What ISO 45001 Looks Like for Tech and Hardware Companies

fortifai

What ISO 45001 Looks Like in Practice for Tech Companies

Digital and SaaS Companies

→ **Workstation and ergonomics risk assessment**

Every employee's working environment — office or home — requires a workstation assessment. Display screen equipment regulations in most EU jurisdictions already require this. ISO 45001 formalises it into a documented, auditable process with follow-up actions tracked to closure.

→ **Remote work safety**

Home office environments are workplaces under most health and safety legislation. Your OHSMS needs to cover how you assess home office risk, what you provide to remote workers (equipment, guidance, support), and how you follow up. This is the control area most tech companies have never documented.

→ **Mental health and psychological safety**

ISO 45001 explicitly includes psychological health within its scope. For tech companies this means documented approaches to workload management, stress risk assessment, manager training on mental health, and clear escalation pathways. Not a wellbeing initiative — a documented, auditable risk control.

→ **Contractor and freelancer safety**

The standard covers anyone performing work on your behalf. If you use contractors, freelancers, or agency workers — which most tech companies do — your OHSMS must include how you communicate safety requirements to them and verify they are operating safely.

→ **Travel and lone working**

Employees travelling for sales, implementation, or conferences, and employees working alone in offices outside core hours, carry specific risk that must be assessed and controlled.

Hardware and Electronics Companies

Everything above, plus:

Prototyping lab and workshop safety

Even a small prototyping environment carries real hazards: soldering fumes, chemical exposure from flux and cleaning agents, electrical risk from high-voltage prototyping, and ergonomic risk from bench work. Each requires a documented hazard assessment with named controls.

Battery and power systems handling

Lithium battery handling, charging, and disposal carry fire and chemical risk. For hardware companies working with high-capacity batteries or power systems, this is a priority risk assessment area.

ESD and electronics handling

Electrostatic discharge protocols protect both people and products. Documentation of ESD controls belongs in your OHSMS for hardware companies.

Small-scale assembly ergonomics

Repetitive hand and wrist movements in assembly work carry musculoskeletal risk even at low volumes. Risk assessment and rotation controls are standard ISO 45001 requirements for any assembly environment.

Supplier and contract manufacturer safety

If you use contract manufacturers or fabrication suppliers, your OHSMS should include how you assess and monitor their safety performance — particularly relevant for hardware companies with offshore or nearshore manufacturing relationships.

High-Level Implementation Checklist

1

Phase 1 — Foundations

- Define OHSMS scope — which locations, activities, and worker categories are included
- Appoint OH&S management representative — not necessarily the CFO but with executive sponsor named
- Complete gap assessment against ISO 45001:2018
- Identify all applicable health and safety legislation for your jurisdictions — build legal compliance register
- Select certification body and confirm audit dates
- Set up document management system with version control

2

Phase 2 — Hazard Identification and Risk Assessment

- Conduct workplace hazard identification — office, lab, remote, travel, contractor activities
- Complete workstation and display screen equipment assessments for all employees including remote workers
- Conduct mental health and stress risk assessment
- For hardware companies: complete lab, workshop, and assembly environment hazard assessments
- Score risks by likelihood and impact
- Document control measures for each identified hazard
- Leadership signs off on risk assessment and treatment plan

3

Phase 3 — Policy and Procedure Documentation

- Draft and approve OH&S Policy — top management sign-off required
- Draft supporting procedures: Incident Reporting, Hazard Reporting, Emergency Response, Contractor Safety, Remote Work Safety, Mental Health and Wellbeing, Display Screen Equipment
- Build legal compliance register and assign review owner
- Obtain formal sign-off from named approver for each document
- Publish to all staff with acknowledgment records

4

Phase 4 — Control Implementation

- Complete all outstanding workstation assessments and action follow-ups
- Issue contractor safety briefings and obtain acknowledgments
- Deliver OH&S awareness training to all staff — record completions
- Deliver manager training on mental health and incident reporting obligations
- Implement incident and near-miss reporting system
- For hardware companies: implement lab safety controls, PPE provision, ventilation checks, battery handling procedures
- Run emergency evacuation drill — document it

5

Phase 5 — Internal Audit

- Conduct internal audit — auditor must be independent of the activities being audited
- Produce internal audit report with findings rated by severity
- Assign corrective actions with owners and due dates
- Close corrective actions and document evidence of closure

6

Phase 6 — Management Review and Certification

- Conduct management review covering: OHSMS performance, audit results, incident trends, legal compliance status, resource requirements, objectives for coming period
- Document all outputs — decisions, actions, resource commitments, sign-off
- Compile full evidence file — every required document, current and retrievable
- Stage 1 audit — document review by certification body
- Remediate any Stage 1 findings
- Stage 2 audit — site visits, worker interviews, evidence testing
- Certificate issued — surveillance audits follow annually, recertification every three years

Manual vs. Automated: What Good Looks Like

ISO 45001 Requires	Manual Reality	With Governance Automation
Workstation assessments for all workers	Spreadsheet, incomplete, home workers missed	Structured workflow with completion tracking and follow-up actions
Incident and near-miss log	Email reports, inconsistent, no trend analysis	Structured log with status tracking and management reporting
Legal compliance register	Created once, never updated when legislation changes	Version-controlled with review reminders and named owner
Management review with documented outputs	Meeting happened, notes in HR's inbox	Structured review with timestamped sign-off and action log
Contractor safety acknowledgments	Verbal briefing, no record	Documented briefing with acknowledgment trail
Certification audit evidence	Week-long pre-audit scramble	Retrievable in minutes, maintained continuously

Manual Compliance

Companies running OH&S compliance manually typically take **6–12 months to certify** and face recurring audit risk at every surveillance year.

With Governance Automation

Companies using governance automation **certify in 6–10 weeks** and enter every subsequent audit with their evidence file already current.

fortifai

Multi-Framework Advantage

If your company is already pursuing or maintaining ISO 27001, SOC 2, NIS2, or ESG reporting frameworks, ISO 45001 is materially cheaper and faster as an additional certification — not a separate project. The three governance workflows are identical across frameworks:

Sign-offs

The same routing, timestamping, and version control infrastructure handles OH&S policy approvals, security policy approvals, and ESG disclosures.

Disclosures

Incident reports, management review outputs, and regulatory submissions use the same document management system regardless of which framework they belong to.

Information requests

Contractor questionnaires, audit evidence requests, and regulatory responses use the same workflow infrastructure.

For companies building a multi-framework compliance programme, each additional certification after the first costs a fraction of the original — because the governance infrastructure is already in place.

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing companies. The platform automates the three workflows ISO 45001 requires: sign-off routing and tracking for top management approvals, disclosure document management for incident reports and management review outputs, and information request handling for contractor assessments and audit evidence — pre-configured for ISO 45001 with templates ready on day one.

The same platform supports ISO 27001, SOC 2, NIS2, GDPR, and ESG frameworks simultaneously. For tech and hardware companies managing multiple certifications, the governance workflows overlap significantly and the evidence base is shared.

Used by compliance teams at **Cognite, Aker BioMarine, and Telenor.**

Book a 30-minute walkthrough at fortifai.co

fortifai