SHIELDWORKZ

IEC 62443 and NIS2 Compliance Checklist

Unified OT Defense

Comprehensive Implementation Guide for IACS Security

Executive Summary

This checklist provides actionable guidance for organizations implementing both IEC 62443 (industrial cybersecurity) and NIS2 Directive (EU network and information security) requirements. It identifies overlapping controls where single implementations can satisfy both frameworks, as well as framework-specific requirements.

Key Principles:

- IEC 62443 provides technical implementation guidance for IACS
- NIS2 sets mandatory legal requirements for critical and important entities in the EU
- Implementation of IEC 62443 helps demonstrate NIS2 compliance for OT environments
- Both frameworks emphasize defense-in-depth, risk-based approaches, and supply chain security

Framework Overview

IEC 62443 Structure

The IEC 62443 series consists of four main categories:

- General (Part 1): Concepts, models, and terminology
- Policies and Procedures (Part 2): Security program requirements for asset owners (2-1) and service providers (2-4)
- System (Part 3): Risk assessment (3-2), system security requirements and security levels (3-3)
- Component (Part 4): Product development lifecycle (4-1), technical component requirements (4-2)

Security Levels (SL):

- SL 0: No protection required
- SL 1: Protection against accidental or casual violations
- SL 2: Protection against intentional violations using simple means
- SL 3: Protection against intentional violations using sophisticated means
- SL 4: Protection against intentional violations using extensive resources (nation-state level)

NIS2 Structure

NIS2 applies to essential and important entities across 18 sectors. Key requirements include:

- Risk management measures: 10 minimum security measures (Article 21)
- Corporate accountability: Management oversight and approval of security measures
- Incident Reporting: 24-hour early warning, 72-hour detailed report, final report within one month
- Business Continuity Planning and Execution: Backup procedures, crisis management, disaster recovery

Enforcement: Penalties up to €10 million or 2% of annual global turnover (whichever is higher).

Section 1: Overlapping Controls

These controls satisfy requirements in both IEC 62443 and NIS2. Implement once to achieve dual compliance.

1.1 Risk Assessment and security policies

- Conduct comprehensive IACS risk assessment using IEC 62443-3-2 methodology
- Identify assets, zones, and conduits
- Determine target Security Levels (SL-T) for each zone
- Document threats, vulnerabilities, and consequences
- Develop risk treatment plan
- Create and maintain security policies for all systems
- Review and update risk assessments annually or after significant changes

1.2 Access Control and Identity Management

- Implement multi-factor authentication (MFA) for all remote access
- Deploy MFA for privileged accounts (admin, engineering)
- Establish unique user identities - no shared accounts
- Implement role-based access control (RBAC)
- Define and enforce least privilege principles
- Establish user provisioning and de-provisioning procedures
- Implement password policies (complexity, expiration, history)
- Review user access rights quarterly
- Log all authentication attempts and access events

1.3 Network Segmentation and restricted data flow

- Design and implement zone and conduit architecture
- Segment OT from IT networks (air gap or DMZ)
- Deploy firewalls between zones with deny-by-default rules
- Implement industrial DMZ for data exchange
- Deploy IDS/IPS at zone boundaries
- Implement unidirectional security gateways where appropriate
- Document and enforce allowed data flows between zones
- Disable unnecessary protocols and services

Section 1:
Overlapping Controls

1.4 Cryptography and data confidentiality

- Implement encryption for data at rest (sensitive databases, backups)
- Implement encryption for data in transit (TLS 1.2+, VPN)
- Use industry-standard cryptographic algorithms (AES-256, RSA-2048+)
- Establish cryptographic key management procedures
- Implement secure key generation, storage, rotation, and destruction
- Deploy certificate management system (PKI) for device authentication
- Document approved cryptographic methods and key lengths

1.5 Incident detection, response and reporting

- Deploy Security Information and Event Management (SIEM) system
- Implement continuous monitoring and anomaly detection
- Establish 24/7 security operations center (SOC) or managed service
- Define incident classification criteria and severity levels
- Create incident response plan with roles and procedures
- Establish notification workflow for 24-hour early warning
- Create detailed reporting template for 72-hour report
- Define escalation paths to national CSIRT/authority
- Conduct incident response drills at least annually
- Implement centralized logging with minimum 12-month retention

1.6 System integrity and vulnerability management

- Establish vulnerability scanning program (monthly minimum)
- Implement patch management process with defined timelines
- Critical patches: deploy within 30 days after risk assessment
- Test patches in non-production environment before deployment
- Document compensating controls for unpatchable legacy systems
- Implement change control process for all system modifications
- Maintain vulnerability disclosure policy
- Deploy anti-malware protection on applicable systems
- Implement application whitelisting for critical systems

Section 1: Overlapping Controls

1.7 Configuration management and asset inventory

- Maintain comprehensive IACS asset inventory
- Document hardware, software, firmware versions, IP addresses
- Classify assets by criticality and security zone
- Implement automated asset discovery tools
- Define and enforce secure baseline configurations
- Disable unnecessary services, ports, and protocols
- Implement configuration management database (CMDB)
- Update asset inventory quarterly or after major changes

1.8 Backup and business continuity

- Implement 3-2-1 backup strategy (3 copies, 2 media types, 1 offsite)
- Schedule automated backups: critical data daily, configurations weekly
- Encrypt backup media and transmissions
- Test backup restoration quarterly
- Store backups offline or in immutable storage (ransomware protection)
- Develop Business Continuity Plan (BCP) with RTO/RPO objectives
- Create Disaster Recovery Plan (DRP) for IACS restoration
- Conduct annual BCP/DRP exercises and tabletop drills
- Establish crisis management team with defined roles

1.9 Supply chain security

- Conduct security assessments of suppliers and service providers
- Include cybersecurity requirements in procurement contracts
- Require IEC 62443-4-2 component certifications where applicable
- Request Software Bill of Materials (SBOM) from vendors
- Establish vendor risk management program
- Monitor third-party access to IACS environments
- Require suppliers to notify of security incidents
- Conduct annual supplier security reviews

Section 1: Overlapping Controls

1.10 Training and awareness

- Provide annual cybersecurity awareness training for all personnel
- Deliver role-specific training (OT engineers, IT staff, management)
- Train management on NIS2 obligations and oversight responsibilities
- Conduct phishing simulation campaigns
- Provide secure coding training for developers
- Establish onboarding security training for new hires
- Document and track training completion

Section 2: IEC 62443-Specific Requirements

These controls are specific to IEC 62443 and provide additional technical depth for IACS security.

2.1 Zones and Conduits Architecture (IEC 62443-3-2)

- Define security zones based on functional requirements and security needs
- Typical zones: Enterprise, Industrial DMZ, Control (L3), Supervisory (L2), Process (L1/0)
- Document conduits (communication pathways) between zones
- Assign target security level (SL-T) to each zone based on risk
- Implement security controls at conduit boundaries
- Create network diagrams showing zones, conduits, and security levels

2.2 Security Levels Achievement (IEC 62443-3-3)

- Assess current security level capability (SL-C) for each zone
- Identify gaps between SL-C and SL-T
- Implement all 7 Foundational Requirements (FR) controls
  - FR 1: Identification and Authentication Control
  - FR 2: Use Control (authorization)
  - FR 3: System Integrity
  - FR 4: Data Confidentiality
  - FR 5: Restricted Data Flow
  - FR 6: Timely Response to Events
  - FR 7: Resource Availability
- Document compensating controls for components that cannot meet SL-T

Section 2:
IEC 62443-Specific Requirements

2.3 Component Security (IEC 62443-4-2)

- Procure IEC 62443-4-2 certified components when available
- Verify component security level matches or exceeds zone SL-T
- Request component security assurance documentation
- Implement secure by default configurations
- Disable or remove default credentials on all devices

2.4 Secure Development Lifecycle (IEC 62443-4-1)

For organizations developing IACS products or custom applications:

- Implement security requirements specification process
- Conduct threat modeling during design phase
- Perform secure code reviews and static analysis
- Execute security testing (penetration testing, fuzzing)
- Establish vulnerability management and disclosure process
- Maintain security updates and patch release capability

2.5 Physical security

- Implement physical access controls for control rooms and equipment areas
- Deploy badge readers, biometric systems, or locks
- Install video surveillance in critical areas
- Secure network equipment in locked cabinets/rooms
- Establish visitor escort procedures
- Log and review physical access events

2.6 Remote access security

- Implement jump servers/bastion hosts for remote access
- Require VPN with strong encryption (IPsec, TLS 1.3+)
- Deploy MFA for all remote connections
- Use session recording for remote privileged access
- Implement time-based access restrictions
- Terminate idle remote sessions automatically
- Review remote access logs regularly

Section 2:
IEC 62443-Specific Requirements

2.7 Wireless security

- Use WPA3-Enterprise for industrial wireless networks
- Implement 802.1X authentication for wireless clients
- Segment wireless networks into separate VLANs/zones
- Conduct wireless site surveys and rogue AP detection
- Disable wireless capabilities on unused devices

2.8 Security monitoring

- Deploy network monitoring tools (passive TAPs, SPAN ports)
- Implement industrial protocol analysis (Modbus, DNP3, OPC UA)
- Deploy anomaly detection for OT traffic patterns
- Monitor for unauthorized devices and connections
- Generate alerts for security events and policy violations
- Correlate OT events with IT security information

Section 3:
NIS2-Specific Requirements

These requirements are unique to NIS2 and may not have direct IEC 62443 equivalents.

3.1 Management Accountability (Article 20)

- Designate management body members responsible for cybersecurity oversight
- Obtain formal approval of cybersecurity risk management measures from management
- Provide cybersecurity training to management team
- Include cybersecurity in board/executive meeting agendas (quarterly minimum)
- Document management oversight activities and decisions
- Ensure management understands personal liability for non-compliance

Section 3:
NIS2-Specific Requirements

3.2 Incident Notification Timeline (Article 23)

Early Warning (24 hours):

- Establish 24-hour incident detection and initial assessment capability
- Create early warning notification template
- Identify national CSIRT or competent authority contact points

Incident Notification (72 hours):

- Prepare detailed incident report template
- Establish workflow for collecting incident data within 72 hours

Final Report (1 month):

- Prepare detailed incident report template
- Establish workflow for collecting incident data within 72 hours

3.3 Registrations and Reporting

- Determine if organization is Essential or Important entity
- Register with national competent authority
- Identify designated single point of contact (SPOC)
- Establish process for responding to supervisory requests
- Maintain documentation for regulatory inspections

3.4 Coordinated Vulnerability Disclosure

- Establish public vulnerability disclosure policy
- Create secure channel for vulnerability reports
- Define response timelines for different severity levels
- Coordinate with national CSIRT for vulnerability handling
- Consider bug bounty program for critical systems

Section 3:
NIS2-Specific Requirements

3.5 Cross-Border Information Sharing

- Participate in sectoral information sharing groups (ISACs)
- Share threat intelligence with peer organizations
- Contribute to EU-wide threat landscape understanding
- Establish data sharing agreements with confidentiality controls

3.6 DNS and Domain Security

- Implement DNSSEC for organizational domains
- Deploy DNS filtering to block malicious domains
- Monitor domain registration for typosquatting/brand abuse
- Implement SPF, DKIM, and DMARC for email domains

3.7 Third-Party Service Provider Management

- Identify all third-party providers with access to systems
- Require NIS2 compliance attestation from service providers
- Include right-to-audit clauses in contracts
- Establish SLAs with security incident notification requirements
- Monitor service provider security posture continuously

Section 4:
Governance and Documentation

Essential documentation and governance structures required for both frameworks.

4.1 Security Program Documentation

- Create IACS Security Program charter
- Develop Security Program Plan addressing all IEC 62443-2-1 elements
- Document security policies (access, network, change, incident, backup, physical)
- Maintain procedures and work instructions
- Review and update documentation annually

Section 4:
Governance and Documentation

4.2 NIS2 Compliance Documentation

- Prepare NIS2 compliance statement documenting Article 21 measures
- Create evidence portfolio for regulatory audits
- Document management approvals and oversight
- Maintain incident notification records
- Keep audit logs and security reports per retention requirements

4.3 Roles and Responsibilities

- Define cybersecurity organizational structure
- Appoint CISO or equivalent
- Establish OT security team or roles
- Define incident response team members
- Document security champion roles
- Create RACI matrix for security activities

4.4 Performance Measurement

- Define Key Performance Indicators (KPIs)
- Track metrics: MTTD/MTTR, patch rates, vulnerability remediation
- Generate monthly security dashboards
- Conduct quarterly program reviews

4.5 Continuous Improvement

- Conduct annual internal audits
- Perform gap assessments against both frameworks
- Engage third-party auditors
- Track and close audit findings
- Review lessons learned from incidents
- Update program based on evolving threats

Section 5:
Testing and Validation

Regular testing ensures controls are effective and comply with both frameworks.

5.1 Security Testing Program

- Conduct annual penetration testing of IACS environments
- Perform red team exercises
- Execute vulnerability assessments quarterly
- Test security controls after significant changes
- Validate network segmentation and firewall rules
- Review and remediate findings based on risk

5.2 Incident Response Exercises

- Conduct tabletop exercises (semi-annually)
- Simulate cyber incidents specific to your sector
- Test incident notification procedures and timelines
- Validate communication channels with authorities
- Exercise BCP and DRP
- Document lessons learned

5.3 Backup and Recovery Testing

- Test backup restoration procedures quarterly
- Validate recovery within RTO objectives
- Test restoration to alternate sites
- Verify backup integrity and completeness
- Document test results

Section 6: Implementation Roadmap

Recommended phased approach for implementing dual compliance.

Phase 1: Foundation (Months 1-3)

- Establish governance structure and assign responsibilities
- Conduct comprehensive asset inventory
- Perform initial gap assessment
- Complete IEC 62443-3-2 risk assessment
- Design zone and conduit architecture
- Document current security policies
- Register with national competent authority

Phase 2: Core Controls (Months 4-9)

- Implement network segmentation and zone boundaries
- Deploy firewalls and IDS/IPS
- Roll out MFA for remote and privileged access
- Implement centralized logging and SIEM
- Establish vulnerability management program
- Deploy backup solution with offsite storage
- Create incident response plan

Phase 3: Advanced Controls (Months 10-15)

- Implement encryption for data at rest and in transit
- Deploy application whitelisting
- Establish 24/7 SOC or managed service
- Implement anomaly detection
- Develop BCP and DRP
- Execute supplier security assessments
- Conduct first penetration test and tabletop exercise

Section 6: Implementation Roadmap

Phase 4: Optimization (Months 16-18)

- Complete training program rollout
- Achieve target security levels for all zones
- Finalize all documentation
- Conduct third-party audit
- Establish continuous monitoring processes
- Present compliance status to management and authorities

Compliance Verification

Use this section to track overall compliance status:

Framework/Area	Completion Status
Overlapping Controls (Section 1)	___ / 10 completed
IEC 62443-Specific (Section 2)	___ / 8 completed
NIS2-Specific (Section 3)	___ / 7 completed
Governance and Documentation (Section 4)	___ / 5 completed
Testing and Validation (Section 5)	___ / 3 completed

Document Information

Version: 1.0 | Date: February 2026

Framework References:

- IEC 62443 series (Parts 2-1, 3-2, 3-3, 4-1, 4-2)
- EU NIS2 Directive (2022/2555)

Notes:

- This checklist is based on publicly available standards as of February 2026
- Implementation requirements may vary by organization size and sector
- Consult legal and compliance experts for jurisdiction-specific requirements
- Regular updates recommended as standards evolve

SHIELDWORKZ

CONTACT US

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

Tenth floor,
FAB BUSINESS CENTER

Abu Dhabi,
United Arab Emirates

+971 56 660 5200

middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com