prior authorisation or right to object to changes; same obligations down the chain.	Rec.	Yes	Yes
6	**Intellectual property and outputs**	Ownership of or rights to use the outputs; indemnity against infringement claims arising from the model or its training data; ownership of bespoke developments.	Rec.	Yes	Yes
7	**Incident notification**	Maximum time limit, minimum content, cooperation in the investigation and in the company's regulatory notifications (document 37).	Rec.	Yes	Yes
8	**Model changes**	Advance notice of changes to version, behaviour or model deprecation; ability to pin versions for a period; sufficient information to evaluate the change before it takes effect.	Rec.	Yes	Yes

#	Clause	What it must ensure	N1	N2	N3
9	**Service levels**	Availability, latency, support, penalties and measurement.	—	Yes	Yes
Sphere map and ambition levels (10)	**Logs and traceability**	Access to the logs needed for oversight, investigation and regulatory obligations, with retention periods.	—	Yes	Yes
Maturity model (11)	**Audit and access**	Right of audit, inspection and access for the company, designated auditors and the competent supervisors.	—	Rec.	Yes
Transformation index (12)	**AI Act obligations along the value chain**	Allocation of roles; delivery of technical documentation and instructions for use; information on capabilities and limitations; cooperation on human oversight, logs, post-market monitoring and serious incidents; written agreement under Art. 25(4) where the third party supplies components to a high-risk system.	Rec.	Yes	Yes
AI thesis, ambition and risk appetite (13)	**Transparency on AI features**	Advance notice of new AI features in the service; ability to keep them disabled until assessed.	Rec.	Yes	Yes
Portfolio management (14)	**Continuity**	Tested continuity and recovery plans, with the company informed of their results.	—	Rec.	Yes
15	**Exit and transition**	Transition period, assistance, export in usable formats (data, configurations, prompts, logs), certified deletion, continuity during the transition.	Rec.	Yes	Yes
16	**Termination**	Right to terminate for serious breach, regulatory change, security breach, change of control or supervisory instruction.	Rec.	Yes	Yes

6.1 AI Act obligations along the value chain

Situation	What it implies for the contract
The company deploys a provider's high-risk system	The provider must supply instructions for use that allow the deployer's obligations to be met (Art. 26): use in accordance with the instructions, human oversight, monitoring, log retention and reporting of risks and serious incidents to the provider. The contract ensures access to that information and cooperation.
The company becomes a provider (Art. 25(1))	Through substantial modification, change of intended purpose or placing on the market under its own name. The initial provider must cooperate and make information available (Art. 25(2)); the contract provides for this.

Situation	What it implies for the contract
A third party supplies tools, services, components or processes to a high-risk system of the company	Written agreement specifying the necessary information, capabilities, technical access and assistance (Art. 25(4)). This is not required for components other than general-purpose AI models made accessible to the public under a free and open-source licence.
The company integrates a general-purpose AI model	The model provider must make information and documentation available to downstream providers to enable them to understand its capabilities and limitations (Art. 53). The contract ensures that these are obtained and updated.

The obligations for high-risk systems in Annex III apply from 2 December 2027, following the Digital Omnibus on AI. Long-term contracts signed before that date **should** already include these clauses.

6.2 DORA for ICT third parties

This applies to financial entities subject to DORA when the AI service is an ICT service provided by a third party:

Requirement	Reference	Fit in SEVEN-G
ICT third-party risk strategy and policy approved by the management body	Art. 28(2); Delegated Regulation (EU) 2024/1773	Corporate policy (31) and C2.
Register of information on all arrangements with ICT third-party service providers	Art. 28(3); Implementing Regulation (EU) 2024/2956	T09 feeds the register.
Pre-contractual analysis, due diligence and conflicts of interest	Art. 28(4)	Stages 1 and 2 of the lifecycle (section 5).
Exit strategies for services supporting critical or important functions	Art. 28(8)	Clause 15; tested exit at N3.
Assessment of concentration risk and of the subcontracting chain	Art. 29; Delegated Regulation (EU) 2025/532	Section 7; clause 5.
Minimum contractual clauses for all ICT services and enhanced clauses for critical or important functions	Art. 30(2) and 30(3)	Section 6; every N3 service of a financial entity is reviewed against Art. 30(3).

Requirement	Reference	Fit in SEVEN-G
Critical ICT third-party service providers designated by the European Supervisory Authorities	Arts. 31 et seq.	European oversight of the provider does not replace risk management by the entity. The ESAs published the first list of designated providers in November 2025; the current list must be consulted.

If the company is not subject to DORA, its requirements **may** be used as a good practice reference for N3 services.

07

Technological dependency and concentration

7.1 Dependency on a supplier

Dependency signal	Measure
Prompts, workflows or agents designed on proprietary features.	Model abstraction layer; prompts and evaluations versioned in the company's own repositories.
Data, indexes or memories exportable only in closed formats.	Export clause; periodic copies in an open format.
Quality evaluations carried out only by the supplier.	In-house evaluation set that allows alternative models to be compared.
Knowledge of the solution held only by the integrator.	Documentation, knowledge transfer and ownership of what is built.
Usage-based pricing without limits or forecasting.	Consumption budgets, alerts and price review clauses.
No tested alternative.	Periodic assessment of at least one alternative for N3 services.

The **portability test** (P57 §7) for N3 services consists of running the in-house evaluation set with an alternative model or provider and documenting the difference in results, cost and migration effort. It is carried out at least once a year or before renewing the contract.

7.2 Concentration

Concentration is measured at portfolio level (document 33 §10) with these indicators:

Indicator	Definition
Systems per supplier	Number of systems in production that depend on each model provider and platform provider.
Dependent value	Proportion of the portfolio's validated value that depends on each supplier.
Dependent critical functions	Critical or important functions supported by each supplier.
N3 suppliers without a tested exit	Number and age.
Common sub-processors	Sub-processors that appear in the chain of several N2 or N3 suppliers.

Concentration limits form part of the risk appetite (document 13). When they are exceeded, the AI Committee decides between diversifying, strengthening the exit or accepting the risk in accordance with 33 §7.

08

Embedded AI in software already contracted

Many business applications incorporate AI features through updates, sometimes enabled by default. They are third-party AI systems embedded in processes (01 §1.2) and must be governed.

8.1 Process

Step	What is done	Owner
1. Identify	Questionnaire (P55, annex A) to current software suppliers on existing and planned AI features; review of release notes; review of configurations. Priority is given to software that processes personal or confidential data or that plays a part in decisions.	AI Office with procurement and technology
2. Inventory	Registration of each relevant AI feature in the inventory (T02), linked to the supplier in T09, with the technology tag "Embedded third-party AI".	AI Office
3. Classify	Determine whether it is general-purpose corporate use or AI that plays a part in decisions, operations or customer relationships; N level; Enterprise criteria; regulatory classification.	AI Risk Owner
4. Decide	Keep disabled, enable with controls or enable as a use case with the full lifecycle.	According to 4.2 and 01 §1.2

Step	What is done	Owner
5. Contract	Addendum (P56 §8) with clauses 1, 3, 8 and 13 as a minimum and those corresponding to the level.	Legal and procurement
6. Monitor	Review of updates and configuration changes at every R6 or, failing that, half-yearly.	Relationship manager

8.2 Rules

- AI features in contracted software that process personal or confidential data **must** remain disabled until assessed, where the configuration allows it.
- If they cannot be disabled, risk RT-TER-06 is recorded, assessed as a priority and decided on at the next AI Committee meeting.
- An embedded feature that plays a part in decisions about people or acts at autonomy level A2 or A3 goes through the full lifecycle, focused on selection, integration, contract and controls.

09

Supplier register

The supplier register is tool **T09**, built on the *Supplier* entity of the common data model (03 §4). Each supplier–service relationship is a record.

Block	Fields
Identification	Internal identifier; legal name; group; country; type of third party (1.1); internal relationship manager.
Service	Plain-language description; models and versions; type of sourcing (build on, buy, adapt, partner); linked systems and use cases (IA-AAAA-NNN).
Classification	N1–N3 level with the value of each factor and justification; critical or important function (yes or no); maximum autonomy level; regulatory role of the supplier and of the company.
Data	Data categories; personal data (yes or no); location; transfers and safeguard; retention; use for training (excluded, authorised or unverified).
Chain	Sub-processors with location and function; subcontracting of critical functions.
Contract	Reference; start, renewal and end dates; notice period; status of the 16 clauses (present, partial, absent, not applicable).
Assessment	Date and result of due diligence (P14); certifications and reports with validity; security assessment; conditions imposed.

Block	Fields
Risk	RT-TER and other linked risks (T06); main residual level.
Monitoring	Service indicators; attributable incidents (INC-AAAA-NNN); notified model changes; date of last and next review.
Dependency and exit	Estimated substitutability; identified alternative; exit plan (yes or no, test date); dependent portfolio value.
Status	Under assessment · Approved · Approved with conditions · Rejected · Exiting · Terminated.
History	Events with date, author and reason.

10

Monitoring and indicators

Indicator	Purpose	Recipient
Suppliers by N1–N3 level and by type	Overview of third-party exposure.	AI Committee
Overdue periodic reviews	Detect relationships without monitoring.	AI Office
N2 and N3 suppliers with missing key clauses	Prioritise renegotiation.	AI Committee
Unverified no-training configuration	Control RT-TER-02.	Data protection
Model changes notified and evaluated before taking effect	Control RT-TER-03.	AI Technical Owners
Incidents attributable to suppliers by severity	Service quality and compliance.	AI Committee; board if S1
N3 suppliers without a tested exit	Control RT-TER-01 and RT-TER-05.	AI Committee; board
Value concentration in the main supplier	Portfolio risk.	Board
Embedded AI features identified and assessed	Control RT-TER-06.	AI Office

The board or its board committee receives a quarterly report on concentration, N3 suppliers without a tested exit, S1 and S2 incidents attributable to third parties and decisions to accept High-level third-party risks.

11

Roles

Role	Responsibility in third-party management
AI Product Owner	Need, requirements, proposed build, buy or partner decision.
AI Technical Owner	Technical assessment, secure integration, portability, technical exit plan.
AI Operations Owner	Service indicators, incidents and model changes in production.
AI Risk Owner	N level, RT-TER risks, clearance.
Procurement	Selection process, questionnaire, register and contract management.
Legal	Clauses, regulatory roles, intellectual property.
Information security	Security assessment and clearance at N2 and N3.
Data protection	Data processing agreement, transfers, impact assessments.
AI Committee	Approval of N3, concentration limits, acceptance of High risks.
AI Auditor	Verifies at G3 and G5 that the assessment and the contract correspond to the level.

12

Associated tools and templates

Name	Use
AI supplier assessment (P14)	N level with factors; build, buy or partner decision; due diligence questionnaire; security and data protection assessment; verification of the 16 clauses; risks; exit plan; clearances and approval. Phase 3; updated at R6 and when triggers occur.
AI supplier register (T09)	Fields in section 9, review and renewal alerts, indicators in section 10 and concentration view. Module of T01; its working format is P57.
AI supplier due diligence questionnaire (P55)	Questionnaire of section 4.3 by level, with scoring and transfer to P14; annex A for embedded AI (section 8). Phase 3.
Model AI contractual clauses (P56)	Model wording of the 16 clauses in section 6, AI annex for existing contracts and embedded AI addendum. Phases 3–4.

Name	Use
Supplier register and exit plan (P57)	Register of section 9, concentration, review minutes, exit plan, portability test, deletion certificate and closure record (sections 5, 7 and 9). Phases 3 to 7.
Feasibility assessment · Risk matrix and register · Scale or retire decision (P10 · P12 · P30)	Sourcing decision, RT-TER risks and exit.
Inventory · Risks · Incidents (T02 · T06 · T08)	Linked systems, third-party risks and incidents.

13

Related documents

Document	Relationship
01 · Foundational methodology	Third-party AI embedded in processes (§1.2), Enterprise criteria (§9.2) and fit of DORA (§13).
13 · AI thesis, ambition and risk appetite	Substitutability time frames, threshold M and concentration limits.
31 · Corporate policy and acceptable use	Corporate use of general-purpose AI and third-party policy.
33 · AI risk methodology	RT-TER risks and portfolio risk.
34 · Regulatory mapping	Value chain obligations under the AI Act , GDPR and DORA.
35 · AI and agent security	SEG and AG controls required of suppliers and components.
37 · Nonconformities and incidents	Supplier incidents and notifications.
42 · AI costs	Total cost and exit cost.

14

Version control

Version	Date	Changes
0.1	16-09-2026	First version. Defines the criteria for building, buying, adapting or partnering; the N1–N3 requirement levels with four factors and requirements by level; the supplier lifecycle; sixteen key contractual clauses, with AI Act obligations along the value chain and DORA; management of dependency and concentration; the treatment of embedded AI and the supplier register fields.
0.2	19-10-2026	Principle 8 "Testing is also using" and AI security purchasing criteria (4.3) (D159).

External sources cited

Links to the official or primary source, checked before publication. Always verify the version in force on the date of use.

Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers · https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/eng · Comisión Europea · 13-03-2024

Commission Delegated Regulation (EU) 2025/532 of 24 March 2025 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when subcontracting ICT services supporting critical or important functions · https://eur-lex.europa.eu/eli/reg_del/2025/532/oj/eng · Comisión Europea · 24-03-2025

Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 with regard to standard templates for the register of information · https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/eng · Comisión Europea · 29-11-2024

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) · https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng · Parlamento Europeo y Consejo de la UE · 27-04-2016

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA) · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng · Parlamento Europeo y Consejo de la UE · 13-06-2024

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) · https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng · Parlamento Europeo y Consejo de la UE · 08-07-2026

The European Supervisory Authorities (EBA, EIOPA and ESMA) designate critical ICT third-party providers under the Digital Operational Resilience Act (18 November 2025) · https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital · Autoridades Europeas de Supervisión (EBA, EIOPA, ESMA) · 18-11-2025

ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system · https://www.iso.org/standard/42001 · ISO/IEC (JTC 1/SC 42) · 18-12-2023