AI Compliance Checklist

A Practical Guide for Technology Companies Deploying AI Systems

LAWSEL ADVISORY | WWW.THELAWSEL.COM

How to Use This Checklist

This checklist is designed for CTOs, General Counsel, and compliance leads at technology companies that build or deploy AI systems. Work through each section sequentially — earlier steps inform later ones. Items marked with [PRIORITY] should be addressed first if you are under time pressure.

---

1. AI Inventory & Classification

- [ ] **[PRIORITY] Catalogue all AI systems** currently in use, in development, or planned — including third-party and embedded AI (e.g., AI features within HR tools, CRM platforms, cybersecurity products)
- [ ] **Classify each system by risk level** using the EU AI Act's four-tier framework: unacceptable, high-risk, limited risk, minimal risk
- [ ] **Identify high-risk systems** under EU AI Act Annex III: credit scoring, employment screening, biometric identification, education assessment, critical infrastructure management
- [ ] **Document the purpose and scope** of each AI system: what decisions it influences, who is affected, and what data it processes
- [ ] **Map AI systems to applicable regulations** by jurisdiction (EU AI Act, NIST AI RMF, India AI Governance Guidelines, sector-specific laws)

---

2. Governance Structure

- [ ] **[PRIORITY] Establish a cross-functional AI governance committee** with representation from legal, compliance, risk, technology, product, and business functions
- [ ] **Assign clear ownership and accountability** for each AI system — define who is responsible for governance, monitoring, and incident response
- [ ] **Define board-level oversight mechanisms** — ensure the board receives regular reporting on AI risk, governance status, and regulatory developments
- [ ] **Create an AI acceptable use policy** that defines permitted and prohibited uses of AI within the organisation
- [ ] **Document governance processes** — even imperfect documentation is dramatically better than none (enforcement actions consistently target organisations with no documented process)

---

3. Risk Assessment & Impact Analysis

- [ ] **[PRIORITY] Conduct risk assessments** for all high-risk AI systems covering: fairness and bias, safety, privacy, transparency, and accountability
- [ ] **Perform algorithmic impact assessments** before deploying AI systems that affect access to services, employment, education, or legal rights
- [ ] **Assess third-party AI risk** — evaluate vendors and partners providing AI models or AI-powered services for governance maturity, data practices, and liability allocation
- [ ] **Evaluate cross-border regulatory exposure** — determine which jurisdictions' AI regulations apply based on where your AI systems operate and who they affect
- [ ] **Document risk tolerance and mitigation strategies** for each identified risk

4. EU AI Act Compliance (if applicable)

- [ ] **Determine your role** under the AI Act: provider, deployer, importer, distributor, or authorised representative
- [ ] **Confirm no systems fall into the "unacceptable risk" category** — these are banned outright (social scoring, manipulative AI, untargeted facial recognition scraping)
- [ ] **For high-risk systems, prepare conformity documentation**: technical documentation, risk management system, data governance measures, human oversight protocols, accuracy and robustness specifications
- [ ] **Implement transparency obligations** for limited-risk systems: disclose AI nature of chatbots, label deepfake content, flag emotion recognition systems
- [ ] **For general-purpose AI (GPAI) models**: prepare technical documentation, comply with copyright provisions, publish training data summaries
- [ ] **Note key deadlines**: GPAI rules apply August 2025; high-risk system requirements enforceable August 2026; full scope by August 2027

5. Data Governance for AI

- [ ] **Audit training data** for quality, representativeness, and potential sources of bias
- [ ] **Verify lawful basis** for processing personal data used in AI training and inference (particularly under GDPR and DPDPA)
- [ ] **Implement data lineage tracking** — document the origin, processing, and use of data throughout the AI pipeline
- [ ] **Assess cross-border data transfer requirements** for AI training data and model outputs
- [ ] **Establish data retention and deletion policies** specific to AI training datasets and model artifacts

6. Transparency & Explainability

- [ ] **Document how each AI system reaches its outputs** at a level appropriate to the risk and audience
- [ ] **Implement user-facing disclosures** where AI is used in decision-making that affects individuals
- [ ] **Create internal decision logs** that record AI-influenced decisions, the data inputs, and the rationale
- [ ] **Prepare explanations for regulators** — ensure you can articulate how high-risk systems work, what safeguards are in place, and how outcomes are monitored

7. Human Oversight & Control

- [ ] **Define human oversight requirements** for each AI system — who reviews outputs, how frequently, and with what authority to override
- [ ] **Implement escalation protocols** for AI decisions that fall outside expected parameters or confidence thresholds
- [ ] **For agentic AI systems**, implement graduated autonomy: Stage 1 (human approval required) before progressing to Stage 2 (human notification) and Stage 3 (fully autonomous)
- [ ] **Train relevant staff** on their oversight responsibilities and the limitations of the AI systems they supervise

8. Monitoring & Audit

- [ ] **Implement continuous monitoring** for model drift, bias emergence, and performance degradation
- [ ] **Schedule periodic audits** — at minimum annually, and triggered by material changes to the system, data, or regulatory environment
- [ ] **Establish incident response procedures** for AI-related failures, bias incidents, or regulatory inquiries
- [ ] **Maintain audit trails** sufficient to reconstruct AI-influenced decisions if challenged

---

9. Vendor & Third-Party AI Management

- [ ] **Conduct due diligence** on all third-party AI providers: governance practices, data handling, model transparency, liability terms
- [ ] **Include AI-specific provisions in vendor contracts**: model performance guarantees, audit rights, incident notification obligations, liability for AI outputs
- [ ] **Monitor third-party AI systems** on an ongoing basis — vendor governance is not a one-time assessment
- [ ] **Assess sub-processor chains** — understand where third-party AI models source their training data and compute

---

10. Certification & Standards

- [ ] **Evaluate ISO/IEC 42001:2023 certification** — the world's first AI-specific management system standard, increasingly required in B2B and government procurement
- [ ] **Align governance practices with NIST AI RMF** (Govern, Map, Measure, Manage) — the most widely referenced voluntary standard
- [ ] **Consider sector-specific standards** where applicable (healthcare, financial services, employment)
- [ ] **Document alignment** with chosen frameworks for investor, client, and regulatory due diligence

---

Key Deadlines

Date	Milestone
February 2025	EU AI Act: Banned AI systems prohibited
August 2025	EU AI Act: GPAI model rules apply
August 2026	EU AI Act: High-risk system requirements enforceable
August 2027	EU AI Act: Full scope applies

Next Steps

This checklist provides a starting framework. The specific requirements for your organisation will depend on your AI systems, jurisdictions, sector, and risk profile.

Lawsel Advisory helps technology companies design and implement AI governance frameworks tailored to their regulatory exposure and business objectives.

Book a consultation: www.thelawsel.com **Email**: rini@thelawsel.com

This document is for informational purposes only and does not constitute legal advice. Regulatory requirements vary by jurisdiction and are subject to change.