Security by sector

Interpret controls through sector-specific impact, dependencies and regulatory scope.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Manufacturing, healthcare, finance, logistics, SaaS and energy examples. Authorized change procedures apply to real critical systems.

Process and expected evidence

1. Define the business outcome

Service and impact record

2. Validate applicability

Dated applicability assessment

3. Choose controls through dependencies

Dependency map and control test

4. Validate with the owner

Service-owner decision and residual risk

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Sector: Manufacturing

Critical service: Example filling line

Dependency: Remote maintenance gateway

Scope decision: Plant + legal review

Control: Time-bound access

Service test: Approved maintenance window

Closure checklist

[ ] Applicability assessed beyond sector label.

[ ] Service and harm scenario explicit.

[ ] Shared dependencies reviewed.

[ ] Service owner involved in closure.

Official sources

NIST Cybersecurity Framework 2.0

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

ENISA — NIS2 technical implementation guidance

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

ESMA — Digital Operational Resilience Act

https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

NIST SP 800-82 Rev. 3 — Final

https://csrc.nist.gov/pubs/sp/800/82/r3/final

Sector working notes

Manufacturing

Safety, production continuity and legacy controllers.

Maintenance windows are limited; supplier support may be critical.

Verify remote maintenance with approval and session evidence; no active test without plant approval.

A second supplier path to a filling line was found through passive flows and rule review.

Healthcare

Continuity of patient care and confidentiality of health data.

Medical-device changes may need manufacturer and clinical approval.

Test device, clinical workflow and emergency access together; preserve ENISA procurement guidance’s healthcare scope.

An approved alternative workflow was rehearsed for lab-result transfer when an integration failed.

Finance

Transaction integrity, critical services and third-party dependencies.

DORA and local regulatory scope are assessed by entity and service.

Connect separation of duties, service inventory and supplier exit to the same business service.

A payment service’s alternate provider shared the same identity platform, revealing a common failure point.

Logistics

Continuity of shipment, routing and warehouse operations.

Field connectivity and mobile devices may be intermittent.

Test offline processing, resynchronization and wrong-delivery controls with synthetic records.

After a warehouse device reconnected, a test verified the same shipment was not processed twice.

SaaS provider

Tenant separation, customer data and release security.

Shared infrastructure changes can affect many customers.

Test object authorization, release provenance and customer export against a specific version.

A synthetic test found that exports crossed tenant boundaries despite correct read permissions.

Energy

Physical service, safety and regional dependencies.

Control center, field systems and communications may share a failure mode.

Assess independent communications, plant access and authorized recovery rehearsal through service impact.

A dependency review revealed that two communications lines shared one physical route.