Security compliance and standards

Suppliers to regulated organisations face security clauses, questionnaires and audits under the Network and Information Security Directive 2 (NIS2). Financial entities must manage technology risk, incidents and suppliers under the Digital Operational Resilience Act (DORA), and Irish credit unions join them on 17 January 2028. Makers of connected products and software must meet the Cyber Resilience Act (CRA) from 11 December 2027.

We start with a readiness check, then build short, practical controls and an evidence pack you can reuse. When customers ask for ISO/IEC 27001, the same programme takes you to certification.

WHAT IT COVERS

ISO/IEC 27001
Taken to certification, or an evidence pack first.

NIS2
Regulated entities and, above all, their suppliers.

DORA
Financial entities, their providers and credit unions.

CRA
Secure products, vulnerability handling and reporting.

HOW IT WORKS

01 Readiness check — 4 TO 6 DAYS
What applies, what customers expect, and a board briefing.

02 Build — 2 TO 6 MONTHS
Policies, incident handling, evidence or registers, and training.

03 Prepare for certification — BEFORE AUDIT
Everything checked before the ISO/IEC 27001 certification audit.

04 Keep it current — 12 MONTHS
Evidence kept up, with help on questionnaires, audits and incidents.

ACROSS EUROPE AND BEYOND

NIS2 works through each EU country's own law, while DORA and the CRA apply directly across the EU. If you operate or sell in several countries, we map one set of controls to each country's rules. ISO/IEC 27001 evidence is recognised worldwide, from the UK to the United States.

WHO IT IS FOR
Suppliers, energy, transport, finance and product makers

CREDIT UNIONS
Five or more can share one group programme

LED BY
Lee Bristow, ISO/IEC 27001 Lead Auditor and Implementer

Start with a 30-minute briefing, at no charge.

DAWN-HORIZON.COM
lee.bristow@dawn-horizon.com
+353 87 153 0447