GRC+ SERVICE SHEET · NOVEMBER 2026

CISO as-a-Service

A named, certified CISO runs your security programme: the ISMS, risk treatment, the NIS2 and DORA measures and the reports your board and customers ask for. Part-time, for a fixed monthly fee.

SERVICE
Managed service

USUALLY TAKES
Weeks, usually, to a security roadmap your board can approve

What It Is

A named, certified CISO who runs your security programme: ISO 27001, NIS2 and DORA, for a fixed monthly fee.

WHY IT MATTERS

Accountability without a leader

- Senior CISOs are scarce, and a hire takes months
- Security sits with IT, which cannot check its own work
- NIS2 and DORA make management answerable for cyber risk
- Customer questionnaires and audits pile up with nobody to own them

THE OUTCOME

Evidence for your board and your customers

- A roadmap your board can approve in the first months
- An ISMS kept ready for audit
- Quarterly reports that show what was done
- Work that continues when someone is away

The NIS2 Security Measures, Each with an Owner and Evidence

Risk management	Policies on risk analysis and information system security.
Incident handling	Detection, response and reporting that meets the deadlines.
Business continuity	Backups, disaster recovery and crisis management.
Supply chain security	Security requirements for suppliers and service providers.
Secure development	Security in acquisition, development and maintenance, including vulnerability handling.
Effectiveness checks	Policies to assess whether the measures work.
Cyber hygiene and training	Basic practices and regular training, management included.
Cryptography	Policies on encryption where it is appropriate.
Access control and assets	HR security, access policies and asset management.
Authentication	Multi-factor or continuous authentication and secured communications where appropriate.

How the First Quarter Usually Runs

1	**Appointment** Named CISO and governance in place, with a shared Slack or Teams channel.	Weeks 1 to 2
2	**Assessment** Controls, risks and suppliers reviewed against ISO 27001, NIS2 or DORA.	Month 1
3	**Roadmap and quick wins** A roadmap your board can approve, with the most urgent gaps closed first.	Months 2 to 3
4	**Run and report** Risk reviews, policies, incidents, audits and management reports, within your plan.	Ongoing

Regulations That Ask for It

NIS2	**CISO as a service** An experienced CISO who owns the Article 21 measures, reports to the management body and keeps the programme moving.
DORA	**CISO as a service** An experienced CISO who owns the ICT risk framework, reports to the management body and keeps the programme moving.
PSD2	**Security leadership for a payment institution** A CISO who owns the security policy, the yearly risk assessment and the evidence your authority asks for.
Swift CSP	**Keep the controls in place all year** A CISO who owns the remediation plan, the incident response plan and the evidence between two assessments.
IEC 62443	A part-time CISO who runs your security programme and reports to your management body.
PCI DSS	**Run the PCI DSS programme** A CISO who owns the scope, the targeted risk analyses, the policies and the evidence your QSA or SAQ needs every year.
ISF SOGP	
NIST CSF	
PDPL (Oman)	A named, certified CISO who runs your security programme: ISO 27001, NIS2 and DORA, for a fixed monthly fee.
CCPA (United States)	
DORA ICT Risk Management RTS	
DORA Incident Classification RTS	

Questions Buyers Ask

What does a CISO as a service do each month?

Your named CISO runs the security programme: risk register, policies, roadmap, supplier questions and reports to management. Hours and meetings per month are set by the plan, and you see what was done in the quarterly management report.

Does this help with NIS2?

Yes. We map your measures to the ten areas in Article 21, set up incident reporting that can meet the 24-hour and 72-hour deadlines, and brief the management body, which NIS2 holds accountable.

Can you get us to ISO 27001 certification?

We run the ISMS work: scope, risk assessment, Statement of Applicability and management review. The internal audit has to be impartial, so the team that runs your ISMS does not do it. The certification audit itself is done by an accredited body you choose; we prepare you and attend.

Do you operate our security tools?

No. We set direction, requirements and oversight. Your IT team or managed service provider runs the tools, and we check that the controls work.

Talk to Us

In 30 minutes you learn which laws apply to you and which plan fits.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/ciso-as-a-service

