

Supplier Standards

A supplier is evaluated on fit, control and evidence—not a logo or certification badge alone.

01 / Due diligence

Assess ownership, security architecture, operational resilience, support, data locations, subcontracting, vulnerability handling and exit options in proportion to the customer's risk. Verify claims against the named legal entity, product and certification scope.

02 / Contract and data

Define security and incident duties, audit evidence, access, change notification and exit in the contract. Where a supplier processes personal data, apply Article 28 GDPR and relevant transfer safeguards. NIS2 supply-chain measures and DORA contractual provisions are assessed when the customer and service are in scope.

03 / Ongoing review

Revisit material supplier changes, incidents and dependency concentration. Significant findings should lead to a documented risk decision, remediation or alternative supplier. No supplier is represented as pre-approved merely by appearing on this site.

Document status

Original VISIONCYBERX working framework for review. This PDF is not an offer, a signed agreement or evidence of an implemented control. Confirm legal entity details, service scope, commercial terms, annexes and approval before use. A signed engagement document governs.

Official EU references

NIS2 Directive, Article 21

DORA, Article 30

GDPR, Article 28