THE CHAIRPERSON

European Banking Authority

Floor 24-27, Tour Europlaza
20 Avenue André Prothin
92400 Courbevoie, France

T: +33 186 526 831
E: JoseManuel.Campa@eba.europa.eu

https://eba.europa.eu

EBA/2025/D/5384

John Berrigan
Director General
Directorate-General for Financial Stability,
Financial Services and Capital Markets Union (FISMA)
European Commission
Rue de Spa 2
1049 Brussels
Belgium

Roberto Viola
Director General
Directorate-General for Communications Networks, Content and Technology (CNECT)
European Commission
Rue de la Loi 51
1040 Brussels
Belgium

21 November 2025

Subject: Outcome of EBA's AI Act mapping exercise

Dear Mr Berrigan, Mr Viola,

The EBA welcomes the forthcoming entry into application of Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence ('AI Act'). The EBA is actively engaged in supporting the EC's work on ensuring a coordinated and consistent implementation of the AI Act across the EU banking and payments sector, including through its role as observer in the EU AI Board's Subgroup on Financial Services.

In January 2025 the EBA established a dedicated workstream to map the AI Act against relevant provisions in EU banking and payments sectoral frameworks applying to the use of AI systems for creditworthiness assessment or credit scoring of natural persons, due to its classification as high-risk under Annex III(5)(b) of the AI Act. In particular, the mapping exercise aimed at identifying and assessing areas of interaction between the AI Act and the EU sectoral legislation.

To this extent, while the AI Act recognises overlaps between some requirements on high-risk AI systems and EU financial sector law and for this purpose envisages targeted derogations and other types of synergies (i.e. integration or combination of requirements) for some requirements, the EBA notes that the AI Act does not envisage targeted derogations or other regulatory synergies for other

requirements on high-risk AI systems (e.g. human oversight, data governance, cybersecurity), for which the EBA has found that the EU financial services law already includes a wide range of requirements. The DORA framework, for instance, extensively covers the cybersecurity and business continuity requirements set out in the AI Act. Similarly, the CRR/CRD requirements already provide a comprehensive and technology-neutral governance and risk management framework that can be leveraged upon when supervising the use of AI tools.

Since Article 96(1)(e) of the AI Act mandates the European Commission to issue Guidelines on the interplay between the AI Act and EU sectoral legislation, including EU banking and payments sector legislation, I am writing to share with you the outcome of the mapping exercise in relation to the application of the regulatory synergies envisaged by the AI Act. In the Annex to this letter, you can find a detailed identification of relevant EU banking and payments sectoral obligations in place related to all AI Act requirements on high-risk AI systems, including where the AI Act does not envisage derogations or other synergies.

The EBA is of the opinion that the list of provisions included in the Annex provides a comprehensive overview of how EU financial services law already addresses relevant AI Act requirements, and will be a useful instrument to inform the Guidelines on the interplay between AI Act and EU sectoral legislation, facilitate management of potential overlaps and complementarities, and ultimately ensure a smooth implementation of the AI Act in the EU banking and payment sector.

The EBA remains committed to supporting the Commission in the implementation of the AI Act, including via the AI Board subgroup on financial services or other relevant sub-structures, and stands ready to contribute further as needed.

Yours sincerely,

José Manuel Campa

CC: Ugo Bassi, Director Dir D, Banking, Insurance and Financial Crime, DG FISMA
Mattias Levin, Head of Unit D1, Bank regulation and supervision, DG FISMA
Lucilla Sioli, Director, AI Office, DG CNECT

Encl: Annex. EU banking and payments sector requirements relevant for AI Act regulatory synergies

Annex. EU banking and payments sector requirements relevant for AI Act regulatory synergies

Glossary:

- **CRR**: Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions. See: http://data.europa.eu/eli/reg/2013/575/2025-06-29
- **CRD**: Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions. See: http://data.europa.eu/eli/dir/2013/36/2025-01-17
- **CDR assessment methodology**: Commission Delegated Regulation (EU) 2022/439 of 20 October 2021 supplementing Regulation (EU) No 575/2013 (CRR) with regard to RTS for the specification of the assessment methodology CAs are to follow when assessing the compliance of credit institutions and investment firms with the requirements to use the IRB Approach. See: https://eur-lex.europa.eu/eli/reg_del/2022/439/oj/eng
- **EBA IG GLs**: Guidelines on internal governance under CRD. See: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-internal-governance-under-crd
- **EBA GLs on PD and LGD estimation**: Guidelines on PD estimation, LGD estimation and treatment of defaulted assets. See: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/model-validation/guidelines-pd-estimation-lgd
- **EBA LOM GLs**: Guidelines on loan origination and monitoring. See: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/credit-risk/guidelines-loan-origination-and-monitoring
- **DORA**: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. See: http://data.europa.eu/eli/reg/2022/2554/oj
- **CDR incident classification**: Commission Delegated Regulation (EU) 2024/1772 on RTS specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents. See: http://data.europa.eu/eli/reg_del/2024/1772/oj
- **CDR ICT risk management framework**: Commission Delegated Regulation (EU) 2024/1774 on RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework. See: http://data.europa.eu/eli/reg_del/2024/1774/2024-06-25
- **CCD2**: Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers. See: http://data.europa.eu/eli/dir/2023/2225/oj
- **MCD:** Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property. See: http://data.europa.eu/eli/dir/2014/17/2023-12-30
- **PSD:** Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. See: http://data.europa.eu/eli/dir/2015/2366/2025-01-17

AI Act requirements contemplating a full or partial derogation:

AI Act		Sectoral requirements
Quality management system	Article 17 (providers)	• **CRR**: Article 174 (use of models), Article 175 (documentation of rating systems), Article 176 (data maintenance), Article 185 (validation of internal estimates) • **EBA IG GLs**: Para 141 (internal control function responsibilities and authority for risk management), Para 145 (internal control framework), Para 167 (regulatory compliance assessment in new product approval policies), Para 172 (internal control unit heads' accountability to management body), Para 218 (internal audit function assessment of quality of control performed), Para 219 (internal audit function evaluation of quality of risk identification and assessment tools) • **DORA**: Article 5 (governance and organisation), Article 6 (ICT risk management framework) • **CCD2**: Article 18.3 (data relevance and accuracy), Article 18.4 (CWA procedures and documentation) • **MCD:** Article 18(2) (procedures and information on which CWA is based to be established, documented and maintained) • **PSD:** Article 5 (measures for safeguarding payment service users' funds, governance arrangements and internal control mechanisms) • **EBA LOM GLs**: para 38 (credit-granting monitoring), para 41 (credit risk policies and automated CWA models), para 54 (automated CWA model methodology), para 55 (model documentation), para 60 (data infrastructure, policies and procedures), para 63 (documentation of credit decision-making framework), para 65 (decision-making powers and limitations over automated CWA models), para 66 (credit decision-making power delegation), para 75 (allocation of credit risk management and internal control responsibilities)
Post-market monitoring	Article 26 (deployers)	• **CRD**: Article 74(1) (governance arrangements and processes to identify, manage, monitor and report risks) • **CRR**: Article 174(d) (regular cycle of model validation), Article 185 (rating system, process and estimation accuracy and consistency), Article 190(2) (CRCU responsibility in changes to rating process, review of rating criteria and ongoing review and alterations to models) • **EBA IG GLs**: Para 26 (management body oversight role for monitoring systems), Para 31 (business line processes and controls to ensure risk monitoring), Para 32 (risk management and compliance function monitoring and oversight of IT and other functions), Para 33 (risk management and compliance function responsibilities on monitoring of risks and compliance with legal requirements and internal policies), Para 191 (monitoring of all risks), Para 194 (business unit monitoring of risks), Para 210 (compliance function monitoring programme and policy) • **EBA LOM GLs**: Para 34 (monitoring of credit risk), Para 35 (proactive approach to monitoring credit quality), Para 38(h) (monitoring of circumstances and conditions for exceptional credit-granting decisions), Para 38(j) (monitoring of credit-granting activities during all phases), Para 42 (monitoring of suspicious or fraudulent behavior), Para 53(f) (model performance monitoring), Para 55(b) (model documentation to monitor automated decisions on the quality of portfolio or products in which models are used), Para 60 (data infrastructure to support credit risk monitoring)
Incident reporting	Article 26 (deployers) Article 73 (providers)	• **DORA**: Article 3(1) (definition of major ICT-related incident), Article 17(3) (ICT-related incident response procedures), Article 18(1) (framework for classification of incidents), Article 19(1) (reporting of major ICT-related incidents), Article 19(6) (reporting process of ICT-related incidents), Article 19(7) (notification process of ICT-related incidents) • **CDR incident classification**[1]: Article 6(2) (initial notification of non-major incidents), Article 6(1) (initial notification)
Consumer right to explanation	Article 86 (deployers)	• **CCD2**: Article 18(8) (consumer right to request and obtain an explanation of the CWA including the logic and risks involved and the significance and effects of decision), Article 18(9) (obligation to inform consumers of rejection and of the automated processing of data)

[1] Commission Delegated Regulation (EU) 2024/1772 on RTS specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents. See: http://data.europa.eu/eli/reg_del/2024/1772/oj

AI Act requirements envisaging their integration or combination with sectoral requirements:

AI Act		Sectoral requirements
Risk management system	Article 9 (providers)	• **CRD**: Article 74(1) (processes to identify, manage, monitor and report risks), Article 76(1) (all material risks to be identified, measures and reported by the risk management function), Article 76(2) (ensure adequate resources for management of all material risks) • **CRR**: Article 144(1) (meaningful obligor and transaction assessment and differentiation of risk), Article 144(1)(f) (validation of rating systems), Article 169(1) (multiple rating systems and level of risk), Article 169(2) (periodical review of rating criteria and processes), Article 174 (regular cycle of model validation), Article 179(1)(a) (PD assessment techniques and evidence), Article 179(1)(c) (review of estimates due to technical advances and new data), Article 189 (MB/SM understanding of rating systems), Article 190 (Credit risk control unit (CRCU) to regularly produce and analyse reports on outputs of rating systems), Article 191 (internal audit to review at least annually rating systems) • **EBA IG GLs**: Para 22(a)(i) (internal control functions to have sufficient authority and resources), Para 61(a) (Risk Committee on actual and future risks), Para 152 (risk management framework (RMF) to include all relevant risks), Para 98 (risk culture to allow for testing of current practices), Para 153 (policies, procedures, risk limits and risk controls), Para 196 (RMF to analyse trends on new or emerging risks and regularly backtest) • **CDR assessment methodology**[2]: Article 16(3) (CRCU to have sufficient resources and experience staff), Article 17(2) (internal audit resources), Article 11(3) (frequency of model validation process), Article 40 (assessment of model predictive power) • **DORA**: Article 6(1) (ICT risk management framework), Article 6(2) (strategies, policies, procedures, ICT protocols and tools), Article 8(2) (continuous identification of sources of ICT risks and assessment of cyber threats and ICT vulnerabilities) • **CDR ICT risk management framework**[3]: Article 3 (ICT risk management policies and procedures), Article 16 (ICT system acquisition, development and maintenance procedures), Article 28 (training and knowledge) • **CCD2**: Article 6 (non-discrimination of consumers), Article 18(8) (consumer right to request and obtain human intervention, consumer right to request and obtain an explanation of the CWA including the logic and risks involved and the significance and effects of decision), Article 18(9) (obligation to inform consumers of rejection, of automated processing of data, of consumer right to human assessment and of the procedure for contesting the decision) • **MCD:** Article 18 (CWA of consumer), Article 20 (verification of consumer information) • **PSD:** Article 95 (management of operational and security risks) • **EBA LOM GLs**: Para 34 (criteria for identification, assessment, approval, monitoring, reporting and mitigation of credit risk in credit risk policies and procedures), Para 35 (proactive approach in monitoring credit quality to identify risk profile of portfolios), Para 38 (content of credit risk policies and procedures), Para 43 (regular review of credit risk policies and procedures), Para 53 (technology-enabled innovation in credit-granting purposes), Para 60 (data infrastructure in credit-grating processes)
Technical documentation	Article 18 (providers)	• **CRR**: Article 144 (documentation of rating system and model design rationale), Article 169(1) (documentation of rationale for assigning obligors or transactions to rating systems where use of multiple systems), Article 170(1)(c) (documentation of relationship between obligor grades), Article 171(1)(b) (documentation to allow third parties to understand, replicate and evaluate assignments to grades or pools), Article 172(3) (documentation of where human judgment may override inputs/outputs), Article 174 (documentation of model input data vetting process, model specification and testing), Article 174(e) (documentation of how human judgment and model results are to be combined), Article 175(1) (documentation of design and

[2] Commission Delegated Regulation (EU) 2022/439 of 20 October 2021 supplementing Regulation (EU) No 575/2013 (CRR) with regard to RTS for the specification of the assessment methodology CAs are to follow when assessing the compliance of credit institutions and investment firms with the requirements to use the IRB Approach. See: https://eur-lex.europa.eu/eli/reg_del/2022/439/oj/eng

[3] Commission Delegated Regulation (EU) 2024/1774 on RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework. See: http://data.europa.eu/eli/reg_del/2024/1774/2024-06-25

		operational details of rating systems), Article 175(2) (documentation of all major changes to risk rating process), Article 175(3) (documentation of default and loss definitions), Article 175(4) (documentation of methodologies of statistical models in rating process), Article 185(b) (documentation of methods and data used in comparisons between realised and estimated parameters), Article 185(d) (documentation of changes in estimation and validation methods and data), Article 452(f) (description of internal ratings process by exposure class) • **CDR assessment methodology**: Article 3(1) (technical documentation characteristics for supervisory review), Article 31(2)(a) (documentation of rating system and model purpose), Article 31(5) (documentation of methodological choices), Article 40 (internal standards for model performance), Article 74 (documentation of data necessary to support credit risk measurement and management) • **DORA**: Article 6(1) (documentation of ICT risk management framework), Article 9(4)(e) (documentation of policies, procedures and controls for ICT change management) • **CDR ICT risk management framework**: Article 17 (ICT change management content), Article 38(2) (simplified ICT change management for small and non-interconnected entities) • **CCD2**: Article 18(4) (documentation of procedures for CWA) • **MCD:** Article 18(2) (documentation of procedures and information for CWA) • **PSD:** Article 5 (description of governance arrangements and internal control mechanism, description of procedure to monitor, handle and follow-up a security incident, description of process to access to sensitive payment data, of business continuity arrangements, security policy document) • **EBA LOM GLs**: Para 41 (specification of use of automated CWA models in credit risk policies and procedures), Para 55 (model documentation covering methodology, assumptions, data inputs, use of model outputs)
Record-keeping	Article 19 (providers and deployers)	• **CRR**: Article 174 (requirements on the assigning of exposures), Article 176 (obligation to collect and store data of internal ratings) • **CDR ICT risk management framework**: Article 12 (logging procedures, protocols and tools, containing identification of events to be logged and alignment of level of detail of logs with their purpose and usage) • **EBA LOM GLs**: Para 38(i) (specification of requirements relating to what is to be documented and recorded as part of the credit-granting process); Para 46 (appropriate checks in place to identify, assess and manage ML/TF risks, and that relevant records are kept, in line with institutions' wider AML/CFT obligations) Para 54 (measures to ensure traceability and auditability), Para 55 (model documentation on data inputs and model outputs to monitor automated decisions), Para 94 (documentation of data leading to credit approval) • **PSD 2:** Article 21 (record keeping);
Post-market monitoring	Article 72 (providers)	• **CRD**: Article 74(1) (governance arrangements and processes to identify, manage, monitor and report risks) • **CRR**: Article 174(d) (regular cycle of model validation), Article 185 (rating system, process and estimation accuracy and consistency), Article 190(2) (CRCU responsibility in changes to rating process, review of rating criteria and ongoing review and alterations to models) • **EBA LOM GLs**: Para 34 (monitoring of credit risk), Para 35 (proactive approach to monitoring credit quality), Para 38(h) (monitoring of circumstances and conditions for exceptional credit-granting decisions), Para 38(j) (monitoring of credit-granting activities during all phases), Para 42 (monitoring of suspicious or fraudulent behavior), Para 53(f) (model performance monitoring), Para 55(b) (model documentation to monitor automated decisions on the quality of portfolio or products in which models are used), Para 60 (data infrastructure to support credit risk monitoring)
Fundamental right impact assessment	Article 27 (deployers)	• **CCD2**: Article 6 (non-discrimination of consumers)

AI Act requirements that do not envisage regulatory synergies, but where existing sectoral requirements apply:

AI Act		Sectoral requirements
Transparency to deployers	Article 13 (providers)	• **CRR**: Article 171(1)(b) (documentation to allow third parties to understand, replicate and evaluate assignments to grades or pools), Article 174 (models not to be distortive) • **CDR assessment methodology**: Article 3(d) (documentation of rating systems must allow third parties to examine and confirm the functioning of rating systems) • **DORA**: Article 17(3)(d) (plans to provide information to financial entities that act as counterparts) • **EBA LOM GLs**: Para 53(b) (obligation to ensure the management body has a sufficient understanding of the use of technology-enabled innovation, its limitation and the impact it has on credit-granting procedures); Para 54(b) (traceability measures and model override and escalation procedures)
Human oversight	Article 14 (providers)	• **CRR**: Article 149(1) (conditions to stop using IRB models), Article 172(3) (model input/output override and personnel responsible for approving overrides), Article 174 (human judgement and human oversight to review model-based assignments), Article 179(1)(d) (adjustments to overcome bias) • **EBA IG GLs**: Para 26 (oversight of risk management and internal controls), Para 31 (business line responsibilities), Para 32 (other function responsibilities), Para 97 (staff responsibilities in risk management), Para 141 (internal control function responsibilities and authority for risk management), Para 144 (internal control framework activities), Para 145 (internal control framework), Para 152 (institution-wide risk management framework), Para 153 (policies, procedures, risk limits and risk controls), Para 159 (awareness of model and metric limitations), Para 202 (head of RMF ability to challenge decisions) • **CDR assessment methodology**: Article 18(2)(d)(ii) (data on rejected credit applications and instances of human overrides), Article 24(2) (situations where human judgement is used to override inputs/outputs of the rating system), Article 39 (implementation of human judgement to complement model), Recital 15 (human override approvals) • **EBA GLs on PD and LGD estimation**: Para 201 (human judgement uses in model application) • **CCD2**: Article 18(8) (consumer right to request and obtain human intervention), Article 18(9) (obligation to inform consumers of right to human assessment and of the procedure for contesting the decision) • **EBA LOM GLs**: Para 38(h) (possible deviations from standard credit policies and procedures), Para 53 (remediation measures in case of detected issues), Para 54 (traceability measures and model override and escalation procedures), Para 238 (criteria for advanced statistical models for valuation)
Accuracy, robustness, cybersecurity	Article 15 (providers)	• **CRR**: Article 144(1)(a) (categorisation of model changes), Article 174 (soundness and integrity of implementation process), Article 179(1) (plausibility and intuitiveness of estimates), Article 185 (validation function analysis and challenge of model design) • **EBA IG GLs**: Para 158 (validation and calibration of purchased risk models), Para 196 (regular back testing to assess and improve the accuracy of the risk management process) • **CDR assessment methodology**: Article 28(d) (verification of IT system identification of defaults), Article 42(d) (accuracy and robustness of risk parameter estimation and quantification), Article 75 (assessment of IT system architecture, IT infrastructure soundness, safety and security and IT infrastructure robustness of relevance to rating systems) • **EBA GLs on PD and LGD estimation**: Para 16 (human judgement uses in model application), Para 36 (identification of deficiencies in risk parameter estimation), Para 37 (consideration of deficiencies in methods, processes, controls, data or IT systems), Para 38 (methodologies to correct identified deficiencies) • **DORA**: Article 6(1) (comprehensive ICT risk management framework to address ICT risk quickly, efficiently and comprehensively), Article 6(2) (ICT risk management framework to protect all information assets and ICT assets), Article 10 (mechanisms for prompt detection of anomalous activities), Article 11 (ICT business continuity policy for response and recovery) • **CDR ICT risk management framework**: Article 21 (prevention of unauthorised access), Article 23(3) (protection of recording of anomalous activities against tampering and unauthorised access)

		• **CCD2**: Article 18 (CWA on the basis of relevant and accurate information, obligation for credit intermediaries to submit accurately necessary information) • **MCD:** Article 20 (completeness of customer information, termination of credit if information was knowingly held or falsified) • **PSD:** Article 5(1)(j) (security policy to describe security control and mitigation measures against risks identified, including fraud and illegal use of sensitive and personal data) Guidelines amending Guidelines EBA/GL/2019/04 on ICT risk and security management (amending PSD2 Article 95 on incident reporting) • **EBA LOM GLs**: Para 54 (control mechanism and model quality assessment), Para 55 (model documentation for monitoring automated decisions), Para 60 (data infrastructure and continuity, integrity and security of information), Para 62 (data infrastructure and data fields from EBA NPL templates)
Data governance	Article 13 (providers)	• **CRR**: Article 144(1)(d) (data collection and storage), Article 174 (data requirements on models to assign exposures to grades or pools, link between model inputs and outputs, Article 176(1) (data collection and storage for internal ratings), absence of material biases), Article 179(1) (risk parameter quantification data), Article 179(1)(f) (adjustments to overcome bias), Article 180 (PD estimation quantification data requirements), Article 185(c) (quantitative validation tools), Article 185(d) (quantitative validation data consistency), Article 190(1) (CRCU responsibility for design, selection, implementation, oversight and performance of rating systems), • **EBA IG GLs**: Para 145(d) (reliability of information), Para 162 (effective risk reporting and risk data relevance), Para 228 (business continuity management plan and data), • **CDR assessment methodology**: Article 37(1) (data input vetting process), Article 37(2) (data representativeness in model development), Article 38 (rating model design), Article 40 (model predictive power assessment), Article 42(1)(a) (data completeness in estimation), Article 42(1)(c) (data representativeness in estimation), Article 42(1)(e) (data cleansing effects on bias), Article 46 (PD estimation method), Article 72(1) (data maintenance), Article 73(1) (quality of data necessary to support credit risk measurement and management), Article 74(1) (data necessary to support credit risk measurement and management) • **EBA GLs on PD and LGD estimation**[4]: Para 10 (data preparation and data quality verification), Para 16 (risk parameter data accuracy, completeness and appropriateness, bias in data), Para 17 (PD model data representativeness), Para 20 (datasets for model development), Para 31 (bias in risk quantification), Para 34 (adjustments for bias correction and margin of conservatism), Para 63 (no material biases due to internal or external rating information), Para 68 (frequency of model validation process), Para 96 (assessment of model predictive power) • **CDR ICT risk management framework**: Article 11 (data and system security procedure) • **CCD2**: Article 18 (CWA on the basis of sufficient information and consultation of relevant database) • **MCD:** Article 18 (the CWA of consumers shall consider factors relevant to verifying the prospect of the consumer to meet his obligations under the credit agreement), Article 20 (information to be obtained from relevant sources and properly verified, necessary, sufficient and proportionate) • **PSD:** Article 66 (rules on access to payment account in case of payment initiation services), Article 67 (rules on access to and use of payment account information in case of account information services) • **EBA LOM GLs**: Para 38 (handling of information and data needed for CWA), Para 53(e) (quality of data and inputs to models and bias detection and prevention), Para 55 (model documentation on methodology, assumptions, data inputs and approach to bias detection and prevention), Para 61 (data infrastructure on loan-by-loan information), Para 87 (relevant and up-to-date use of customer and borrower information), Para 88 (collection of necessary information and data from borrower or third-parties), Para 89 (information checks and enquiries to verify information and data collected), Para 196 (relevant documentation of credit decisions and loan agreements)
AI literacy	Article 4 (providers, deployers)	• **CRD**: Article 76(2) (MB to ensure adequate resources to manage all material risks) • **CRR**: Article 189 (MB, SM and designated committees to have a general understanding of rating system design and operation and associated management reports)

[4] EBA Guidelines on PD estimation, LGD estimation and treatment of defaulted assets. See: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/model-validation/guidelines-pd-estimation-lgd

		• **CDR assessment methodology**: Article 16(3) (CRCU to be proportionate to nature, size and degree of complexity of rating systems and have adequate resources and experienced and qualified personnel), Article 17(2) (internal audit to be proportionate to nature, size and degree of complexity of rating systems and to have adequate resources and experiences and qualified personnel) • **EBA IG GLs**: Article 22(a)(i) (internal risk management, compliance and audit functions that have sufficient authority, status and resources to perform their functions) • **DORA**: Article 5(2)(g) (MB to allocate and periodically review appropriate budget to fulfil digital operational resilience needs), Article 13 (learning and evolving, capabilities and staff, ICT security awareness programmes and digital operational resilience training) • **CCD2**: Article 33 (knowledge and competence requirements for staff) • **MCD:** Article 9 (knowledge and competence requirements for staff) • **EBA LOM GLs**: Para 53 (MB to have sufficient understanding of use of technology-enable innovation, its limitation and impact on credit-granting procedures), Para 66 (staff members to be adequately trained and hold relevant expertise and seniority), Para 79 (sufficient resources and staff allocated to credit risk taking), Para 80 (staff involved in credit granting to have appropriate level of experience, skills and credit-related competence), Para 81 (staff involved in credit granting to frequently receive training)