AI Best Practices Checklist

Your Framework for Safe & Effective AI Deployment

Joel & Nanz Inc. | AI Consulting & Integration Services

Purpose & Scope

Before You Deploy

- [ ] Define clear business objectives for AI implementation
- [ ] Identify specific use cases and success metrics
- [ ] Assess current data readiness and quality
- [ ] Evaluate budget and resource requirements
- [ ] Determine compliance requirements (GDPR, HIPAA, SOC 2, etc.)

Security & Access Control

Authentication & Authorization

- [ ] Implement role-based access control (RBAC)
- [ ] Use strong authentication (MFA/SSO)
- [ ] Define least-privilege access policies
- [ ] Audit and rotate API keys regularly
- [ ] Monitor access logs for anomalies

Data Protection

- [ ] Encrypt data at rest and in transit
- [ ] Implement data retention and deletion policies
- [ ] Use secure storage for sensitive information
- [ ] Establish data classification levels
- [ ] Create backup and disaster recovery procedures

Agent Supervision & Governance

Guardrails & Boundaries

- [ ] Define explicit action boundaries for AI agents
- [ ] Implement approval workflows for high-risk actions
- [ ] Set spending limits and rate limits
- [ ] Create escalation procedures for edge cases
- [ ] Document prohibited actions clearly

Monitoring & Oversight

- [ ] Log all AI agent actions and decisions
- [ ] Set up real-time alerting for anomalies
- [ ] Review agent behavior regularly
- [ ] Track accuracy and error rates
- [ ] Monitor for bias and fairness issues

Human-in-the-Loop

- [ ] Require human approval for sensitive operations
- [ ] Establish clear escalation paths
- [ ] Train staff on AI oversight procedures
- [ ] Create feedback mechanisms
- [ ] Plan for graceful degradation (fallback to humans)

Data Quality & Training

Data Preparation

- [ ] Audit training data for bias and completeness
- [ ] Validate data sources and provenance
- [ ] Clean and normalize datasets
- [ ] Test with representative samples
- [ ] Document data processing steps

Model Selection & Testing

- [ ] Choose appropriate models for use cases
- [ ] Test accuracy across diverse scenarios
- [ ] Validate against edge cases
- [ ] Benchmark against alternatives
- [ ] Document model limitations

Continuous Improvement

Performance Monitoring

- [ ] Track key performance indicators (KPIs)
- [ ] Monitor response times and latency
- [ ] Measure user satisfaction
- [ ] Analyze cost per transaction
- [ ] Review uptime and reliability

Iteration & Updates

- [ ] Schedule regular model retraining
- [ ] Update based on new data and feedback
- [ ] Version control all changes
- [ ] Test updates in staging environment
- [ ] Communicate changes to stakeholders

Compliance & Documentation

Regulatory Compliance

- [ ] Map AI use to applicable regulations
- [ ] Implement required consent mechanisms
- [ ] Create data processing agreements
- [ ] Prepare for audits and inspections
- [ ] Stay current with changing regulations

Documentation

- [ ] Maintain system architecture diagrams
- [ ] Document data flows and integrations
- [ ] Create runbooks for common scenarios
- [ ] Write user guides and training materials
- [ ] Keep incident response plans updated

Risk Management

Threat Assessment

- [ ] Identify potential attack vectors
- [ ] Assess impact of system failures
- [ ] Evaluate reputational risks
- [ ] Consider adversarial manipulation risks
- [ ] Plan for worst-case scenarios

Mitigation Strategies

- [ ] Implement input validation and sanitization
- [ ] Use prompt injection defenses
- [ ] Set up anomaly detection
- [ ] Create incident response procedures
- [ ] Maintain insurance coverage if applicable

Team & Training

Staff Readiness

- [ ] Train teams on AI capabilities and limitations
- [ ] Establish AI ethics guidelines
- [ ] Define roles and responsibilities
- [ ] Create communication protocols
- [ ] Foster a culture of responsible AI use

External Partners

- [ ] Vet AI vendors and service providers
- [ ] Review third-party compliance certifications
- [ ] Establish SLAs and support agreements
- [ ] Define data ownership and usage rights
- [ ] Plan for vendor lock-in or migration

Next Steps

Immediate Actions:

1. [ ] Print this checklist and review with your team
2. [ ] Prioritize items based on your risk profile
3. [ ] Assign owners to each section
4. [ ] Set quarterly review milestones
5. [ ] Contact Joel & Nanz Inc. for expert guidance

Need Help?

Our AI consultants can help you implement these best practices, audit your current setup, and build a custom governance framework.

contact@joelnanz.com
joelnanz.com
Available upon request

Additional Resources

- ☐ **OpenAI Safety Best Practices:** platform.openai.com/docs/guides/safety-best-practices
- ☐ **NIST AI Risk Management Framework:** nist.gov/itl/ai-risk-management-framework
- ☐ **EU AI Act:** digital-strategy.ec.europa.eu
- ☐ **Anthropic's Responsible Scaling Policy:** anthropic.com

---

Version 1.0 | February 2026 | Joel & Nanz Inc.