Provided by SDPPA.com (Security, Data Protection & Privacy Advisory)

Practical compliance guidance for Industrial Control Systems (ICS), OT environments, and critical infrastructure operators.

ICS Compliance Implementation Checklist for OT Environments

This checklist is designed for **operators, engineers, and managers** responsible for securing and maintaining compliant ICS environments.
It emphasizes **safety-first security**, operational realism, and alignment with recognized frameworks such as **NIST SP 800-82, ISA/IEC 62443, and NERC CIP**.
This checklist supports compliance readiness and gap identification.
It does not replace formal risk assessments, safety analyses, or regulatory audits.

---

1. Assessment

- ☐ Identify all ICS assets (hardware, software, network, sensors, **Safety Instrumented Systems**)
- ☐ Classify systems by criticality (High, Medium, Low)
- ☐ Map data flows and interconnections (OT ↔ IT boundaries)
- ☐ Identify threats (physical, network, insider) **and perform Cyber-PHA (Process Hazard Analysis)**
- ☐ **Assess Supply Chain Risk** (Hardware/Software Bill of Materials, vendor dependencies)
- ☐ Check current regulatory requirements (NERC CIP, NIST 800-82, ISA/IEC 62443)

---

2. Documentation

- ☐ Maintain an **asset inventory** with versioning and patch levels
- ☐ Establish **“Known Good” Configuration Baselines** for PLCs, RTUs, and protection relays
- ☐ Maintain a **network diagram** showing ICS segmentation and trust zones
- ☐ Maintain an **access control list** (users, roles, privileges)
- ☐ Create **SOPs** for ICS operations, **Disaster Recovery**, and incident response
- ☐ Document **vendor / third-party access policies**
- ☐ Maintain **change management logs** for all ICS components

---

3. Technical Controls

- ☐ Implement **network segmentation** (IT/OT separation, DMZs, data diodes where appropriate)
- ☐ Ensure **firewalls and IDS/IPS** are operational and monitored
- ☐ Implement **physical security controls** (cabinet locks, port blockers, restricted access)
- ☐ Enforce **strong authentication** (MFA where feasible; physical tokens preferred)
- ☐ Apply **vendor-validated patch management** (**never auto-update live ICS systems**)
- ☐ Conduct **passive vulnerability monitoring** (avoid active scanning on production systems)
- ☐ Implement **application whitelisting** on HMIs and engineering workstations
- ☐ Ensure **backups** are taken regularly, stored **offline (air-gapped)**, and tested
- ☐ Implement **endpoint monitoring** for critical ICS components

---

4. Operational Controls & Procedures

- ☐ Verify **vendor remote access** uses secure jump hosts with session logging
- ☐ Establish a **formal incident response plan** tailored specifically to ICS/OT
- ☐ Conduct **regular drills**, including **manual override and switch-to-manual tests**
- ☐ Restrict **portable media usage** and enforce malware scanning / sanitization kiosks
- ☐ Monitor **audit logs** and review them on a defined schedule

---

5. Training & Awareness

- ☐ Conduct **ICS cybersecurity training** emphasizing **safety–security convergence**
- ☐ Ensure **management understands ICS compliance and risk exposure**
- ☐ Provide **vendor and contractor training** on access and security requirements
- ☐ Conduct **OT-specific social engineering tests** (e.g., USB drop scenarios)

---

6. Review & Audit

- ☐ Schedule **internal compliance audits** at least quarterly
- ☐ Document **audit findings and corrective actions**
- ☐ Review **policies and procedures** annually or after significant system changes
- ☐ Track **regulatory and framework updates** and revise the compliance program accordingly

About SDPPA.com

SDPPA specializes in **ICS / OT security, compliance readiness, and documentation frameworks** for small to mid-sized utilities, manufacturers, and critical infrastructure operators.

Looking for more than a checklist?

- **ICS Compliance Kit (Paid)**
  Templates, examples, framework mappings, and implementation guidance that expand this checklist into a complete, auditable compliance package. Asset inventories, SOPs, incident response plans, and change-management logs tailored for OT environments.

- **Async Review (Paid)**
  Receive instructions for passive, non-intrusive data collection on your network, perform the data collection fully and upload the data to our secure portal. Pay the fee and receive your full security review within 7-10 business days. NDA compliance available for an additional fee.

- **Short Courses (Paid)**
  Step-by-step implementation guides aligned with NIST 800-82, IEC 62443, and NERC CIP.

Reproducibility

This checklist is provided free of charge to support awareness and readiness.