Comprehensive AI Regulatory Compliance Requirements

Research compiled: July 30, 2025

This document provides detailed compliance requirements for AI systems across major regulatory frameworks, including specific article references, evidence requirements, compliance checklists, and official guidance links.

Table of Contents

1. GDPR - Data Protection Requirements
2. NIS2 Directive - Cybersecurity Requirements
3. DORA Regulation - Digital Operational Resilience
4. EU AI Act - AI-Specific Requirements
5. NIST AI Risk Management Framework
6. OWASP AI Security Principles
7. ISO Standards for AI Governance

---

1. GDPR - Data Protection Requirements

1.1 Article 35 - Data Protection Impact Assessment (DPIA)

Official Source: EUR-Lex GDPR Article 35 (https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng)

Key Requirements:

- **Mandatory DPIA** for processing likely to result in high risk to rights and freedoms
- **Prior to processing** - must be conducted before data processing begins
- **Consultation with DPO** where designated

Specific Triggers for AI Systems:

- **Article 35(3)(a):** Systematic and extensive evaluation based on automated processing (including profiling)
- **Article 35(3)(b):** Large scale processing of special categories of data
- **Article 35(3)(c):** Systematic monitoring of publicly accessible areas

Evidence Requirements:

- **Article 35(7)** mandates DPIA must contain:
- Systematic description of processing operations and purposes
- Assessment of necessity and proportionality
- Assessment of risks to rights and freedoms
- Measures to address risks, including safeguards and security measures

Compliance Checklist:

- [ ] Conduct DPIA screening assessment for all AI systems

- [ ] Document systematic description of AI processing operations
- [ ] Assess necessity and proportionality of data processing for AI purposes
- [ ] Identify and evaluate risks to individual rights and freedoms
- [ ] Design and implement risk mitigation measures
- [ ] Consult with DPO throughout DPIA process
- [ ] Review and update DPIA when processing changes (Article 35(11))
- [ ] Maintain DPIA documentation for supervisory authority inspection

Official Guidance:

- **EDPB DPIA Guidelines:** PDF Link (https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=611236&format=pdf)

1.2 Article 25 - Data Protection by Design and by Default

Official Source: EUR-Lex GDPR Article 25 (https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng)

Key Requirements:

- **Data Protection by Design:** Technical and organizational measures from determination of means
- **Data Protection by Default:** Only necessary data processed by default
- **State of the art consideration** in measure selection

Evidence Requirements:

- Documentation of technical and organizational measures implemented
- Evidence of data minimization in AI system design
- Demonstration of privacy-preserving techniques (pseudonymization, encryption)
- Records of design decisions considering data protection principles

Compliance Checklist:

- [ ] Implement privacy-by-design principles in AI system architecture
- [ ] Configure systems to process only necessary data by default
- [ ] Apply pseudonymization and encryption where appropriate
- [ ] Document state-of-the-art considerations in design decisions
- [ ] Implement access controls limiting data accessibility
- [ ] Regular review of technical and organizational measures
- [ ] Consider certification mechanisms (Article 25(3))

Official Guidance:

- **EDPB Guidelines 4/2019:** Data Protection by Design and by Default (https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)

1.3 Articles 33-34 - Breach Notification

Official Source: EUR-Lex GDPR Articles 33-34 (https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng)

Article 33 - Notification to Supervisory Authority:

- **72-hour notification** to supervisory authority
- **Without undue delay** after becoming aware
- **Exception:** If unlikely to result in risk to rights and freedoms

Article 34 - Communication to Data Subjects:

- **High risk threshold** for data subject notification
- **Without undue delay** direct communication required
- **Clear and plain language** requirement

Evidence Requirements:

- **Article 33(5):** Documentation of all personal data breaches including:
- Facts relating to the breach
- Effects of the breach
- Remedial action taken

Compliance Checklist:

- [ ] Establish breach detection mechanisms for AI systems
- [ ] Implement 72-hour notification procedures to supervisory authority
- [ ] Create breach assessment framework for AI-specific incidents
- [ ] Document all breach incidents comprehensively
- [ ] Prepare data subject notification templates and procedures
- [ ] Train AI operations teams on breach identification and response
- [ ] Maintain breach register with all required information
- [ ] Regular testing of breach response procedures

Official Guidance:

- **EDPB Guidelines 9/2022:** Personal Data Breach Notification (https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf)

---

2. NIS2 Directive - Cybersecurity Requirements

2.1 Article 21 - Cybersecurity Risk Management Measures

Official Source: EUR-Lex NIS2 Directive (https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng)

Key Requirements:

Essential and important entities must implement technical, operational and organizational measures based on all-hazards approach.

Minimum Measures (Article 21(2)):

- **(a)** Policies on risk analysis and information system security
- **(b)** Incident handling procedures
- **(c)** Business continuity, backup management, disaster recovery
- **(d)** Supply chain security (including direct suppliers and service providers)
- **(e)** Security in acquisition, development and maintenance
- **(f)** Procedures to assess effectiveness of risk management measures
- **(g)** Basic cyber hygiene practices and cybersecurity training
- **(h)** Cryptography and encryption policies
- **(i)** Human resources security, access control policies, asset management
- **(j)** Multi-factor authentication and secured communications

Evidence Requirements:

- Risk analysis documentation
- Information system security policies
- Supply chain security assessments
- Effectiveness measurement procedures
- Training records and cyber hygiene evidence
- Cryptographic implementation documentation

Compliance Checklist:

- [ ] Develop comprehensive cybersecurity risk management framework
- [ ] Implement all-hazards approach covering physical and cyber threats
- [ ] Create and maintain risk analysis and security policies
- [ ] Establish incident handling procedures and capabilities
- [ ] Implement business continuity and disaster recovery plans
- [ ] Conduct supply chain security assessments for AI vendors
- [ ] Secure acquisition, development and maintenance processes
- [ ] Establish effectiveness assessment procedures with regular reviews
- [ ] Provide cybersecurity training and implement cyber hygiene practices
- [ ] Deploy encryption and cryptographic controls
- [ ] Implement access controls, asset management, and HR security
- [ ] Deploy multi-factor authentication and secure communications

Official Guidance:

- **ENISA Technical Implementation Guidance:** PDF Link (https://www.enisa.europa.eu/sites/default/files/2025-06/EN-ISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf)

2.2 Article 23 - Incident Reporting

Official Source: EUR-Lex NIS2 Article 23 (https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng)

Significant Incident Definition (Article 23(3)):

- Caused or capable of causing severe operational disruption or financial loss
- Affected or capable of affecting others by causing considerable material/non-material damage

Reporting Timeline (Article 23(4)):

- **24 hours:** Early warning notification
- **72 hours:** Incident notification with initial assessment
- **1 month:** Final report after incident notification

Evidence Requirements:

- Incident detection and classification procedures
- Early warning and incident notification templates
- Impact assessment methodologies
- Final report documentation standards

Compliance Checklist:

- [ ] Establish significant incident identification criteria
- [ ] Implement 24-hour early warning notification procedures
- [ ] Create 72-hour incident notification capabilities

- [ ] Develop comprehensive final reporting procedures
- [ ] Train incident response teams on NIS2 requirements
- [ ] Establish communication channels with national CSIRT
- [ ] Document all incident handling procedures
- [ ] Regular testing of incident reporting processes

2.3 Supply Chain Security (Article 21(2)(d))

Key Requirements:

Entities must consider vulnerabilities of direct suppliers and service providers, including:
- Overall quality of products and cybersecurity practices
- Secure development procedures of suppliers
- Results of Union-level coordinated risk assessments

Evidence Requirements:

- Supplier cybersecurity assessment documentation
- Supply chain risk assessment procedures
- Contractual security requirements for suppliers
- Monitoring and review processes for supplier compliance

Compliance Checklist:

- [ ] Conduct cybersecurity assessments of all AI suppliers and vendors
- [ ] Implement supplier qualification and onboarding security procedures
- [ ] Establish contractual cybersecurity requirements for suppliers
- [ ] Regular monitoring and review of supplier security posture
- [ ] Document supply chain risk assessment methodology
- [ ] Maintain supplier cybersecurity incident response coordination

---

3. DORA Regulation - Digital Operational Resilience

3.1 Articles 6-7 - ICT Risk Management Framework

Official Source: EUR-Lex DORA Regulation (https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng)

Article 6 - ICT Risk Management Framework:

Financial entities must maintain a comprehensive, well-documented ICT risk management framework including:
- Strategies, policies, procedures, ICT protocols and tools
- Complete information on ICT risk provided to authorities upon request
- Independence of ICT risk management function (except micro/small/medium enterprises)

Article 7 - ICT Systems, Protocols and Tools:

Systems must be:
- Appropriate to magnitude and complexity
- Reliable with sufficient capacity
- Resilient against unauthorized access
- Configured with security-by-design principles
- Tested before deployment and after changes

Evidence Requirements:

- **Article 6(5):** Framework documentation and annual review reports
- **Article 6(8):** Digital operational resilience strategy document
- **Article 7(3):** Inventory of ICT systems, protocols and tools
- **Article 7(4):** Contractual arrangements with third-party providers

Compliance Checklist:

- [ ] Establish comprehensive ICT risk management framework
- [ ] Assign dedicated ICT risk management control function
- [ ] Document digital operational resilience strategy
- [ ] Maintain complete inventory of ICT systems and tools
- [ ] Implement security-by-design and security-by-default principles
- [ ] Establish testing procedures for all system changes
- [ ] Create contractual security requirements for ICT service providers
- [ ] Implement continuous monitoring and anomaly detection
- [ ] Regular framework review and updates
- [ ] Ensure compliance with cryptographic standards

3.2 Articles 28-30 - Third Party Risk Management

Official Source: EUR-Lex DORA Articles 28-30 (https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng)

Article 28 - General Principles:

- Full responsibility retained despite outsourcing
- Proportionality principle application
- Formal ICT third-party risk strategy
- Central register of ICT service contracts
- Due diligence before contracting
- Right to audit and inspect providers

Article 29 - ICT Concentration Risk Assessment:

- Identify concentration risk from limited providers
- Assess substitutability and systemic impact
- Factor concentration into overall ICT risk profile

Article 30 - Key Contractual Provisions:

- Escrow and data portability clauses
- Clear service level agreements
- Notification obligations for incidents
- Access rights for audits and inspections
- Exit planning clauses

Evidence Requirements:

- ICT third-party risk strategy documentation
- Central register of all ICT service contracts
- Due diligence assessment records
- Concentration risk assessment documentation
- Contractual arrangements with required provisions

Compliance Checklist:

- [ ] Develop formal ICT third-party risk strategy
- [ ] Maintain central register of all ICT service contracts
- [ ] Conduct comprehensive due diligence before contracting
- [ ] Perform concentration risk assessments
- [ ] Include all required contractual provisions
- [ ] Establish audit and inspection rights with providers
- [ ] Create comprehensive exit strategies
- [ ] Regular review and updating of third-party arrangements

3.3 Articles 25-27 - Digital Operational Resilience Testing

Official Source: EUR-Lex DORA Articles 25-27 (https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng)

Article 25 - Testing Requirements:

Must include: vulnerability assessments, network security assessments, penetration testing, scenario-based tests, compatibility testing, performance testing, end-to-end testing.

Article 26 - Threat-Led Penetration Testing (TLPT):

- **Minimum every 3 years** for advanced testing
- Based on comprehensive threat intelligence
- Simulate realistic threat scenarios
- Production-equivalent environment testing

Article 27 - Tester Requirements:

- Certified by recognized accreditation body
- Proven technical capabilities
- Professional indemnity insurance
- Demonstrable reputation and confidentiality safeguards

Evidence Requirements:

- Digital operational resilience testing programme documentation
- Testing results and remediation records
- TLPT reports and findings
- Tester certifications and qualifications

Compliance Checklist:

- [ ] Establish comprehensive testing programme
- [ ] Conduct vulnerability assessments before deployments
- [ ] Perform regular penetration testing
- [ ] Implement threat-led penetration testing every 3 years
- [ ] Ensure tester qualifications and certifications
- [ ] Document all testing results and remediation actions
- [ ] Regular review and update of testing procedures

Official Guidance:

- **EBA DORA Implementation Hub:** Link (https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act)

- **FS-ISAC DORA Implementation Guide:** PDF (https://www.fsisac.com/hubfs/Knowledge/DORA/FS-ISAC_DORA-ImplementationGuidance.pdf)

---

4. EU AI Act - AI-Specific Requirements

4.1 Articles 9-15 - High-Risk AI Systems Requirements

Official Source: EUR-Lex AI Act (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689)

Article 9 - Risk Management System:

Continuous, iterative risk management system throughout entire lifecycle including:
- Identification and analysis of known and foreseeable risks
- Risk estimation and evaluation
- Adoption of targeted risk management measures
- Testing against predefined metrics

Article 10 - Data and Data Governance:

- Training, validation and test datasets must be relevant, representative, error-free and complete
- Implementation of data governance measures including bias detection and mitigation
- Maintenance of compliance records

Article 11 - Technical Documentation:

Detailed technical documentation covering:
- System architecture and development process
- Intended purpose and design choices
- Results of testing and validation
- Instructions for use and maintenance

Article 12 - Record-keeping:

Automatic recording of events (logs) sufficient to:
- Reconstruct system operation
- Demonstrate compliance
- Include inputs, outputs, decisions, performance metrics, anomalies

Article 13 - Transparency and Information Provision:

Information to deployers must include:
- System capabilities and limitations
- Performance, accuracy, robustness and security information
- Foreseeable risks and residual risk levels
- Required human oversight measures

Article 14 - Human Oversight:

Systems must allow effective human oversight including:
- Understanding of system capacities and limitations
- Anomaly detection capabilities
- Correct interpretation of outputs
- Override or disregard system recommendations

Article 15 - Accuracy, Robustness and Cybersecurity:

- Appropriate levels of accuracy and robustness
- Resilience against tampering and attacks
- Adversarial-robust training and anomaly detection
- Access controls and data integrity checks

Evidence Requirements:

- Risk management system documentation
- Data governance procedures and bias mitigation records
- Comprehensive technical documentation
- System logs and operational records
- Human oversight procedures and training records
- Security testing and validation results

Compliance Checklist:

- [ ] Establish comprehensive AI risk management system
- [ ] Implement data governance with bias detection and mitigation
- [ ] Create and maintain detailed technical documentation
- [ ] Implement automatic logging and record-keeping systems
- [ ] Provide comprehensive information to deployers
- [ ] Design effective human oversight mechanisms
- [ ] Ensure appropriate accuracy, robustness and cybersecurity measures
- [ ] Regular testing and validation of AI systems
- [ ] Continuous monitoring and risk assessment updates

4.2 Articles 16-17 - Quality Management Systems

Article 16 - Provider Obligations:

Providers must ensure compliance before market placement including:
- Risk management system implementation
- Technical documentation and logging
- Human oversight measures
- Data governance procedures
- Accuracy, robustness and cybersecurity
- Information provision to users
- Serious incident reporting
- Post-market monitoring

Article 17 - Quality Management System Requirements:

Systematic and orderly QMS including:
- Strategy for regulatory compliance
- Design control and verification procedures
- Examination, test and validation procedures
- Technical specifications and standards
- Data management systems and procedures
- Risk management system integration
- Post-market monitoring system
- Incident reporting procedures
- Resource management and accountability framework

Evidence Requirements:

- Quality Management System documentation
- Regulatory compliance strategy
- Design control and verification procedures
- Post-market monitoring plans and results
- Incident reporting procedures and records

Compliance Checklist:

- [ ] Establish comprehensive Quality Management System
- [ ] Document regulatory compliance strategy
- [ ] Implement design control and verification procedures
- [ ] Create examination, test and validation procedures
- [ ] Establish data management systems
- [ ] Integrate risk management system
- [ ] Implement post-market monitoring system
- [ ] Create incident reporting procedures
- [ ] Establish resource management measures
- [ ] Define accountability framework

4.3 Articles 61-68 - Governance Framework

Article 64 - European AI Office:

Coordination of AI Act implementation, supervision of general-purpose AI models, support to national authorities.

Article 65-66 - European AI Board:

Representative body for coordination and guidance on AI Act implementation.

Article 67 - Advisory Forum:

Multi-stakeholder feedback mechanism including industry, civil society, academia.

Article 68 - Scientific Panel:

Independent experts providing scientific and technical advice on AI developments.

Compliance Checklist:

- [ ] Monitor guidance from European AI Office
- [ ] Follow European AI Board recommendations
- [ ] Participate in Advisory Forum consultations where relevant
- [ ] Stay informed of Scientific Panel recommendations
- [ ] Implement governance updates as required

Official Guidance:

- **European Commission AI Act Guidelines:** Implementation Documents (https://artificialintelligenceact.eu/implementation-documents/)
- **Guidelines on AI System Definition:** Link (https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application)

---

5. NIST AI Risk Management Framework

5.1 Framework Overview

Official Source: NIST AI RMF 1.0 (https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf)

The NIST AI RMF provides a structured approach to AI risk management through four core functions: Govern, Map, Measure, and Manage.

5.2 GOVERN Function

Purpose:

Establish organization-wide culture, structure, and processes for AI risk identification, documentation, and oversight.

Key Outcomes:

- **GOVERN-1.1:** Legal and regulatory requirements affecting AI design, development, and deployment are understood and managed
- **GOVERN-1.2:** Human considerations are factored into AI system design and deployment decisions
- **GOVERN-1.3:** AI system business value is articulated and integrated into organizational decision-making
- **GOVERN-2.1:** Roles and responsibilities are clearly defined for AI system development and deployment
- **GOVERN-2.2:** Accountability structures are in place for AI decisions and outcomes
- **GOVERN-3.1:** Workforce diversity, equity, inclusion and accessibility processes are prioritized
- **GOVERN-4.1:** Organizational culture emphasizes continuous risk communication
- **GOVERN-5.1:** Processes are in place for stakeholder feedback on AI systems
- **GOVERN-6.1:** Third-party AI resources are managed according to organizational risk tolerances

Evidence Requirements:

- AI governance policies and procedures
- Roles and responsibilities documentation
- Stakeholder engagement records
- Third-party risk management documentation
- Training records for AI teams

Compliance Checklist:

- [ ] Establish AI governance program with clear policies
- [ ] Define roles and responsibilities for AI systems
- [ ] Create accountability structures for AI decisions
- [ ] Implement diversity, equity, inclusion processes
- [ ] Establish continuous risk communication culture
- [ ] Create stakeholder feedback mechanisms
- [ ] Manage third-party AI resources according to risk tolerance

5.3 MAP Function

Purpose:

Frame context for AI system design, development, deployment, and use to identify assumptions, interdependencies, and potential impacts.

Key Outcomes:

- **MAP-1.1:** Intended purposes, contexts of use, and risks are understood and documented
- **MAP-1.2:** Interdependencies and external factors are characterized
- **MAP-1.3:** AI system requirements are documented and managed
- **MAP-2.1:** Categorization of AI systems and their components is performed
- **MAP-3.1:** System requirements are captured and evaluated for consistency
- **MAP-3.2:** Organizational risk tolerance is articulated and integrated
- **MAP-4.1:** Appropriate mapping to legal and regulatory requirements
- **MAP-5.1:** Impacts to individuals, communities, and society are characterized

Evidence Requirements:

- System purpose and context documentation
- Risk assessment documentation
- Requirements specifications
- Impact assessments for individuals and society
- Legal and regulatory mapping documentation

Compliance Checklist:

- [ ] Document intended purposes and contexts of use
- [ ] Characterize interdependencies and external factors
- [ ] Document and manage AI system requirements
- [ ] Perform systematic categorization of AI systems
- [ ] Evaluate requirements for consistency
- [ ] Articulate and integrate organizational risk tolerance
- [ ] Map to applicable legal and regulatory requirements
- [ ] Characterize impacts to individuals and society

5.4 MEASURE Function

Purpose:

Use quantitative, qualitative, or mixed methods to assess, benchmark, and monitor AI risks and trustworthiness.

Key Outcomes:

- **MEASURE-1.1:** Appropriate methods and metrics for measuring AI risks are identified and documented
- **MEASURE-2.1:** Test datasets are representative of deployment environment
- **MEASURE-2.2:** Evaluation methods are validated and documented
- **MEASURE-2.3:** AI system performance is systematically tracked
- **MEASURE-3.1:** Mechanisms for tracking identified AI risks are implemented
- **MEASURE-3.2:** Measurement results are documented and shared
- **MEASURE-4.1:** AI model and system performance metrics are validated

Evidence Requirements:

- Measurement methodology documentation
- Test dataset validation records
- Performance monitoring results
- Risk tracking mechanisms and results

- Validation evidence for measurement methods

Compliance Checklist:

- [ ] Identify and document appropriate AI risk measurement methods
- [ ] Ensure test datasets are representative of deployment environment
- [ ] Validate and document evaluation methods
- [ ] Systematically track AI system performance
- [ ] Implement mechanisms for tracking identified risks
- [ ] Document and share measurement results
- [ ] Validate AI model and system performance metrics

5.5 MANAGE Function

Purpose:

Prioritize, plan, and execute actions to treat and mitigate AI risks based on insights from Map and Measure functions.

Key Outcomes:

- **MANAGE-1.1:** Responses to AI risks are prioritized and planned
- **MANAGE-1.2:** Treatment of documented AI risks is implemented
- **MANAGE-2.1:** Strategies to maximize AI benefits and minimize harms are developed
- **MANAGE-2.2:** AI system modifications are implemented to reduce negative impacts
- **MANAGE-3.1:** AI risks from third-party resources are monitored
- **MANAGE-3.2:** Responses to third-party AI risks are implemented
- **MANAGE-4.1:** Response and recovery procedures are established
- **MANAGE-4.2:** AI incidents are documented and communicated

Evidence Requirements:

- Risk treatment plans and implementation records
- Benefit maximization and harm minimization strategies
- Third-party risk monitoring results
- Incident response procedures and records
- Recovery procedure documentation

Compliance Checklist:

- [ ] Prioritize and plan responses to AI risks
- [ ] Implement treatment of documented AI risks
- [ ] Develop strategies to maximize benefits and minimize harms
- [ ] Implement AI system modifications to reduce negative impacts
- [ ] Monitor AI risks from third-party resources
- [ ] Implement responses to third-party AI risks
- [ ] Establish response and recovery procedures
- [ ] Document and communicate AI incidents

Official Guidance:

- **NIST AI RMF Generative AI Profile:** Link (https://www.nist.gov/system/files/documents/2024/10/07/09-24-about-the-ai-rmf-for-distro-9-25_508-edit.pdf)
- **NIST AI RMF Resource Center:** Link (https://airc.nist.gov/airmf-resources/airmf/5-sec-core/)

6. OWASP AI Security Principles

6.1 Framework Overview

Official Source: OWASP AI Security & Privacy Guide (https://owasp.org/www-project-ai-security-and-privacy-guide/)

OWASP provides comprehensive AI security controls organized into five key pillars covering over 200 pages of guidance.

6.2 AI Governance Controls

AIPROGRAM - AI Governance Program:

- Inventory AI initiatives across organization
- Assign clear accountability for AI risks
- Perform risk analyses covering risks by AI (fairness, safety) and to AI (security, privacy)
- Enforce legal and regulatory guardrails

SECPROGRAM - Security Program Integration:

- Include AI-specific assets in information security management system
- Cover training data, model parameters, documentation, inputs/outputs
- Include AI threats in security policies and incident response
- Conduct compliance audits including AI components

SECDEVPROGRAM - Secure Development:

- Extend secure software development lifecycle to AI engineering
- Implement secure coding for data pipelines
- Conduct threat modeling for poisoning and prompt injection
- Integrate AI-specific CI/CD tests (bias checks, adversarial robustness)

Evidence Requirements:

- AI governance program documentation
- Security program integration evidence
- Secure development lifecycle procedures
- Training records for AI security

Compliance Checklist:

- [ ] Establish comprehensive AI governance program
- [ ] Integrate AI security into existing security programs
- [ ] Extend secure development practices to AI systems
- [ ] Implement AI-specific threat modeling
- [ ] Create AI security training programs
- [ ] Establish AI incident response procedures

6.3 Conventional IT Security Controls

Runtime Security:

- Secure model hosting with appropriate isolation
- Enforce input/output validation for AI systems
- Implement rate limiting and compute isolation
- Apply API security controls (authentication, RBAC)

- Encrypt or obfuscate model parameters

Development Security:

- Protect data and model repositories
- Enforce supply chain integrity for AI components
- Segregate development, testing, and production environments
- Implement encryption at rest for training data

Evidence Requirements:

- IT security control implementation records
- API security configuration documentation
- Environment segregation evidence
- Encryption implementation records

Compliance Checklist:

- [ ] Implement comprehensive runtime security controls
- [ ] Secure AI development environments
- [ ] Apply supply chain security to AI components
- [ ] Implement appropriate encryption controls
- [ ] Configure API security for AI services
- [ ] Monitor and log AI system activities

6.4 AI-Specific Technical Controls

Input Protection:

- **PROMPTINPUTVALIDATION:** Sanitize inputs to prevent prompt injection
- **INPUTSEGREGATION:** Sandbox inputs to prevent adversarial queries

Model Protection:

- **MODELOBFUSCATION:** Protect model intellectual property via packing/encryption
- **CONFCOMPUTE:** Use hardware-enforced enclaves for sensitive operations

Monitoring and Access Control:

- **MONITORUSE:** Detect anomalous usage patterns
- **MODELACCESSCONTROL:** Implement appropriate access controls for models
- **RATELIMIT:** Throttle untrusted clients and unusual usage patterns

Evidence Requirements:

- Input validation and sanitization procedures
- Model protection implementation records
- Monitoring and alerting system configuration
- Access control policies and implementation evidence

Compliance Checklist:

- [ ] Implement prompt injection prevention controls
- [ ] Create input segmentation and sandboxing
- [ ] Protect model intellectual property
- [ ] Deploy usage monitoring and anomaly detection
- [ ] Implement model access controls
- [ ] Configure rate limiting for AI services

6.5 Data Science Security Controls

Data Protection:

- **DATAMINIMIZE:** Enforce data minimization before training
- **ALLOWEDDATA:** Implement purpose limitation for data usage
- **SHORTRETAIN:** Apply appropriate data retention policies

Privacy-Preserving Techniques:

- **DISCRETE:** Anonymize or coarsen sensitive attributes
- **OBFUSCATETRAININGDATA:** Remove linkable identifiers from training data

Model Governance:

- **OVERSIGHT:** Restrict model capabilities appropriately
- **LEASTMODELPRIVILEGE:** Apply principle of least privilege to model access
- **CONTINUOUSVALIDATION:** Automate periodic fairness and accuracy testing
- **UNWANTEDBIASTESTING:** Implement bias detection and testing

Evidence Requirements:

- Data minimization and retention procedures
- Privacy-preserving technique implementation
- Model governance and oversight procedures
- Continuous validation and bias testing results

Compliance Checklist:

- [ ] Implement data minimization and purpose limitation
- [ ] Apply privacy-preserving techniques to training data
- [ ] Establish model capability restrictions
- [ ] Implement continuous validation and monitoring
- [ ] Deploy automated bias detection and testing
- [ ] Create model governance oversight procedures

6.6 Privacy and Rights Controls

Transparency and Explainability:

- Maintain dataset and model documentation
- Log data provenance and model decisions
- Support Article 22 GDPR rights (meaningful information, human review)

Individual Rights:

- Operationalize access, correction, erasure rights
- Support objection and portability rights for both raw data and model outputs
- Implement consent management for AI processing

Evidence Requirements:

- Data and model documentation (data cards)
- Individual rights procedure documentation
- Consent management system records
- Transparency and explainability evidence

Compliance Checklist:

- [ ] Create comprehensive data and model documentation

- [ ] Implement individual rights procedures for AI systems
- [ ] Deploy consent management for AI processing
- [ ] Provide transparency and explainability mechanisms
- [ ] Support data subject rights across AI lifecycle
- [ ] Maintain audit trails for rights requests

Official Resources:

- **OWASP AI Exchange:** Link (https://owaspai.org/docs/ai_security_overview/)
- **OWASP AI Security Verification Standard:** GitHub Repository (https://github.com/OWASP/AISVS/)

---

7. ISO Standards for AI Governance

7.1 ISO 27001:2022 - Information Security Management

Official Source: ISO/IEC 27001:2022 Standard

Annex A Controls Relevant to AI Systems:

Organizational Controls (A.5):

- **A.5.7 Threat Intelligence:** Use AI-specific threat feeds for data poisoning and adversarial exploits
- **A.5.14 Information Transfer:** Define policies for sharing training data and model artifacts
- **A.5.19 Supplier Relationships:** Ensure third-party AI vendors meet security requirements
- **A.5.23 Cloud Services:** Govern AI workloads in IaaS/PaaS environments

People Controls (A.6):

- **A.6.3 Security Awareness:** Provide AI-focused security training
- **A.6.4 Disciplinary Process:** Enforce AI system configuration and usage policies

Technological Controls (A.8):

- **A.8.9 Configuration Management:** Apply IaC and drift detection to AI pipelines
- **A.8.10 Information Deletion:** Implement data sanitization for training datasets
- **A.8.11 Data Masking:** Mask sensitive features during training and inference
- **A.8.12 Data Leakage Prevention:** Block exfiltration of proprietary models
- **A.8.16 Monitoring Activities:** Monitor AI system logs and performance metrics
- **A.8.28 Secure Coding:** Apply secure development to ML pipelines

Evidence Requirements:

- AI asset inventory including training data, models, and infrastructure
- AI-specific risk assessments and treatment plans
- Security policies covering AI systems and data
- Training records for AI security awareness
- Monitoring and logging evidence for AI systems

Compliance Checklist:

- [ ] Include AI assets in information security asset inventory
- [ ] Conduct AI-specific risk assessments
- [ ] Implement appropriate Annex A controls for AI systems

- [ ] Provide AI security training to relevant personnel
- [ ] Monitor and log AI system activities
- [ ] Apply secure development practices to AI/ML pipelines
- [ ] Implement data protection controls for training data
- [ ] Establish AI supplier security requirements

7.2 ISO 23053:2022 - AI Framework Standard

Official Source: ISO/IEC 23053:2022 Framework for AI Systems Using Machine Learning

Framework Components:

Data Acquisition and Preparation:

- Data types and labeling requirements
- Quality considerations and preprocessing steps
- Feature extraction and data cleaning procedures

Model Development:

- ML task definitions (classification, regression, clustering)
- Algorithm categories and optimization methods
- Development lifecycle management

Verification and Validation:

- Evaluation metrics (accuracy, recall, AUC, false positive/negative rates)
- Overfitting and underfitting assessment
- Model validation procedures

Deployment and Operation:

- Model deployment patterns and configurations
- Monitoring and maintenance procedures
- Lifecycle management processes

Governance and Oversight:

- Terminology and system breakdown for governance alignment
- Data provenance and transparency requirements
- Responsibility and accountability frameworks

Evidence Requirements:

- System architecture documentation using ISO 23053 framework
- Data acquisition and preparation procedures
- Model development and validation records
- Deployment and operational procedures
- Governance framework documentation

Compliance Checklist:

- [ ] Document AI system architecture using ISO 23053 framework
- [ ] Implement data acquisition and preparation procedures
- [ ] Establish model development and validation processes
- [ ] Create deployment and operational procedures
- [ ] Align governance frameworks with ISO 23053 structure
- [ ] Maintain comprehensive system documentation
- [ ] Implement lifecycle management processes

7.3 AI Risk Management with ISO 27001

Integration Approach:

- **Clause 4 (Context):** Include AI-relevant legal, technological and societal factors
- **Clause 6 (Planning):** Include AI-related risks in risk assessments
- **Clause 7.2 (Competence):** Ensure AI threat awareness training
- **Control 5.7 (Threat Intelligence):** Include AI-specific threat feeds
- **Control 8.28 (Secure Coding):** Include AI/ML development guidelines

AI-Specific Threat Mapping:

- **Data Poisoning → Integrity & Availability**
- **Model Inversion → Confidentiality**
- **Adversarial Inputs → Integrity**
- **Unauthorized API Abuse → Confidentiality & Integrity**
- **Shadow AI → Compliance & Accountability**

Evidence Requirements:

- AI threat landscape assessment
- AI-specific control implementation evidence
- AI system change management records
- AI incident response procedures and records
- Regular AI risk assessment updates

Compliance Checklist:

- [ ] Integrate AI risks into ISMS risk assessment
- [ ] Map AI threats to CIA triad and other security objectives
- [ ] Implement AI-specific controls within existing framework
- [ ] Establish AI change advisory processes
- [ ] Create AI incident response procedures
- [ ] Maintain AI asset register within ISMS
- [ ] Conduct regular AI risk reviews and updates

Official Resources:

- **ISO 27001:2022 Standard:** Available via ISO Store
- **ISO 23053:2022 Framework:** Available via ISO Store
- **Implementation Guidance:** Various consulting and certification bodies

---

Summary and Next Steps

This comprehensive compliance framework covers seven major regulatory areas affecting AI systems. Organizations should:

1. **Prioritize** based on applicable jurisdictions and business sectors
2. **Integrate** requirements into existing governance frameworks where possible
3. **Establish** clear ownership and accountability for each compliance area
4. **Implement** systematic documentation and evidence collection processes
5. **Monitor** regulatory developments and guidance updates continuously

For specific implementation support, organizations should engage with qualified legal counsel, compliance professionals, and technical specialists familiar with AI governance requirements.

Document Version: 1.0
Last Updated: July 30, 2025
Next Review: October 30, 2025