Audit report

NIS2 compliance dossier (Art. 20/21/23) - organisation

Organisation	**Example Machine Works B.V.**
Source snapshot	be4aea5f · 2026-09-16 21:03

Contents

1. Entity and scope

Field	Value
Entity	Example Machine Works B.V.
Sector	Industrial automation / machinery
NIS2 gap analysis	in scope

> Record the entity classification (essential or important, Art. 3) and the registration with the national authority - both follow from the national transposition and live outside Crosswalk.

2. Governance (Art. 20)

Art. 20 requires the management bodies to APPROVE the risk-management measures, OVERSEE their implementation, and FOLLOW TRAINING (and offer it to staff).

- Approval and oversight: the sign-off blocks of the audit report set record management approval; the version history evidences oversight over time. (!) File the management-body approval decision explicitly.
- Training: 7 entry(ies) in the training & awareness register (Tools > Training & awareness register).

3. Risk-management measures (Art. 21(2)(a)-(j))

Overall assessment: 20 of 20 requirements assessed; 20 in place, 0 partial, 0 open. (Assessment: Organisation > NIS2 gap analysis.) The per-measure mapping:

Art. 21(2)	Measure	Where this dossier holds it
(a)	Risk analysis & information-system security policies	Risk register (6 risk(s))
(b)	Incident handling	Incident reporting & response (2 case(s)) · Incident & vulnerability reporting assessment
(c)	Business continuity: backup, disaster recovery, crisis management	ISO 22301 (BCMS) assessment in scope
(d)	Supply-chain security	Supplier register with due-diligence fields (4 supplier(s))
(e)	Acquisition, development & maintenance incl. vulnerability handling & disclosure	Secure development lifecycle · CVD assessment · disclosure policy/security.txt
(f)	Effectiveness assessment of the measures	The audit report set + maturity report (re-generated per review cycle; provenance-stamped)
(g)	Cyber hygiene & training	Training & awareness register (7 entry(ies))
(h)	Cryptography & encryption policies	NIS2 gap analysis (cryptography measures)
(i)	HR security, access control, asset management	Contacts & role catalog (5 person(s)) · component/asset registers
(j)	MFA, secured communications	NIS2 gap analysis (authentication & communications measures)

4. Incident notification readiness (Art. 23)

Significant incidents notify the CSIRT/authority in stages: early warning within 24 hours, incident notification within 72 hours, final report within one month (intermediate updates on request).

- The incident-reporting tool (Tools > Incident reporting & response) walks each case through receipt, the becoming-aware triage and exactly these clocks.
- Reporting assessment: 7 of 7 requirements assessed; 7 in place, 0 partial, 0 open. (Assessment: Organisation > Incident & vulnerability reporting.)
- (!) Record the national notification channel (CSIRT portal / authority contact) for your Member State.

5. Evidence and registers

Register snapshots (risks, suppliers, cases, trainings) and every evidence attachment travel in the audit binder with the SHA-256 manifest; the audit trail records who changed what, when.

Role	Name	Date	Signature
Compiled by			
Approved by (management body, Art. 20)			

> Generated with Crosswalk as a compliance-support aid; it is not legal advice and is not, by itself, proof of compliance. Verify against Directive (EU) 2022/2555 and the national transposition.