TLP:RED RESTRICTED — Named recipients only. Do NOT share outside the named project group without explicit authorisation from the document owner. TLP: https://www.first.org/tlp/ | DK: https://www.cfcs.dk/da/handelser/traffic-light-protocol/

defecia.dk

Critical Questions to Ask Vendors Before Purchasing

Vendor Selection Questionnaire & Scorecard

Revision	*X.X*	**Classification**	**TLP:RED**
Responsible	*[Management name / Department]*	**Project Manager**	*[Name]*

TEMPLATE GUIDANCE *TLP:RED means named recipients only. This document may contain vendor names, pricing intelligence, and strategic procurement intent that must not be shared outside the named project group. Adapt all questions to your specific procurement. Ensure the same questions are put to all vendors being evaluated for fairness and comparability. Consider maintaining a linked Excel/CSV scoring sheet with all responses. Email: xleb@defecia.dk.*

Version History

Version	Date	Author	Change Description
1.0			Initial version

Purpose

This document provides a structured set of questions to ask vendors before making a purchasing decision. The purpose is to maintain an objective, comparable view across multiple vendors and to ensure that security, compliance, and operational requirements are evaluated consistently.

All vendors in scope for a given procurement should be asked the same questions. Deviations must be documented and justified.

REMARK This is not a fixed list. Add questions specific to your procurement context. If additional questions are added, ensure they are put to all competing vendors. Consider linking a structured Excel/CSV response sheet to capture all vendor answers for side-by-side comparison.

Justification for Vendor Evaluation

Why are we evaluating this product/service?	*[Business need or gap this addresses]*
Procurement trigger	*[Contract expiry / new capability / cost reduction / compliance requirement / incident]*
Budget reference	*[Internal budget code or project reference number]*
Vendors being evaluated	*[List vendor names. Note: consider whether to share this list with vendors — they may position differently against named competitors]*
Decision deadline	*[When must a decision be made?]*
Decision authority	*[Who approves the final decision? C-level? Procurement committee?]*
Linked documents	*[Risk assessment, BIA, NDA, existing contracts, Excel scorecard]*

Question Areas

1. Product Information and Specifications

- Can you provide detailed technical specifications of the product/service?
- Are there different models, tiers, or versions available? What are the differences?
- What are the key features and differentiators compared to your main competitors?
- What are the non-functional requirements for the system to operate? (Infrastructure, OS, network, browser, minimum specs)
- Encryption keys: who controls them? Who is the Certificate Authority?
  → *Can defecia.dk accept the risk if the vendor controls the encryption keys and CA? What is the key rotation policy?*
- Where is data physically stored? Which countries and data centres?
  → *Relevant for GDPR data residency requirements. EU/EEA preferred.*
- Does the product support Single Sign-On (SSO) and MFA? Which standards? (SAML 2.0, OIDC, FIDO2)
- Is there an API? What authentication does it use? Is there an OpenAPI/Swagger spec?
- What logging and audit trail capability does the product provide?
  → *Critical for forensic investigation and compliance. Can we export logs? In what format?*

2. Quality, Security and Compliance

- Do you hold ISO 27001 certification? If so, provide certificate and scope statement.
  → *Or SOC 2 Type II, CSA STAR, or equivalent. Request the most recent certificate.*
- Do you have a documented Information Security Management System (ISMS)? Can you demonstrate it?
- How do you handle Confidentiality, Integrity, and Availability (CIA triad) for our data?
- Are you GDPR compliant? Can you sign a Data Processing Agreement (DPA) under GDPR Article 28?
  → *Mandatory if you process personal data on our behalf. Request their standard DPA draft.*
- Are you subject to NIS2 obligations as an essential or important entity? How does this affect your supply chain security posture?
- Do you perform regular vulnerability assessments? What is your patching SLA for critical CVEs?
- Have you experienced any data breaches or significant security incidents in the last 3 years? If yes, describe what happened and what was done.
- Do you have a published Responsible Disclosure / Bug Bounty policy?
- If applicable, are you compliant with the EU AI Act? Is AI used in this product's core functionality?
  → *Relevant if the product uses AI/ML for decision-making, risk scoring, or content generation.*

3. Pricing and Total Cost of Ownership

- What is the pricing structure? (Per user, per seat, per transaction, flat fee, consumption-based?)
- What is included in the base price? What requires add-ons or separate licensing?
- Are there discounts for multi-year contracts or volume commitments?
- What are all additional costs? (Onboarding, professional services, training, support tiers, API calls, storage overage)
- What is the price escalation policy at renewal?
  → *Typical SaaS contracts allow 3-0% annual increase. Uncapped escalation is a risk.*
- What happens to pricing if we exceed usage limits or scale significantly?
- Are there any exit fees or contractual penalties for early termination?

4. Delivery, Lead Times and Service Levels

- What are the typical lead times for deployment and go-live?
- Can a Service Level Agreement (SLA) be negotiated? What uptime do you guarantee? (99.9%? 99.95%?)
- What are the financial penalties / service credits for SLA breaches?
- What is the process for reporting and tracking incidents and outages?
- Is a Proof of Concept (PoC) or free trial available? For how long? What is in scope?
- What onboarding and implementation support is included?
- How are planned maintenance windows communicated?

5. Warranty and Support

- What support tiers do you offer? (e.g. 24/7, business hours, email only, dedicated CSM)
- What are the response time SLAs for critical, high, medium, and low severity issues?
- What is your escalation path if a critical issue is not resolved within SLA?
- Is local-language support available (Danish / Scandinavian)? What is the primary support language?
- What is the process for reporting security vulnerabilities in your product?

6. Vendor Reputation, Stability and Experience

- How long have you been in business? What is your ownership structure? (Private, PE-backed, public, subsidiary?)
- Can you provide 2–3 customer references from organisations similar to ours in size and sector?
- What is your annual revenue / number of employees? (Indicator of financial stability)
- Have you been acquired, merged, or significantly restructured in the last 3 years? Any planned changes?
  → *Vendor acquisition is a major risk factor for continuity of support and product direction.*
- Have you been involved in any litigation related to product defects, data breaches, or contract disputes?
- How do you ensure business continuity for your own operations? Do you have a tested BCP/DR plan?

7. Customisation and Flexibility

- Can the product be configured or customised to meet our specific requirements?
- Are there modular features that can be enabled or disabled independently?
- How is the product roadmap determined? Can customers influence the direction?
- What is the process for requesting new features or enhancements?

8. Payment Terms and Conditions

- What are your standard payment terms? (Net 30? Annually in advance? Monthly?)
- What is your policy on price adjustments during the contract term?
- What is your returns / refund policy for licensed software or prepaid services?
- Do you accept purchase orders or require credit card payment?

9. Ongoing Maintenance and Upgrades

- How frequently are product updates and new versions released?
- How are updates communicated and deployed? Is downtime required?
- Are security patches included in the base licence, or do they require additional cost?
- What is the expected product lifecycle before a major upgrade or version migration is required?
- What is your end-of-life (EOL) / end-of-support (EOS) policy and notice period?

10. Future-Proofing and Security Assurance

- How do you ensure the product remains relevant as technology and threats evolve?
- Are penetration tests performed regularly on the product and infrastructure? By whom? How often?
  → *Request the most recent executive summary of a pentest report. Refusal is a red flag.*
- How do you handle zero-day vulnerabilities and CVEs affecting your product stack?
- What is your cloud provider? What shared responsibility model applies?
- Do you have a published security whitepaper or trust centre?
- Does the product comply with relevant EU cybersecurity frameworks (NIS2, Cyber Resilience Act, ENISA guidelines)?

11. Critical Information Exchange and Breach Notification

NIS2 SUPPLY CHAIN	NIS2 Article 21(2)(d) requires essential and important entities to address supply chain security. Your vendors are part of your attack surface. These questions are mandatory for critical suppliers.

- How will defecia.dk be notified in the event of a security breach on your side that may affect our data?
- What is your maximum notification time from discovery of a breach to customer notification?
  → *GDPR requires notification within 72 hours. What is the vendor's contractual commitment?*
- What information will be provided in a breach notification? (Scope, data types affected, remediation steps, timeline)
- Who is our named point of contact for security incidents? (Name, role, 24/7 contact details)
- What is the process for shutting down integrations in an emergency? (File exchange, APIs, SSO, webhooks)
- Do you participate in any threat intelligence sharing communities? (ISACs, FIRST, national CSIRTs)
- Can you provide evidence of your incident response plan and any past tabletop exercises?

12. Termination and Exit of Collaboration

DATA PORTABILITY	GDPR Article 20 provides a right to data portability for personal data. Contractually, you should secure the right to export ALL organisational data in a machine-readable format regardless of GDPR scope.

- How can defecia.dk export all our data from your platform? What is the self-service export process?
- In what format(s) is data exported? (CSV, JSON, XML, database dump?) Is it machine-readable and complete?
- How long does a full data export take? Is there a cost?
- How long after contract termination does our data remain accessible for export?
- What is the certified data deletion process after termination? Can you provide a deletion certificate?
- If your company is acquired, goes bankrupt, or ceases operations: what is the data extraction timeline and process?
  → *This should be contractually defined. Aim for minimum 90 days notice and guaranteed export capability.*
- Are there any vendor lock-in mechanisms that would make migration to a competitor difficult or costly?

Vendor Comparison Scorecard

Score each vendor 1–5 per category. Multiply by weight (1=low, 2=medium, 3=high priority). The highest weighted total indicates the preferred vendor, to be validated against qualitative factors.

Category	Weight (1-3)	Vendor A Score (1-5)	Vendor B Score (1-5)	Notes
Product fit & specifications				
Security posture (ISO 27001 / SOC 2 / ISMS)				
GDPR & data protection compliance				
NIS2 supply chain risk				
Pricing & total cost of ownership				
SLA & support quality				
Vendor financial stability				
Incident notification process				
Data portability & exit terms				
Future-proofing & roadmap				
References & experience				
Penetration testing & vulnerability mgmt.				
WEIGHTED TOTAL				

Risk Register for this Procurement

Document any risks identified during vendor evaluation. These feed into the final decision and any required risk acceptance.

Risk Identified	Likelihood (H/M/L)	Impact (H/M/L)	Mitigation / Decision

Conclusion and Decision

	Pros	Cons
Vendor A		
Vendor B		
Recommended choice		

Internal procurement reference number	*[Reference number for business justification and future audit trail]*
Follow-up meeting required?	*[Yes / No — if yes, date and agenda]*
Risk assessment required?	*[Yes / No — if yes, reference to risk assessment document]*
Recommended decision	*[Vendor name and brief rationale]*
Approved by	*[Name, title, date]*

Tips for Vendor Interactions

DOCUMENTATION	Request written answers to all questions. Verbal assurances have no legal value. Vendor responses should feed into your linked Excel/CSV scoring sheet.
DEMOS & POCS	Always request a Proof of Concept before committing to a major purchase. Define clear PoC success criteria in writing before starting.
NEGOTIATIONS	Never accept the first pricing offer. Multi-year commitments, reference partnerships, and competitor quotes are all negotiation levers. Get concessions in writing as contract addenda.
VENDOR INTELLIGENCE	Be careful about revealing which other vendors you are evaluating. Vendors may use this to undercut competitors or adjust their pitch. Consider keeping competitor names confidential.
NIS2 SUPPLY CHAIN	Document your supply chain risk assessment for critical vendors. This is required under NIS2 Article 21(2)(d) for essential and important entities. Retain vendor responses as evidence.