CreativeCyber.

AI SECURITY

AI Security Governance

20 controls for AI Security Governance -- BFSI AI risk teams

GOVERNANCE & STRATEGY

- [ ] Board-approved AI Security Policy with defined scope and accountability
- [ ] AI governance roles defined: AI Risk Owner, Model Owner, Data Steward
- [ ] Central AI model inventory maintained with risk classification
- [ ] AI risk appetite statement defined and approved by board

DATA PRIVACY & INFRASTRUCTURE

- [ ] Personal data usage in AI model training identified and documented
- [ ] Data minimisation principles applied to all AI training datasets
- [ ] AI model access controls implemented with role-based permissions
- [ ] AI model outputs subject to DPDP Act data principal rights compliance

AI DEVELOPMENT & SUPPLY CHAIN

- [ ] Third-party AI models and APIs assessed for security and compliance risk
- [ ] Training data provenance documented with lineage and quality controls
- [ ] Model versioning and rollback capability operational
- [ ] AI bias assessment conducted for all customer-facing models

USE CASES & FAIRNESS

- [ ] Automated decision-making use cases identified and catalogued
- [ ] DPIA completed for AI-driven credit scoring, KYC, and risk assessment
- [ ] Customer notification mechanism for AI-driven decisions operational
- [ ] Human review override available for all material automated decisions

POST-MARKET GOVERNANCE

- [ ] AI model performance monitoring operational with drift detection
- [ ] AI incident response procedure documented with escalation path

- [ ] Annual AI audit programme established with independent review
- [ ] Regulatory reporting requirements for AI identified across RBI, SEBI, IRDAI

SCORING GUIDE

18-20	14-17	10-13	<10
Audit-ready	Functional gaps	Material remediation	Escalate

Automate this checklist >> dpdp-assessment.creativecyber.in