Critical Questions to Ask Vendors Before Purchasing

[TEMPLATE TEXT:
This is just a example on what to put into a Vendor questionnaire.
Considerations for additional information is if its under GDPR regulations or External delivery (fx NIS2 requirements)
Please add you own thoughts and considerations to the requirements of you company

Consider if you have a excel sheet with all questions and answer. This needs to be linket to the file

TLP: **TLP:RED**
Consider this is a confidential material for only a selected few. As this can be part of a project path that is secret for others
LINK DK :https://www.cfcs.dk/da/handelser/traffic-light-protocol/
LINK EN: https://www.first.org/tlp/
 ]

[Company Name]
Vendor Questionaire

Revision X.X

Responsible: [Management name / Department]

Project manager: [name]

Purpose:

This is for asking the right questions before purchasing a product. The purpose is also to maintain an objective view on the vendor/s to achieve a fair set of points to compare against.

Justification for looking to the vendor

- Why are we looking to this product ?
- What is the justification to look at
- What are the reason for looking into this vendor? or vendors (Consider id you share what vendors you are looking for ? how do they talk about eachother?)

List of areas and questions

Remark It's not a fixed list, if there needs to be added additional questions, please make sure that the same questions are asked to the competitors if that apply

1. Product Information and Specifications

- Can you provide detailed specifications of the product?
- Are there different models or versions of this product?
- What are the key features and benefits of your product compared to competitors?
- What setup is required for the system to run (non functional requirements)
- Encryptions keys (if applicable), who have access to them, who is Certificate Authority?
    - Can [Company name] accept the risk if vendor controls the keys ?

2. Quality and Compliance

- How do you ensure the quality of your products?
- Do your products meet industry standards and regulations?
- Can you provide any certifications or test results for your products?

3. Pricing and Costs

- What is the pricing structure for the product?
- Are there discounts for bulk purchases or long-term contracts?
- Are there any additional costs (e.g., shipping, installation, training)?

4. Delivery and Lead Times

- What are the typical lead times for delivery?
- Do you offer expedited shipping options?
- How are products packaged and shipped?
- Can a Service Level Agreement be scoped ? Expectancy?
- Proof of concept / trial time ?

5. Warranty and Support

- What warranty do you offer on your products?
- What does the warranty cover and what are the limitations?
- What post-purchase support do you provide (e.g., customer service, technical support)?

6. Vendor Reputation and Experience

- How long have you been in business?
- Can you provide references or case studies from other clients?
- Have you worked with businesses similar to ours?
- How is privacy controlled
  - Do the vendor have a certification (fx ISO 27001) or have a ISMS in place and can document this ?
  - How do the vendor handle this ?
- How do they handle the Confidentiality, Integrity and Avalibility ? (CIA triad)

7. Customization and Flexibility

- Can the product be customized to meet our specific needs?
- Are there flexible options available (e.g., modular features, scalability)?

8. Payment Terms and Conditions

- What are your payment terms?
- Do you offer any financing options?
- What is your policy on returns or exchanges?

9. Ongoing Maintenance and Upgrades

- Is ongoing maintenance or servicing required?
- How often do you release product updates or upgrades?
- Are there additional costs for updates or maintenance services?
- What is the expected lifecycle for the system before major upgrades

10. Future-proofing

- How do you ensure the product remains relevant with changing technology and market trends?
- Are there plans for future enhancements or new models?
- Are penetration tests regularly being carried out? If so how often

11. Critical information exchange

- How are [Company name] informed in case of a breach from the vendor side ?
- What kind of information is provided and expected ?
- How fast will we be informed ?
- What process is for shutting down connections (fx file exchange, API´s etc.

12. Termination and exit of collaboration

- Wow can we export data from the vendor ?
- What format can we expect?
- How long time will this take ?
- If vendor closes down what is the expected timeframe for extracting / export of our data ?

Conclusion

- How is the verdict in the company ?
- Do we need a second meeting to get further clarifications ?
- What are the pros and cons with this ?
  - Do we need to make a risk assessment to identify anything further
- Internal number for reference the purchase and business justification for future proof.

Tips for Vendor Interactions

- Documentation: Request written documentation for all important information.
- Samples/Demos: If possible, ask for a product sample or demo before making a large purchase.
- Negotiations: Don't hesitate to negotiate terms that better suit your business needs.