



**TURUN
YLIOPISTO**
UNIVERSITY
OF TURKU

Generative AI in the banking sector

A regulatory mapping

Mika Viljanen and Nea Lepinkäinen

University of Turku 2026



TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

TIIVISTELMÄ

Raportti kartoittaa luottolaitosten kohtaamia sääntelyvelvoitteita, kun ne ottavat käyttöön generatiivisia tekoälysovelluksia.

Rahoituslaitokset käyttävät monenlaisia tekoälysovelluksia, joiden taustateknologiat vaihtelevat. Raportti keskittyy sovelluksiin, joiden ytimessä on generatiivinen tekoäly. Tällaiset sovellukset hyödyntävät neuroverkkopohjaisia, hyvin monimutkaisia ja tulkitsemattomia laajoja kieli- tai multimodaalimalleja. Mallit tuottavat erityyppisiä tulosteita erityyppisten syötteiden pohjalta.

Analyysi kattaa kaksi sääntelykokonaisuutta: EU:n tekoälyasetuksen ja sektorikohtaisen pankkisääntelyn (CRR, CRD ja EBA:n ohjeet luotonannosta ja luottojen seurannasta). Tietosuoja, operatiivinen häiriönsietokyky ja pankkisalaisuus jäävät raportin ulkopuolelle.

Raportti tarkastelee neljää arkkityyppistä käyttötapausta ja neljää käyttöönoton arkkityyppiä. Käyttötapaukset heijastavat mahdollisia generatiivisen tekoälyn sovelluksia rahoituslaitoksissa. Käyttöönoton arkkityypit kuvaavat erilaisia teknisiä toteutustapoja eri käyttötapauksissa.

Käyttötapaukset ovat 1) henkilöstön kopilotti, 2) asiakaschatbotti, 3) luottopäätöskopilotti ja 4) luottopäätösautomaattiikka. Käyttöönoton arkkityyppejä ovat valmis pilvipalvelu (SaaS), pilvipohjainen API-integraatio, hakuun tukeutuva generointi (RAG) ja oma hienosäätö. Kunkin yhdistelmän sääntelyriskiprofiili eroaa muista.

Velvoitteet vaihtelevat käyttötapauksen ja arvoketjuroolin mukaan. Tekoälyasetus rakentuu käyttötapaus- ja arvoketjurooliperusteiseen sääntelyrakenteeseen. Käyttötapaus määrittää sääntelyn yleisen intensiteetin. Arvoketjun rooli ratkaisee vastuiden jakautumisen.

Käyttötapaus määrittää sääntelyn intensiteetin ja toteutettavuuden. Henkilöstön kopilotti ja asiakaschatbotti ovat rajoitetun riskin tekoälyjärjestelmiä. Niihin kohdistuu vain läpinäkyvyysvelvoitteita ja vaatimustenmukaisuus on saavutettavissa. Luottopäätöskopilotti on todennäköisesti suuren riskin järjestelmä. Sen toteutettavuus on oikeudellisesti epävarma. Valvojat saattavat kohdella sitä tosiasiallisena automaationa, jos ihmisellä päätöksentekijällä ei ole todellisia mahdollisuuksia kyseenalaistaa järjestelmän tuotoksia. Luottopäätösautomaattiikka ei ole nykytulkintojen valossa toteutettavissa. Esteet eivät juonnu tekoälyasetuksesta vaan pankkisääntelyn ja yleisen tietosuoja-asetuksen selitettävyyssvaatimuksista.

Käyttöönottotapa ratkaisee velvoitteiden allokoinnin. SaaS-käyttöönotossa rahoituslaitos on käyttöönottaja ja sille jää suhteellisen vähän velvoitteita. Toimittaja kantaa sekä yleiskäyttöistä tekoälymallia (GPAI) että tekoälyjärjestelmää (AIS) koskevat tarjoajavelvoitteet. API-, RAG- ja hienosäätökäyttöönotoissa laitos siirtyy itse tekoälyjärjestelmän tarjoajaksi ja vastaa kaikista tarjoajavelvoitteista. Tavanomainen RAG-toteutus ei muokkaa mallin painoja eikä siten tee laitoksesta GPAI-mallin tarjoajaa. Hienosäätö johtaa GPAI-mallin tarjoajan asemaan vain, jos hienosäätöön käytetty laskenta ylittää kolmasosan alkuperäisen mallin koulutuslaskennasta.

Selitettävyysskuilu on keskeinen este. Suuret kielimallit eivät tuota niitä yksityiskohtaisia, toistettavia ja eriteltäviä perusteluita, joita pankkisääntely edellyttää luottopäätöksiltä. EBA:n ohjeet vaativat, että laitokset ymmärtävät automatisoitujen mallien menetelmät, oletukset ja rajoitukset. CRR:n 179 artikla edellyttää sisäisten luottoluokitusten menetelmiä käyttäviltä laitoksilta tappiokokemuksen erittelyä luottoriskiparametrien mukaan. Kielimallit eivät salli tällaista erittelyä. Ongelma ei ole vaatimustenmukaisuuden suunnittelussa vaan teknologian rakenteessa.

Tiedollinen epäsymmetria GPAI-arvoketjussa heikentää alavirran vaatimustenmukaisuutta. Tekoälyasetuksen toimintasäännöstö sallii GPAI-mallien tarjoajien jakavan vinoumien havainnointiin ja datan laatuun liittyvät tiedot vain valvojille. Alavirran luottolaitokset eivät välttämättä saa niitä tietoja, joita ne tarvitsevat omien EBA-pohjaisten hallintovelvoitteidensa täyttämiseen.

Infrastruktuuri on edellytys. Luottoa koskevissa käyttötapauksissa julkisen pilven API-käyttöönotto luo itsenäisiä esteitä yleisen tietosuojaa-asetuksen tietosijaintivaatimusten, pankkisalaisuuden ja DORA:n ulkoistussäännösten valossa. Yksityinen tai hallittu pilviympäristö lienee välttämätön ennen kuin tekoälyasetuksen vaatimustenmukaisuusarviointi muuttuu mielekkääksi.

Tekoälyasetus ja pankkisääntely menevät päällekkäin, mutta eivät muodollisesti ristiriitaa. Molemmat edellyttävät riskienhallintaa, datan hallintoa, dokumentointia ja testausta. Tekoälyasetus sallii rahoituslaitosten integroida useita velvoitteistaan olemassa oleviin sisäisiin hallintorakenteisiin. Vaatimusten painopisteet kuitenkin eroavat. Tekoälyasetus painottaa järjestelmätason terveys-, turvallisuus- ja perusoikeusriskejä. Pankkisääntely painottaa mallitason selitettävyyttä ja auditoitavuutta. Molemmat edellyttävät testausta, mutta EBA:n ohjeet vaativat lisäksi takaisinarviointia historiallisia vertailukohtia vasten.

ASIASANAT: tekoäly, generatiivinen tekoäly, EU:n tekoälyasetus, pankkisääntely, luottopäätös, GPAI, CRR, CRD, EBA, selitettävyys

ABSTRACT

This report maps the regulatory requirements that credit institutions face when deploying generative AI applications.

While financial institutions use a wide variety of artificial intelligence applications with divergent underlying technologies, this report focuses on applications with generative AI backbones. These applications use massive, highly complex, uninterpretable neural network-based large language or multimodal models to generate a wide range of outputs in response to a wide range of inputs.

The analysis covers two regulatory frameworks: the EU AI Act and sectoral banking regulation (CRR, CRD, EBA Guidelines on loan origination and monitoring). Data protection, operational resilience and banking secrecy rules fall outside the report's scope.

The report examines four archetypal use cases and four archetypal deployment modalities. The use cases reflect possible generative AI deployments in financial institutions. The deployment modalities reflect possible technical implementations in different use cases.

The use cases are 1) employee copilot, 2) customer chatbot, 3) credit decision co-pilot and 4) credit decision automation. The deployment modalities are system-as-a-service (SaaS), cloud-based API integration, retrieval-augmented generation (RAG) integration and proprietary fine-tuning. Each combination produces a distinct regulatory risk profile.

Obligations vary based on use case and value chain role. The AI Act establishes a use case and value chain role based regulatory regime. The use case determines overall regulatory intensity, while the value chain determines the allocation of responsibilities.

Use case determines regulatory intensity and feasibility. The employee copilot and customer chatbot are limited-risk AI systems. They face transparency obligations only. Compliance is achievable. The credit decision copilot is likely a high-risk system. Its feasibility is legally uncertain because supervisors may treat it as de facto automation if the human decision-maker cannot effectively challenge the system's outputs. Credit decision automation is not feasible under current interpretations. The constraints do not flow from the AI Act but banking regulation (and GDPR) explainability requirements.

Deployment modality determines obligation allocation. In SaaS deployments the financial institution is a deployer and subject to relatively few obligations,

while the vendor bears both GPAI and AIS provider obligations. In API, RAG and fine-tuning deployments the institution becomes the AI system provider and faces the full AIS provider obligation stack. Standard RAG does not modify model weights and therefore does not push the institution into GPAI model provider status. Fine-tuning triggers GPAI model provider status only in the unlikely case that fine-tuning compute exceeds one-third of the original model's training compute.

The explainability gap is the central obstacle. LLMs cannot produce the granular, reproducible and decomposable justifications that banking regulation requires for credit decisions. EBA Guidelines demand that institutions understand the methodology, assumptions and limitations of automated models. CRR Article 179 requires IRB institutions to break down loss experience by credit risk parameters. LLMs do not permit such breakdowns. The obstacle is not a compliance design problem. It is an architectural one.

Information asymmetry in the GPAI value chain weakens downstream compliance. The AI Act Code of Practice permits GPAI model providers to reserve bias detection and data quality information for regulators. Downstream institutions may not receive the information they need to satisfy their own EBA governance obligations.

Infrastructure is a prerequisite. For credit-related use cases, public cloud API deployment creates independent obstacles under GDPR data residency rules, banking secrecy laws and DORA outsourcing requirements. A private or controlled-cloud environment is likely necessary before AI Act compliance analysis becomes meaningful.

The AI Act and banking regulation overlap but do not conflict in formal terms. Both require risk management, data governance, documentation and testing. The AI Act allows financial institutions to integrate several of its obligations into existing internal governance structures. The requirements diverge in emphasis. The AI Act focuses on system-level health, safety and fundamental rights risks. Banking regulation focuses on model-level explainability and auditability. Both require testing, but the EBA Guidelines additionally require backtesting against historical benchmarks.

KEYWORDS: artificial intelligence, generative AI, EU AI Act, banking regulation, credit decisions, GPAI, CRR, CRD, EBA, explainability

1 Introduction

1.1 Purpose, design and limitations

Generative AI applications use massive, highly complex, uninterpretable neural network-based large language or multimodal models to generate a wide range of outputs in response to inputs. Agentic AI applications use large language models as reasoning engines to autonomously plan, execute and adjust multi-step tasks with minimal human oversight. They interact with external tools, databases and APIs to achieve goals defined by the user. While generative AI applications produce outputs in response to single inputs, agentic AI applications pursue objectives across multiple steps and adapt their behaviour based on intermediate results.

The report canvasses the regulatory environment for generative and agentic AI by credit institutions. It outlines the constraints that selected use cases and technical implementations of generative and agentic AI technologies face in credit decision related operations.

The report has a limited scope.

First, the report only discusses AI-specific aspects of regulation. The focus is on the EU Artificial Intelligence Act (AIA, 2024/1698/EU), the Capital Requirements Regulation (CRR, 2013/575/EU), the Capital Requirements Directive (CRD, 2013/36/EU) and the EBA Guidelines on loan origination and monitoring (EBA/GL/2024/14). While highly pertinent to generative AI applications, the report does not discuss the General Data Protection Regulation (GDPR, 2016/679/EU) or the Digital Operational Resilience Act (DORA, 2022/2554/EU). Both introduce concerns that are non-specific to generative AI.

Second, the report is structured as a series of case studies centering around a limited selection of archetypal use cases and technical implementations.

The report examines four archetypal use cases.

Report use cases

Employee copilot (ECP)	Generates drafts for communications, reports, and code to accelerate internal workflows. ECP functions as an intelligent assistant for content creation and data synthesis, reducing manual drafting time. The system requires human verification of all outputs, serving purely to augment employee productivity rather than replace judgment.
Customer chatbot(CCB)	Operates as a strictly informational interface for general banking queries. It uses natural language processing to explain policies and products without performing actions. CCB is hard-coded to decline all requests for financial advice, sales, or transaction execution, serving solely as a passive support layer.
Credit decision copilot (CDC)	Processes unstructured applicant data to generate standardized credit memos and risk summaries. It organizes financial narratives and highlights key metrics to prepare a case file for human review. CDC streamlines the pre-analysis phase but holds no authority to assess creditworthiness or execute lending decisions.
Credit decision robot (CDR)	Autonomously evaluates credit applications to issue binding approvals or rejections. It uses generative models to interpret complex borrower data and infer risk profiles without human intervention. CDR aims to automate the full decision lifecycle, prioritizing speed and scalability in the adjudication process.

The archetypal use cases are stylised representations of potential use cases. They were chosen after limited stakeholder consultations with FLAIG partners and a small-scale literature review. The consultations and the literature review indicated that institutions may seek to deploy generative AI in these use cases, in addition to others such as investment advice, fraud detection and fulfilling know-your-customer obligations.

The report discusses four archetypal deployment modalities for each generative or agentic AI.

Deployment modalities	
System as a Service	Pre-built system procured from a third-party vendor who retains control over the underlying model, its updates, output filtering, and system-level configurations. The institution uses the system through a vendor-defined interface with limited ability to modify its behaviour.
API integration	Connects banking applications directly to a vendor-hosted model (e.g., OpenAI, Anthropic) via secure endpoints. Model maintenance is offloaded entirely to the third-party provider. API-based or on-premise access to the model offers instant scalability and access to state-of-the-art capabilities but forgoes adaptation to institution-specific data.
RAG integration	Couples a generative model with an internal, vectorized knowledge base. The system retrieves relevant banking documents to augment the prompt context before generation occurs. RAG integration ensures responses are grounded in the bank's specific data and policies while maintaining the underlying model as a frozen, reasoning engine.

In-house finetuning	Retrains specific layers of a generative model using a curated dataset of the bank's historical data. This embeds domain-specific terminology, style, and logic directly into the model's weights. Finetuning moves beyond context injection to fundamentally alter how the model processes information, tailoring it to niche financial tasks.
----------------------------	---

The archetypal deployment modalities reflect possible state-of-the-art technical implementations in different use cases. The analysis suggests that many use case and deployment modality combinations present unique regulatory risk profiles.

1.2 Structure

The first chapter sets out the regulatory environment. It covers the relevant banking regulation, namely CRD Article 79, CRR Article 179 and the EBA Guidelines on loan origination and monitoring, before turning to the EU AI Act. The Act discussion includes the risk classification system, the provider/deployer distinction, high-risk system obligations, transparency requirements for limited-risk systems and the GPAI model framework. The chapter closes with an analysis of how the two frameworks interact.

The second chapter presents four use case analyses: the employee copilot, the customer chatbot, the credit decision copilot and credit decision automation. Each use case is examined along two dimensions, system function and deployment modality. The latter covers SaaS, cloud API, RAG and proprietary fine-tuning architectures. For each combination, the chapter maps the applicable AIA obligations and identifies the relevant banking regulation constraints.

The third chapter draws conclusions. It assesses the regulatory feasibility of each use case, identifies the explainability gap as the central structural obstacle for credit-related automation and notes two cross-cutting issues: the information asymmetry inherent in the GPAI value chain, and the infrastructure prerequisites that must be addressed before AIA compliance analysis becomes meaningful.

1.3 Existing research

The regulatory implications of AI in the financial sector have attracted growing academic attention since the AI Act proposal in 2021. The existing literature can be grouped into three strands.

The first strand examines the AI Act's general regulatory framework. Veale and Zuiderveen Borgesius provided an early critical assessment of the draft regulation. Almada and Petit analysed the tension between the Act's product safety logic and its fundamental rights ambitions. Hacker mapped the broader trajectory of EU AI regulation beyond the Act itself. Several comprehensive AI Act handbooks and commentaries are also on the market.

The second strand focuses specifically on the AI Act's impact on the financial sector. Passador provides a comprehensive overview of the Act's governance architecture from the perspective of banking supervision, with particular attention to the roles of the AI Office, AI Board and ECB. Hacker and Eber analyse the Act's implications for credit underwriting and insurance, mapping AI Act obligations against CRR/CRD provisions in a detailed crosswalk table. They also examine the deployer-to-provider transition under Article 25 and the interaction between AI Act transparency requirements and GDPR obligations following the CJEU's *Dun & Bradstreet* ruling. Arnal discusses the AI Act in passing, but focuses mainly on GDPR-related concerns in automated credit underwriting processes. The EBA's mapping exercise confirms that no significant contradictions exist between the AI Act and existing banking legislation, classifying the interaction into derogations, integrations and divergences.

The third strand addresses AI governance in the financial sector more broadly. Sciarrone Alibrandi et al. examine the Act's impact on financial markets from a co-regulation perspective. Mazzini and Bagni consider the regulation of AI systems in the financial sector under the Act. Krause and Krause add a transatlantic dimension, examining the compliance challenges US fintech firms face under the Act.

The report contributes to the second strand but differs from existing work in two respects. First, it analyses four deployment modalities (SaaS, cloud API, RAG, proprietary fine-tuning) and shows that obligation allocation across the AI value chain depends on architectural choices that existing literature does not examine. Second, it focuses specifically on generative AI and identifies the explainability gap as a structural obstacle to LLM-based credit decision automation under current banking regulation. Hacker and Eber and the EBA mapping exercise address the AI Act's interaction with financial regulation but do not analyse how deployment architecture affects compliance or how LLM-specific characteristics create binding constraints under CRR Article 179 and EBA Guidelines on loan origination.

2 Regulatory environment

2.1 Purpose and design of the regulatory environment mapping

Generative and agentic artificial intelligence operations in credit institutions are subject to a multi-layered regulatory framework comprising banking regulation, general digital and data regulation, and AI-specific rules. The report addresses the interplay between AI-specific rules and banking regulation through the analysis of four use cases. Broader implications of general digital and data regulation fall outside the scope.

The chapter first examines the specific banking regulations relevant to AI deployment. It then turns to the EU Artificial Intelligence Act. The chapter closes with a synthesis and an account of the interaction between the two regulatory frameworks.

2.2 Banking regulation

The Capital Requirement Regulation and the Capital Requirements Directive make up the backbone of EU banking regulation. The EBA guidelines add detail to the high-level rules in the CRR and the CRD.

In addition to high-level operational risk rules, CRR, CRD and DORA contain no rules that would be relevant to the employee copilot and customer chatbot use cases. The credit decision copilot and credit automation use cases, however, fall under the CRR and CRD credit risk and credit decision-making rules.

Credit decisions and credit decision-making are subject to a split treatment based on how sophisticated methods banks use for calculating their credit risk regulatory capital charges. All banks face a uniform base level of requirements. Banks using the Internal Risk-Based Approach (IRBA) to credit risk capital allocation face additional demands on how internal methodologies for credit risk capital allocation should be used in internal decision-making.

2.2.1 Base-level obligations

CRD Article 79 constitutes the legislative base level for all credit decision making in credit institutions. Loan origination is a multi-step process. Creditworthiness assessment is the key decision point. The rules that deal with loan origination center around that decision.

Under CRD Article 79, institutions must first base credit-granting on sound and well-defined criteria. For the creditworthiness assessment part, the CRD Article 79 obligation primarily entails that institutions must design and document written criteria for credit decisions. The criteria must be defensible from a prudential perspective. Second, institutions must also have documented procedures for credit approval, clear lines of authority and responsibility, and defined processes for modifying existing credit arrangements. Third, institutions must have internal methodologies that allow them to assess credit risk of exposures to individual obligors, in securities, in securitization positions and at the portfolio level. The methodologies must not rely solely or mechanistically on external credit ratings.

EBA Guidelines on loan origination and monitoring provide further guidance. The Guidelines framework requires that banks systematically identify, assess, approve, monitor, report and mitigate credit risk. Institutions must set out the criteria for these activities in their credit risk policies and procedures. The framework must be documented and updated regularly.

Policies and procedures for credit assessment and approval are further specified in paragraphs 63 to 66. The first requirement is that institutions should establish “a clear and well-documented credit decision-making framework”. The framework should contain a clear and sound structure for the credit decision-making responsibilities. There should be “a hierarchy of the credit decision-makers” integrated into the institution’s organisational and business structure and reporting lines (para 63) and attuned to the risk appetite and limits (para 64).

Second, EBA requires that the framework should “clearly articulate the decision-making powers and limitations of each decision-maker and of any automated models for credit decision-making purposes” (para 65).

Third, if the institution chooses to use “technology-enabled innovations” for credit granting purposes, several obligations kick in. The institution should understand the underlying models used, including their capabilities, assumptions and limitations, along with ensuring their traceability, auditability, and robustness and resilience.

The institution must also:

1. ensure that the models are fit for purpose,
2. understand the quality of data and inputs to the model,
3. detect and prevent bias in the credit decision-making process, and
4. ensure that appropriate safeguards are in place to provide confidentiality, integrity and availability of information and systems.

Fourth, if technology-enabled innovation leads to automated models for creditworthiness assessment and credit decision-making, institutions should have in place:

1. internal policies and procedures detecting and preventing bias and ensuring the quality of the input data,
2. measures to ensure the traceability, auditability and robustness and resilience of the inputs and outputs,
3. internal policies and procedures ensuring that the quality of the model output is regularly assessed, including backtesting the performance of the model, and
4. control mechanisms, model overrides and escalation procedures within the regular credit decision-making framework, including qualitative approaches, qualitative risk assessment tools and quantitative limits.

The models should have adequate documentation that covers:

1. methodology, assumptions and data inputs,
2. an approach to detecting and preventing bias and ensuring the quality of input data,
3. the use of model outputs in the decision-making process, and
4. the monitoring of these automated decisions on the overall quality of the portfolio or products in which these models are used.

Institutions should also specify the use cases for any automated models in the creditworthiness assessment and credit decision-making processes. Models may only be used “in a way that is appropriate to the size, nature and complexity of the credit facility and the types of borrowers”. In practice, the requirement bars banks from using models for large exposures and complex facilities.

2.2.2 IRBA bank obligations

A subset of credit institutions may use the Internal Ratings-Based Approach to calculate capital charges for credit risk under CRR Article 143.

IRBA requires that banks build internal methodologies for assessing the probability of default (PD), loss given default (LGD) and exposure at default (EAD) for eligible credit risk exposures.

CRR requires that banks integrate their IRBA methodologies into their internal governance structures. CRR Article 144(1)(b) requires that the IRBA “internal ratings and default and loss estimates [...] shall play an essential role in the risk management and decision-making process, and in the credit approval, internal capital allocation and corporate governance functions of the institution.” In practice, the obligation entails that the institutions must incorporate the IRBA methodologies into their credit assessment and decision-making criteria and policies.

2.2.3 Banking regulation obstacles to generative and agentic AI use in credit decision-making

While banking rules do not significantly constrain the employee copilot and customer chatbot use cases, credit decision automation that uses generative or agentic AI technologies faces severe obstacles arising from banking regulation.

CRR Article 179 requires that IRB institutions’ risk calculation models be “plausible and intuitive” and reflect “the material drivers of the respective risk parameters”. The institution must be able to break down its loss experience by credit risk parameters. LLMs do not permit such breakdowns.

EBA Guidelines require institutions to understand the models they use, their methodology, assumptions and limitations. For LLMs, the requirement is problematic. The model produces responses probabilistically, and the same input may produce different outputs.

Credit decision automation using generative or agentic AI is thus likely not allowed under current interpretations of banking regulation. The situation may change if supervisors accept that banks have developed explanation methods that meet regulatory standards or if technology evolves toward greater reliability.

2.3 AI regulation

In the EU, AI systems are governed by the Artificial Intelligence Act (AIA), a regulation that adopts a risk-based approach to regulating AI. As a regulation, AIA is directly applicable law in all member states.

The chapter outlines the AIA's regulatory design, the classification of AI entities and the specific obligations imposed on actors within the AI value chain.

2.3.1 Regulated AI entities under AIA

The AI Act distinguishes between three core AI entities: Article 3(1) AI systems, Article 3(63) general-purpose AI models, and Article 3(66) general-purpose AI systems.

Article 3(1) AI systems (AIS) and Article 3(66) GPAI systems (GPAIS) are the operational AI entities in the AIA.

AI systems are 1) machine-based systems 2) designed to operate with varying levels of autonomy. They 3) may exhibit adaptiveness after deployment. An AI system 4) infers from its input how to generate outputs 5) for explicit or implicit objectives. These outputs 6) include predictions, content, recommendations or decisions that 7) can influence physical or virtual environments.

General-purpose AI models display significant generality and are capable of competently performing a wide range of distinct tasks. A pre-agentic large language model is a typical example. As “models”, GPAIMs lack direct use opportunities. In the AI Act imaginary, they are the architecture and parameter weights.

General-purpose AI systems emerge when a GPAI model gains operationality. The transition happens when a GPAI model is combined with a user interface or integrated into another system. A GPAI system is therefore an AI system with a GPAI model as a part of its inference engine. A GPAI system has the capability to serve a variety of purposes, both for direct use and for integration in other AI systems.

The rise of agentic AI technologies complicates the picture. Agentic AI technologies strain the boundary between GPAI models and systems. First, agentic AI technologies comprise GPAI models that invoke tools, spawn sub-agents and orchestrate other models. Second, agentic AI is capable of pursuing complex goals across extended action sequences, planning, delegating, invoking tools and adjusting behaviour based on environmental feedback.

2.3.2 Value chain actors

The AIA imposes obligations on actors across the AI value chain. While the rules distinguish between multiple roles, providers and deployers are the relevant roles for the report use cases and implementation modalities.

A provider is a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model (or has it developed) and places it on the market or puts it into service under its own name or trademark. The provider bears the primary responsibility for ensuring AI system compliance with the AIA.

A deployer is any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. In the financial sector, a bank typically acts as a deployer when procuring off-the-shelf AI systems.

A single entity can occupy multiple roles simultaneously. A financial institution may simultaneously be an AIS, GPAIS or GPAIM provider (when developing systems in-house) and a deployer (when using them under its authority). Furthermore, under Article 25(1), a deployer may legally become a provider if they:

1. put their name or trademark on a high-risk AI system already on the market;
2. make a substantial modification to a high-risk AI system; or
3. modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk, in such a way that it becomes a high-risk AI system.

2.3.3 Risk categories

The AIA enacts a pyramid-like risk-based regulatory structure for AI entities. The key design parameter was that regulatory burdens should increase in proportion to the risks the system poses to health, safety and fundamental rights.

At the apex of the risk pyramid, Article 5 addresses prohibited AI practices deemed to pose unacceptable risks. The prohibited practices include manipulative or deceptive techniques to distort behaviour, the exploitation of vulnerabilities (such as age or disability) and social scoring by public or private actors. The list also prohibits untargeted scraping of facial images from the internet or CCTV for facial recognition databases, emotion recognition in the

workplace or educational institutions, and certain forms of predictive policing aimed at individuals.

The second pyramid level contains high-risk AI systems (HRAIS). These include systems used for the purposes listed in Annex III, such as critical infrastructure, education and employment, and AI systems used as safety components in products subject to Union harmonization legislation.

In the financial sector, evaluation of creditworthiness and credit scoring and risk assessment and pricing for life and health insurance constitute the relevant high-risk use cases. However, financial institutions must also comply with HRAIS requirements when first using AI within human resources contexts, such as using AI for recruitment or evaluating employee performance and when using AI systems used for biometric identification.

HRAISs are subject to an extensive set of compliance requirements, which are detailed in the following section.

The requirements scale down for limited-risk AI systems (LRAIS). LRAISs are AI systems designed to interact with natural persons or to generate synthetic content. LRAIS face custom transparency requirements. Minimal or no-risk AI systems, on the other hand, face no AI Act requirements but are within its scope.

Because the AI Act is a harmonizing EU regulation, it has a “preemption effect”. Member States lose the competence to regulate within the Act’s substantive scope of application. The preemption effect effectively shields minimal-risk systems from further national-level regulation, ensuring a unified internal market.

2.3.4 High-risk AI systems

2.3.4.1 HRAIS regulatory framework

The regulatory framework for high-risk AI systems follows the design of EU product safety legislation. The framework places the primary burden of ensuring AIA compliance on the HRAIS providers. However, unlike traditional product safety regimes, the AI Act also imposes regulatory obligations on deployers.

The allocation of these roles is not static. Under AIA Article 25, a deployer may be reclassified as a provider if it markets a system under its own name, makes substantial modifications to it, or changes the intended purpose of a non-high-risk system to a high-risk use. In the banking sector, the possible role changes are an important concern. A financial institution deploying an off-the-shelf AI

system will be subject to full provider responsibilities if it modifies a general-purpose AI system to be used for creditworthiness assessments, thereby changing its intended purpose to a high-risk category.

2.3.4.2 Provider obligations

When a financial institution is a provider of a high-risk AI system, for instance after developing a credit decision automation tool in-house, it faces the most extensive obligations.

Core design and governance obligations. The most critical HRAIS requirements concern risk management, data governance and oversight. Under Article 9, providers must establish a risk management system. The risk management system is a continuous, iterative process that includes identifying AIS health, safety and fundamental rights risks and eliminating, reducing, mitigating and managing the risks so that the residual risks are judged acceptable. As a crucial part of risk management, all AIA systems must also undergo testing against pre-defined metrics and probabilistic thresholds to ensure consistent performance. Financial institutions regulated under Union law may integrate the AIA risk management process into their existing internal risk management processes.

Article 10 mandates that training, validation and testing datasets be subject to appropriate data governance. The datasets must be relevant, representative and, to the best extent possible, free of errors and complete. Article 10 also requires that providers actively detect and mitigate biases in training, validation and testing datasets.

Article 14 is particularly significant in banking automation use cases. The Article requires that HRAISs are designed to enable effective human oversight. HRAISs must provide human overseers with the necessary tools to interpret system outputs and, crucially, to disregard, override or reverse the system's decisions. The human oversight rules entrench the human operator as the final authority, mitigating automation bias risks.

Transparency, technical accuracy, robustness and cybersecurity. To enable appropriate usage and support effective oversight, Article 13 requires providers to design systems that are sufficiently transparent for deployers to interpret system outputs. This obligation includes providing concise instructions for use that detail the system's characteristics, capabilities and limitations. Article 15 requires that high-risk systems achieve an appropriate level of accuracy, robustness and cybersecurity, ensuring resilience against errors or malicious attempts to alter the system's performance.

Documentation obligations. Providers must also maintain technical documentation (Article 11) and keep it for ten years (Article 18) to allow authorities to assess conformity. Article 12 requires the system to automatically generate logs of events over its lifetime. The logs must be kept for at least six months to ensure traceability of the system's functioning (Article 19). Financial institutions may maintain the required technical documentation and logs as part of the documentation and record-keeping already required under relevant Union financial services law, rather than creating separate AI-specific records.

Operational requirements. In addition to Chapter III Section 2 HRAIS requirements, providers face several operational requirements under Section 3 rules. Article 17 mandates a quality management system (QMS) to ensure compliance. The QMS serves as a comprehensive blueprint for AI development, covering aspects ranging from compliance strategies and design control procedures to data management techniques and validation processes. Financial institutions are exempt from creating a duplicate system if their existing internal governance arrangements under banking regulations are compliant. Despite the broad exemption, financial institutions must still adhere to Article 17(1) requirements regarding the integration of the risk management system, post-market monitoring and serious incident reporting.

Article 20 and Article 21 obligate providers to take immediate corrective actions if a system is non-compliant and to cooperate fully with competent authorities upon request.

Taulukko 1. AIA: High-Risk AI System Provider Obligations — A. System Technical & Design Requirements

AIA: High-Risk AI System Provider Obligations						
A. System Technical & Design Requirements (Ensuring System Safety & Quality)						
	Risk Management System	Data Governance	Technical Documentation & Logging	Transparency	Human Oversight	Accuracy, Robustness & Cybersecurity
AIA Article(s)	Art. 9	Art. 10	Art. 11, 12	Art. 13	Art. 14	Art. 15
Key Obligation	Establish, implement, and maintain a continuous risk management system that includes identifying, analysing, evaluating and mitigating risks throughout the system's entire lifecycle. Test the system to identify the best risk management measures and to ensure it works as intended.	Implement appropriate data governance and management practices for training, validation, and testing data sets (including bias mitigation).	Draw up, maintain, and keep comprehensive technical documentation and ensure automatic logging of events for traceability and auditability.	Design the system to be transparent and to technically facilitate the provision of information concerning the system's capabilities, limitations, potential risks, and (if relevant) how to collect, store and interpret data logs.	Design the system with technical features that enable appropriate human oversight, including the ability to intervene and override the system's decisions.	Design and develop the system to achieve an appropriate level of accuracy, robustness, and resilience against cybersecurity threats (e.g., adversarial attacks).

Taulukko 2. AIA: High-Risk AI System Provider Obligations — B. Governance & Process Requirements

AIA: High-Risk AI System Provider Obligations							
B. Governance & Process Requirements (Ensuring Compliance Management)							
	Quality Management System (QMS)	Technical Documentation & Logging	Information to Deployers	Conformity Assessment & CE Marking	EU Registration	Post-Market Monitoring	Reporting of Serious Incidents
AIA Article(s)	Art. 17	Art. 18, 19	Art. 13	Art. 43, 47, 48	Art. 49	Art. 72	Art. 73
Key Obligation	Establish, document, and maintain a formal quality management system covering the entire development and compliance process. Financial institutions can meet these requirements by complying with Union financial services law.	Keep technical documentation for 10 years from the moment the system is released. ^[EU] Keep comprehensive logs for traceability and auditability for at least six months. ^[EU] A financial institution must keep the documentation and logs as part of their documentation under financial services law.	Ensure the provision of clear instructions (documentation) that cover the information about the provider and instructions on how to interpret the system's output, and address any uncertainty regarding the system's results.	Carry out the required conformity assessment procedure (self-assessment or third-party) to verify compliance. Draw up a written EU declaration of conformity and affix the CE marking to indicate the system meets all requirements.	Register the system in the EU database for high-risk AI systems before placing it on the market or putting it into service.	Establish a post-market monitoring system that collects and analyses data on the performance of the AI systems throughout their lifetime, ensuring they continue to comply with regulations. The monitoring system should be based on a plan that is part of the technical documentation.	Report any serious incident to the market surveillance authorities of the Member States where the incident occurred, as soon as a possible link between AI system and the incident is found.

2.3.4.3 Deployer obligations

When a bank uses a high-risk system developed by a third party, it is a HRAIS deployer. Article 26 outlines the deployer's primary duties. Deployers face few obligations: they must conduct human oversight and monitor the system operations.

First, deployers must assign competent human overseers to supervise the system's use and intervene if necessary. Second, the deployer must monitor the system based on the system's instructions for use, for example to detect anomalies. The AI Act provides a specific financial sector carve-out for the latter obligation. The duty to monitor the operations is deemed fulfilled if the financial institution complies with the rules on internal governance arrangements and processes under applicable Union financial services law.

Article 27 imposes an obligation to conduct a fundamental rights impact assessment (FRIA). The obligation primarily applies to HRAIS deployers who are public bodies. However, financial institutions deploying creditworthiness assessment, credit scoring, or insurance risk selection or pricing must also conduct a FRIA. The FRIA must identify the specific categories of natural persons affected and the risks of harm to their rights, as well as the measures to be taken in case these risks materialise, including arrangements for internal governance and complaint mechanisms. Deployers must also inform individuals that they are subject to a high-risk AI system.

Taulukko 3. AIA: High-Risk AI System Deployer Obligations

AIA: High-Risk AI System Deployer Obligations						
	Operational Use & Human Oversight	Monitoring & Incident Reporting	Data Governance	Worker Transparency	Registration	Fundamental Rights Impact Assessment
AIA Article(s)	Art. 26(1), 26(2)	Art. 26(5)	Art. 26(4), 26(6)	Art. 26(7)	Art. 26(8), 49	Art. 27
Key Obligation	Take appropriate technical and organisational measures to ensure the system is used in accordance with the instructions for use. Assign human oversight to natural persons who are competent, properly trained, and have the necessary authority and support.	Monitor the operation of the system. If it presents a risk or serious incident, suspend use and inform the provider and market surveillance authority. Financial institutions can fulfil the obligation by complying with the relevant financial service law.	If the deployer exercises control over the input data: Ensure that input data is relevant and sufficiently representative. If the deployer has control over logs: Keep automatically generated logs for at least six months. Financial institutions must maintain the logs as part of the documentation kept pursuant to the relevant financial service law.	Before putting a high-risk AI system into service in the workplace, inform workers and their representatives that they will be subject to the system.	(For bodies governed by public law): Register yourself as a user of the system in the EU database before putting it into service.	(For bodies governed by public law & private entities providing public services): Conduct an assessment of the system's impact on fundamental rights prior to deployment. This includes identifying risks to marginalized groups and detailing oversight measures.

2.3.5 Limited-risk AI systems

Article 50 addresses limited-risk AI systems that are designed for direct interaction with natural persons, the generation of synthetic content, or emotion recognition, regardless of their high-risk classification. The primary objective of the rules is to ensure that natural persons are explicitly informed if they are interacting with AI systems, exposed to synthetic content or subject to emotion recognition.

Both providers and deployers are subject to transparency obligations, but the scope of duties varies.

For financial institutions who are providers (e.g. an in-house customer service chatbot), two primary obligations apply.

Under Article 50(1), providers must ensure that AI systems intended to interact directly with natural persons inform the user that they are interacting with an AI system. For instance, a customer service chatbot must explicitly state its artificial nature unless it is obvious to a “reasonably well-informed, observant and circumspect person”. Conversely, internal tools that assist employees without engaging in direct conversational exchange do not trigger the obligation.

Based on Article 50(2), providers must ensure that system outputs (audio, image, video, or text) are marked as artificially generated in a machine-readable format, to the degree technically feasible. The requirement poses significant technical challenges for text-generating systems, as plain text does not easily support persistent metadata.

Financial institutions acting as deployers face disclosure duties in certain cases. As Article 50(3) demands, an institution employing an emotion recognition or biometric categorisation system must inform natural persons that they are exposed to the system. Such systems must be distinguished from standard biometric verification tools used for authentication. However, specific applications, such as analysing voice stress markers to infer fraudulent intent (emotion recognition) or using facial analysis for automatic age estimation (biometric categorization) will likely trigger the transparency requirement.

Following Article 50(4), deployers must disclose that deep fake content is of artificial origin. If a deployer uses an AI system to generate text to be published to inform the public on matters of public interest, such as automatically posting market updates to social media, it must disclose that the text is AI-generated and has not been human-reviewed. While a one-to-one customer service exchange generally does not fall under the “public interest” provision, the

obligation becomes relevant if AI-generated content is broadcast or published without human editorial oversight.

For all the above obligations, the disclosures must be provided in a clear and distinguishable manner at the latest at the time of the first interaction or exposure (Article 50(5)).

Taulukko 4. AIA: Limited-Risk AI System Transparency Obligations

AIA: Limited-Risk AI System Transparency Obligations						
Use case	1. Direct Interaction (e.g., chatbots, customer service AI)	2. Synthetic Content (AI-generated text, audio, video)	3. Emotion Recognition & Biometric Categorisation	4. Deepfakes (Manipulated content resembling real persons/places)	5. Text of Public Interest (e.g., news, public information)	All of the cases (General conditions for transparency)
AIA Article(s)	Art. 50(1)	Art. 50(2)	Art. 50(3)	Art. 50(4)	Art. 50(4)	Art. 50(5)
Key Obligation	Natural persons must be informed that they are interacting with an AI system (unless obvious from the context).	Content must be marked in a machine-readable and detectable format as artificially generated or manipulated (watermarking).	Natural persons must be informed of the operation of the system before the processing of their data.	It must be clearly disclosed that the content has been artificially generated or manipulated.	If the text of public interest is generated by AI, this must be disclosed (unless a human has reviewed and holds editorial responsibility).	Information must be provided in a clear, distinguishable, and accessible manner, at the latest at the first interaction or exposure.
Responsible party	Provider (ensures technical capability) Deployer (ensures practical implementation)	Provider	Deployer	Deployer	Deployer	Provider or Deployer depending on the case

2.3.6 GPAI regulatory framework

2.3.6.1 Framework design

The regulatory framework for general-purpose AI (GPAI) models applies exclusively to model providers. However, the rules have significant implications for financial institutions acting as downstream HRAIS providers. Since banks rely on external GPAI models to build their own systems, their ability to fulfill HRAIS and banking regulation governance and risk management obligations depends on the documentation provided by the upstream GPAI provider.

A financial institution only falls directly under the scope of the GPAI provider rules if it becomes a provider itself. The shift occurs in three specific situations:

1. In-house development: The institution develops a GPAI model from scratch.
2. Significant fine-tuning: The institution fine-tunes an existing model to such an extent that it results in a “significant change” in capabilities. Commission guidelines suggest the threshold is met when the additional training compute exceeds roughly one-third of that used for the original model.
3. Adaptive RAG implementations: The institution implements a retrieval-augmented generation (RAG) architecture that effectively alters the model’s functioning, for instance by enabling it to adapt its internal parameters based on institutional data. While standard RAG implementations do not trigger provider status, adaptive RAG architectures, while currently rarely used, can amount to a “significant modification”.

2.3.6.2 Obligations for all GPAI models

The AI Act establishes a baseline regulatory framework for all GPAI models in Article 53. The core obligations impose transparency requirements through two distinct layers of documentation. First, providers must draw up and keep up-to-date detailed technical documentation for national competent authorities. Second, and crucially for downstream value chain actors, providers must supply documentation to downstream providers that enables them to understand the model’s capabilities and limitations.

The Code of Practice clarifies the requirements. While the Code is voluntary, it effectively sets detailed requirements for the minimum disclosure. The Code’s “Model Documentation Form” distinguishes between information reserved for authorities and information shared with downstream providers. The

benchmark for disclosure to downstream providers is risibly low. For instance, the template suggests describing the model architecture in merely 20 words and data curation methods in approximately 300 words.

Even more risibly, the form suggests that information on measures to detect identifiable biases or unsuitable data sources is to be provided only to authorities, leaving downstream providers without visibility into these fundamental safety aspects. The choice raises concerns about whether financial institutions acting as downstream providers will receive sufficient information to fully comply with their own governance obligations.

In addition to documentation, Article 53 requires that providers implement a policy to comply with Union copyright law and to publish a “detailed” but low-detail summary of training content. The Code of Practice emphasises that providers must respect rights reservations made by rights-holders through machine-readable means, such as the robots.txt protocol.

Taulukko 5. AIA: Obligations for Providers of All General-Purpose AI Models

AIA: Obligations for Providers of All General-Purpose AI Models				
	Technical Documentation	User Information	Copyright Policy	Public Summary of the Training
AIA Article(s)	Art. 53(1)(a) & Annex XI	Art. 53(1)(b) & Annex XII	Art. 53(1)(c)	Art. 53(1)(d)
Key Obligation	Draw up and keep up-to-date technical documentation, including training and testing processes and evaluation results. Recipient: Provided upon request to the AI Office and national competent authorities to demonstrate compliance.	Draw up and provide information to enable the safe integration of the model into AI systems. Recipient: Provided to downstream providers so they understand the model's capabilities and limitations.	Put in place a policy to ensure compliance with Union copyright law. Identify and comply with rights reservations (opt-outs) expressed by rightsholders pursuant to Art. 4(3) of the DSM Directive (e.g., via robots.txt).	Draw up and make publicly available a sufficiently detailed summary of the content used for training the model. Format must follow the template provided by the AI Office.

2.3.6.3 Obligations for systemic risk models

Models classified as presenting “systemic risk” face an additional layer of obligations under Article 55. A GPAI model is presumed to carry systemic risk if it has “high-impact capabilities” and could have a significant impact on public health, safety, public security, fundamental rights or society as a whole. AIA also includes a technical definition: a GPAI model with systemic risk (SRGPAI model) is one trained using a cumulative amount of computation greater than 10²⁵ floating point operations (FLOPs).

Providers of SRGPAI models must perform model evaluations, assess and mitigate systemic risks, track serious incidents, and ensure adequate cybersecurity. The Code of Practice encourages providers to establish a detailed and comprehensive Safety and Security Framework, including undertaking a full systemic risk assessment before the model is placed on the market or put into use. Regarding security, the Code stipulates that adequate measures must remain in place as long as the provider retains control over the model’s weights. The Code also sets out strict timelines for reporting serious incidents to the AI Office. However, the Code avoids setting substantive thresholds for “acceptable” risk or “adequate” security.

For a financial institution acting as a SRGPAIM provider, the additional layer implies a significant shift in responsibility. Since the regulation does not prescribe specific external safety metrics or limits, the institution must define its own risk acceptance levels. Compliance is thus demonstrated not by adhering to pre-defined regulatory numbers, but by relying on procedural safeguards to justify the institution’s internal risk decisions.

Taulukko 6. AIA: Extra Obligations for Providers of GPAI Models with Systemic Risk

AIA: Extra Obligations for Providers of General-Purpose AI Models with Systemic Risk				
	Model Evaluation & Adversarial Testing	Systemic Risk Assessment & Mitigation	Serious Incident Reporting	Cybersecurity Protection
AIA Article(s)	Art. 55(1)(a)	Art. 55(1)(b)	Art. 55(1)(c)	Art. 55(1)(d)
Key Obligation	Perform model evaluation in accordance with state-of-the-art protocols and tools. Specifically, conduct adversarial testing ("red-teaming") to	Assess and mitigate systemic risks at the Union level. Continuously identify, analyse, and determine the acceptability of	Keep track of, document, and report relevant information about serious incidents and possible corrective measures to the	Ensure an adequate level of cybersecurity protection for the model and its physical infrastructure to protect them against e.g.

	identify vulnerabilities, offensive capabilities, and refuse-to-answer failures throughout the development cycle.	risks. Implement safety mitigations (e.g., guardrails, refusal mechanisms) if risks are unacceptable based on defined criteria.	AI Office (and national competent authorities if appropriate). Specific deadlines for reporting apply for different severities, e.g., critical infrastructure disruption.	model theft, unauthorized access, model weights exfiltration, and data poisoning attacks.
--	---	---	---	---

2.4 Interplay of financial and AI regulation

Banking regulation rules and the AIA establish overlapping obligations. The primary overlapping requirements relate to risk management. Both require that banks run a risk management process designed to mitigate risks.

AIA rules explicitly account for the overlapping obligations. They allow high-risk system providers to integrate the Article 9 risk management process and Article 17 quality management process into the bank's internal management procedures. The carve-out eases the compliance burden for financial institutions with established risk management processes. However, the requirements are conflicting in part. The AIA emphasises system-level requirements that focus on mitigating health, safety and fundamental rights risks. Banking regulation emphasises model-level requirements by focusing on explainability and model performance. Both require testing, but the EBA Guidelines also explicitly focus on backtesting to test model performance against real-world historical benchmarks.

AIA Article 10 and the EBA Guidelines both require institutions to engage in data governance, input data verification and bias detection. The obligation details differ slightly.

AIA Article 11 and the CRD, the CRR and the EBA Guidelines impose extensive documentation obligations.

3 Use case and deployment modality studies

3.1 Use cases and deployment modalities

The report analyses LLM technology deployments in banks using a two-dimension matrix.

The first dimension is the use case. The report examines four use cases for LLMs within banks.

Report use cases	
Employee copilot (ECP)	Generates drafts for communications, reports, and code to accelerate internal workflows. ECP functions as an intelligent assistant for content creation and data synthesis, reducing manual drafting time. The system requires human verification of all outputs, serving purely to augment employee productivity rather than replace judgment.
Customer chatbot(CCB)	Operates as a strictly informational interface for general banking queries. It uses natural language processing to explain policies and products without performing actions. CCB is hard-coded to decline all requests for financial advice, sales, or transaction execution, serving solely as a passive support layer.
Credit decision copilot (CDC)	Processes unstructured applicant data to generate standardized credit memos and risk summaries. It organizes financial narratives and highlights key metrics to prepare a case file for human review. CDC streamlines the pre-analysis phase but holds no authority to assess creditworthiness or execute lending decisions.
Credit decision robot (CDR)	Autonomously evaluates credit applications to issue binding approvals or rejections. It uses generative models to interpret complex borrower data and infer risk profiles without human intervention. CDR aims to automate the full decision lifecycle, prioritizing speed and scalability in the adjudication process.

The employee copilot assists staff with drafting and synthesis. The customer chatbot answers customer queries but does not execute contracts or provide investment advice. The credit decision copilot supports human decision-makers by summarising loan applicant data and flagging risks. Credit decision automation makes binding credit decisions without human intervention.

The use case-based analysis is augmented by considering AI system deployment modality within each use case as the second analysis dimension.

The assumption is that a financial institution could build tools for each use case.

Deployment modalities	
System as a Service	Pre-built system procured from a third-party vendor who retains control over the underlying model, its updates, output filtering, and system-level configurations. The institution uses the system through a vendor-defined interface with limited ability to modify its behaviour.
API integration	Connects banking applications directly to a vendor-hosted model (e.g., OpenAI, Anthropic) via secure endpoints. Model maintenance is offloaded entirely to the third-party provider. API-based or on-premise access to the model offers instant scalability and access to state-of-the-art capabilities but forgoes adaptation to institution-specific data.
RAG integration	Couples a generative model with an internal, vectorized knowledge base. The system retrieves relevant banking documents to augment the prompt context before generation occurs. RAG integration ensures responses are grounded in the bank's specific data and policies while maintaining the underlying model as a frozen, reasoning engine.
In-house finetuning	Retrains specific layers of a generative model using a curated dataset of the bank's historical data. This embeds domain-specific terminology, style, and logic directly into the model's weights. Finetuning moves beyond context injection to fundamentally alter how the model processes information, tailoring it to niche financial tasks.

Both dimensions are crucial to the analysis. The use case determines, e.g., whether the system is a HRAIS and thus the AIA rules applicable to it. Deployment modality affects how AIA responsibilities are allocated within the value chain. For example, in a SaaS-based credit automation implementation, the vendor is subject to GPAIM and HRAIS provider obligations, while the bank is only a HRAIS deployer. In a proprietary fine-tuning implementation, the vendor likely remains the GPAIM provider but the bank must assume the role of the HRAIS provider.

The same use case can generate different obligation sets depending on how the underlying model is accessed and integrated.

Where the use case and deployment modality fall on the two matrix dimensions determines feasibility. An API LLM powering an employee copilot tool faces minimal regulatory friction. The same LLM integrated into a credit scoring workflow using a RAG implementation becomes a high-risk AI system subject to extensive provider obligations under the AIA and, more critically, to banking regulation requirements that may prove prohibitive. The four use cases thus

illustrate a regulatory spectrum: from extremely limited transparency-only obligations at the low end to effective prohibition at the high end.

3.2 Customer chatbot: analysis

3.2.1 Regulatory burden

3.2.1.1 AIA status

The customer chatbot is an Article 50 limited-risk system under the AIA. It does not fall under HRAIS rules as it is not intended for creditworthiness assessment or insurance risk pricing. The regulatory burden is moderate but manageable.

Customer chatbot: AIA status per deployment modality and value chain actor	
System as a Service	The institution procures a fully packaged AI application from a vendor. The vendor controls model weights, training data, inference architecture, and system design. The institution operates the application as delivered.
Vendor AIA status	(SR)GPAIM, GPAIS, LRAIS provider.
Institution AIA status	LRAIS deployer.
API integration	The institution accesses a vendor model through a cloud API and builds its own application layer around it. The institution designs the system. The vendor supplies the inference engine.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS and LRAIS provider and deployer.
RAG integration	The institution connects a model to proprietary or external knowledge bases to ground its outputs. Retrieval augmentation is an architectural feature that can combine with any other configuration.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS and LRAIS provider and deployer.
Proprietary finetuning	The institution has modified model weights through additional training on proprietary data. The institution controls both the model and any system layer built on top of it.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	Potentially GPAIM provider, if the compute threshold is met. GPAIS and LRAIS provider and deployer.

3.2.1.2 AIA obligations

AIA obligations centre on Article 50 transparency requirements. Article 50(1) requires that customers are informed they are interacting with an AI system. A simple introductory message likely suffices. Article 50(2) requires providers to mark synthetic content in a machine-readable format. For plain text, persistent marking is technically challenging as watermarks or metadata are easily stripped when content is copied. Compliance is, however, assessed against what is currently technically feasible.

Deployer obligations under Articles 50(3) and 50(4) are not triggered in typical one-to-one customer service exchanges. Article 50(3) mandates disclosure if the

system employs emotion recognition or biometric categorisation. Article 50(4) could apply if the system generates text that is published to inform the public on matters of public interest. The latter could happen, for example, if chatbot outputs are reused as public FAQs or posted on social media without human review.

Customer chatbot: AIA obligations per deployment modality and value chain actor	
SaaS	
Vendor obligations	GPAIM provider: Art. 53Potentially SRGPAIM provider: Art. 55LRAIS provider: Art. 50
Institution obligations	LRAIS deployer: Art. 50
API integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	LRAIS provider: Art. 50 LRAIS deployer: Art. 50
RAG integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	LRAIS provider: Art. 50 LRAIS deployer: Art. 50
Proprietary finetuning	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	Potentially GPAIM provider: Art. 53 LRAIS provider: Art. 50 LRAIS deployer: Art. 50

3.2.1.3 Banking regulation obligations

Banking regulation imposes no AI-specific requirements. Investor protection rules impose constraints on the chatbot’s functional scope, prohibiting, for example, investment advice without appropriate authorisation. To avoid the risk, the chatbot use case must be technically restricted to general information provision only. Banking secrecy requires that the model architecture prevent cross-contamination of customer data.

Banking regulation obligations	
EBA Guidelines on arrangements(EBA/GL/20 19/02) (Now integrated into DORA)	Outsourcing requires precontractual risk analysis and mitigation. Outsourcing requires obtaining access, information, and audit rights to outsourced assets. Outsourcing requires exit plans.

3.2.2 Analysis

SaaS and Cloud-based API access modalities raise non-AIA concerns. DORA outsourcing requirements, banking secrecy and GDPR compliance become salient when customer data flows to external providers.

Cloud-based API and RAG implementations shift AIS responsibilities to the institution while leaving GPAIM obligations with the vendor. As the system is not used in an AIA high-risk use case, the AIS provider is subject to no substantive AIA requirements beyond Article 50 transparency obligations.

In fine-tuned LLM implementations, the institution is a non-high-risk LRAIS provider, mirroring the burden institutions face in RAG implementations. Fine-tuning may push the institution into GPAI model provider status if the training compute exceeds one-third of the original model's compute, a threshold unlikely to be reached in practice. Even then, the institution will be the provider for the retrained parts of the model only.

Customer chatbot analysis		
SaaS	Technical feasibility.	Reliability may be adequate, but the institution has limited control over localization, output behaviour, and version updates, which are managed by the vendor.
	AI Act red flags.	None. Institution assumes LRAIS deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Risk that informational outputs are perceived as or drift into financial advice, potentially triggering conduct-of-business rules.
API integration	Technical feasibility.	Reliability may be adequate and the institution retains control over prompt design, output processing, and UI behaviour. However, localization of the underlying model and vendor-side version changes remain challenging.
	AI Act red flags.	None. Institution assumes LRAIS provider and deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Informational-to-advice drift risk.
RAG integration	Technical feasibility.	Reliability sweet spot with localized data and cheap data updates.
	AI Act red flags.	None. Institution assumes LRAIS provider and deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Local retrieval component reduces data exposure, but retrieved context may still be transmitted to an externally hosted model for generation. Informational-to-advice drift risk.

Proprietary finetuning	Technical feasibility.	Reliability overkill and brittle. Data updates likely prohibitively expensive.
	AI Act red flags.	Financial institution is possibly a GPAIM provider on top of LRAIS provider and deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance mitigated by likely local cloud deployment. Informational-to-advice drift risk.

3.3 Employee copilot: analysis

3.3.1 Regulatory burden

3.3.1.1 AIA status

The employee copilot is an Article 50 limited-risk system under the AIA. It does not fall under HRAIS rules unless repurposed for workforce monitoring, recruitment or credit decisions.

Employee copilot: AIA status per deployment modality	
System as a Service	The institution procures a fully packaged AI application from a vendor. The vendor controls model weights, training data, inference architecture, and system design. The institution operates the application as delivered.
Vendor AIA status	(SR)GPAIM, GPAIS, LRAIS provider.
Institution AIA status	LRAIS deployer.
API integration	The institution accesses a vendor model through a cloud API and builds its own application layer around it. The institution designs the system. The vendor supplies the inference engine.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS and LRAIS provider and deployer.
RAG integration	The institution connects a model to proprietary or external knowledge bases to ground its outputs. Retrieval augmentation is an architectural feature that can combine with any other configuration.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS and LRAIS provider and deployer.
Proprietary finetuning	The institution has modified model weights through additional training on proprietary data. The institution controls both the model and any system layer built on top of it.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	Potentially GPAIM provider, if the compute threshold is met. GPAIS and LRAIS provider and deployer.

3.3.1.2 AIA obligations

AIA obligations are limited to Article 50 transparency requirements. Article 50(1) requires providers to build system features that ensure users are informed when they are interacting with an AI system. As long as the system is not publicly deployed and does not produce deepfake content, Articles 50(3) and 50(4) deployer obligations are not triggered.

Employee copilot: AIA obligations per deployment modality and value and chain actor
System as a service

Vendor obligations	GPAIM provider: Art. 53Potentially SRGPAIM provider: Art. 55LRAIS provider: Art. 50
Institution obligations	LRAIS deployer: Art. 50
API integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	LRAIS provider: Art. 50 LRAIS deployer: Art. 50
RAG integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	LRAIS provider: Art. 50 LRAIS deployer: Art. 50
Proprietary finetuning	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	Potentially GPAIM provider: Art. 53 LRAIS provider: Art. 50 LRAIS deployer: Art. 50

3.3.1.3 Banking regulation obligations

Banking regulations impose no specific requirements. CRR operational risk management necessitates human verification of outputs before use, but the requirement is a general governance one rather than an AI-specific obligation.

Employee copilot: banking regulation obligations	
EBA Guidelines on arrangements (EBA/GL/2019/02) (Now integrated into DORA)	Outsourcing requires precontractual risk analysis and mitigation. Outsourcing requires obtaining access, information, and audit rights to outsourced assets. Outsourcing requires exit plans.

3.3.2 Analysis

SaaS and Cloud-based API access modalities raise non-AIA concerns. DORA outsourcing requirements, banking secrecy and GDPR compliance become salient when customer data flows to external providers. If these concerns can be addressed, cloud-based API access minimises the institution's regulatory exposure. The vendor bears GPAI model and system provider obligations. The institution's duties are limited to deployer-side transparency.

Cloud-based API and RAG implementations shift AIS responsibilities to the institution while leaving GPAIM obligations with the vendor. As the system is not used in an AIA high-risk use case, the AIS provider is subject to no substantive AIA requirements beyond Article 50 transparency obligations.

In fine-tuned LLM implementations, the institution is a non-high-risk LRAIS provider, mirroring the burden institutions face in RAG implementations. Fine-tuning may push the institution into GPAI model provider status if the training compute exceeds one-third of the original model's compute, a threshold unlikely to be reached in practice. Even then, the institution will be the provider for the retrained parts of the model only.

Employee copilot: analysis		
SaaS	Technical feasibility.	Reliability may be adequate, but the institution has limited control over localization, output behaviour, and version updates, which are managed by the vendor.
	AI Act red flags.	None. Institution assumes LRAIS deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance.
API integration	Technical feasibility.	Reliability may be adequate and the institution retains control over prompt design, output processing, and UI behaviour. However, localization of the underlying model and vendor-side version changes remain challenging.
	AI Act red flags.	None. Institution assumes LRAIS provider and deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance.
RAG integration	Technical feasibility.	Reliability sweet spot with localized data and cheap data updates.
	AI Act red flags.	None. Institution assumes LRAIS provider and deployer role with associated system-level obligations.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Local retrieval component reduces data exposure, but retrieved context may still be transmitted to an externally hosted model for generation.
Proprietary finetuning	Technical feasibility.	Reliability overkill and brittle. Data updates likely prohibitively expensive.
	AI Act red flags.	Financial institution is possibly a GPAIM provider on top of LRAIS provider and deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance mitigated by likely local cloud deployment.

3.4 Credit decision copilot

3.4.1 Regulatory burden

3.4.1.1 AIA status

Credit decision copilot systems are unambiguously high-risk AI systems under AIA Annex III point 5(b). Except in the SaaS case, the institution is both a HRAIS provider and deployer, triggering the full range of HRAIS obligations. In the SaaS case, the institution is a deployer only.

Credit decision copilot: AIA status per deployment modality and value and chain actor	
System as a Service	Pre-built system procured from a third-party vendor who retains control over the underlying model, its updates, output filtering, and system-level configurations. The institution operates the system through a vendor-defined interface with limited ability to modify its behaviour.
Vendor AIA status	(SR)GPAIM, GPAIS, LRAIS, HRAIS provider.
Institution AIA status	LRAIS and HRAIS deployer.
API integration	Connects banking applications directly to a vendor-hosted model (e.g., OpenAI, Anthropic) via secure endpoints. Model maintenance is offloaded entirely to the third-party provider. User interface created and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
RAG integration	Couples a generative model with an internal, vectorized knowledge base. The system retrieves relevant banking documents to augment the prompt context before generation occurs. Model maintenance is offloaded entirely to the third-party provider. RAG integration implemented and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
Proprietary finetuning	Adapts a generative model to institution-specific tasks by further training it on a curated dataset of the bank's historical data, embedding domain-specific terminology, style, and logic directly into the model's parameters. Fine-tuning may range from parameter-efficient methods to full retraining of all model weights. Model and user interface maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	Potentially GPAIM provider, if the compute threshold is met. GPAIS, LRAIS and HRAIS provider and deployer.

3.4.1.2 AIA obligations

AIA HRAIS obligations are substantial. Providers must comply with Articles 9 to 15. Article 14 human oversight is critical. The institution must maintain technical capability to interpret outputs, intervene and override decisions. Effective oversight with complex generative models is challenging. Deployers must

comply with Articles 26 to 27, including the Article 27 fundamental rights impact assessment.

Credit decision copilot: AIA obligations per deployment modality and value and chain actor	
System as a Service	Pre-built system procured from a third-party vendor who retains control over the underlying model, its updates, output filtering, and system-level configurations. The institution operates the system through a vendor-defined interface with limited ability to modify its behaviour.
Vendor AIA status	(SR)GPAIM, GPAIS, LRAIS, HRAIS provider.
Institution AIA status	LRAIS and HRAIS deployer.
API integration	Connects banking applications directly to a vendor-hosted model (e.g., OpenAI, Anthropic) via secure endpoints. Model maintenance is offloaded entirely to the third-party provider. User interface created and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
RAG integration	Couples a generative model with an internal, vectorized knowledge base. The system retrieves relevant banking documents to augment the prompt context before generation occurs. Model maintenance is offloaded entirely to the third-party provider. RAG integration implemented and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
Proprietary finetuning	Adapts a generative model to institution-specific tasks by further training it on a curated dataset of the bank's historical data, embedding domain-specific terminology, style, and logic directly into the model's parameters. Fine-tuning may range from parameter-efficient methods to full retraining of all model weights. Model and user interface maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	Potentially GPAIM provider, if the compute threshold is met. GPAIS, LRAIS and HRAIS provider and deployer.

3.4.1.3 Banking regulation obligations

Within banking regulation, credit decision automation is permitted for credits for which it is “appropriate” (EBA Guidelines, para 41). Credit decision automation is thus *prima facie* feasible for a subset of credits.

The scope of credits eligible for automation is unclear. The “appropriateness” standard in EBA Guidelines is ambiguous. More critically, supervisory approval of generative AI-based credit decision automation solutions seems unlikely.

CRD Article 79 requires that credit granting is based on sound criteria and internal credit risk methodologies. EBA Guidelines permit automated models

but require that institutions understand the models, their methodology, assumptions, limitations and outputs (EBA Guidelines, para 54). The requirement is problematic for LLMs. Generic language models cannot be explained as traditional statistical models can. Unlike traditional statistical scorecards, LLMs cannot produce consistent, reproducible and granular explanations for credit decisions. The features may create prohibitive barriers to generative AI adoption in credit decision automation.

The Guidelines further require bias detection procedures, backtesting and model override mechanisms. The mechanisms are potentially feasible but demanding to implement.

CRR Article 179 imposes additional requirements on IRB institutions. The institution must be able to break down its loss experience by credit risk parameters (PD, LGD, conversion factor and expected loss) and use the breakdown in credit decision-making. The requirement appears insurmountable for LLM-based systems.

In sum, implementing a credit decision automation solution where a generative AI module executes the creditworthiness assessment is unlikely to be approved by supervisors. Embedding generative AI components into credit decision automation workflows where creditworthiness assessment is performed by statistical models seems possible. The caveats identified in the credit decision copilot case, however, apply.

Banking regulation obligations		
EBA Guidelines: institutions should		
	understand the models used, and their methodology, input data, assumptions, limitations and outputs.	Compliance may be impossible, but GenAI models could perform limited tasks within broader support systems.
	have in place internal policies and procedures detecting and preventing bias and ensuring the quality of the input data	Compliance may be challenging for bias analysis and prevention.
	have in place measures to ensure the traceability, auditability, and robustness and resilience of the inputs and outputs;	Compliance may be challenging for ensuring robustness and resilience.
	have in place internal policies and procedures ensuring that the quality of the model output is regularly assessed, using measures appropriate to the model's use, including backtesting the performance of the model	Compliance may be challenging.
	have in place control mechanisms, model overrides and escalation procedures within the regular credit decision-making framework, including qualitative	Compliance likely feasible.

	approaches, qualitative risk assessment tools (including expert judgement and critical analysis) and quantitative limits.	
	have adequate model documentation covering methodology, assumptions and data inputs, and an approach to detecting and preventing bias and ensuring the quality of input data;	Compliance may be challenging.
	have adequate model documentation covering the use of model outputs in the decision-making process and the monitoring of these automated decisions on the overall quality of the portfolio or products in which these models are used.	Compliance likely feasible.
CRR Art 179: Break down		
	loss experience by credit risk parameters (PD, LGD, conversion factor and expected loss) and use the breakdown in credit decision-making.	Compliance likely impossible.

3.4.2 Analysis

Banking regulation demands on model explainability and methodologies jeopardise feasibility regardless of deployment modality.

SaaS and cloud-based API access modalities raise additional non-AIA concerns. DORA outsourcing requirements, banking secrecy and GDPR compliance become salient when customer data flows to external providers. As the institution is a financial sector HRAIS deployer in both modalities, it is subject to AIA Articles 26 and 27, including the obligation to conduct a fundamental rights impact assessment.

In non-SaaS deployments, the institution is a HRAIS provider and subject to the full gamut of HRAIS provider rules. The vendor's GPAIM provider obligations under Article 53 run in parallel but do not substitute the institution's own HRAIS obligations.

Credit decision co-pilot: analysis		
SaaS	Technical feasibility.	Possible mismatch in model capability and need. The institution has limited control over localization, output behaviour, and version updates, which are managed by the vendor. Version control may be challenging or impossible.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS deployer.
	Other regulatory red flags.	EBA Guidelines (requirements for automation in credit assessment/decision-making) and CRR requirements likely render credit decision copilot use infeasible.

		DORA outsourcing, banking secrecy, and GDPR compliance likely challenging.
API integration	Technical feasibility.	Possible mismatch in model capability and need. Version control may be challenging. The institution retains control over prompt design, output processing, and UI behaviour. However, localization of the underlying model and vendor-side version changes remain challenging.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS provider and deployer.
	Other regulatory red flags.	EBA Guidelines (requirements for automation in credit assessment/decision-making) and CRR requirements likely render credit decision copilot use infeasible. DORA outsourcing, banking secrecy, and GDPR compliance likely challenging.
RAG integration	Technical feasibility.	Possible mismatch in model capability and need. Reliability increased by localized data and cheap data updates.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS provider and deployer.
	Other regulatory red flags.	EBA Guidelines (requirements for automation in credit assessment/decision-making) and CRR requirements likely render credit decision copilot use infeasible. DORA outsourcing, banking secrecy, and GDPR compliance. Local retrieval component reduces data exposure, but retrieved context may still be transmitted to an externally hosted model for generation.
Proprietary finetuning	Technical feasibility.	Possible mismatch in model capability and need. Brittle, updates expensive.
	AI Act red flags.	Financial institution is possibly a GPAIM provider as well as HRAIS provider and deployer.
	Other regulatory red flags.	EBA Guidelines (requirements for automation in credit assessment/decision-making) and CRR requirements likely render credit decision copilot use infeasible. DORA outsourcing, banking secrecy, and GDPR compliance mitigated by likely local cloud deployment.

3.5 Credit decision automation

3.5.1 Regulatory burden

3.5.1.1 AIA status

Credit decision automation systems are unambiguously high-risk AI systems under AIA Annex III point 5(b). Except for the SaaS case, the institution is both a HRAIS provider and deployer, triggering the full range of HRAIS obligations. In the SaaS case, the institution would be a HRAIS deployer.

Credit decision automation: AIA status per deployment modality and value and chain actor	
System as a Service	Pre-built system procured from a third-party vendor who retains control over the underlying model, its updates, output filtering, and system-level configurations. The institution operates the system through a vendor-defined interface with limited ability to modify its behaviour.
Vendor AIA status	(SR)GPAIM, GPAIS, LRAIS, HRAIS provider.
Institution AIA status	LRAIS and HRAIS deployer.
API integration	Connects banking applications directly to a vendor-hosted model (e.g., OpenAI, Anthropic) via secure endpoints. Model maintenance is offloaded entirely to the third-party provider. User interface created and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
RAG integration	Couples a generative model with an internal, vectorized knowledge base. The system retrieves relevant banking documents to augment the prompt context before generation occurs. Model maintenance is offloaded entirely to the third-party provider. RAG integration implemented and maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	GPAIS, LRAIS and HRAIS provider and deployer.
Proprietary finetuning	Adapts a generative model to institution-specific tasks by further training it on a curated dataset of the bank's historical data, embedding domain-specific terminology, style, and logic directly into the model's parameters. Fine-tuning may range from parameter-efficient methods to full retraining of all model weights. Model and user interface maintained by the institution.
Vendor AIA status	(SR)GPAIM provider.
Institution AIA status	Potentially GPAIM provider, if the compute threshold is met. GPAIS, LRAIS and HRAIS provider and deployer.

3.5.1.2 AIA obligations

AIA HRAIS obligations are substantial. Providers must comply with Articles 9 to 15. Article 14 human oversight is critical. The institution must maintain technical capability to interpret outputs, intervene and override decisions. Effective oversight with complex generative models is challenging. Deployers must comply with Articles 26 to 27, including the Article 27 fundamental rights impact assessment.

Credit Decision Automation: AIA Obligations per deployment modality and value and chain actor	
SaaS	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55 HRAIS provider: Art. 9–19 (and all procedural obligations) Art. 50 provider transparency obligations apply
Institution obligations	HRAIS deployer: Art. 26, 27 Art. 50 deployer transparency obligations apply
API integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	HRAIS provider: Art. 9–19 (and all procedural obligations) HRAIS deployer: Art. 26, 27 Art. 50 transparency obligations apply
RAG integration	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	HRAIS provider: Art. 9–19 (and all procedural obligations) HRAIS deployer: Art. 26, 27 Art. 50 transparency obligations apply
Proprietary finetuning	
Vendor obligations	GPAIM provider: Art. 53 Potentially SRGPAIM provider: Art. 55
Institution obligations	Potentially GPAIM provider: Art. 53 Potentially (but unlikely) SRGPAIM provider: Art. 55 HRAIS provider: Art. 9–19 (and all procedural obligations) HRAIS deployer: Art. 26, 27 Art. 50 deployer transparency obligations apply

3.5.1.3 Banking regulation obligations

Within banking regulation, credit decision automation is permitted for credits for which it is “appropriate” (EBA Guidelines, para 41). Credit decision automation is thus prima facie feasible and permitted for a subset of credits.

The scope of credits eligible for automation is first unclear, as the “appropriateness” standard in EBA Guidelines is ambiguous. Second, and

critically, supervisors seem unlikely to approve generative AI-based credit decision automation solutions.

CRD Article 79 requires that credit granting is based on sound criteria and internal credit risk methodologies. The EBA Guidelines permit automated models but require that institutions understand the models, their methodology, assumptions, limitations and outputs (EBA Guidelines, para 54). The requirement is problematic for LLMs. Generic language models cannot be explained as traditional statistical models can. Unlike traditional statistical scorecards, LLMs cannot produce consistent, reproducible and granular explanations for credit decisions. The features may create prohibitive barriers to generative AI adoption in credit decision-making automation.

The Guidelines further require bias detection procedures, backtesting and model override mechanisms (EBA Guidelines, paras 53 and 55). The mechanisms are potentially feasible but demanding to implement.

CRR Article 179 imposes additional requirements on IRB institutions. The institution must be able to break down its loss experience by credit risk parameters (PD, LGD, conversion factor, expected loss) and use the breakdown in its credit decision-making. The requirement appears insurmountable for LLM-based systems.

In sum, implementing a credit decision automation solution where a generative AI module executes the creditworthiness assessment is unlikely to be approved by supervisors. Embedding generative AI components into credit decision automation workflows where creditworthiness assessment is performed, e.g., by statistical models seems possible. The caveats identified in the credit decision copilot case, however, apply.

Banking regulation obligations		
EBA Guidelines: institutions may use automated decision-making in the credit-granting process, but		
	Credit risk policies and procedures should specify [...] conditions for the application of automated decision-making in the credit-granting process,	Compliance is feasible.
	Institutions may use automated decision-making only when “appropriate”.including identifying products, segments and limits for which automated decision-making is allowed.	Compliance is feasible.
EBA Guidelines: institutions should		

	understand the models used, and their methodology, input data, assumptions, limitations and outputs.	Compliance may be impossible, but GenAI models could perform limited tasks within broader support systems.
	have in place internal policies and procedures detecting and preventing bias and ensuring the quality of the input data	Compliance may be challenging for bias analysis and prevention.
	have in place measures to ensure the traceability, auditability, and robustness and resilience of the inputs and outputs;	Compliance may be challenging for ensuring robustness and resilience.
	have in place internal policies and procedures ensuring that the quality of the model output is regularly assessed, using measures appropriate to the model's use, including backtesting the performance of the model	Compliance may be challenging.
	have in place control mechanisms, model overrides and escalation procedures within the regular credit decision-making framework, including qualitative approaches, qualitative risk assessment tools (including expert judgement and critical analysis) and quantitative limits.	Compliance likely feasible.
	have adequate model documentation covering methodology, assumptions and data inputs, and an approach to detecting and preventing bias and ensuring the quality of input data;	Compliance may be challenging.
	have adequate model documentation covering the use of model outputs in the decision-making process and the monitoring of these automated decisions on the overall quality of the portfolio or products in which these models are used.	Compliance likely feasible.
CRR Art 179: Break down		
	loss experience by credit risk parameters (PD, LGD, conversion factor and expected loss) and use the breakdown in credit decision-making.	Compliance likely impossible.

3.5.2 Analysis

Banking regulation demands on model explainability and methodologies jeopardize feasibility regardless of deployment modality.

SaaS and cloud-based API access modalities raise additional non-AIA concerns: DORA outsourcing requirements, banking secrecy and GDPR compliance become salient when customer data flows to external providers. As the institution is a financial sector HRAIS deployer in both modalities, it is subject to AIA Article 26 and 27 requirements imposing, e.g., an obligation to conduct a fundamental rights impact assessment.

In non-SaaS deployments, the institution is a HRAIS provider and subject to the full gamut of HRAIS provider rules. The vendor's GPAIM provider obligations (Article 53) run in parallel but do not substitute the institution's HRAIS obligations.

Credit decision automation: analysis		
SaaS	Technical feasibility.	Possible mismatch in model capability and need. The institution has limited control over localization, output behaviour, and version updates, which are managed by the vendor. Version control may be challenging or impossible.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Following from EBA Guidelines (para 54, requirements for automation in credit assessment/decision-making), credit decision automation is likely not allowed.
API integration	Technical feasibility.	Possible mismatch in model capability and need. Version control may be challenging. The institution retains control over prompt design, output processing, and UI behaviour. However, localization of the underlying model and vendor-side version changes remain challenging.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS provider and deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Following from EBA Guidelines (para 54, requirements for automation in credit assessment/decision-making), credit decision automation is likely not allowed.
RAG integration	Technical feasibility.	Possible mismatch in model capability and need. Reliability increased by localized data and cheap data updates.
	AI Act red flags.	The system is a HRAIS and the financial institution is a HRAIS provider and deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance. Local retrieval component reduces data exposure, but retrieved context may still be transmitted to an externally hosted model for generation. Following from EBA Guidelines (para 54, requirements for automation in credit assessment/decision-making), credit decision automation is likely not allowed.
Proprietary finetuning	Technical feasibility.	Possible mismatch in model capability and need. Brittle, updates expensive.
	AI Act red flags.	Financial institution is possibly a GPAIM provider as well as HRAIS provider and deployer.
	Other regulatory red flags.	DORA outsourcing, banking secrecy, and GDPR compliance mitigated by likely local cloud deployment. Following from EBA Guidelines (para 54, requirements for automation in credit assessment/decision-making), credit decision automation is likely not allowed.

4 Conclusions

4.1 The regulatory framework in brief

Generative AI deployments in credit institutions are governed by multiple overlapping regulatory frameworks. The report examines two: the EU AI Act and sectoral banking regulation, specifically the CRR, CRD and the EBA Guidelines on loan origination and monitoring. Data protection rules, operational and cyber resilience regulation, and banking secrecy rulesets are relevant to generative AI deployments but fall outside the report's scope.

The AI Act and banking regulation frameworks are built on divergent conceptual grounds, but they share some common traits.

The objectives for the rulesets differ. The AIA seeks to protect individuals' health, safety and fundamental rights from harms generated by AI systems. Banking regulation serves primarily micro and macroprudential goals.

The regulatory approaches differ. In the AIA, the level of obligations that AI systems providers and deployers face follows the perceived risks of AI system types. The AIA prohibits excessive risk AI applications. High-risk AI systems are subject to relatively strict, yet mainly process-based regulatory requirements. Limited risk AI system providers and deployers face transparency demands. General-purpose AI providers are subject to a sui generis regulatory framework, while the AIA imposes no regulatory requirements on minimal risk AI systems and preempts member state regulation targeting the systems.

Banking regulation is a complex amalgam of varying regulatory approaches. It combines capital adequacy rules, conduct of business requirements, process-based internal control rules and supervisory review processes with a market discipline framework to build an interlocking compliance framework. The capital adequacy and market discipline rules target banks by manipulating group level incentives, but the other rulesets extend to banks' organizational practices and even individual employees.

In the four use cases, all AIA obligation levels except the bans are relevant. The banking regulation aspects focus primarily on bank internal control processes, but capital adequacy rules play a limited role. Here the similarities between the two frameworks become visible. Both deploy regulatory strategies that target technologies and internal control mechanisms. The AIA seeks to regulate high-risk AI systems through setting technical requirements on the systems. The requirements impose process-based obligations on deployers and providers. Banking regulation similarly imposes requirements on technologies that banks use for credit decisions, but also seeks to affect banks' internal organisation. Details, however, differ. Where the AIA forces providers to implement and run a risk management system to curb health, safety and fundamental rights risks in the AI systems, banking regulation focuses on model-level explainability and auditability of credit decision algorithms. Both also require testing and data governance, but the EBA Guidelines additionally require backtesting.

4.2 Use cases and deployment modalities

4.2.1 Analysis structure

The report examined four use cases:

1. employee copilot,
2. customer chatbot,
3. credit decision copilot, and
4. credit decision automation,

and four deployment modalities for each use case:

1. SaaS service procurement,
2. API-based access to vendor LLM,
3. RAG implementation, and
4. Proprietary fine-tuned LLM.

The use cases were chosen based on a limited literature review and a limited number of stakeholder interactions to reflect possible applications in which banks could utilize GenAI technologies.

The interviews suggested that banks had multiple options for how they could technically implement and deploy the applications. Based on a limited number of stakeholder interactions, the four deployment modalities the report discusses were chosen. While other reports often do not discuss the

deployment modalities, they are important. A preliminary analysis of AIA compliance suggested that the deployment modality affects the allocation of AIA obligations along the value chain.

4.2.2 Use cases

The employee copilot is an internal productivity tool for bank staff. The system assists with document summarisation, drafting and internal communication. It does not interact with customers or make decisions.

The customer chatbot is an LLM-based system that answers customer queries and provides general product information. It does not execute transactions, make credit decisions or provide investment advice. The system operates in direct one-to-one exchanges with customers.

The credit decision copilot is an LLM-based tool that supports human credit decision-makers. The system summarises loan applicant data and flags risks. A human officer retains formal decision-making authority.

Credit decision automation implements an LLM-based system that makes binding credit decisions without human intervention. The system autonomously assesses creditworthiness and produces loan decisions.

4.2.3 Deployment modalities

In the SaaS deployment modality, the institution procures a fully packaged system from a vendor and acts as a pure deployer. The vendor supplies and operates the entire stack. No internal development is required.

In the cloud-based API deployment modality, the institution builds the application layer and calls a third-party LLM through an API. The vendor hosts and operates the underlying model. The institution controls application logic but not the model.

In the RAG deployment modality, the institution integrates its own knowledge sources with a base LLM at inference time using retrieval-augmented generation. Model weights are not modified. The system combines vendor model capabilities with institution-controlled data.

In the proprietary fine-tuning deployment modality, the institution fine-tunes a base LLM on proprietary data to adapt it to domain-specific tasks. Model weights are modified. The vendor supplies the base model. The institution controls the adaptation process and the resulting model variant.

4.3 Findings

The findings follow the two analytical dimensions of the report. The first subsection addresses how deployment modality affects the allocation of AIA obligations along the value chain. The subsection also makes limited observations related to other relevant regulations. The second subsection addresses feasibility by use case.

4.3.1 By deployment modality

In SaaS deployments, the institution is a pure deployer. For low-risk use cases, obligations are limited to Article 50 transparency. For HRAIS use cases, the institution's obligations are limited to Articles 26 to 27, including the FRIA. The vendor bears all provider-side obligations. The arrangement minimises AIA burden but creates independent problems. DORA outsourcing rules, banking secrecy obligations and GDPR data residency requirements all become acute when customer data leaves the institution's environment. For credit-related processes, SaaS is therefore typically problematic regardless of AIA classification.

In the cloud-based API deployment modality, the institution becomes the system provider while the LLM vendor remains the model provider. For low-risk use cases the modality adds no substantive obligations beyond Article 50. For HRAIS use cases it triggers the full Articles 9 to 21 provider stack. The vendor retains GPAI model obligations under Articles 53 and potentially 55, but they run in parallel and do not substitute for the institution's own HRAIS duties. The same DORA and data residency concerns as in SaaS apply if the API call involves customer data leaving the institution's environment.

The RAG deployment modality carries the same AIA obligation profile as cloud API. The institution is system provider, the LLM vendor is model provider. Standard RAG does not modify model weights and therefore does not push the institution into GPAI model provider status. The boundary is meaningful. A well-designed RAG architecture limits the institution's AIA exposure to the system layer while keeping the regulatory burden of the underlying model with the vendor. RAG also offers a partial answer to the infrastructure problem. A RAG implementation running on private or controlled-cloud infrastructure can avoid the DORA and banking secrecy issues that public API calls raise.

The proprietary fine-tuning deployment modality carries the same HRAIS obligation profile as RAG and cloud API for system-level purposes. The additional question is whether fine-tuning volume crosses the one-third-of-original-compute threshold that would push the institution into GPAI model

provider status under Articles 53 and potentially 55. In practice the threshold is rarely reached in standard domain adaptation fine-tuning. Below the threshold, the institution is provider only for the modified components, with the base model vendor retaining model-level obligations.

4.3.2 By use case

Employee copilot — feasible. The system is a limited-risk AI system under Article 50 AIA. Banking regulation imposes no AI-specific obligations. The institution's compliance burden is minimal: inform users they are interacting with an AI, and enforce human verification of outputs as an operational risk control. The main constraint is governance rather than law.

Customer chatbot — feasible. Also a limited-risk system under Article 50. The key obligations are transparency toward customers and strict scope limitation. The chatbot must be technically restricted from offering investment advice or executing transactions, which would trigger MiFID II liability. Model architecture must prevent cross-contamination of customer data. Compliance is achievable but requires deliberate technical design.

Credit decision copilot — legally uncertain. The system likely falls under HRAIS classification as a creditworthiness assessment tool, triggering Articles 9 to 21 (provider) and 26 to 27 (deployer), including a fundamental rights impact assessment. The more acute problem is definitional. If the copilot filters and summarises applicant data in a way the human decision-maker cannot effectively challenge, supervisors may treat it as de facto automation regardless of formal role allocation. The ambiguity is unresolved in current regulation and guidance. Establishing a defensible position requires proactive engagement with the competent supervisory authority.

Credit decision automation — not feasible under current interpretations. The system is unambiguously high-risk under Annex III AIA, triggering the full provider and deployer compliance stack. The binding constraint is not the AIA but banking regulation. EBA Guidelines require institutions to understand model methodology, assumptions and limitations, and to produce consistent, auditable, backtestable outputs. LLMs are probabilistic and non-deterministic. The same input may produce different outputs, and the model cannot be decomposed into the credit risk parameters the Guidelines contemplate. For IRB institutions, CRR Article 179 adds a further requirement to break down loss experience by PD, LGD and conversion factor, a requirement that appears insurmountable for LLM-based systems. Full automation may become feasible if supervisors accept new interpretability methods or if model technology evolves toward greater determinism. Neither condition is currently met.

4.3.3 Cross-cutting observations

The explainability gap is the central obstacle. The AIA's human oversight requirements and banking regulation's explainability demands converge on the same technical problem. LLMs cannot produce the granular, reproducible justifications that regulators and courts require for consequential credit decisions. The gap is not a compliance design problem but a fundamental architectural one.

Information asymmetry in the GPAI value chain. Financial institutions deploying third-party foundation models face a structural gap. The AIA Code of Practice permits GPAI providers to reserve bias detection and data quality information for regulators rather than disclosing the information to downstream deployers. Institutions may therefore be unable to fully satisfy their own EBA governance obligations through the information available to them.

Infrastructure is a prerequisite, not an afterthought. For all credit-related use cases, public cloud API deployment creates independent obstacles under GDPR data residency rules, banking secrecy laws and DORA outsourcing requirements. A private or controlled-cloud environment is likely necessary before AIA compliance analysis becomes relevant.