2026

Auditoría ISO 42001 tool

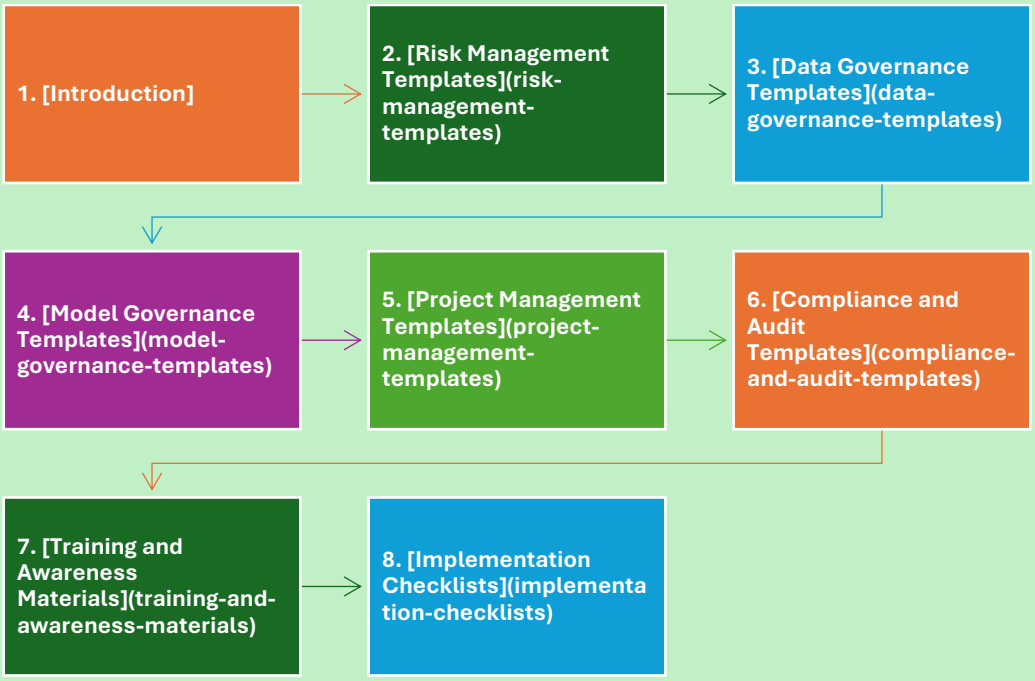
SCI

1/1/2026

INDEX

ISO 42001 Lead Implementer Toolkit

This toolkit provides practical resources for ISO 42001 Lead Implementers to successfully implement AI security management systems. The toolkit includes templates, checklists, guides, and examples that can be customized for your organization.



Introduction

This toolkit provides practical resources for ISO 42001 Lead Implementers to successfully implement AI security management systems. The toolkit includes templates, checklists, guides, and examples that can be customized for your organization.

1. **Assess Your Needs: Review the case studies to understand different implementation approaches**
2. **Select Relevant Templates: Choose templates that match your organization's needs**
3. **Customize for Your Organization: Adapt templates to your specific context**
4. **Follow Implementation Sequence: Use the checklists and flowcharts to guide your implementation**
5. **Collect Evidence: Use the templates to systematically collect evidence of implementation**
6. **Prepare for Audit: Use the audit templates to prepare for compliance verification**

Risk Assessment Report

- Assessment Date: _____
- Assessor: _____
- Department/System: _____
- Assessment Scope: _____

Risk Identification

- Risk ID: R-001
- Risk Description: _____
- Risk Category: ☐ Data ☐ Model ☐ Operational ☐ Compliance
- Risk Source: _____
- Current Controls: _____

Risk Analysis

- Likelihood Assessment
- Likelihood: ☐ Low ☐ Medium ☐ High
- Justification: _____
- Impact Assessment

Impact: ☐ Low ☐ Medium ☐ High ☐ Critical
Justification: _____
Risk Score: Likelihood × Impact = _____

```
├── Risk Evaluation
│   ├── Risk Level: ☐ Low ☐ Medium ☐ High ☐ Critical
│   ├── Acceptable? ☐ Yes ☐ No
│   └── Justification: _____
├── Risk Treatment
│   ├── Treatment Option: ☐ Mitigate ☐ Accept ☐ Avoid ☐ Transfer
│   ├── Proposed Control: _____
│   ├── Responsibility: _____
│   ├── Timeline: _____
│   └── Budget: _____
└── Approval
    ├── Risk Owner: _____
    ├── Risk Manager: _____
    └── Date: _____
```

****Risk Scoring Matrix: ****

| Likelihood | Low Impact | Medium Impact | High Impact | Critical Impact |
| **Low | 1 | 2 | 3 | 4 |**
| **Medium | 2 | 4 | 6 | 8 |**
| **High | 3 | 6 | 9 | 12 |**

Risk Level Thresholds:
- Score 1-2: Low Risk (Monitor)
- Score 3-4: Medium Risk (Mitigate)
- Score 6-8: High Risk (Mitigate Immediately)
- Score 9-12: Critical Risk (Mitigate Urgently)

Risk Register Template

Risk ID	Description	Category	Owner	Likelihood	Impact	Score	Status	Control	Target Date	Progress
R-001	Model bias in credit scoring	Model	John Smith	High	Critical	12	Active	Fairness testing	2025-12-31	75%
R-002	Data breach of customer data	Data	Jane Doe	Medium	Critical	8	Active	Encryption	2025-12-15	90%
R-003	Inadequate model monitoring	Operational	Bob Johnson	High	High	9	Active	Monitoring system	2026-01-15	50%

Risk Register Maintenance:

- Update weekly during implementation
- Review monthly with risk management team
- Update status and progress regularly
- Close risks when controls are effective

Risk Treatment Plan Template

Risk Treatment Plan
- Risk ID: R-001
- Risk Description: Model bias in credit scoring
- Current Risk Score: 12 (Critical)
- Target Risk Score: 3 (Medium)
- Treatment Strategy: Mitigate
- Proposed Controls
  - Control 1: Fairness testing in model development
    - Description: Implement fairness metrics testing
    - Responsibility: Data Science Team
    - Timeline: 2025-12-31
    - Budget: $50,000
    - Success Criteria: Demographic parity >95%
  - Control 2: Fairness monitoring in production
    - Description: Monitor fairness metrics continuously
    - Responsibility: ML Operations
    - Timeline: 2026-01-15
    - Budget: $30,000
    - Success Criteria: Alert if parity <95%
  - Control 3: Fairness incident response
    - Description: Respond to fairness issues
    - Responsibility: Risk Management
    - Timeline: 2026-01-31
    - Budget: $20,000
    - Success Criteria: Response within 4 hour
- Implementation Timeline
  - Phase 1 (Weeks 1-4): Design and develop fairness tests
  - Phase 2 (Weeks 5-8): Implement in development pipeline
  - Phase 3 (Weeks 9-12): Deploy monitoring system
  - Phase 4 (Weeks 13-16): Establish incident response
- Budget Summary
  - Development: $50,000
  - Operations: $30,000
  - Management: $20,000
  - Total: $100,000
- Success Metrics
  - Fairness metric: Demographic parity >95%
  - Monitoring: Real-time fairness alerts
  - Response time: <4 hours
  - Stakeholder satisfaction: >85%
- Approval
  - Risk Owner: John Smith
  - Risk Manager: Risk Management Team
  - Date: _____

Classify data by sensitivity level and define protection requirements

Data Element	Source	Sensitivity Level	Owner	Steward	Protection Requirements	Retention	Deletion
Customer Name	CRM	Level 3 (Confidential)	Sales	John Smith	Encryption, Access control	7 years	Secure delete
Customer Email	CRM	Level 2 (Internal)	Sales	John Smith	Access control	3 years	Standard delete
Medical Records	EHR	Level 4 (Restricted)	Medical	Jane Doe	Encryption, MFA, Audit log	10 years	Secure delete
Aggregated Analytics	Data Warehouse	Level 1 (Public)	Analytics	Bob Johnson	None	Indefinite	N/A

Sensitivity Level Definitions:

Level	Definition	Examples	Controls
1 - Public	Non-sensitive, no restrictions	Aggregated statistics, public info	None
2 - Internal	Internal use only, limited distribution	Employee data, internal reports	Access control
3 - Confidential	Restricted access, audit logging	Customer data, financial data	Encryption, Access control, Audit log
4 - Restricted	Highly sensitive, minimal access	Medical records, payment info	Encryption, MFA, Audit log, Segregation

Data Quality Standards

- Data Element: Customer Age
- Quality Dimensions
  - Completeness
    - Definition: All records have age value
    - Target: 99%
    - Measurement: Count of non-null values / Total records
    - Frequency: Daily
  - Accuracy
    - Definition: Age matches source of truth
    - Target: 98%
    - Measurement: Validation against source system
    - Frequency: Weekly
  - Consistency
    - Definition: Age consistent across systems
    - Target: 99%
    - Measurement: Cross-system comparison
    - Frequency: Weekly
  - Validity
    - Definition: Age within valid range (0-120)
    - Target: 99.5%
    - Measurement: Range validation
    - Frequency: Daily
  - Timeliness
    - Definition: Age current within 30 days
    - Target: 95%
    - Measurement: Freshness check
    - Frequency: Daily
- Quality Monitoring
  - Monitoring Tool: Data Quality Platform
  - Monitoring Frequency: Daily
  - Alert Threshold: <95% quality score
  - Escalation: Quality Manager if alert triggered
- Remediation
  - Remediation Process: Manual review and correction
  - Responsibility: Data Steward
  - Timeline: Within 5 business days
  - Documentation: Quality incident log
- Approval
  - Data Owner: _____
  - Data Steward: _____
  - Date: _____

Data Governance Policy Template

1. Purpose and Scope
   - **Define purpose of data governance**
   - **Define scope (which data, which systems)**
   - **Define applicability (who must comply)**
2. Roles and Responsibilities
   - Chief Data Officer
     - Responsibility 1: Oversee data governance program
     - Responsibility 2: Set data governance strategy
     - Responsibility 3: Report to executive leadership
   - Data Governance Manager
     - Responsibility 1: Coordinate data governance activities
     - Responsibility 2: Manage data governance council
     - Responsibility 3: Track implementation progress
   - Data Owner
     - Responsibility 1: Define data requirements
     - Responsibility 2: Approve data access
     - Responsibility 3: Ensure data quality
   - Data Steward
     - Responsibility 1: Manage day-to-day data governance
     - Responsibility 2: Monitor data quality
     - Responsibility 3: Handle data access requests

3. Data Classification
- Define sensitivity levels
- Define classification criteria
- Define classification process
- Define classification review frequency

4. Data Quality
- Define quality dimensions
- Define quality standards
- Define quality monitoring
- Define quality remediation

5. Data Privacy
- Define privacy requirements
- Define consent management
- Define data minimization
- Define data retention and deletion

6. Data Access Control
- Define access control principles
- Define access request process
- Define access approval process
- Define access review frequency

7. Data Governance Meetings
- Data Governance Council (monthly)
- Data Quality Working Group (weekly)
- Data Steward Meetings (weekly)

8. Compliance and Auditing
- Define audit procedures
- Define compliance verification
- Define remediation procedures
- Define reporting requirements

9. Review and Update
- Annual policy review
- Update as needed for regulatory changes
- Update as needed for business changes

10. Approval
- Chief Data Officer: _____
- Chief Information Officer: _____
- Date: _____

1. Model Details
- Model Name: [Name]

- Version: [Version number]
- Release Date: [Date]
- Owner: [Team/Person]
- Status: ☐ Development ☐ Testing ☐ Production ☐ Retired
- Purpose: [One sentence description]

2. Intended Use
- Primary Use Case: [Description]
- Intended Users: [Who uses the model]
- Use Scope: [Where it's used]
- Limitations: [What it can't do]
- Contraindications: [When not to use]

3. Training Data
- Data Source: [Where data comes from]
- Data Period: [Date range]
- Data Size: [Number of records]
- Features: [Number and description]
- Quality Score: [Percentage]
- Bias Mitigation: [Techniques used]
- Data Lineage: [Source to model pipeline]

4. Model Architecture
- Algorithm: [Type of algorithm]
- Framework: [TensorFlow, PyTorch, etc.]
- Model Size: [Parameters, memory]
- Inference Time: [Latency]
- Computational Requirements: [GPU, CPU, memory]

5. Model Performance
- Accuracy: [Percentage]
- Precision: [Percentage]
- Recall: [Percentage]
- F1 Score: [Score]
- AUC-ROC: [Score]
- Test Set Size: [Number of records]
- Confidence Interval: [Range]

6. Fairness Assessment
- Demographic Parity: [Percentage]
- Equalized Odds: [Percentage]
- Calibration: [Percentage]
- Bias Assessment: [Findings]
- Mitigation Strategies: [Actions taken]
- Monitoring Plan: [Ongoing monitoring]

7. Explainability
- Explainability Method: [SHAP, LIME, etc.]
- Top Features: [Feature importance]
- Feature Descriptions: [What each feature means]
- Example Explanation: [Sample explanation]
- Explanation Quality Score: [Percentage]
- Audit Trail: [Logging capability]

8. Ethical Considerations
- Potential Harms: [What could go wrong]
- Mitigation Strategies: [How to prevent harm]
- Monitoring Plan: [Ongoing monitoring]
- Governance Oversight: [Who oversees]
- Stakeholder Engagement: [Who's involved]

9. Security and Privacy
- Data Privacy: [Privacy protections]
- Model Security: [Security measures]
- Access Control: [Who can access]
- Encryption: [Encryption methods]
- Audit Logging: [Logging capability]

10. Monitoring and Maintenance
- Performance Monitoring: [Frequency and metrics]
- Drift Monitoring: [Detection methods]
- Fairness Monitoring: [Frequency and metrics]
- Retraining Plan: [When and how]
- Incident Response: [SLA and procedures]

- Maintenance Schedule: [Regular updates]

11. Version History

- v1.0: [Description and date]
- v1.1: [Description and date]
- v[Current]: [Description and date]

12. Contact Information

- Model Owner: [Name and contact]
- Technical Lead: [Name and contact]
- Data Owner: [Name and contact]
- Governance Lead: [Name and contact]

13. Approvals

- Model Owner: _____ Date: _____
- Data Owner: _____ Date: _____
- Compliance Officer: _____ Date: _____
- Governance Council: _____ Date: _____

Model Testing Checklist

Model Testing Checklist: [Model Name] v[Version]

Unit Tests

- ☐ Test individual components
- ☐ Test edge cases
- ☐ Test error handling
- ☐ Achieve >90% code coverage
- ☐ Document test results

Integration Tests

- ☐ Test component interactions
- ☐ Test data pipeline
- ☐ Test model inference
- ☐ Test output format
- ☐ Document test results

Performance Tests

- ☐ Accuracy: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Precision: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Recall: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ F1 Score: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Latency: Target ___ms Achieved ___ms ☐ Pass ☐ Fail

Fairness Tests

- ☐ Demographic Parity: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Equalized Odds: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Calibration: Target ___% Achieved ___% ☐ Pass ☐ Fail
- ☐ Identify any bias issues: [Description]
- ☐ Plan mitigation if needed: [Plan]

Security Tests

- ☐ Test model extraction resistance
- ☐ Test adversarial robustness
- ☐ Verify no sensitive data in model
- ☐ Verify access controls
- ☐ Verify audit logging
- ☐ Identify any security issues: [Description]

Stress Tests

- ☐ Test with maximum load
- ☐ Test with edge cases
- ☐ Test error recovery
- ☐ Verify performance under stress
- ☐ Document results: [Results]

Adversarial Tests

- ☐ Test with adversarial examples
- ☐ Verify robustness
- ☐ Document findings: [Findings]

Explainability Tests

- ☐ Generate sample explanations
- ☐ Verify explanation quality
- ☐ Verify explanation accuracy
- ☐ Document sample explanations: [Examples]

Overall Assessment

- ☐ All tests passed

☐ Issues identified and documented
☐ Mitigation plans created
☐ Ready for deployment: ☐ Yes ☐ No

Test Report

- Tested By: _____
- Test Date: _____
- Total Tests: _____
- Passed: _____
- Failed: _____
- Pass Rate: _____%
- Issues Found: _____
- Recommendation: ☐ Approve ☐ Reject ☐ Conditional
- Approver: _____

Performance Metrics (Daily)

- Accuracy: ___% (Target: ___%)
- Precision: ___% (Target: ___%)
- Recall: ___% (Target: ___%)
- F1 Score: ___% (Target: ___%)
- Latency: ___ms (Target: <___ms)
- Predictions/Day: _____

Drift Indicators (Daily)

- Feature Distribution Drift: ☐ Low ☐ Medium ☐ High
- Target Distribution Drift: ☐ Low ☐ Medium ☐ High
- Concept Drift: ☐ Low ☐ Medium ☐ High
- Drift Alert Triggered: ☐ Yes ☐ No

Fairness Metrics (Weekly)

- Demographic Parity: ___% (Target: >___%)
- Equalized Odds: ___% (Target: >___%)
- Calibration: ___% (Target: >___%)
- Fairness Alert Triggered: ☐ Yes ☐ No

Security Metrics (Weekly)

- Access Control Violations: _____
- Unauthorized Access Attempts: _____
- Audit Log Completeness: ___% (Target: 100%)
- Security Alert Triggered: ☐ Yes ☐ No

Incidents (Weekly)

- Critical Incidents: _____
- High Incidents: _____
- Medium Incidents: _____
- Low Incidents: _____
- Average Resolution Time: ___hours

Health Status

- Overall Status: ☐ Healthy ☐ Caution ☐ Critical
- Performance Status: ☐ Healthy ☐ Caution ☐ Critical
- Drift Status: ☐ Healthy ☐ Caution ☐ Critical
- Fairness Status: ☐ Healthy ☐ Caution ☐ Critical
- Security Status: ☐ Healthy ☐ Caution ☐ Critical

Actions Taken (Weekly)

- Retraining: ☐ Yes ☐ No
- Configuration Changes: ☐ Yes ☐ No
- Incident Response: ☐ Yes ☐ No
- Monitoring Updates: ☐ Yes ☐ No

ISO 42001 Implementation Project Plan

1. Project Overview
- Project Name: ISO 42001 Implementation
- Project Duration: [Start Date] to [End Date]
- Project Budget: $[Amount]
- Project Sponsor: [Name and Title]
- Project Manager: [Name and Title]
- Project Scope: [Description]

2. Project Objectives
- Objective 1: Implement risk management framework
- Objective 2: Implement data governance
- Objective 3: Implement model governance
- Objective 4: Achieve ISO 42001 compliance
- Objective 5: Prepare for external audit

3. Project Phases
- Phase 1: Assessment and Planning (Weeks 1-6)
  - Task 1.1: Establish project team
  - Task 1.2: Conduct current state assessment
  - Task 1.3: Define scope and objectives
  - Task 1.4: Develop project plan
  - Deliverables: Project charter, assessment report
- Phase 2: Design (Weeks 7-14)
  - Task 2.1: Design risk management framework
  - Task 2.2: Design data governance framework
  - Task 2.3: Design model governance framework
  - Task 2.4: Design compliance procedures
  - Deliverables: Framework documents, procedures
- **Phase 3: Implementation (Weeks 15-28)**
  - Task 3.1: Implement risk management
  - Task 3.2: Implement data governance
  - Task 3.3: Implement model governance
  - Task 3.4: Implement compliance procedures
  - Deliverables: Implemented controls, evidence
- **Phase 4: Testing and Validation (Weeks 29-34)**
  - Task 4.1: Test controls
  - Task 4.2: Conduct internal audit
  - Task 4.3: Remediate findings
  - Task 4.4: Prepare for external audit
  - Deliverables: Test reports, audit reports
- **Phase 5: Closure and Handover (Weeks 35-36)**
  - Task 5.1: Finalize documentation
  - Task 5.2: Conduct training
  - Task 5.3: Transition to operations
  - Task 5.4: Close project
  - Deliverables: Final documentation, training materials

4. Resource Plan
- Project Manager: 100% allocation
- Compliance Manager: 80% allocation
- IT Manager: 60% allocation
- Data Manager: 60% allocation
- Business Unit Heads: 20% allocation each
- External Consultant: As needed

5. Budget Plan
- Personnel: $[Amount]
- Tools and Systems: $[Amount]
- Training: $[Amount]
- External Consulting: $[Amount]
- Total Budget: $[Amount]

6. Risk Management

- Risk 1: Scope creep
  - Mitigation: Clear scope definition, change control
  - Owner: Project Manager
- Risk 2: Resource constraints
  - Mitigation: Prioritization, external support
  - Owner: Project Manager
- **Risk 3: Stakeholder resistance**
  - Mitigation: Communication, engagement
  - Owner: Project Sponsor

7. Communication Plan

- Executive Steering Committee: Monthly
- Project Team: Weekly
- Stakeholders: Bi-weekly
- Status Reports: Weekly
- Escalation: As needed

8. Success Criteria

- Scope: 100% of planned work completed
- Schedule: On-time delivery
- Budget: Within 10% of budget
- Quality: All deliverables meet standards
- Compliance: 95%+ compliance achieved
- Stakeholder Satisfaction: >85%

9. Approval

- Project Sponsor: _____ Date: _____
- Project Manager: _____ Date: _____
- Steering Committee: _____ Date: _____

Internal Audit Checklist: ISO 42001 Implementation

- **Audit Information**
- **Audit Date:** _____
- **Auditor:** _____
- **Department/System:** _____
- **Audit Scope:** _____
- **Audit Objective:** _____

Risk Management (A.5)
☐ Risk assessment process documented
☐ Risk assessment conducted
☐ Risks identified and documented
☐ Risk treatment plans developed
☐ Risk treatment plans implemented
☐ Risk monitoring procedures in place
☐ Risk review conducted regularly
☐ Evidence collected and organized

Data Governance (A.8)
☐ Data classification policy documented
☐ Data classified appropriately
☐ Data quality standards defined
☐ Data quality monitored
☐ Data governance structure established
☐ Data owners assigned
☐ Data stewards assigned
☐ Data governance meetings held

Model Governance (A.7)
☐ Model development standards documented
☐ Models tested before deployment
☐ Model validation procedures in place
☐ Model monitoring procedures in place
☐ Model incidents tracked and resolved
☐ Model documentation complete
☐ Model governance structure established
☐ Model governance meetings held

Compliance (A.5, A.6, A.9)
☐ Compliance requirements identified
☐ Compliance procedures documented
☐ Compliance monitoring in place
☐ Compliance violations tracked
☐ Compliance violations remediated
☐ Audit evidence collected
☐ Audit trails maintained
☐ Regulatory requirements met

People (A.6)
☐ Competence requirements defined
☐ Staff training conducted
☐ Awareness program implemented
☐ Training records maintained
☐ Competence assessed
☐ Training effectiveness evaluated

Technology (A.9)

☐ Access controls implemented
☐ Encryption implemented
☐ Audit logging implemented
☐ Monitoring systems in place
☐ Security incidents tracked
☐ Security patches applied
☐ Security testing conducted

Findings
├── Finding 1: [Description]
│ ├── Severity: ☐ Critical ☐ Major ☐ Minor
│ ├── Root Cause: [Analysis]
│ ├── Remediation: [Action plan]
│ ├── Owner: [Name]
│ └── Target Date: [Date]
│
└── Finding 2: [Description]
 ├── Severity: ☐ Critical ☐ Major ☐ Minor
 ├── Root Cause: [Analysis]
 ├── Remediation: [Action plan]
 ├── Owner: [Name]
 └── Target Date: [Date]

Overall Assessment
├── Compliance Level: _____%
├── Strengths: [List]
├── Weaknesses: [List]
├── Recommendations: [List]
└── Overall Rating: ☐ Compliant ☐ Partially Compliant ☐ Non-Compliant

Audit Report
├── Prepared By: _____
├── Reviewed By: _____
├── Approved By: _____
└── Date: _____
Audit Evidence Checklist

Documentation Evidence
☐ Risk Management Policy
☐ Risk Assessment Reports
☐ Risk Register
☐ Risk Treatment Plans
☐ Data Governance Policy
☐ Data Classification Matrix
☐ Data Quality Standards
☐ Model Development Standards
☐ Model Cards
☐ Compliance Procedures
☐ Training Materials
☐ Incident Response Procedures

Process Evidence
☐ Risk Assessment Process Documentation
☐ Risk Treatment Process Documentation
☐ Data Governance Process Documentation
☐ Model Development Process Documentation
☐ Model Validation Process Documentation
☐ Incident Response Process Documentation
☐ Audit Process Documentation

Records Evidence
☐ Risk Assessment Records
☐ Risk Treatment Records
☐ Data Quality Monitoring Records
☐ Model Testing Records
☐ Model Validation Records
☐ Training Records
☐ Incident Response Records
☐ Audit Records
☐ Management Review Records

System Evidence
☐ Risk Management System
☐ Data Governance System
☐ Model Registry
☐ Monitoring Systems
☐ Audit Logging Systems
☐ Access Control Systems

Interview Evidence
☐ Risk Manager Interview
☐ Data Manager Interview
☐ Model Owner Interview
☐ Compliance Officer Interview
☐ IT Manager Interview
☐ Business Unit Head Interview

Evidence Organization
├── Folder Structure
│ ├── /Documentation
│ ├── /Process
│ ├── /Records
│ ├── /Systems
│ └── /Interviews
│
├── Evidence Index
│ ├── Document ID
│ ├── Document Name
│ ├── Location
│ ├── Date
│ └── Relevance
│
└── Evidence Summary
  ├── Total Documents: _____
  ├── Total Records: _____
  ├── Total System Artifacts: _____
  └── Overall Completeness: _____%

Evidence Verification
├── Verified By: _____
├── Verification Date: _____
├── Completeness: ☐ Complete ☐ Partial ☐ Incomplete
└── Audit Readiness: ☐ Ready ☐ Needs Work

ISO 42001 Awareness Training

Module 1: Introduction to ISO 42001 (30 minutes)
- What is ISO 42001?
- Why is it important?
- What are the main requirements?
- How does it affect our organization?
- Q&A

Module 2: AI Security Risks (45 minutes)
- What are AI-specific risks?
- Data risks (bias, quality, privacy)
- Model risks (drift, adversarial attacks)
- Operational risks (monitoring, incident response)
- Compliance risks (transparency, accountability)
- Q&A

Module 3: Our Implementation (45 minutes)
- Our scope and objectives
- Our implementation approach
- Our timeline and milestones
- Our roles and responsibilities
- How to get involved
- Q&A

Module 4: What This Means for You (30 minutes)
- Your role in implementation
- Your responsibilities
- What you need to do
- How to get help
- Resources available
- Q&A

Module 5: Key Controls (60 minutes)
- Risk management
- Data governance
- Model governance
- Compliance procedures
- Incident response
- Q&A

Total Duration: 3.5 hours (can be split into multiple sessions)

Training Materials
- Presentation slides
- Handouts
- Quick reference guides
- FAQ document
- Contact information

Assessment
- Knowledge check quiz
- Feedback survey
- Attendance tracking
- Certification of completion

- Risk Assessment Process
- Risk Scoring Methodology
- Risk Treatment Planning
- Risk Monitoring
- Risk Reporting
- Tools and Templates

For Data Managers:

├── Data Classification
├── Data Quality Standards
├── Data Governance Framework
├── Data Privacy
├── Data Lineage Tracking
└── Tools and Templates

For Model Owners:
├── Model Development Standards
├── Model Testing Requirements
├── Model Validation Procedures
├── Model Monitoring
├── Model Documentation (Model Card)
└── Tools and Templates

For IT Security:
├── Access Control Implementation
├── Encryption Standards
├── Audit Logging
├── Security Monitoring
├── Incident Response
└── Tools and Templates

For Compliance Officers:
├── Compliance Requirements
├── Audit Procedures
├── Evidence Collection
├── Remediation Procedures
├── Regulatory Reporting
└── Tools and Templates

For Business Unit Heads:
├── How ISO 42001 Affects Your Unit
├── Your Responsibilities
├── How to Support Implementation
├── Timeline and Milestones
├── Resources Available
└── Q&A

Executive Sponsorship
☐ Executive sponsor identified
☐ Executive sponsor committed
☐ Executive sponsor involved in planning
☐ Executive sponsor will provide resources

Project Team
☐ Project manager identified
☐ Project team members identified
☐ Team members allocated adequate time
☐ Team members have required expertise

Scope and Objectives
☐ Scope clearly defined
☐ Scope documented and approved
☐ Objectives clearly defined
☐ Objectives documented and approved

Budget and Resources
☐ Budget approved
☐ Budget allocated
☐ Resources identified
☐ Resources allocated

Stakeholder Engagement
☐ Stakeholders identified
☐ Stakeholder analysis completed
☐ Engagement plan developed
☐ Initial engagement conducted

Current State Assessment
☐ Assessment planned
☐ Assessment conducted
☐ Assessment report prepared
☐ Assessment findings reviewed

Risk Assessment
☐ Risk assessment planned
☐ Risk assessment conducted
☐ Risks identified and documented
☐ Risk mitigation planned

Implementation Plan
☐ Implementation plan developed
☐ Implementation plan reviewed
☐ Implementation plan approved
☐ Implementation plan communicated

Tools and Systems
☐ Tools identified
☐ Tools procured
☐ Tools configured
☐ Tools tested

Training and Awareness
☐ Training plan developed
☐ Training materials prepared
☐ Training schedule set
☐ Awareness campaign planned

Governance Structure
☐ Governance structure defined
☐ Roles and responsibilities assigned
☐ Decision-making authority defined
☐ Governance meetings scheduled

Post Implementation Completion Checklist

Risk Management
☐ Risk assessment process implemented
☐ Risk register created and maintained
☐ Risk treatment plans developed
☐ Risk treatment plans implemented
☐ Risk monitoring in place
☐ Risk review conducted
☐ Risk documentation complete

Data Governance
☐ Data governance framework implemented
☐ Data classification completed
☐ Data quality standards defined
☐ Data quality monitoring in place
☐ Data governance structure established
☐ Data owners and stewards assigned
☐ Data governance meetings held

Model Governance
☐ Model development standards implemented
☐ Model testing procedures in place
☐ Model validation procedures in place
☐ Model monitoring in place
☐ Model governance structure established
☐ Model governance meetings held
☐ Model documentation complete

Compliance
☐ Compliance procedures documented
☐ Compliance monitoring in place
☐ Audit procedures established
☐ Evidence collection procedures in place
☐ Remediation procedures established
☐ Regulatory requirements met

People
☐ Training conducted
☐ Awareness program implemented
☐ Competence assessed
☐ Training records maintained
☐ Roles and responsibilities assigned

Technology
☐ Access controls implemented
☐ Encryption implemented
☐ Audit logging implemented
☐ Monitoring systems in place
☐ Security testing completed
☐ Incident response procedures in place

Documentation
☐ All policies documented
☐ All procedures documented
☐ All templates created
☐ All evidence collected

☐ All records maintained

Testing and Validation
☐ Internal audit conducted
☐ Findings remediated
☐ Controls tested
☐ Controls validated
☐ Audit readiness confirmed

Handover and Operations
☐ Operations team trained
☐ Operations procedures documented
☐ Monitoring procedures established
☐ Escalation procedures established
☐ Support procedures established

Overall Completion: _____%

Completion Assessment
├── Assessed By: _____
├── Assessment Date: _____
├── Status: ☐ Complete ☐ Partial ☐ Incomplete
├── Issues: [List any remaining issues]
├── Approval: _____
└── Approval Date: _____
```
```

Risk Treatment Decision Tree

```
├─ Risk Score < 3 (Low)
│  └─ ACCEPT RISK
│     (Monitor regularly)
├─ Risk Score 3-6 (Medium)
│  └─ MITIGATE RISK
│     ├─ Design controls
│     ├─ Implement controls
│     └─ Monitor effectiveness
├─ Risk Score 6-9 (High)
│  └─ MITIGATE IMMEDIATELY
│     ├─ Design controls urgently
│     ├─ Implement controls urgently
│     └─ Monitor closely
└─ Risk Score 9+ (Critical)
   └─ MITIGATE URGENTLY or AVOID
      ├─ Design emergency controls
      ├─ Implement emergency controls
      ├─ Monitor continuously
      └─ Consider risk avoidance
```

3. Model Deployment Decision Tree

Model Development Complete

- Testing
  - All unit tests passed? NO → Fix and retest
  - All integration tests passed? NO → Fix and retest
  - Performance tests passed? NO → Improve model
  - All tests passed? YES → Continue
- Validation
  - Fairness assessment complete? NO → Conduct assessment
  - Fairness acceptable? NO → Mitigate bias or reject
  - Explainability assessment complete? NO → Conduct assessment
  - Explainability acceptable? NO → Improve explainability
  - Security assessment complete? NO → Conduct assessment
  - Security acceptable? NO → Fix security issues
  - All validations passed? YES → Continue
- Documentation
  - Model card complete? NO → Complete model card
  - Development log complete? NO → Complete development log
  - Testing report complete? NO → Complete testing report
  - All documentation complete? YES → Continue
- Approval
  - Model owner approval? NO → Get approval
  - Data owner approval? NO → Get approval
  - Compliance approval? NO → Get approval
  - All approvals obtained? YES → Continue
- Deployment Planning
  - Deployment plan developed? NO → Develop plan
  - Monitoring plan developed? NO → Develop plan
  - Incident response plan developed? NO → Develop plan
  - All plans developed? YES → Continue

- **READY FOR DEPLOYMENT**
  - Staged rollout
  - Close monitoring
  - Rapid rollback capability

ISO 42001 Control Summary

ISO 42001 Control Summary

A.5: Organizational Controls
├── A.5.1: Risk Assessment
│ └── Establish and maintain risk assessment process
├── A.5.2: Risk Treatment
│ └── Establish and maintain risk treatment process
└── A.5.3: Risk Evaluation
└── Evaluate risks and determine treatment approach

A.6: People Controls
├── A.6.1: Competence
│ └── Ensure staff have required competence
├── A.6.2: Awareness
│ └── Implement awareness program
└── A.6.3: Training
└── Provide training on requirements and controls

A.7: Process Controls
├── A.7.1: AI System Development
│ └── Establish development lifecycle and standards
├── A.7.2: AI System Validation
│ └── Validate models before deployment
├── A.7.3: AI System Deployment
│ └── Establish deployment procedures
├── **A.7.4: AI System Monitoring**
│ └── Monitor models in production
└── A.7.5: Incident Management
└── Establish incident response procedures

A.8: Information Controls
├── A.8.1: Data Classification
│ └── Classify data by sensitivity
├── A.8.2: Data Governance
│ └── Establish data governance framework
└── A.8.3: Data Quality
└── Ensure data quality

A.9: Technology Controls
├── A.9.1: Access Control
│ └── Implement access control
├── A.9.2: Cryptography
│ └── Implement encryption
└── A.9.3: AI System Monitoring
└── Monitor systems for security
```
```

Implementation Roadmap

ISO 42001 Implementation Roadmap

Month 1-2: Assessment and Planning
- Establish project team
- Conduct current state assessment
- Define scope and objectives
- Develop implementation plan
- Secure executive sponsorship

Month 3-4: Foundation (Risk Management)
- Develop risk management framework
- Conduct risk assessment
- Create risk register
- Develop risk treatment plans
- Implement risk monitoring

Month 5-6: Data Governance
- Develop data governance framework
- Classify data
- Define data quality standards
- Implement data monitoring
- Establish data governance structure

Month 7-8: Model Governance
- Develop model development standards
- Establish model testing procedures
- Implement model validation
- Establish model monitoring
- Create model governance structure

Month 9-10: Compliance and Operations
- Develop compliance procedures
- Implement audit procedures
- Establish incident response
- Conduct training
- Prepare for external audit

Month 11-12: Testing and Audit
- Conduct internal audit
- Remediate findings
- Prepare audit evidence
- Conduct external audit
- Achieve certification

Conclusion

This comprehensive toolkit provides all the practical resources needed for successful ISO 42001 implementation. Use these templates, checklists, and guides as starting points for your organization's implementation, customizing them to fit your specific context and requirements.

Key Success Factors:

1. Adapt templates to your organization
2. Follow the implementation sequence
3. Engage all stakeholders
4. Collect evidence systematically
5. Maintain momentum throughout implementation
6. Plan for continuous improvement