Where ISO 27001 incident response lands in NIST CSF 2.0

The question. We hold ISO/IEC 27001:2022 certification; our US parent reports on NIST CSF 2.0. Which canonical control sits behind Annex A.5.26 (response to information security incidents), where does it land in CSF 2.0, and what is the provenance of each mapping?

The pivot: one canonical control. The control library resolves ISO/IEC 27001:2022 Annex **A.5.26** onto the canonical spine at **IR-4 — Incident Handling** (NIST SP 800-53 Rev 5, catalog release 5.2.0). The edge is a NIST OLIR informative reference — the SP 800-53 Rev 5 → ISO/IEC 27001:2022 mapping, 2023-10-12 update, sheet IR row 22 — carried in the library as a review-approved `related-to` edge with `provenance_origin: nist-published`.

IR-4's statement is the implement-once definition your evidence hangs on: an incident handling capability consistent with the incident response plan covering preparation, detection and analysis, containment, eradication and recovery; coordinated with contingency planning; lessons learned folded back into procedures, training and testing; rigor and scope comparable and predictable across the organization.

Across to CSF 2.0 — 24 subcategories, the whole incident lifecycle. From IR-4 the crosswalk lands on 24 CSF 2.0 subcategories:

Lifecycle slice	Subcategories
Detect & analyze	DE.AE-02, DE.AE-03, DE.AE-06, DE.AE-08
Respond — manage & triage	RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05
Respond — analyze & preserve	RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08
Respond — communicate & mitigate	RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02
Recover	RC.RP-01, RC.RP-02, RC.RP-06, RC.CO-03, RC.CO-04
Improve	ID.IM-01, ID.IM-02, ID.IM-03

Each row arrives with its subcategory title, a citation into the CSF 2.0 corpus (CSWP 29), and the stored edge facts for both hops — which control pivoted the path, the stored direction of each edge, and the OLIR source reference down to the sheet row.

What the library will not claim. Every one of those paths is returned as a navigation link, not a coverage claim. The stored edges are NIST-published informative references (`related-to` , untyped upstream); the library derives no equivalent, superset, subset, partial or coverage relationship without a direct reviewed cross-framework edge. Weakest-link semantics: a chain through an untyped reference never over-claims. When your auditor asks "does A.5.26 cover DE.AE-08?", the honest answer the library gives is "here is the NIST-published path and its provenance — the set-theory judgment is pending review", not a silent yes.

The NIS2 angle. The requirement register also carries NIS2 (48 normative requirements). `resolve("nis2:2022#art-21")` returns the citation descriptor — *Cybersecurity risk-management measures*, normative, active — with the live resolution parameters: `get_provision(jurisdiction=EU, law=NIS2, article=21)` against the `eu-regulations` corpus, ELI link into EUR-Lex, licence `EUR-Lex-Decision-2011-`

`833`. The library stores the pointer, never the requirement text: the clause text always comes from the licensed corpus at call time, under your tier's entitlements.

Captured 2026-08-04 against gateway.ansvar.eu (Ansvar control library, catalog 800-53r5 5.2.0) — a real session, tool trace and citations at ansvar.eu/use-cases/control-library-crosswalk. Ansvar Systems AB.