# High-Risk AI Systems Compliance Checklist

**Type:** Compliance Checklist

**Target Audience:** AI Providers, Compliance Teams, Legal

This checklist covers the seven core requirements (Articles 9-15) that high-risk AI systems must meet to be placed on the EU market. Complete all sections before deployment.

## 1. Risk Management System (Article 9)

- ☐ Establish risk management system maintained throughout AI lifecycle
- ☐ Identify and analyze known and reasonably foreseeable risks
- ☐ Evaluate risks when system is used as intended
- ☐ Evaluate risks from reasonably foreseeable misuse
- ☐ Implement appropriate risk mitigation measures
- ☐ Test system to ensure risks are eliminated or reduced
- ☐ Document all risk management activities

## 2. Data and Data Governance (Article 10)

- ☐ Training data is relevant to the intended purpose
- ☐ Training data is sufficiently representative
- ☐ Training data is free from errors to extent possible
- ☐ Training data examined for possible biases
- ☐ Appropriate data governance practices implemented
- ☐ Data collection and processing choices documented
- ☐ Personal data handling complies with GDPR

## 3. Technical Documentation (Article 11)

- ☐ Documentation created BEFORE market placement
- ☐ General description of AI system included
- ☐ Detailed design specifications documented
- ☐ Development process described
- ☐ Intended purpose clearly stated
- ☐ Reasonably foreseeable misuse described
- ☐ Explanation of how system meets all requirements

## 4. Record-Keeping / Logging (Article 12)

□ Automatic recording of events (logs) enabled
□ Logs enable traceability of system operation
□ Monitoring capability throughout lifecycle
□ Logs retained for appropriate period
□ Logs accessible for conformity assessment

## 5. Transparency and Information to Deployers (Article 13)

□ System designed for transparent operation
□ Instructions of use provided to deployers
□ Provider identity and contact information included
□ Characteristics and capabilities described
□ Limitations clearly documented
□ Required human oversight measures specified
□ Expected lifetime and maintenance requirements stated

## 6. Human Oversight (Article 14)

□ System allows effective oversight by natural persons
□ Oversight measures proportionate to risks
□ Human can understand system capabilities and limitations
□ Human can monitor system operation
□ Intervention capability enabled (stop/override)
□ Interface designed to prevent automation bias
□ "Stop" button or similar procedure available

## 7. Accuracy, Robustness, and Cybersecurity (Article 15)

□ Appropriate levels of accuracy achieved
□ Accuracy levels declared in documentation
□ System resilient against errors and inconsistencies
□ System resistant to adversarial attacks
□ Cybersecurity measures implemented
□ Redundancy/fail-safe mechanisms where appropriate

## Compliance Summary

| Requirement | Status | Notes |
|---|---|---|
| 1. Risk Management | [ ] Complete [ ] Partial [ ] Not Started | |
| 2. Data Governance | [ ] Complete [ ] Partial [ ] Not Started | |
| 3. Technical Docs | [ ] Complete [ ] Partial [ ] Not Started | |
| 4. Record-Keeping | [ ] Complete [ ] Partial [ ] Not Started | |
| 5. Transparency | [ ] Complete [ ] Partial [ ] Not Started | |
| 6. Human Oversight | [ ] Complete [ ] Partial [ ] Not Started | |
| 7. Accuracy/Security | [ ] Complete [ ] Partial [ ] Not Started | |

**AI System Name:** _______________________________

**Compliance Officer:** _________________________ **Date:** ______________

**Technical Lead:** _________________________ **Date:** ______________