Back to Document Index

Compliance & Policy Alignment Checklist

Business Analysis Template for AI Projects

Template ID:	6.3
Category:	AI Governance, Risk & Compliance
Version:	1.0
Last Updated:	January 2026
Prerequisites:	AI Opportunity Assessment (1.1) High-Level AI Solution Architecture (1.3) AI Risk Assessment Report (6.1) Model Governance Framework (6.2)

1. Document Purpose

This Compliance & Policy Alignment Checklist provides a comprehensive framework for assessing AI projects against applicable laws, regulations, industry standards, organizational policies, and ethical guidelines. The checklist ensures AI initiatives meet all compliance obligations before, during, and after deployment, reducing legal, regulatory, reputational, and operational risks.

Key purposes of this checklist include:

- Systematically identify all applicable compliance requirements for AI project
- Assess project compliance status across multiple regulatory frameworks
- Document compliance evidence and gaps requiring remediation
- Create audit trail demonstrating compliance due diligence
- Align AI initiatives with organizational policies and ethical standards
- Support regulatory submissions, examinations, and audits
- Inform governance committee decisions with compliance assessment
- Prioritize compliance activities based on risk and regulatory requirements
- Enable proactive compliance management rather than reactive responses
- Provide stakeholder transparency on compliance posture

Back to Document Index

2. When to Use This Checklist

Complete this checklist at multiple points throughout the AI project lifecycle to ensure continuous compliance. Different sections may be relevant at different stages.

Key Usage Points:

Project Initiation (Planning Phase): Conduct initial compliance assessment to identify applicable regulations, assess compliance complexity, inform project planning and resource allocation, and identify early compliance risks. Complete Sections 1-3 of the checklist.

Design Phase: Assess compliance implications of proposed solution architecture, data sources, model methodology, and use cases. Identify design choices that support or hinder compliance. Complete Sections 4-6.

Development Phase: Ensure development practices align with compliance requirements (data handling, testing, documentation). Build compliance controls into models. Complete Sections 7-9.

Pre-Deployment Review: Comprehensive compliance assessment before production deployment. Verify all requirements met, documentation complete, and residual risks acceptable. Complete the entire checklist. Required governance gate.

Periodic Compliance Reviews: Quarterly or semi-annual review to ensure ongoing compliance as regulations change or model evolves. Re-complete relevant sections.

Regulatory Examination Preparation: Prepare for regulator inquiries or audits by documenting compliance status. The checklist serves as evidence of due diligence.

Post-Incident Assessment: After compliance issues or incidents, use a checklist to identify gaps and implement corrective actions.

Change Management: Assess compliance impact of material changes to model, data, or use cases. Determine if re-validation or approvals needed.

Merger/Acquisition Due Diligence: Evaluate compliance posture of AI systems being acquired or integrated.

New Regulation Adaptation: When new regulations take effect (e.g., EU AI Act enforcement), assess existing models for compliance.

3. How to Use This Checklist

Step 1: Determine Applicable Sections

Not all sections apply to every AI project. Use the following decision tree to identify relevant sections:

Back to Document Index

• Section 1 (EU AI Act): Applies if system will be deployed in EU or affects EU residents

• Section 2 (GDPR/Data Privacy): Applies if processing personal data of EU residents

• Section 3 (US Federal Regulations): Applies if operating in US or subject to US federal law

• Section 4 (Industry-Specific): Applies based on industry (financial services, healthcare, etc.)

• Section 5 (International Standards): Recommended for all projects as best practice

• Section 6 (Ethical AI): Applies to all projects

• Section 7 (Internal Policies): Applies to all projects

• Section 8 (Documentation): Applies to all projects

• Section 9 (Approval & Sign-off): Applies to all projects

Step 2: Complete Checklist

For each applicable item:

1. Status: Mark as Compliant, Partial, Not Compliant, or N/A

2. Evidence: Document how compliance is demonstrated (location of evidence)

3. Owner: Identify person responsible for this requirement

4. Due Date: For Partial or Not Compliant items, set remediation date

5. Notes: Capture additional context, exceptions, or planned actions

Step 3: Assess Overall Compliance

After completing checklist, assess overall compliance posture:

• Fully Compliant: All applicable items marked Compliant or N/A - ready for deployment

• Substantially Compliant: >90% compliant, minor gaps with remediation plan - conditional approval

Back to Document Index

• Partially Compliant: 70-90% compliant, significant gaps - deployment blocked pending remediation

• Non-Compliant: <70% compliant - major remediation required before deployment

Step 4: Create Remediation Plan

For any items marked Partial or Not Compliant:

• Document specific gap or deficiency

• Define remediation actions required

• Assign clear ownership

• Set realistic target dates

• Prioritize based on regulatory risk

• Track remediation progress

Step 5: Obtain Required Approvals

Based on compliance assessment results, obtain appropriate sign-offs:

• Compliance/Legal review and approval

• Privacy Officer approval (if processing personal data)

• Governance committee approval (based on risk tier)

• Document all approvals and conditions

Back to Document Index

4. Compliance Checklist

Section 1: EU AI Act Compliance

Applicability: Complete this section if the AI system will be placed on the EU market, put into service in the EU, or outputs are used in the EU, regardless of where the provider is located.

1.1 Risk Classification Assessment

Determine AI system risk classification per EU AI Act:

☐ Prohibited AI System: System falls under Article 5 prohibited practices
Examples: Social scoring by governments, real-time biometric identification in public spaces (with exceptions), exploitation of vulnerabilities, subliminal manipulation

☐ High-Risk AI System: System listed in Annex III or is safety component per Annex I/II
Examples: Biometric identification/categorization, critical infrastructure, education/training access, employment/HR, essential services (credit scoring, emergency response), law enforcement, migration/border control, justice systems

☐ Limited Risk AI System: Transparency obligations apply
Examples: Chatbots, emotion recognition, biometric categorization, deepfakes, AI-generated content

☐ Minimal Risk AI System: No specific obligations beyond general law
Examples: AI-enabled video games, spam filters, inventory optimization

Evidence: Document risk classification determination and rationale

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

1.2 High-Risk System Requirements (if applicable)

If classified as High-Risk, verify compliance with all requirements:

☐ Risk management system established (Article 9) - documented process for identifying, analyzing, and mitigating risks

☐ Data governance measures implemented (Article 10) - training/validation data quality, relevance, representativeness

Back to Document Index

☐ Technical documentation prepared (Article 11, Annex IV) - comprehensive documentation per Annex IV requirements

☐ Record-keeping capabilities (Article 12) - automatic logging of events, ability to provide logs to authorities

☐ Transparency and user information (Article 13) - clear, adequate information for deployers and users

☐ Human oversight measures (Article 14) - appropriate human-in-the-loop or on-the-loop controls

☐ Accuracy, robustness, cybersecurity (Article 15) - appropriate levels of accuracy, resilience to errors/attacks

☐ Quality management system (Article 17) - documented QMS ensuring compliance throughout lifecycle

☐ Conformity assessment completed (Article 43) - required conformity assessment procedure conducted

☐ CE marking affixed (Article 49) - CE marking applied before placing on market

☐ EU Declaration of Conformity prepared (Article 47) - declaration of conformity drawn up and retained

☐ Registration in EU database (Article 71) - system registered in EU database before market placement

☐ Post-market monitoring system (Article 72) - plan for collecting and analyzing data on performance

Evidence: Conformity assessment documentation, CE marking, EU database registration confirmation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

1.3 Transparency Obligations (for certain systems)

☐ Users informed when interacting with AI system (e.g., chatbot disclosure)

☐ Emotion recognition systems - users informed before processing

☐ Biometric categorization - individuals informed before processing

☐ AI-generated content labeled as such (deepfakes, synthetic media)

☐ Text/audio content disclosure - if manipulated, users informed

Back to Document Index

Evidence: User interface screenshots, disclosure language, labeling procedures

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

1.4 General Purpose AI (GPAI) Models (if applicable)

☐ Technical documentation prepared (Article 53)

☐ Information provided to downstream providers

☐ Copyright compliance policy in place (Article 53(1)(c))

☐ Training content summary publicly available

☐ If systemic risk: model evaluation, adversarial testing, incident tracking (Article 55)

Evidence: GPAI model documentation, copyright policy, public content summary

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 2: GDPR and Data Privacy Compliance

Applicability: Complete processing of personal data of individuals in the EU/EEA, regardless of organization location.

2.1 Lawful Basis for Processing

☐ Lawful basis identified for processing personal data (Article 6)

- ☐ Consent (freely given, specific, informed, unambiguous)
- ☐ Contract performance
- ☐ Legal obligation
- ☐ Vital interests
- ☐ Public task
- ☐ Legitimate interests (balance test conducted)

☐ Special category data: additional lawful basis under Article 9 (if applicable)

☐ Lawful basis documented and communicated to data subjects

Evidence: Legal basis analysis, consent mechanisms, privacy notices

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

2.2 Data Protection Principles

☐ Lawfulness, fairness, transparency - processing is lawful, fair, and transparent to data subjects

☐ Purpose limitation - data collected for specified, explicit, legitimate purposes only

☐ Data minimization - adequate, relevant, and limited to what is necessary

☐ Accuracy - data is accurate and kept up to date; inaccurate data corrected or deleted

☐ Storage limitation - kept only as long as necessary for purposes

☐ Integrity and confidentiality - appropriate security measures in place

☐ Accountability - organization can demonstrate compliance with principles

Evidence: Data flow mapping, retention policies, security controls documentation

Back to Document Index

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

2.3 Data Subject Rights

☐ Right to be informed - privacy notices provided, clear and accessible

☐ Right of access - procedures for data subjects to access their data

☐ Right to rectification - process for correcting inaccurate data

☐ Right to erasure ("right to be forgotten") - process for deletion requests

☐ Right to restrict processing - ability to limit processing in certain circumstances

☐ Right to data portability - can provide data in structured, machine-readable format

☐ Right to object - data subjects can object to processing (including automated decisions)

☐ Rights related to automated decision-making - safeguards for automated decisions with legal/significant effects

☐ Response procedures established - documented process to respond within 30 days

Evidence: Privacy notice, data subject request procedures, response templates

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

2.4 Data Protection Impact Assessment (DPIA)

☐ DPIA requirement assessed - determined if required based on risk criteria

☐ If required: DPIA conducted and documented (Article 35)

☐ DPIA includes: description of processing, necessity/proportionality assessment, risk assessment, mitigation measures

☐ Data Protection Officer consulted (if appointed)

☐ If high residual risk: supervisory authority consulted before processing (Article 36)

☐ DPIA reviewed and updated when changes occur to processing

Evidence: DPIA document, supervisory authority consultation records (if applicable)

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

2.5 Security and Breach Requirements

☐ Appropriate technical and organizational security measures implemented

Back to Document Index

☐ Encryption in transit and at rest (where appropriate)

☐ Access controls and authentication

☐ Pseudonymization or anonymization considered

☐ Regular security testing and assessment

☐ Data breach notification procedures established

☐ Ability to detect, investigate, and report breaches within 72 hours to supervisory authority

☐ Data processor agreements in place (Article 28) with all processors

Evidence: Security controls documentation, processor agreements, breach response plan

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

2.6 International Data Transfers

☐ All international transfers identified and documented

☐ Transfer mechanism in place (adequacy decision, Standard Contractual Clauses, BCRs, or derogation)

☐ If using SCCs: appropriate SCC template selected and executed

☐ Transfer Impact Assessment (TIA) conducted for transfers to non-adequate countries

☐ Supplementary measures implemented if required by TIA

Evidence: Data transfer inventory, SCCs, Transfer Impact Assessment

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 3: US Federal Regulations

Applicability: Complete if operating in the United States or subject to US federal law.

3.1 Executive Order on AI (EO 14110)

☐ Safety and security standards considered for AI systems

☐ If using foundation models: red-team testing conducted for CBRN risks (if applicable)

☐ Watermarking for AI-generated content implemented (if creating synthetic content)

☐ Privacy-preserving techniques considered in AI development

☐ Equity and civil rights considerations assessed

Evidence: Safety testing documentation, watermarking implementation, equity assessment

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

3.2 Federal Trade Commission (FTC) Guidance

☐ Claims about AI capabilities are truthful and not deceptive

☐ Algorithmic bias does not result in discriminatory outcomes

☐ Consumer data used for AI training obtained lawfully

☐ Appropriate data security measures in place

☐ Transparency regarding AI use in consumer-facing applications

☐ If making automated decisions: fairness and accuracy validated

Evidence: Marketing materials review, bias testing results, data collection notices

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

3.3 Equal Employment Opportunity Commission (EEOC)

Applies to: AI systems used in employment decisions (hiring, promotion, termination)

☐ AI tool does not discriminate based on protected characteristics (race, color, religion, sex, national origin, age, disability)

☐ Adverse impact analysis conducted

Back to Document Index

☐ If disparate impact found: business necessity justified and no less discriminatory alternative exists

☐ Reasonable accommodations available for individuals with disabilities

☐ Testing and validation conducted before deployment

☐ Ongoing monitoring for discriminatory patterns

Evidence: Adverse impact analysis, fairness testing, reasonable accommodation procedures

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

3.4 State-Level AI Regulations

Note: Multiple US states have enacted or proposed AI-specific laws. Review requirements for states where operating.

☐ California (if applicable): Consumer Privacy Act (CCPA/CPRA) compliance for automated decision-making

☐ Colorado (if applicable): AI Act compliance for high-risk systems

☐ Illinois (if applicable): Biometric Information Privacy Act (BIPA) compliance

☐ New York City (if applicable): Automated Employment Decision Tools (AEDT) law compliance

☐ Other state laws reviewed and compliance assessed

Evidence: State-specific compliance documentation, bias audit reports (NYC), BIPA consent (IL)

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 4: Industry-Specific Regulations

4.1 Financial Services

Applicability: AI systems used in banking, lending, insurance, investment, or other financial services

☐ Model Risk Management (SR 11-7 or equivalent) - comprehensive model risk management framework

☐ Independent model validation conducted by qualified validators

☐ Model inventory maintained with all production models

☐ Fair lending laws compliance - Equal Credit Opportunity Act (ECOA), Fair Housing Act

☐ Adverse action notices provided when credit denied or terms less favorable

☐ Explanation of decision factors available to consumers

☐ Fair Credit Reporting Act (FCRA) compliance if using consumer reports

☐ Bank Secrecy Act / Anti-Money Laundering compliance if used for AML/KYC

☐ If insurance: compliance with state insurance regulations on algorithmic underwriting

☐ Consumer Financial Protection Bureau (CFPB) guidance reviewed

☐ Stress testing and scenario analysis for material models

☐ Third-party risk management for vendor models or data

Evidence: Model validation reports, fair lending testing, adverse action notice templates, MRM policy

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

4.2 Healthcare

Applicability: AI systems used in healthcare delivery, medical devices, clinical decision support, or processing protected health information

☐ HIPAA Privacy Rule compliance - protected health information (PHI) safeguards

☐ HIPAA Security Rule compliance - administrative, physical, technical safeguards for ePHI

Back to Document Index

☐ Business Associate Agreements (BAA) with all entities accessing PHI

☐ Minimum necessary standard applied - only minimum PHI needed

☐ If medical device: FDA regulatory pathway determined (510(k), PMA, or exempt)

☐ If Software as Medical Device (SaMD): FDA guidance followed

☐ Clinical validation conducted demonstrating safety and effectiveness

☐ Good Machine Learning Practice (GMLP) principles applied

☐ Algorithm change protocol if continuous learning

☐ Clinical decision support transparency - clinician understands AI role

☐ Patient safety monitoring and adverse event reporting

☐ If used for diagnosis/treatment: appropriate clinical oversight

Evidence: HIPAA compliance documentation, BAAs, FDA submissions (if applicable), clinical validation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

4.3 Government/Public Sector

☐ Algorithmic accountability requirements met (if applicable to jurisdiction)

☐ Impact assessment for automated decision systems completed

☐ Public notice and comment process followed (if required)

☐ Transparency reporting on AI system use

☐ Procurement regulations compliance for AI acquisition

☐ Due process safeguards for decisions affecting individual rights

☐ Human review and override capabilities

☐ Accessibility requirements (Section 508, ADA) met

Evidence: Impact assessment, public notices, accessibility testing, procurement documentation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

4.4 Education

☐ Family Educational Rights and Privacy Act (FERPA) compliance for student data

☐ Children's Online Privacy Protection Act (COPPA) compliance if collecting data from children under 13

☐ Bias assessment for educational assessments or admissions

☐ Transparency to students/parents about AI use in educational decisions

☐ Accessibility for students with disabilities

☐ Vendor agreements include data privacy protections

Evidence: FERPA compliance documentation, COPPA consent mechanisms, bias testing

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 5: International Standards and Frameworks

Applicability: While not legally binding, these standards represent industry best practices and may be referenced in regulations or contracts. Recommended for all AI projects.

5.1 ISO/IEC AI Standards

☐ ISO/IEC 42001:2023 (AI Management System) - management system approach considered

☐ ISO/IEC 23894:2023 (AI Risk Management) - risk management principles applied

☐ ISO/IEC 22989:2022 (AI Concepts and Terminology) - consistent terminology used

☐ ISO/IEC 23053:2022 (AI Framework for using ML) - ML framework principles considered

☐ ISO/IEC 38507:2022 (Governance of IT - AI) - governance implications assessed

Evidence: Documentation referencing ISO standards, gap analysis, implementation evidence

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

5.2 NIST AI Risk Management Framework

☐ AI RMF Core Functions addressed: Govern, Map, Measure, Manage

☐ Trustworthy characteristics considered: Valid/Reliable, Safe, Secure/Resilient, Accountable/Transparent, Explainable/Interpretable, Privacy-Enhanced, Fair

☐ Risk mapping conducted identifying context, categorizing AI system, mapping risks

☐ Risks measured using appropriate tools and methods

☐ Risk management strategies documented and implemented

Evidence: AI RMF implementation documentation, risk mapping, measurement results

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

5.3 IEEE Standards for Ethical AI

☐ IEEE 7000 (Model Process for Addressing Ethical Concerns) - ethical values identified and addressed

☐ IEEE 7010 (Wellbeing Impact Assessment) - wellbeing impact considered

Back to Document Index

☐ IEEE 2700 series (Data Privacy) - privacy considerations embedded

☐ Transparency and accountability mechanisms implemented

Evidence: Ethical values documentation, wellbeing assessment, transparency mechanisms

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

5.4 OECD AI Principles

☐ AI should benefit people and planet (inclusive growth, sustainable development, well-being)

☐ AI systems should be designed to respect rule of law, human rights, democratic values, diversity

☐ Transparency and responsible disclosure about AI systems

☐ AI systems should function robustly, securely, and safely throughout lifecycle

☐ Organizations deploying AI should be accountable for proper functioning

Evidence: Benefit assessment, human rights impact assessment, accountability documentation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 6: Ethical AI Guidelines

Applicability: All AI projects should consider ethical implications

6.1 Fairness and Non-Discrimination

☐ Bias assessment conducted across demographic groups (race, gender, age, disability)

☐ Fairness metrics defined and measured (demographic parity, equal opportunity, predictive parity)

☐ Training data assessed for representation and historical bias

☐ Fairness testing conducted in realistic deployment conditions

☐ If bias detected: mitigation strategies implemented (data rebalancing, algorithmic fairness, human review)

☐ Ongoing fairness monitoring in production

☐ Disparate impact reviewed and justified (if exists)

Evidence: Bias assessment report, fairness testing results, monitoring dashboards

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

6.2 Transparency and Explainability

☐ Stakeholders informed that AI is being used in decision process

☐ Purpose and capabilities of AI system clearly communicated

☐ Limitations and potential errors disclosed

☐ Explanation of how AI makes decisions available (appropriate to audience)

☐ Model interpretability techniques used (SHAP, LIME, attention mechanisms) where needed

☐ Decision factors disclosed to affected individuals

☐ Model documentation available to appropriate stakeholders

Evidence: Disclosure language, explanation mechanisms, model card, stakeholder communications

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

6.3 Human Oversight and Control

☐ Appropriate level of human oversight defined based on risk

☐ Human-in-the-loop (HITL) for high-stakes decisions

☐ Human-on-the-loop (HOTL) monitoring for automated decisions

☐ Human-in-command maintains overall control

☐ Humans can override AI decisions

☐ Emergency stop/pause capabilities for critical systems

☐ Escalation procedures for uncertain or high-risk cases

☐ Training provided to humans overseeing AI system

Evidence: Human oversight procedures, override mechanisms, training materials, escalation protocols

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

6.4 Privacy and Data Protection

☐ Privacy by design principles applied from inception

☐ Data minimization - only necessary data collected and used

☐ Purpose limitation - data used only for specified purposes

☐ Consent obtained where required (informed, specific, freely given)

☐ Privacy-enhancing technologies considered (differential privacy, federated learning, homomorphic encryption)

☐ De-identification or anonymization applied where possible

☐ Individual privacy rights respected (access, correction, deletion)

☐ Privacy impact assessed and documented

Evidence: Privacy by design documentation, data minimization justification, consent mechanisms, PETs implementation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

6.5 Safety and Security

☐ Safety risks identified and assessed (potential for harm)

☐ Safety testing conducted before deployment

☐ Robustness testing - performance under edge cases and adversarial conditions

☐ Security measures to prevent unauthorized access or manipulation

☐ Adversarial testing conducted

☐ Model security - protection against model theft, poisoning, inference attacks

☐ Incident response plan for AI failures or security breaches

☐ Continuous monitoring for safety and security issues

Evidence: Safety assessment, robustness testing, adversarial testing, security controls, incident response plan

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

6.6 Accountability and Responsibility

☐ Clear accountability established for AI system outcomes

☐ Roles and responsibilities documented (owner, developer, operator)

☐ Governance structure in place with oversight committee

☐ Audit trails maintained for key decisions and changes

☐ Performance metrics tracked and reported

☐ Mechanism for redress if AI causes harm

☐ Regular reviews and assessments conducted

☐ Lessons learned captured and applied to future systems

Evidence: Governance documentation, RACI matrix, audit logs, performance reports, redress procedures

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 7: Internal Organizational Policies

Applicability: All AI projects must comply with internal organizational policies

7.1 AI Governance Policies

☐ AI Governance Framework requirements met (Template 6.2)

☐ Model risk tier determined and documented

☐ Appropriate governance gates completed for risk tier

☐ Required approvals obtained (Model Risk Committee, AI Governance Committee)

☐ Model registered in organizational model inventory

☐ Lifecycle stage documented and governance requirements met

☐ Change management procedures followed

Evidence: Governance approvals, model inventory registration, lifecycle documentation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

7.2 Data Governance Policies

☐ Data sourcing complies with data governance policies

☐ Data classification requirements met (confidential, restricted, public)

☐ Data quality standards met

☐ Data lineage documented

☐ Data retention policies followed

☐ Data access controls appropriate for sensitivity

☐ Data sharing agreements in place for third-party data

Evidence: Data governance approvals, data quality reports, lineage documentation, access logs

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

7.3 Information Security Policies

☐ Security classification determined

Back to Document Index

☐ Security requirements defined and met

☐ Security assessment/review completed

☐ Penetration testing conducted (if required)

☐ Access controls meet security standards

☐ Encryption requirements met

☐ Logging and monitoring per security policy

☐ Vulnerability management procedures followed

☐ Security incident response plan includes AI system

Evidence: Security assessment report, penetration testing results, security controls documentation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

7.4 Responsible AI Policy

☐ Responsible AI principles acknowledged and applied

☐ Ethics review conducted (if required by policy)

☐ Responsible AI assessment completed

☐ Use case aligns with organizational values

☐ Potential negative impacts assessed and mitigated

☐ Stakeholder concerns addressed

Evidence: Ethics review documentation, responsible AI assessment, stakeholder consultation

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

7.5 Procurement and Vendor Management

☐ If using third-party AI: vendor assessment completed

☐ Vendor contracts include appropriate AI/data provisions

☐ Service Level Agreements (SLAs) defined

☐ Vendor compliance with applicable regulations verified

Back to Document Index

☐ Vendor risk assessment completed

☐ Data Processing Agreement in place (if vendor processes personal data)

☐ Exit strategy and data portability considered

Evidence: Vendor assessment, contracts, SLAs, vendor compliance attestations

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 8: Documentation Requirements

Applicability: All AI projects require comprehensive documentation

8.1 Business Documentation

☐ AI Opportunity Assessment completed (Template 1.1)

☐ Business case with ROI analysis

☐ Stakeholder analysis

☐ Use case documentation

☐ Success criteria and KPIs defined

☐ Implementation plan

☐ Communication plan

Evidence: Templates 1.1, business case, stakeholder register, implementation plan

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

8.2 Technical Documentation

☐ High-Level AI Solution Architecture (Template 1.3)

☐ Model development documentation (algorithm, methodology, assumptions)

☐ Data requirements and sources

☐ Feature engineering documentation

☐ Model training and tuning procedures

☐ Testing results (accuracy, performance, bias)

☐ Model limitations and constraints

☐ Version control and change history

☐ Deployment architecture

☐ Integration documentation

☐ API documentation (if applicable)

Back to Document Index

Evidence: Architecture documents, model documentation, testing reports, deployment guides

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

8.3 Risk and Compliance Documentation

☐ AI Risk Assessment Report (Template 6.1)

☐ Model Governance Framework compliance (Template 6.2)

☐ This Compliance & Policy Alignment Checklist (Template 6.3)

☐ Model validation report

☐ Data Protection Impact Assessment (if applicable)

☐ Privacy Impact Assessment

☐ Security assessment

☐ Bias and fairness assessment

☐ Regulatory compliance documentation

☐ Audit trail and decision log

Evidence: Templates 6.1-6.3, validation reports, impact assessments, audit logs

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

8.4 Operational Documentation

☐ User guides and training materials

☐ Operational runbooks

☐ Monitoring and alerting procedures

☐ Incident response procedures

☐ Maintenance and support procedures

☐ Performance dashboards

☐ Troubleshooting guides

☐ Rollback procedures

Back to Document Index

Evidence: User guides, runbooks, monitoring dashboards, incident response plan

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

8.5 Stakeholder-Facing Documentation

☐ Model Card for transparency (High/Critical risk systems)

☐ Privacy notices/disclosures

☐ Terms of service or user agreements

☐ Stakeholder communication materials

☐ Training and enablement materials

☐ FAQ and help documentation

Evidence: Model card, privacy notices, user agreements, training materials

Owner: _____ Status: ☐ Compliant ☐ Partial ☐ Not Compliant ☐ N/A

Back to Document Index

Section 9: Required Approvals and Sign-off

Applicability: All AI projects require formal approvals before deployment

9.1 Compliance Review and Approval

☐ Compliance Officer Review
Reviewer Name: _____
Review Date: _____
Status: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

☐ Legal Counsel Review
Reviewer Name: _____
Review Date: _____
Status: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

☐ Privacy Officer Review (if processing personal data)
Reviewer Name: _____
Review Date: _____
Status: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

☐ Information Security Review
Reviewer Name: _____
Review Date: _____
Status: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

9.2 Governance Approval

☐ Model Risk Manager Approval
Approver Name: _____
Approval Date: _____
Status: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

☐ Model Risk Committee Approval (Medium/High/Critical risk)
Approval Date: _____
Committee Decision: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

Back to Document Index

☐ AI Governance Committee Approval (High/Critical risk)
Approval Date: _____
Committee Decision: ☐ Approved ☐ Approved with Conditions ☐ Rejected
Conditions/Comments: _____

☐ Board Notification (Critical risk with significant strategic impact)
Notification Date: _____
Board Response: _____

9.3 Business Owner Sign-off

I confirm that:
• All applicable compliance requirements have been assessed
• Required documentation is complete and accurate
• Identified compliance gaps have remediation plans with target dates
• Residual risks are understood and acceptable
• The AI system is ready for deployment subject to approvals

Model Owner Name: _____
Signature: _____
Date: _____

Business Unit Leader Name: _____
Signature: _____
Date: _____

Back to Document Index

5. Best Practices for Compliance Management

1. Start Early and Integrate Throughout Lifecycle

Begin compliance assessment during project initiation, not before deployment. Integrate compliance into design, development, and testing. Early assessment prevents costly late-stage remediation and ensures compliance is built-in.

2. Maintain a Compliance Matrix

Create and maintain a compliance requirements matrix mapping each applicable regulation/standard to specific project controls and evidence. This provides clear traceability and simplifies audits. Update as regulations evolve.

3. Engage Compliance Early and Often

Involve compliance, legal, and privacy teams from project inception. Regular touchpoints prevent surprises and enable proactive issue resolution. Compliance should be a partner, not a gatekeeper.

4. Document Everything

Comprehensive documentation is essential for demonstrating compliance. Document decisions, rationale, testing, controls, and remediation actions. If not documented, it didn't happen from a compliance perspective.

5. Prioritize Based on Risk

Focus compliance efforts on highest-risk requirements first. Not all requirements carry equal regulatory risk. Allocate resources proportionately based on potential impact of non-compliance.

6. Create Reusable Compliance Artifacts

Develop templates, checklists, and standard procedures that can be reused across AI projects. This accelerates compliance assessment, ensures consistency, and captures organizational learning.

7. Stay Current with Regulations

AI regulations are evolving rapidly. Monitor regulatory developments in applicable jurisdictions, participate in industry forums, engage with legal counsel. Build time into projects for regulation adaptation.

8. Conduct Regular Compliance Reviews

Compliance is not a one-time gate but an ongoing obligation. Conduct quarterly or semi-annual reviews to ensure continued compliance as models, data, uses, or regulations change.

Back to Document Index

9. Build Compliance into Culture

Foster organizational culture where compliance is valued, not viewed as an obstacle. Train teams on the importance of compliance, celebrate compliance successes, and learn from failures. Leadership tone matters.

10. Prepare for Audits and Examinations

Maintain organized compliance documentation assuming regulatory examination. Create audit-ready documentation packages. Conduct periodic internal compliance audits to identify and remediate gaps proactively.

11. Leverage Automation

Automate compliance checking where possible (bias testing, privacy analysis, documentation generation). Automation ensures consistency, scalability, and frees human expertise for judgment tasks.

12. Learn from Others' Mistakes

Monitor AI compliance incidents and enforcement actions in your industry. Learn from others' compliance failures. Adapt your compliance program based on observed patterns.

Back to Document Index

6. Common Compliance Pitfalls to Avoid

1. Compliance as Afterthought

Treating compliance as a box-checking exercise before deployment rather than integrated throughout the lifecycle. Results in rushed assessments, incomplete documentation, deployment delays, and increased risk of non-compliance.

2. Over-Reliance on Legal/Compliance Team

Believing compliance is solely the responsibility of legal/compliance teams. In reality, model owners, developers, and business stakeholders must understand and own compliance. Legal/compliance provide guidance, not execution.

3. Incomplete Regulatory Landscape Assessment

Missing applicable regulations because assessment was too narrow. AI may trigger regulations across data privacy, consumer protection, employment, industry-specific, and emerging AI-specific laws. Cast a wide net.

4. Superficial Compliance Assessment

Checking boxes without substantive evaluation. For example, marking "bias testing conducted" without rigorous testing across demographic groups. Regulators and auditors look for evidence, not checkmarks.

5. Ignoring State and Local Regulations

Focusing only on federal regulations while missing state/local requirements. Many US states and cities have AI-specific laws. Multi-jurisdictional compliance requires awareness of all applicable levels.

6. Documentation Gaps

Inadequate documentation of compliance analysis, testing, controls, and decisions. When regulators or auditors request evidence, documentation gaps appear as non-compliance even if requirements were actually met.

7. Static Compliance Assessment

Completing compliance checklist once and never revisiting. Regulations change, models evolve, use cases expand. Compliance requires ongoing assessment and adaptation.

8. Assuming International Operations Are Compliant

Believing compliance with one jurisdiction's regulations (e.g., US) satisfies all requirements. International regulations like GDPR and EU AI Act have extraterritorial reach and different requirements.

Back to Document Index

9. Underestimating Remediation Time

Not allowing sufficient time in the project plan for compliance remediation. Some remediation (e.g., model retraining for bias, implementing differential privacy) takes months. Plan accordingly.

10. No Escalation Path for Issues

When compliance concerns arise, there is no clear path to raise issues or get decisions. Concerns languish unresolved. Establish clear escalation procedures with timely response requirements.

11. Treating Compliance as Negotiable

Viewing compliance requirements as suggestions that can be compromised to meet timelines or budgets. Non-compliance carries legal, financial, and reputational risks that far exceed project constraints.

12. Ignoring Third-Party Risk

Not assessing compliance of third-party data, models, or platforms. Organization remains liable even when using vendors. Vendor contracts must include compliance obligations with audit rights.

Back to Document Index

7. Appendices

Appendix A: Compliance Status Summary Template

Use this template to summarize overall compliance assessment:

PROJECT: _____
ASSESSMENT DATE: _____
ASSESSOR: _____

REGULATORY SCOPE:
☐ EU AI Act ☐ GDPR ☐ US Federal ☐ Financial Services ☐ Healthcare
☐ Government ☐ Education ☐ Other: _____

COMPLIANCE SUMMARY:
Section 1 (EU AI Act): ___% compliant (___ of ___ applicable items)
Section 2 (GDPR): ___% compliant (___ of ___ applicable items)
Section 3 (US Federal): ___% compliant (___ of ___ applicable items)
Section 4 (Industry): ___% compliant (___ of ___ applicable items)
Section 5 (Standards): ___% compliant (___ of ___ applicable items)
Section 6 (Ethical AI): ___% compliant (___ of ___ applicable items)
Section 7 (Internal): ___% compliant (___ of ___ applicable items)
Section 8 (Documentation): ___% compliant (___ of ___ applicable items)

OVERALL COMPLIANCE: ___% (___ of ___ applicable items across all sections)

COMPLIANCE POSTURE:
☐ Fully Compliant (>95%) - Ready for deployment
☐ Substantially Compliant (90-95%) - Minor gaps, conditional approval
☐ Partially Compliant (70-89%) - Significant gaps, deployment blocked
☐ Non-Compliant (<70%) - Major remediation required

CRITICAL GAPS (Must remediate before deployment):
1. _____
2. _____
3. _____

REMEDIATION PLAN:
Gap #1: _____
  Action: _____
  Owner: _____
  Due Date: _____

Back to Document Index

[Continue for each critical gap]

APPROVALS REQUIRED:
☐ Compliance Officer
☐ Legal Counsel
☐ Privacy Officer
☐ Information Security
☐ Model Risk Manager
☐ Model Risk Committee
☐ AI Governance Committee

OVERALL RECOMMENDATION:
☐ Approve for deployment
☐ Approve with conditions (specify): _____
☐ Reject - remediation required

Appendix B: Sample Compliance Evidence Documentation

Examples of acceptable evidence for common compliance requirements:

Requirement: Bias testing conducted

Acceptable Evidence:
• Bias testing report showing performance metrics by demographic group
• Statistical analysis (disparate impact ratios, demographic parity differences)
• Testing methodology documentation
• Mitigation actions taken for identified bias
• Validation of fairness post-mitigation

Requirement: Privacy Impact Assessment completed

Acceptable Evidence:
• Completed Privacy Impact Assessment document
• Privacy risk identification and assessment
• Mitigation strategies for privacy risks
• Sign-off from Privacy Officer
• Evidence of privacy-by-design implementation

Requirement: Human oversight implemented

Acceptable Evidence:
• Human oversight procedures documentation
• User interface showing human review workflow
• Override capability demonstration
• Training materials for human reviewers
• Logs showing human interventions

Back to Document Index

Requirement: Transparency disclosures provided

Acceptable Evidence:
• Screenshots of user interface with AI disclosure
• Privacy notice including AI processing description
• Model card or algorithmic transparency document
• User testing showing disclosures are understood
• Approved disclosure language

Appendix C: Professional Standards Alignment

This Compliance & Policy Alignment Checklist aligns with industry standards:

BABOK (Business Analysis Body of Knowledge) Alignment:

• Requirements Analysis and Design Definition (3.2-3.4): Ensuring requirements include compliance obligations
• Solution Evaluation (6): Evaluating solution compliance with regulations and policies
• Compliance Analysis: Assessing alignment with regulatory requirements
• Risk Analysis and Management (10.5): Identifying and managing compliance risks

PMBOK (Project Management Body of Knowledge) Alignment:

• Project Compliance Management: Ensuring project meets legal and regulatory requirements
• Risk Management (11): Compliance risk identification and mitigation
• Quality Management (8): Ensuring deliverables meet compliance standards
• Stakeholder Management (13): Engaging compliance stakeholders

DMBOK (Data Management Body of Knowledge) Alignment:

• Data Governance (3): Governance of data used in AI systems
• Data Security (7): Security compliance for data protection
• Data Quality (13): Ensuring data meets compliance quality standards
• Regulatory Compliance: Managing data to meet regulations

AI-Specific Standards and Frameworks:

• EU AI Act: Comprehensive compliance checklist
• GDPR: Data protection and privacy compliance
• NIST AI Risk Management Framework: Risk-based compliance approach
• ISO/IEC 42001 (AI Management System): Management system compliance
• ISO/IEC 23894 (AI Risk Management): Risk management standards
• OECD AI Principles: Ethical AI compliance
• IEEE Standards: Ethical considerations in AI

Back to Document Index

Document Usage Rights and Disclaimer

This Business Analysis Template for AI Projects is provided as a starter document to assist business analysts in assessing organizational readiness for AI adoption.

Usage Rights:

✓ You may freely use, modify, and customize this template for your projects

✓ You may adapt the readiness assessment framework to fit your needs

✓ You may incorporate this into your organizational assessment processes

✓ You may share this template within your organization

Restrictions:

✗ You may not resell, redistribute, or commercialize this template

✗ You may not claim original authorship of this framework

✗ You may not remove these usage rights statements

Disclaimer:

This template is provided as-is without warranties. While it incorporates professional best practices for readiness assessment and organizational change management, users are responsible for adapting methods to their specific context. The template should be customized based on your unique needs and validated with appropriate subject matter experts including change management professionals, organizational development specialists, and business leaders. Readiness assessment requires understanding of both technical capabilities and organizational dynamics.