



Defence IT & Secure Infrastructure Procurement

Procure secure, resilient and AI-ready IT - from requirement to lifecycle.

WHAT IT MEANS

Enterprise, defence and AI/HPC infrastructure cannot be procured on technical specifications alone. Availability, data sovereignty, supply chains, power, support, export controls, obsolescence and total cost determine whether hardware becomes an operational capability. SYBX brings these factors together in a structured, defensible procurement decision.

01 Mission & architecture

Clarify use case, workloads, classification, availability, capacity, deployment and scaling before selecting a product.

02 Market & suppliers

Source independently; assess delivery capability, defence experience, ownership, local support and supply-chain exposure.

03 AI/HPC & infrastructure

Evaluate compute, GPUs/accelerators, storage, networking, software, power and cooling as one system.

04 Security & compliance

Resolve data sovereignty, cyber security, export controls, sanctions, end use and supply-chain transparency before RFx.

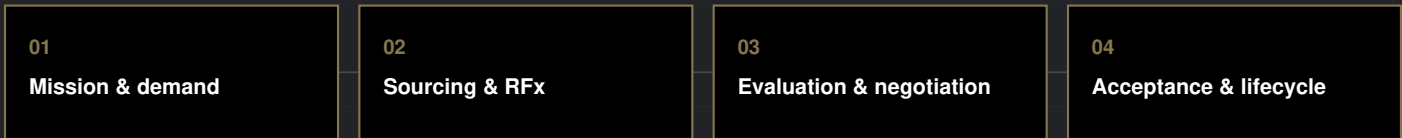
05 Commercial, TCO & FinOps

Compare capital and operating costs, licences, energy, support, risk cost and time to capacity.

06 Contract & lifecycle

Secure acceptance, service levels, spares, patching, end of life, refresh, exit and obsolescence in the contract.

FROM REQUIREMENT TO OPERATIONAL CAPABILITY



The outcome Clear options. Comparable bids. Documented risks. An implementable recommendation.

FOR BUYERS

Assessment, sourcing strategy, RFx, TCO/FinOps, evaluation, negotiation, contract and acceptance structure.

FOR SUPPLIERS

Market and tender readiness for national, NATO and EU procurement, bid/no-bid, compliance matrix and commercial strategy.

Buyer and supplier mandates are kept strictly separate; no parallel support in the same procurement.

Clarity for complex procurement decisions.

REDEFINING PROCUREMENT