CASE STUDY 09 · CONFIDENTIAL CLIENT ENGAGEMENT

ISO/IEC 27001 gap analysis and certification readiness

Preparing a platform that handles sensitive customer and financial data for ISO/IEC 27001 certification.

CLIENT SECTOR Data platform handling sensitive customer and financial data	MY ROLE ISMS gap analysis and readiness adviser
WORKED WITH Chief information security officer, executive sponsor, audit	FOCUS Annex A controls, risk method, Statement of Applicability

The situation

The platform was preparing for certification for the first time. It needed to know where its controls fell short and be able to justify each control decision.

What I did

1. **Annex A gap analysis**
   Each control compared with current practice, prioritised by the risk each gap represented.
2. **Risk assessment method**
   An approach aligned to ISO/IEC 27005 for identifying and scoring information security risk.
3. **Statement of Applicability**
   A completed statement with the reason recorded for including or excluding each control.
4. **Risk treatment plan**
   The highest-risk gaps addressed first, on realistic timelines.

HOW I APPROACHED IT

I recorded the reasoning behind every control decision, so the organisation can explain it to an auditor even after the person who made it has moved on.

Similar work I take on

- Organisations seeking ISO/IEC 27001 certification for the first time
- Platforms handling sensitive or regulated data
- Companies facing procurement checks that ask for ISO 27001 evidence

The client's name and working documents are withheld under confidentiality.

Adenola Adegbesan · adenolaadegbesan.co.uk · adenola.adegbesan@gmail.com