AI Risk Management in Practice

Banks

FINANS FORENINGEN

CFA Society Denmark

2021.AI

AGENDA

AI Risk Management in Practice

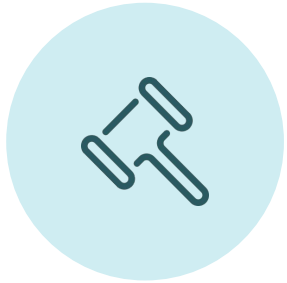
1. FROM STATISTICAL MODELS TO MACHINE LEARNING- MRM in the AI AGE
2. IS THERE A CASE FOR IRB?
3. ENTERPRISE RISK AMPLIFIED
4. DEMO- MANAGING AI CREDIT RISK MODEL RISKS, WITH AI
5. Q&A

AI IN BANKS

MODEL RISK MANAGEMENT EVOLUTION, NOT REVOLUTION

DYNAMIC & SELF LEARNING

Adapt to the dynamic and self-learning nature of AI and ML models, which can change their behaviour over time or in different contexts.



NEW VALIDATION METHODS

Incorporate new methods and tools for validating, testing and monitoring AI and ML models, such as sensitivity analysis, stress testing, scenario analysis and counterfactual analysis.

INTERDISCIPLINARY EFFORT

Model risk management will need to involve more interdisciplinary collaboration and communication among model developers, users, risk managers and auditors, as well as external stakeholders such as customers, regulators and society

RISK TRADE OFFS

MRM needs to trade off model performance vs. compliance and reputational risks. Will a marginal increase in performance or prediction accuracy worth the compliance burden and additional risks?

AI IN BANKS

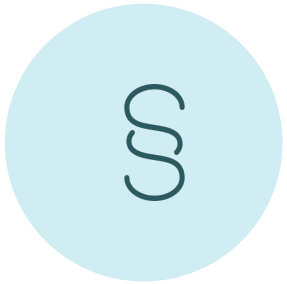
THE CASE FOR IRB- CREDIT RATING & CAPITAL REQUIREMENTS

Model Complexity

The challenge: models are inherently very complex

Solution:overweight explainability risk mitigations in data and architecture/design

Feasibility: explainability is still developing

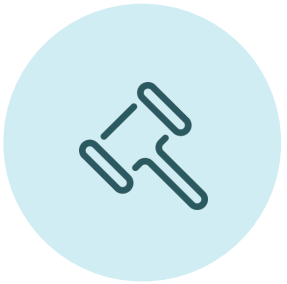


BASEL III Capital Floors

The challenge: capital floors simplify IRB calculations

Solution: not needed, would simplify the model

Feasibility: feasible today, but may hinder adoption



Regulatory Scrutiny

The challenge: model parameter calibration very frequent

Solution: automating documentation, model monitoring and data governance

Feasibility: feasible today

AI IN BANKS

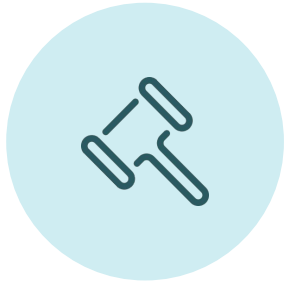
SAME RISK TAXONOMY, AMPLIFIED RISKS

OPERATIONAL RISKS

The same: IT risks associated with development, security and deployment of an AI system remain

Changed: Shadow AI and extended attack surface, including rogue models and prompt injections

How to handle:AI impact assessments, risk aware model registration, education/awareness



LEGAL & COMPLIANCE RISKS

The same: litigations, disputes and enforcements actions, or non-compliance with regulations.

Changed:fair treatment, capital requirements, privacy and data protection.

How to handle: update current risk registers with specific AI risks, controls and regularly measure AI compliance

REPUTATIONAL RISKS

The same: media exposure, issue management, regulatory attention following non-compliance/litigation

Changed: the AI powered knowledge worker, scale, cross border

How to handle: continuous explainability, model inventory

MODEL RISKS

The same: non-transparent human decisions, model design, data sets and model quality

Changed: larger scale and velocity algo/data discrimination. New areas for model use (cap, commercial)

How to handle: lifecycle approach to governance, human intervention, model inventory

DEMO

RISKGPT- MANAGING AI RISKS WITH AI

Consumer Loan Credit Risk Model

Why?: a very common use case

How? Pre-filled model “risk card” (the risk/governance part of the model card)

EU AI ACT/NIST RMF Compliant

Why?: the ruling standards for the foreseeable future

How? the model inventory, risks and impact domains (SHREC) and handling (no monitoring, yet)

For AI/Tech Risk Teams

Why? “what the f is risk management?”

How? Dead simple, offload the difficult part (risk quantification and prioritization)

Explainable By Design

Why? audit readiness and user education

How? human in the loop (“oversight”), refresh model choices, learn from all actions including discards