Data security standards decision-making checklist

Identify Your Data

- Have we listed all the types of data we collect and store?
- Do we handle sensitive or personal data?
- Do we know where this data is stored (cloud, on-premises, hybrid)?

Understand Industry Requirements

- Have we checked which regulations or standards apply to our industry (e.g. DSPT, PCI DSS, ISO 27001, GDPR)?
- Do clients, partners or regulators expect specific certifications?

Consider Geographic Scope

- Do we operate in the UK or internationally?
- If international, have we reviewed global frameworks (e.g. SOC 2, ISO)?
- What 3rd party tools and platforms do we use? Are these all in support and secure?

Assess Infrastructure and Technology

- Is our data primarily cloud-based, on-premises or both?
- Do the chosen standards support our infrastructure model?

Evaluate Internal Capabilities

- Do we have the right expertise in-house to meet compliance requirements?
- Are our processes and policies aligned with best practices?
- Do we need external support or training?

Plan for Compliance and Maintenance

- Have we defined a roadmap for achieving compliance?
- Do we have monitoring / auditing processes?
- Is there an ongoing review cycle to keep up with changes in standards/regulations?