INFOSECTRAIN

Azpirant TECHNOLOGIES

AI GRC Implementation Checklist

www.azpirantz.com

Section	Checklist Item
Governance & Ethics	Comprehensive AI Policy Framework is defined and enforced
	Permissible and prohibited AI use cases are documented
	Accountability for AI decisions is assigned
	Ethical AI guidelines are developed and integrated into workflows
	Cross-functional AI leads are appointed across departments
Compliance & Legal Alignment	AI systems are reviewed against GDPR, CCPA, EU AI Act, HIPAA, etc.
	Mapping of applicable regulatory frameworks is completed
	Universal opt-out signals and consent preferences are honoured
	Transparent, accessible privacy policies are published
	Data practices are clearly communicated to users
Risk Management	End-to-end AI risk assessments are conducted regularly
	Risks related to bias, adversarial inputs, and privacy violations are documented
	Risk scoring methods are defined and applied to AI systems
	Dedicated AI Risk Management Program is established
	Enterprise Risk Management is integrated with AI risk oversight
Privacy & Security by Design	Privacy by Design and Security by Design principles are embedded in all AI development
	Data minimization practices are enforced at every stage
	PETs (Differential Privacy, Federated Learning, Synthetic Data) are implemented
	Consent is granular and revocable
	Users are empowered to manage their own data
Data Governance & Provenance	Data governance policies are defined and documented
	Clear data inventories are maintained and updated regularly
	Data provenance is tracked across all AI systems
	AI datasets are vetted for bias, quality, and completeness
	AI asset inventories are kept current
Security Architecture & Controls	Encryption is applied to data at rest and in transit
	Role-based access controls (RBAC) are enforced
	Real-time monitoring tools are deployed
	Multi-factor authentication is enabled for access to AI systems
	Patch management and network segmentation practices are followed
	Data masking/redaction is used in non-production environments
	Threat modelling for AI is conducted

Monitoring, Audits & Response	AI models are continuously monitored for bias and data drift
	AI audits are scheduled and logged
	AI incident response plan is in place and tested
	Logs of AI decisions are maintained and reviewable
	Automated alerts are set for anomalous AI behaviour

Culture & Awareness	AI ethics and privacy training is conducted across roles
	Awareness programs promote trust, privacy, and secure AI practices
	Security is promoted as a shared responsibility
	Developers and data scientists are partners in compliance
	Agile, iterative, and privacy-conscious development culture is cultivated

Technology & Tools	PETs and compliance tools are integrated into DevOps workflows
	Licensing agreements reflect transparency and data usage terms
	Real-time insights into data pipelines and AI model behaviours are available
	Tools enable easy audit, traceability, and evidence capture
	AI models are evaluated for adversarial robustness

Azpirantz TECHNOLOGIES

Found this **useful?**

Get More Insights Through our **FREE**

Courses | Webinars | eBooks | Whitepapers | Checklists | Mock Tests

www.azpirantz.com

This content is created by the Azpirantz Marketing Team.