



Supportimize

Smart Support Solutions

Audit-ready IT support

ISO 27001 · NIS2 · DORA · A practical guide

1 · Why support is at the centre of audits

Support is where incidents are first detected, logged and classified, and where access and changes flow every day. That is exactly where an auditor looks for evidence that you operate the way your policies say. The good news: support run the ITIL way already covers most of what these frameworks ask for. This guide shows what to have in place and what to be ready to show.

Mind the reporting deadlines. NIS2 and DORA put incident reporting on a clock: an early warning within 24 hours, a notification within 72 hours, and a final report within one month. If the service desk cannot classify and escalate an incident in time, you miss a regulatory deadline. Support has to be wired into the reporting process, not cut off from it.

2 · The three frameworks at a glance

Framework	What it is	What it wants from support
ISO 27001	Information security management system (ISMS), a voluntary certification.	Managed incidents, access, changes, logs, suppliers, continuity, and evidence for all of it.
NIS2	EU cybersecurity directive, transposed into national law across the EU.	Risk management measures and incident reporting on strict deadlines, with management accountability.
DORA	EU digital operational resilience regulation, in force since 17 Jan 2025.	Classification and reporting of major ICT incidents, resilience, testing, and third party risk.

3 · Nine pillars of audit-ready support

Pillar	What to have in place	Covers
1 · Incident management and reporting	A classification and severity matrix with a clear “reportable to a regulator” threshold. An escalation path and templates for the 24h and 72h notifications. Every incident fully recorded.	ISO · NIS2 · DORA
2 · Logging and evidence	Every ticket and action timestamped and retained per a retention policy. When the auditor says “show me”, you can.	ISO · NIS2 · DORA
3 · Access management	Joiner, mover and leaver handled through the service desk with approvals. A privileged account list. A regular access review.	ISO · NIS2
4 · Change and configuration mgmt	Changes logged, assessed, approved, tested, with a back-out plan. An asset inventory or CMDB.	ISO · DORA
5 · Continuity and resilience	Runbooks for outages, a DR plan, a communication plan. For DORA, evidence that you tested resilience.	ISO · NIS2 · DORA
6 · Third party risk	A register of support suppliers (ITSM tool, outsourced L1, remote access) with contracts, SLAs and exit plans.	NIS2 · DORA
7 · Documented processes	SOPs, runbooks, an escalation matrix and policies. Versioned and reviewed on a schedule.	ISO · NIS2

Pillar	What to have in place	Covers
8 · Measurement and reporting	Defined SLAs, MTTR, incident trends, a monthly report to management.	ISO · NIS2
9 · Roles and training	A clear RACI, defined ownership, security awareness training (the service desk is a social engineering target).	ISO · NIS2 · DORA

4 · Readiness checklist

- ✓ Incident register with classification, timestamps and a “reportable” flag.
- ✓ Severity matrix mapped to NIS2 and DORA reporting thresholds, plus 24h and 72h templates.
- ✓ Escalation matrix that names who notifies the regulator.
- ✓ Access approval records, a privileged account list, and the date of the last review.
- ✓ Change log with approvals and back-out plans, and a current asset list or CMDB.
- ✓ Versioned SOPs and runbooks with last-review dates.
- ✓ SLA definitions and the last 6 to 12 months of SLA and MTTR reports.
- ✓ Supplier list with contracts, SLAs and exit plans.
- ✓ A business continuity or disaster recovery plan with a recent test on record.
- ✓ Security training records for the support team.
- ✓ A retention policy for support records and logs.
- ✓ An evidence pack: a few sample tickets that show the whole process end to end.

5 · How we help

Consult

A gap analysis of your support against the framework: where the missing processes and evidence are, with a prioritised action plan.

Transform

Putting it in place: the ITSM tool, SLAs, escalations, runbooks, and the change and access trails.

Operate

Keeping the evidence trail alive month after month, so the next audit is a formality.

Get support audit-ready before the auditor arrives.

Start with a free 30-minute call. We will see where you stand and tell you what to tighten.

Milan Meszaros · info@supportimize.com · **+421 904 704 135** · supportimize.com