JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

Banking - AI Risk

AI

AI risk in banking is critical because banks rely on AI to make fast, high impact decisions (spotting fraud, assessing customers, and managing funds) and failures can cause financial loss, legal trouble, and harm to customers. Managing AI risk ensures data is accurate and private, models are fair and explainable, systems are secure, and humans can step in when needed. Good AI risk practices protect customers, preserve trust, and keep the bank compliant and resilient as technology and threats evolve.

RISK ASSESSMENT
(WHAT TO CHECK)

Know what you use: list all AI tools, the data they use, and any outside vendors.
Ask "what can go wrong?": think about fraud, data errors, system crashes, or someone tricking the system.
Prioritize: focus first on problems that could cost money, break rules, or hurt customers.
Keep a plan: write down risks, who owns them, and how often you'll review.

DATA GOVERNANCE
(HOW DATA IS HANDLED)

Assign owners: someone must be responsible for each dataset.
Check data quality: make sure data is complete, accurate, and up to date.
Protect privacy: hide or remove personal data when not needed and follow consent rules.
Log changes: track who accessed or changed data and keep records for audits.

MODEL TRANSPARENCY & EXPLAINABILITY
(UNDERSTANDING DECISIONS)

Document purpose: say what each AI model does and what data it uses.
Explain decisions simply: for any decision that affects a customer, show plain reasons and what the customer could do to change the result.
Keep version logs: record which model version made each decision and why a human overrode it.

BIAS DETECTION & MITIGATION
(FAIRNESS)

Watch for unfairness: check if certain groups are treated worse by the model.
Use simple fairness checks: compare error rates across groups and fix big gaps.
Fix data or settings: rebalance or clean data and adjust thresholds to reduce unfairness.
Give people recourse: let customers appeal if they think a decision was unfair.

SECURITY MEASURES
(PROTECTING SYSTEMS)

Know assets: list models and where data lives.
Limit access: only give people the permissions they need; use strong logins.
Separate environments: use different systems for testing and live production.
Monitor and respond: watch for suspicious activity and have a plan to contain breaches.

www.jupiter-cap.com Email: rod.boothe@jupiter-cap.com

JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

Banking - AI Risk

AI

AI risk in banking is critical because banks rely on AI to make fast, high impact decisions (spotting fraud, assessing customers, and managing funds) and failures can cause financial loss, legal trouble, and harm to customers. Managing AI risk ensures data is accurate and private, models are fair and explainable, systems are secure, and humans can step in when needed. Good AI risk practices protect customers, preserve trust, and keep the bank compliant and resilient as technology and threats evolve.

COMPLIANCE MONITORING
(FOLLOWING RULES)

Map rules: connect each AI use to the laws and rules that apply (privacy, AML, etc.).
Keep evidence: save training data snapshots and model reports for audits.
Automate checks: build simple rule-checks into pipelines and review results regularly.
Respond quickly: have templates and steps for regulator or customer requests.

STAKEHOLDER ENGAGEMENT
(KEEPING PEOPLE INFORMED)

Identify audiences: regulators, customers, internal teams, and partners.
Communicate clearly: share short, regular updates and explain impacts in plain language.
Invite feedback: provide simple channels for questions and complaints.
Include outside voices: get input from customer advocates or regulators when needed.

INCIDENT RESPONSE PLANNING
(WHAT TO DO IF SOMETHING GOES WRONG)

Define incidents: be clear what counts as a problem (data leak, wrong decisions, attacks).
Form a team: include IT, legal, compliance, operations, and communications.
Follow a checklist: detect → contain → investigate → fix → notify → review.
Practice: run tabletop exercises so everyone knows their role.

PERFORMANCE MONITORING & EVALUATION
(MAKING SURE MODELS WORK)

Watch simple KPIs: detection rate, false alarms, and time to resolve an alert.
Detect drift: look for when model results change over time or stop matching reality.
Feed outcomes back: use investigator results to retrain and improve models.
Regular reviews: schedule model checks, revalidations, and retire outdated models.

TRAINING & AWARENESS
(TEACHING STAFF)

Role-based training: different short courses for executives, model owners, ops, and front line.
Hands-on practice: use simple simulations so staff practice reading model outputs.
Ongoing refreshers: short refreshers and quick reminders to keep skills current.
Measure learning: track completions and basic assessments.

CHECKLIST TO START
(APPRAISAL OF AI SYSTEMS)

- [x] Make an inventory of AI tools and datasets.
- [x] Assign an owner for each critical dataset and model.
- [x] Put basic access controls in place (least privilege + MFA).
- [x] Run a quick fairness check and a basic security scan.
- [x] Create an incident contact list and one simple response checklist.

www.jupiter-cap.com Email: rod.boothe@jupiter-cap.com