

Dazr Compliance · Factsheet · Business continuity

Business continuity and incident response, run as one programme.

ISO 22301:2019 as 25 recurring controls with evidence, the continuity controls of ISO 27001, NIS2 and DORA next to it, readiness checks for the BIA, the BC/DR test and the exercise programme, and an incident register with GDPR and NIS2 clocks on every plan.

Edit incident



Logged 2 Oct 2026 by sanne.devries@brightwater.example

Personal-data breach: GDPR 72-hour clock ● **Notify authority in 17h**

Notify the supervisory authority within 72 hours of detection (GDPR Art. 33): by 3 Oct 2026, 10:33. The clock includes weekends.

Title

Discharge letter emailed to the wrong GP practice

Severity

● Low ● Medium ● **High** ● Critical

Status

Investigating Contained Resolved Closed

Key capabilities

- ✓ **ISO 22301:** 25 recurring controls across clauses 4-10 (from Pro).
- ✓ **Incident register** on every plan: 12 incident types, phases, timeline, GDPR 72-hour and NIS2 24h / 72h / one-month clocks.
- ✓ **Suppliers:** vendor register with review and contract-expiry alerts (Pro and Enterprise).
- ✓ **Continuity controls** in ISO 27001 (A.5.29, A.5.30, A.8.13, A.8.14), NIS2 Art. 21(2)(c) and DORA Art. 11 and 12.
- ✓ **Readiness checks** for the BC policy, BIA, BC/DR test, backup-restore test, exercise programme, BCMS audit and management review.

ISO 22301 as a working programme

Enable ISO 22301 and its 25 controls, clauses 4 to 10, recur with an owner, a due date, a description, a recommendation and a default cadence: 20 yearly, 4 quarterly and 1 half-yearly.

Clause	Control	Default cadence
8.2.1	Business impact analysis: priorities, dependencies and resource requirements	Yearly
8.2.2	Risk assessment of disruption	Yearly
8.3	Business continuity strategies and solutions	Yearly
8.4	Business continuity plans and procedures	Yearly
8.5	Exercise programme: an annual tabletop at minimum and a live test of one critical service a year	Yearly
8.6	Evaluation of business continuity documentation and capabilities	Yearly

ISO 22301 is included from Pro (€99 a month), next to up to four other frameworks.

Continuity controls in your other frameworks

The incident register and its clocks

Area	What is recorded
Classification	12 types (data breach, account takeover, ransomware, DDoS, phishing, insider, vendor, system failure, misconfiguration, lost device, physical, other) and 4 severities
Phases	Investigating, contained, resolved, closed, with timestamps for detection, containment, eradication and resolution
Timeline	Entries of type note, update, containment, communication, evidence and decision, each with who and when
Clocks	GDPR Art. 33: notify within 72 hours of awareness. NIS2 Art. 23: early warning in 24 hours, notification in 72 hours, final report in one month
Notification	Authority, report date and case reference, data subjects notified, and the Art. 33(3) fields: DPO contact, likely consequences, measures taken
Learning	Root cause, mitigation, lessons learned, forensic preservation note and the linked corrective-action task

- The NIS2 significant-incident checker (Implementing Regulation (EU) 2024/2690) evaluates the answers against your entity type and turnover and stores the outcome with the incident.
- The dashboard shows incidents by severity and the share of personal-data breaches reported within 72 hours over the last 12 months.
- Running clocks appear in the "What needs you now" list with the time left or the time over.
- On Enterprise, a public breach-report portal lets anyone report without an account; reports wait in a queue until an admin approves them into the register.

Platform

- | | | |
|--|--|---|
| ✓ Hosted in the EU, built by Dazr in Italy | ✓ Records encrypted at rest with AES-256-GCM | ✓ Sign in with Google, Microsoft or an email code |
| ✓ Roles: owner, admin, member, auditor | ✓ Searchable, exportable activity log | ✓ English, Dutch, Italian, German, French, Spanish and Polish |