COMPLIANCE TESTING CHECKLIST

Pre-Launch AI System Compliance Verification

BlackIndian AI Professional Framework Version 1.0 | December 2025 Read Time: 8 minutes

TABLE OF CONTENTS

1. HOW TO USE THIS CHECKLIST

Purpose

This checklist ensures your AI system meets regulatory requirements before launch. Use it as:

- **Pre-launch verification** (complete before production deployment)
- **Audit preparation** (demonstrate compliance to regulators)
- **Gap analysis** (identify missing compliance elements)

Instructions

For Each Item:

- ✅ **Compliant** - Requirement met, evidence documented
- ⚠️ **Partial** - Requirement partially met, gaps exist
- ❌ **Non-Compliant** - Requirement not met
- ⊗ **N/A** - Not applicable to this system

Required for Launch:

- All applicable items must be ✅ or ⊗
- No ❌ items allowed
- ⚠️ items require documented remediation plan with timeline

2. GDPR COMPLIANCE (EU DATA PROTECTION)

Applies If: Processing personal data of EU residents

Article 5: Principles of Processing

#	Requirement	Status	Evidence	Notes
2.1	**Lawfulness, Fairness, Transparency** Legal basis for processing identified (consent, contract, legitimate interest, etc.)	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Legal basis: _____
2.2	**Purpose Limitation** Data used only for specified, explicit purposes	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Purpose documented: ☐ Yes ☐ No
2.3	**Data Minimization** Only necessary data collected and processed	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Data minimization review completed: ☐ Yes ☐ No
2.4	**Accuracy** Mechanisms to ensure data accuracy and enable corrections	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Correction process: ☐ Implemented
2.5	**Storage Limitation** Retention periods defined and enforced	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Retention period: _____ days/years
2.6	**Integrity & Confidentiality** Appropriate security measures implemented	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Security testing completed: ☐ Yes ☐ No

Article 13-14: Transparency & Information

#	Requirement	Status	Evidence	Notes
2.7	**Privacy Notice** Clear privacy policy provided to users	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	URL: _____	Last updated: _____
2.8	**AI Disclosure** Users informed that AI is processing their data	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Location: _____	Clear and prominent: ☐ Yes ☐ No
2.9	**Purpose Disclosure** Specific purposes of AI processing explained	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Reference: _____	Understandable to layperson: ☐ Yes ☐ No
2.10	**Contact Information** Data controller contact info provided	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Email: _____	DPO appointed: ☐ Yes ☐ No ☐ N/A

Article 15-22: Data Subject Rights

#	Requirement	Status	Evidence	Notes
2.11	**Right of Access (Article 15)** Users can request their data	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Response time: _____ days
2.12	**Right to Rectification (Article 16)** Users can correct inaccurate data	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Correction mechanism: ☐ Automated ☐ Manual
2.13	**Right to Erasure (Article 17)** Users can request data deletion	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Deletion verified: ☐ Yes ☐ No
2.14	**Right to Data Portability (Article 20)** Users can export their data	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Export format: _____	Tested: ☐ Yes ☐ No
2.15	**Right to Object (Article 21)** Users can object to processing	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Objection honored: ☐ Yes ☐ No
2.16	**Right to Human Review (Article 22)** Users can request human review of automated decisions	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Human-in-the-loop: ☐ Yes ☐ No

Article 32: Security of Processing

#	Requirement	Status	Evidence	Notes
2.17	**Encryption at Rest** Personal data encrypted when stored	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Algorithm: _____	Tested: ☐ Yes ☐ No
2.18	**Encryption in Transit** Personal data encrypted during transmission	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Protocol: _____	TLS 1.2+: ☐ Yes ☐ No
2.19	**Access Controls** Role-based access to personal data	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	System: _____	Least privilege: ☐ Yes ☐ No
2.20	**Audit Logging** All personal data access logged	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Retention: _____ days	Log review: ☐ Regular

Article 35: Data Protection Impact Assessment (DPIA)

#	Requirement	Status	Evidence	Notes
2.21	**DPIA Required?** High-risk processing (profiling, sensitive data, large-scale)	□ Yes (DPIA required) □ No	Assessment: _____	Risk level: □ Low □ Medium □ High
2.22	**DPIA Completed** If required, DPIA conducted and documented	□ ✅ □ ⚠️ □ ❌ □ ⊗	Document: _____	Date: _____
2.23	**DPIA Consultation** DPO consulted during DPIA	□ ✅ □ ⚠️ □ ❌ □ ⊗	Consulted: _____	Date: _____

Article 33-34: Data Breach

#	Requirement	Status	Evidence	Notes
2.24	**Breach Notification Plan** Documented process to notify within 72 hours	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Plan: _____	Tested: ☐ Yes ☐ No
2.25	**Breach Detection** Monitoring to detect breaches	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Tools: _____	Alert threshold: _____

GDPR COMPLIANCE STATUS

☐ COMPLIANT

All applicable items ✅

☐ PARTIAL COMPLIANCE

Some ⚠️ items, remediation plan documented

☐ NON-COMPLIANT

One or more ❌ items, cannot launch

Penalty if Non-Compliant: Up to €20M or 4% of global annual revenue, whichever is higher

Assessor: _____ **Date:** _____

3. HIPAA COMPLIANCE (US HEALTHCARE)

Applies If: Processing Protected Health Information (PHI) of US patients

HIPAA Security Rule - Administrative Safeguards

#	Requirement	Status	Evidence	Notes
3.1	**Security Management Process** Risk analysis conducted	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Document: _____	Date: _____
3.2	**Risk Management** Mitigation strategies implemented	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Plan: _____	All risks addressed: ☐ Yes ☐ No
3.3	**Workforce Security** Access authorization procedures	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Policy: _____	Role-based access: ☐ Yes ☐ No
3.4	**Training** Workforce trained on HIPAA	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Records: _____	All employees: ☐ Yes ☐ No
3.5	**Business Associate Agreements (BAAs)** BAAs with all vendors handling PHI	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Signed BAAs: _____	All vendors: ☐ Yes ☐ No

HIPAA Security Rule - Physical Safeguards

#	Requirement	Status	Evidence	Notes
3.6	**Facility Access Controls** Physical access to servers restricted	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Controls: _____	Cloud: ☐ AWS ☐ Azure ☐ GCP ☐ Other
3.7	**Workstation Security** Workstations secured	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Policy: _____	Auto-lock: ☐ Yes ☐ No
3.8	**Device & Media Controls** Secure disposal of devices/media	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Data wiping: ☐ Yes ☐ No

HIPAA Security Rule - Technical Safeguards

#	Requirement	Status	Evidence	Notes
3.9	**Access Controls** Unique user IDs, authentication	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	System: _____	MFA enabled: ☐ Yes ☐ No
3.10	**Audit Logs** All PHI access logged and retained	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Retention: _____ years	Minimum 6 years: ☐ Yes ☐ No
3.11	**Encryption** PHI encrypted at rest and in transit	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	At rest: _____ In transit: _____	
3.12	**Transmission Security** TLS 1.2+ for PHI transmission	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Protocol: _____	Verified: ☐ Yes ☐ No

HIPAA Privacy Rule

#	Requirement	Status	Evidence	Notes
3.13	**Minimum Necessary** Only minimum PHI accessed	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Review: _____	Enforced: ☐ Yes ☐ No
3.14	**Privacy Notice** Notice of Privacy Practices provided	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	URL: _____	HIPAA-compliant: ☐ Yes ☐ No
3.15	**Patient Rights** Access, amendment, accounting of disclosures	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Documented: ☐ Yes ☐ No

HIPAA Breach Notification Rule

#	Requirement	Status	Evidence	Notes
3.16	**Breach Notification Plan** Process to notify within 60 days	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Plan: _____	Tested: ☐ Yes ☐ No
3.17	**Breach Risk Assessment** Process to assess if incident is reportable breach	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Four-factor test: ☐ Documented

HIPAA COMPLIANCE STATUS

☒ COMPLIANT

All applicable items ✅

☒ PARTIAL COMPLIANCE

Some ⚠️ items, remediation plan documented

☒ NON-COMPLIANT

One or more ❌ items, cannot launch

Penalty if Non-Compliant: $100 - $50,000 per violation, up to $1.5M per year per violation category

Assessor: _____ **Date:** _____

4. EU AI ACT COMPLIANCE

Applies If: Deploying AI in EU or affecting EU residents

Risk Classification

#	Requirement	Status	Evidence	Notes
4.1	**Risk Level Determined** System classified as: Minimal, Limited, High, or Unacceptable	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Classification: _____	Assessment date: _____
4.2	**Unacceptable Risk Check** System does NOT fall under prohibited uses (social scoring, manipulation, real-time biometric in public)	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Verified: _____	If prohibited, CANNOT DEPLOY

High-Risk AI Requirements (if applicable)

#	Requirement	Status	Evidence	Notes
4.3	**Risk Management System (Article 9)** Documented risk management throughout lifecycle	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Document: _____	Continuous: ☐ Yes ☐ No
4.4	**Data Governance (Article 10)** Training data quality, relevance, representativeness	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Report: _____	Bias mitigated: ☐ Yes ☐ No
4.5	**Technical Documentation (Article 11)** Comprehensive technical documentation	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Document: _____	Complete: ☐ Yes ☐ No
4.6	**Record-Keeping (Article 12)** Automatic logging of events	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	System: _____	Tamper-proof: ☐ Yes ☐ No
4.7	**Transparency (Article 13)** Users informed of AI use, how it works, human oversight	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Disclosure: _____	Clear: ☐ Yes ☐ No
4.8	**Human Oversight (Article 14)** Humans can understand, monitor, intervene	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Oversight plan: _____	Override capability: ☐ Yes ☐ No
4.9	**Accuracy, Robustness, Cybersecurity (Article 15)** System tested for accuracy, resilience, security	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Test report: _____	BlackIndian AI test: ☐ Complete
4.10	**Conformity Assessment (Article 43)** Third-party assessment by notified body	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Assessment: _____ Notified body: _____	
4.11	**CE Marking** CE mark affixed to high-risk AI	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Applied: _____	Date: _____
4.12	**Registration** System registered in EU database	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Registration #: _____	Date: _____

Limited Risk AI (Transparency Obligations)

#	Requirement	Status	Evidence	Notes
4.13	**AI-Generated Content Disclosure** Users informed content is AI-generated	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Disclosure: _____	Prominent: ☐ Yes ☐ No
4.14	**Deepfake Disclosure** Manipulated images/audio/video labeled	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Watermark: _____	Machine-readable: ☐ Yes ☐ No

EU AI ACT COMPLIANCE STATUS

☐ COMPLIANT

All applicable items ✅

☐ PARTIAL COMPLIANCE

Some ⚠️ items, remediation plan documented

☐ NON-COMPLIANT

One or more ❌ items, cannot launch in EU

☐ **Penalty if Non-Compliant:** Up to €35M or 7% of global annual revenue (for prohibited AI), €15M or 3% (for non-compliance with obligations)

Assessor: _____ **Date:** _____

5. FAIR LENDING COMPLIANCE (US FINANCIAL SERVICES)

Applies If: AI used for credit decisions, lending, insurance

Equal Credit Opportunity Act (ECOA)

#	Requirement	Status	Evidence	Notes
5.1	**Prohibited Bases** System does NOT discriminate based on race, color, religion, national origin, sex, marital status, age, receipt of public assistance	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Test report: _____	Disparate impact test: ☐ Pass
5.2	**Adverse Action Notices** Applicants notified if denied with reasons	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Notice template: _____	Specific reasons: ☐ Yes ☐ No
5.3	**Record Retention** Applications retained 25 months	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Retention policy: _____	Automated: ☐ Yes ☐ No

Fair Credit Reporting Act (FCRA)

#	Requirement	Status	Evidence	Notes
5.4	**Adverse Action Notice (FCRA)** If credit report used, specific notice required	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Notice: _____	CRA info included: ☐ Yes ☐ No
5.5	**Accuracy Requirements** Reasonable procedures to ensure accuracy	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Procedures: _____	Tested: ☐ Yes ☐ No

Fair Lending Examination (Disparate Impact Testing)

#	Requirement	Status	Evidence	Notes
5.6	**Comparative Analysis** Approval rates compared across protected classes	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Test date: _____ Report: _____	
5.7	**Four-Fifths Rule** Protected group approval rate >= 80% of highest group	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Ratio: _____	Pass: ☐ Yes ☐ No
5.8	**Interest Rate Analysis** No systematic differences in pricing	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Analysis: _____	Fair: ☐ Yes ☐ No

FAIR LENDING COMPLIANCE STATUS

☐ COMPLIANT

All applicable items ✅

☐ PARTIAL COMPLIANCE

Some ⚠️ items, remediation plan documented

☐ NON-COMPLIANT

One or more ❌ items, cannot launch

☐ **Penalty if Non-Compliant:** $5,000 per violation (ECOA), up to $5,000 per violation (FCRA), potential class action lawsuits

Assessor: _____ **Date:** _____

6. EMPLOYMENT AI COMPLIANCE (US/NYC)

Applies If: AI used for hiring, promotion, termination decisions

EEOC Guidelines

#	Requirement	Status	Evidence	Notes
6.1	**Uniform Guidelines on Employee Selection** Selection process doesn't have adverse impact	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Analysis: _____	Four-fifths rule: ☐ Pass
6.2	**Protected Classes Tested** Impact analyzed for race, color, religion, sex, national origin, age (40+), disability	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Test report: _____	All classes: ☐ Yes ☐ No
6.3	**Business Necessity** If adverse impact, job-relatedness demonstrated	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Justification: _____	Validated: ☐ Yes ☐ No

NYC Local Law 144 (AI Hiring Tools)

Applies If: Using AI for hiring in NYC

#	Requirement	Status	Evidence	Notes
6.4	**Annual Bias Audit** Independent bias audit conducted within past year	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Audit date: _____ Auditor: _____	
6.5	**Audit Summary Published** Summary posted on website	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	URL: _____ Date published: _____	
6.6	**Candidate Notification** Candidates notified AI tool used (at least 10 days before)	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Notice: _____ Timing: _____	
6.7	**Alternative Process** Candidates can request alternative selection process	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Documented: ☐ Yes ☐ No
6.8	**Data Retention** Audit results retained 3 years	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Location: _____	Accessible: ☐ Yes ☐ No

EMPLOYMENT AI COMPLIANCE STATUS

☒ COMPLIANT

All applicable items ✅

☒ PARTIAL COMPLIANCE

Some ⚠️ items, remediation plan documented

☒ NON-COMPLIANT

One or more ❌ items, cannot launch

Penalty if Non-Compliant (NYC): $500 for first violation, $500-$1,500 for each subsequent violation (per day)

Assessor: _____ **Date:** _____

7. GENERAL DATA PROTECTION

Applies to: All AI systems processing user data

Basic Security Requirements

#	Requirement	Status	Evidence	Notes
7.1	**Authentication** Strong authentication for system access	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Method: _____	MFA: ☐ Enabled
7.2	**Authorization** Role-based access controls	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	System: _____	Least privilege: ☐ Yes
7.3	**Data Encryption (At Rest)** Sensitive data encrypted when stored	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Algorithm: _____ Key mgmt: _____	
7.4	**Data Encryption (In Transit)** TLS 1.2+ for data transmission	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Protocol: _____	Cert valid: ☐ Yes
7.5	**Secure Development** Security integrated into SDLC	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Testing: ☐ Regular
7.6	**Vulnerability Management** Regular security testing	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Last test: _____	BlackIndian AI: ☐ Yes
7.7	**Incident Response Plan** Documented breach response procedures	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Plan: _____	Tested: ☐ Yes ☐ No
7.8	**Logging & Monitoring** Security events logged and monitored	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	System: _____ Alert threshold: _____	
7.9	**Backup & Recovery** Regular backups, tested recovery	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Frequency: _____ Last test: _____	
7.10	**Patch Management** Systems kept up-to-date	☐ ✅ ☐ ⚠️ ☐ ❌ ☐ ⊗	Process: _____	Automated: ☐ Yes ☐ No

8. DOCUMENTATION REQUIREMENTS

Required Documentation

#	Document	Status	Location	Last Updated
8.1	**System Architecture Diagram**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.2	**Data Flow Diagram**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.3	**Privacy Policy**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.4	**Terms of Service**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.5	**AI Disclosure / Transparency Notice**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.6	**Risk Assessment Report**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.7	**Security Testing Report**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.8	**Bias Testing Report**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.9	**Incident Response Plan**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.10	**Data Retention Policy**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.11	**Training Records (Staff HIPAA/GDPR/etc.)**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.12	**Vendor Agreements (BAAs, DPAs)**	☐ Complete ☐ Partial ☐ Missing	_____	_____
8.13	**Model Card / AI Documentation**	☐ Complete ☐ Partial ☐ Missing	_____	_____

9. SIGN-OFF & CERTIFICATION

Pre-Launch Checklist Sign-Off

I certify that:

- ☐ All applicable compliance requirements have been reviewed
- ☐ All ✅ items are complete with documented evidence
- ☐ All ⚠️ items have documented remediation plans with timelines
- ☐ No ❌ items remain (or documented executive approval for launch with risk)
- ☐ All required documentation is complete and accessible
- ☐ The AI system is ready for production deployment from a compliance perspective

Completed by:

Name: _____

Title: _____

Signature: _____ **Date:** _____

Reviewed by (Legal/Compliance):

Name: _____

Title: _____

Signature: _____ **Date:** _____

Approved for Launch:

Name: _____

Title: _____

Signature: _____ **Date:** _____

BlackIndian AI Certification

If BlackIndian AI conducted testing:

- ☐ **CERTIFIED SECURE** - System passed comprehensive security testing across all 7 vulnerability categories with all critical and high-severity issues remediated.

Certification Valid Through: _____ (typically 6-12 months)

BlackIndian AI Assessor: _____

Signature: _____ **Date:** _____

APPENDIX A: REMEDIATION PLAN TEMPLATE

For any ⚠️ or ❌ items:

Item #	Issue Description	Priority	Assigned To	Due Date	Status	Notes
_____	_____	P0/P1/P2	_____	_____	☐ Open ☐ In Progress ☐ Complete	_____
_____	_____	P0/P1/P2	_____	_____	☐ Open ☐ In Progress ☐ Complete	_____
_____	_____	P0/P1/P2	_____	_____	☐ Open ☐ In Progress ☐ Complete	_____

Priority Definitions:

- **P0 (Critical):** Must fix before launch, blocks deployment
- **P1 (High):** Fix within 30 days post-launch
- **P2 (Medium):** Fix within 90 days post-launch

APPENDIX B: AUDIT PREPARATION

For Regulatory Audits:

1. **Gather All Documents** (from Section 8)
2. **Prepare Evidence** (test reports, logs, screenshots)
3. **Create Executive Summary** (compliance status overview)
4. **Assign Point of Contact** (who will interface with auditors)
5. **Schedule Mock Audit** (practice run with internal team)

Common Auditor Requests:

- Privacy policy and disclosures
- Security testing reports
- Bias/fairness testing results
- Access control configurations
- Incident logs (if any)
- Training records
- Vendor agreements

Have ready: Document links, login credentials (read-only), sample data (anonymized)

Document Information

Author: BlackIndian AI Compliance Team

Company: BlackIndian AI

Version: 1.0

Last Updated: December 2025

Next Review: Quarterly

For compliance consulting or full assessment:

security@blackindianai.com

blackindianai.com

END OF DOCUMENT