



THE CYBER **SCHEME**

BUYER CHECKLIST

CYBER SECURITY PROCUREMENT CHECKLIST FOR BUYERS

We developed this checklist after speaking to organisations across the cyber security sector about the procurement challenges they encounter most frequently. It is designed to help buyers create clearer requirements, support fair competition and improve procurement outcomes.

These ten questions will help buyers check that a tender is clear, proportionate and likely to produce bids they can compare properly.

1. Have we defined the outcome?

Explain the risk, business need or assurance objective rather than beginning with a preferred product, supplier or activity.

2. Is the technical scope clear enough?

Describe the relevant assets, environments, constraints, dependencies, timescales and expected deliverables.

3. Are specialists able to propose an appropriate approach?

Avoid fixing the duration or method before the work has been assessed, unless there is a clear and justified reason.

4. Can suppliers realistically provide the evidence requested?

Consider confidentiality, non-disclosure obligations and the sensitivity of previous cyber security work.

5. Are certification requirements relevant and proportionate?

Connect every required credential clearly to the work, level of risk or role being procured.

6. Have we separated organisational assurance from individual competence?

State whether evidence applies to the supplier organisation, the people delivering the work, or both.

7. Are equivalent assurance pathways recognised?

Focus on the capability or outcome that must be evidenced and explain how legitimate alternatives will be evaluated.

8. Can bids be compared on a like-for-like basis?

Ensure suppliers are responding to the same assumptions, scope and expected level of effort.

9. Does price carry the right weight?

Check that the scoring model does not reward a cheaper but materially weaker activity.

10. Can we explain the final decision?

Keep a clear evaluation record and provide useful feedback that relates to the published criteria.

Help improve cyber security procurement. Report unfair, unclear or disproportionate requirements through our Procurement Fairness and Framework Review initiative here:

<https://thecyberscheme.org/procurement-fairness-and-framework-review/>

