Production Readiness Checklist for Azure Deployment

1. Code & Repository Readiness

☐ Code is modular, DRY, and well-documented
☐ Sensitive info stored securely (e.g., .env or Azure Key Vault – never in code)
☐ Version control with proper branching strategy (e.g., main, develop, feature/*)
☐ Automated tests (unit/integration/e2e) written and passing
☐ Code linting and formatting enabled (ESLint, Prettier, etc.)
☐ README with setup, deployment, and contribution guide
☐ Type safety checks (e.g., TypeScript if used)

2. Frontend (React App)

☐ Environment-specific configs (REACT_APP_API_URL, etc.)
☐ Bundle optimization using Webpack/Vite
☐ Code splitting & lazy loading for large routes/components
☐ Helmet for SEO and meta tags
☐ Proper error boundaries in place
☐ Service worker for PWA (optional)
☐ Secure headers (CSP, XSS, HSTS) via Azure Front Door or CDN

3. Backend API

☐ Input validation and sanitization
☐ Rate limiting & throttling
☐ Authentication & Authorization (JWT, OAuth2, etc.)
☐ CORS properly configured
☐ Logging and centralized error handling
☐ Secure communication (HTTPS only)
☐ Health check endpoint (/health, /status)
☐ OpenAPI (Swagger) documentation available

4. GenAI Integration (e.g., Azure OpenAI)

☐ Rate limiting to avoid overuse
☐ Fallbacks for failed completions

☐ Prompt engineering reviewed for context safety
☐ Sensitive data not passed to prompts without masking
☐ Azure OpenAI quota and usage tracking enabled
☐ Prompt & response logging for auditing (with PII redaction)

5. Azure Infrastructure Setup

☐ Web App/Static Web App for React (Azure Static Web Apps or Azure App Service)
☐ App Service / Container Apps / AKS for API
☐ Autoscaling enabled
☐ Custom domain & HTTPS enabled
☐ WAF (Web Application Firewall) if exposed to the public
☐ Azure Front Door / CDN for global performance & protection
☐ Azure Key Vault for secrets & API keys
☐ Managed Identity for secure service-to-service communication
☐ Role-Based Access Control (RBAC) in Azure
☐ Private Endpoints for APIs if needed
☐ Application Gateway with WAF (if complex security layer needed)

6. Monitoring & Logging

☐ Azure Monitor configured
☐ Application Insights for performance tracking
☐ Log Analytics workspace for structured querying
☐ Alerts set for errors, downtime, quota limits, etc.

7. CI/CD Pipeline

☐ GitHub Actions / Azure DevOps pipeline configured
☐ Separate pipelines for staging and production
☐ Automated deployments with environment tagging
☐ Rollback plan in case of failure
☐ Secret management using Azure Key Vault in CI/CD

8. Database (if used)

☐ Connection strings managed securely
☐ Backups enabled
☐ Indexes and query optimization reviewed
☐ Data encryption at rest and in transit

☐ Auditing and access policies configured

9. Performance & Scalability

☐ Load testing done (using Azure Load Testing, JMeter, k6)
☐ Performance budget set for frontend
☐ Caching enabled (Redis, CDN, etc.)
☐ Database performance monitored and indexed
☐ AI completion rate monitored for latency

10. Final Touches

☐ User Acceptance Testing (UAT) completed
☐ Documentation for infra, API, onboarding, monitoring
☐ On-call alerts and support runbook ready
☐ Security audit / Pen test completed (optional)
☐ Post-deployment checklist ready for launch day