GRC+ SERVICE SHEET · NOVEMBER 2026

ISO 27001 Implementation

We build your information security management system with your team: scope, risk method, risk treatment, Statement of Applicability, policies and the evidence an auditor will ask for. We stay with you through the certification audit.

SERVICE
Advisory service

USUALLY TAKES
Months, usually, from kick-off to certification readiness

What It Is

Build an ISMS that is ready for certification and stays useful: scope, risk assessment, Statement of Applicability, policies and evidence.

Who It Is For

- An ISMS built with your team, around how you actually work
- With you through the stage 1 and stage 2 audits
- An accredited body you choose certifies you; we never certify our own work
- Professional indemnity insurance on every engagement

What an ISO 27001 ISMS Needs

Scope and context	A clear ISMS scope, interested parties and their requirements.
Leadership	Top management commitment, policy, roles and responsibilities.
Risk assessment	A repeatable method to identify and rate information security risks.
Risk treatment	A treatment plan and a Statement of Applicability.
Objectives	Measurable security objectives and plans to reach them.
Competence and awareness	People know their role in the ISMS and are trained for it.
Documented information	Policies, procedures and records kept current and controlled.
Monitoring	Measurement of how the ISMS and its controls perform.
Internal audit	Independent audits of the ISMS at planned intervals.
Management review	Regular reviews by management, and continual improvement.

From Gap Analysis to Certification

1 **Gap analysis**
Your controls and documents against clauses 4 to 10 and Annex A, with a plan to close the gaps.

2 **Design**
Scope, risk method, risk assessment and treatment, Statement of Applicability and policies, drafted with your team.

3 **Operate**
The ISMS runs for a period, so the records an auditor asks for exist: risk reviews, incidents, training and supplier checks.

4 **Internal audit**
An internal audit by a party independent of the implementation team, as clause 9.2 requires. We never audit work we built.

5 **Management review**
Top management reviews the ISMS and its results, as clause 9.3 requires, and records its decisions.

6 **Stage 1 audit**
The certification body reviews your documentation and readiness. We help you close any points it raises.

7 **Stage 2 audit**
The certification body audits the ISMS in operation. We stay with you until the audit closes.

Regulations That Ask for It

ISO 27001	Build an ISMS that is ready for certification and stays useful: scope, risk assessment, Statement of Applicability, policies and evidence.
NIS2	An information security management system that covers the Article 21 measures and that national laws often accept as evidence.
NN 14/2019 (Croatia)	The internal security structure, procedures and checks that Article 31 asks of controllers and processors.
Dz.U. 2020 poz. 666 (Poland)	Risk management and documented security procedures that meet § 1(5).
Uradni list RS 106/2023	An ISMS and BCMS ready for the certification Article 14 requires.
UN R155 / R156	
Part-IS	
TISAX	
MDR	
ISO/SAE 21434	
SOC 2	
CMMC (United States)	

Questions Buyers Ask

How long does certification take?

It depends on your scope and starting point. Many organisations reach certification readiness within several months.

Do you issue the certificate?

No. An accredited certification body issues the certificate. We prepare you and support you during the audits, which keeps the certification independent.

What happens after certification?

Your team runs the ISMS with the processes we set up, or we keep it running for you with our CISO as-a-Service.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/iso-27001-implementation

