european corporate governance institute

ecgi

AI Gatekeepers

Law Working Paper N° 932/2026
May 2026

Katja Langenbucher
Goethe Universität - House of Finance, SciencesPo, Fordham Law School and ECGI

© Katja Langenbucher 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

This paper can be downloaded without charge from:
https://doi.org/10.67929/ecgi-law-932-2026

european corporate governance institute

ECGI Working Paper Series in Law

AI Gatekeepers

Working Paper N° 932/2026
May 2026

Katja Langenbucher

© Katja Langenbucher 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Abstract

The paper gives an overview on what established gatekeeper theory on financial markets was designed to achieve. It moves on to introduce three groups of AI-gatekeepers: established auditors, new entrants, and publicly accredited gatekeepers. Then, the paper describes designated AI-laws and designated AI-gatekeepers, both optional and mandatory. It concludes with a preliminary roadmap for regulating AI-gatekeepers. The paper makes three contributions to the debate. First, it shows why a transplant of the proposal to introduce a version of strict gatekeeper liability from the financial-market setting is inadequate for AI-gatekeepers. Second, it suggests a two-layer transparency regime: aggregate disclosure of testing methodologies and standards, combined with compact certifications or scores at the individual level. Third, the paper proposes ex ante governance requirements operating at two sites: At the gatekeeper itself, through accreditation and independence requirements modelled on the EU's notified-body regime. Additionally, at the interface of the gatekeeper with the client, through institutional structures analogous to the audit committee but designed for the interdisciplinary translation problem that distinguishes AI-compliance review from classical audit.

Keywords: Gatekeepers, AI, compliance, governance, liability, corporate scandals, auditors

JEL Classification: K13, K22, K23

Katja Langenbucher

Goethe Universität - House of Finance, SciencesPo, Fordham Law School and ECGI

AI-Gatekeepers

Langenbucher[1]

I. The Anatomy of Gatekeeping 5
1. Gatekeepers and Liability 6
2. Gatekeepers and Governance 9
II. Defining AI-Gatekeepers 10
1. Market Overview 11
2. The Three Groups of AI-Gatekeepers 13
III. Defining Designated AI Laws and Designated AI-Gatekeepers 15
1. „Old" Law and AI-Compliance 15
2. Designated AI-Law 16
a) U.S. State Law 16
b) The EU AI Act 17
3. Designated AI-Gatekeepers 19
a) AI-audits under U.S. State Law 20
b) Notified Bodies under the AI Act 21
IV. Mandatory and Optional AI-Gatekeepers 23
1. Optional AI-Gatekeepers 24
2. The Exception: Required Audits 25
3. The (likely) Rule: Market Expectations 26
V. A Preliminary Roadmap for AI-gatekeepers 28
1. AI-Gatekeepers and Liability 30
a) From Financial Markets to Products: Liability of Certifying Bodies 31
b) From a Rule-Bound World to a State in Flux 34
2. Transparency 35
2. Governance 39
a) Gatekeeper Governance 39

[1] I am most grateful to participants of the Comparative conference on Gatekeepers organized by the Forum *Unternehmensrecht im Vergleich* at ETH Zurich, 9 April 2026, to participants in NYU Law School's Information Law Institute workshop on 13 April 2026, and to participants in the LiaNs Seminar at Pompeu Fabra, Barcelona, on 6 May 2026. Remaining errors are entirely my own. An abbreviated version of this paper will appear in Zeitschrift für Vergleichende Rechtswissenschaft, 2026.

b) Interface Governance 40
VI. Conclusion 42

A classical tenet of corporate governance theory is to ensure agents act in the interest of their principals. To that end, principals enjoy appointment, removal, and decision rights. Independent directors and supervisory board members help to monitor management. Agents face liability. But contributing to good governance is not limited to principals and their agents. Further institutions outside this two-party relationship provide additional services. One such institution are gatekeepers.

Classical definitions of gatekeepers start from their role as intermediaries on capital markets where investors lack sufficient information about issuers.[2] Gatekeepers mitigate information asymmetries, for example by monitoring and rating issuers, or by validating and certifying financial statements.[3] In that way they „guard the gate" to financial markets. There is no settled terminology on who qualifies as a gatekeeper.[4] The paradigm gatekeeper is the auditor.[5] Investment banks, for instance when accompanying an IPO, securities attorneys, for example when producing an opinion on due diligence disclosure,[6] or credit rating agencies,[7] have all been called gatekeepers.[8] The same goes for securities analysts[9] and even for independent company board members.[10]

---

[2] *Gilson/Kraakman*, The Mechanisms of Market Efficiency, 70 Virginia Law Review 549, 620 (1984); *Coffee*, Gatekeepers: The Professions and Corporate Governance, 2006, p. 305; *Coffee*, Gatekeeper Failure and Reform: The Challenges of Fashioning Relevant Reforms, 84 Boston University Law Review 301, 308 (2004); *Coffee*, The Acquiescent Gatekeeper: Reputational Intermediaries, Auditor Independence and the Governance of Accounting, Columbia Law & Economics Working Paper No. 191, 2001, p. 2 (available at: https://scholarship.law.columbia.edu/faculty_scholarship/1249/, call-off date for all hyperlinks, unless otherwise stated: 5 May 2026); on signaling see *Spence*, Job Market Signaling, 87 The Quarterly Journal of Economics 355 (1973).

[3] Overview at *Coffee*, 84 Boston University Law Review 301, 309 (2004); on multiple gatekeepers: *Tuch*, Multiple Gatekeepers, 96 Virginia Law Review 1583 (2010).

[4] *Infra* I.1.

[5] Note, however, that auditor firms often cross-sell consulting services to their clients.

[6] *Gilson/Kraakman*, 70 Virginia Law Review 549, 620 (1984); generally critical for attorney as gatekeepers: *Fisch/Rosen*, Is There a Role for Lawyers in Preventing Future Enrons, 48 Vill. L. Rev. 1097 (2003).

[7] *Partnoy*, Strict Liability for Gatekeepers: a Reply to Professor *Coffee*, 84 Boston University Law Review 365 (2004).

[8] *Hamdani*, Gatekeeper Liability, 77 Southern California Law Review 53 (2003); On distinguishing dependent from independent gatekeepers: *Laby*, Differentiating Gatekeepers, 1 Brook. J. Corp. Fin. & Comm. L. 119 (2006).

[9] *Laby*, 1 Brook. J. Corp. Fin. & Comm. L. 119, 124 (2006).

[10] On board members as gatekeepers: *Nili*, Board Gatekeepers, 72 Emory L.J. 91 (2022).

Beyond mitigating information asymmetries, gatekeepers have been conceptualized as contributing to issuer compliance with the law.[11] Gatekeepers have usually less to gain from misconduct than their principal, but more to lose. They build reputational capital through engaging with many clients. Participating in one client's misconduct puts this capital at risk which, under ordinary circumstances, makes it a suboptimal strategy.[12] This mechanism is especially potent if issuers must seek mandatory gatekeeper validation or certification, allowing the gatekeeper to withhold its cooperation from wrongdoing clients.[13]

In the rapidly evolving area of laws that target providers and users of AI, a mix of old and new actors have started to offer gatekeeping services. Well-established audit firms provide „AI audits". [14] Small market-entry gatekeepers have spawned, often focusing on specific technical questions or particular laws.[15] Additionally, there are public bodies or publicly accredited gatekeepers that issue certifications or support AI-providers in their self-validation efforts. I address all three groups of gatekeepers as „*AI-gatekeepers*",[16] and identify gatekeepers that are publicly accredited for some form of monitoring AI as „*designated AI-gatekeepers"*.

This paper investigates what established, financial markets-centered gatekeeper theory can teach us for the new world of gatekeepers that monitor, validate, or certify compliance with laws that focus on AI-providers and users. A host of laws,

---

[11] Foundational: *Kraakman*, Corporate Liability Strategies and the Costs of Legal Controls, 93 The Yale Law Journal 857, 888 et seq. (1984); *Kraakman*, Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy, 2 Journal of Law, Economics & Organization 53 (1986); see further *Hamdani*, 77 Southern California Law Review 53, 66 (2003) arguing that, via fees for their services, gatekeepers can raise costs for misbehaving clients, which, eventually, should lead to these firms deciding not to enter the market; see critique at *Jackson*, Reflections on Kaye, Scholer: Enlisting Lawyers to Improve the Regulation of Financial Institutions, 66 Southern California Law Review 1019, 1047 et seq. (1993); On "compliance gatekeepers": *Eckstein/Shapira*, Compliance Gatekeepers, 41 Yale Journal on Regulation 469, 477 (2024).

[12] *Kraakman*, 93 The Yale Law Journal 857, 891 (1984); *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 8; *Coffee*, 84 Boston University Law Review 301, 308 (2004).

[13] *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 11; *Partnoy*, Barbarians at the Gatekeepers?: A Proposal for a Modified Strict Liability Regime, 79 Washington University Law Quarterly 491, 503 (2001); see further *Kraakman*, 2 Journal of Law, Economics & Organization 53 et seq. (1986); *Hamdani*, 77 Southern California Law Review 53, 98 et seq. (2003); *Kim*, Gatekeepers Inside Out, 21 The Georgetown Journal of Legal Ethics 411, 414 (2008).

[14] PwC is reported to be furthest along, see The Finance Story, Big 4 to Launch AI Assurance Services, June 2025, available at: https://thefinancestory.com/big-4-to-launch-ai-assurance-services; see overview at Center for Audit Quality, The Role of the Auditor in AI, October 2025, available at: https://thecaq.wpenginepowered.com/wp-content/uploads/2025/10/caq_the-role-of-the-auditor-in-ai_2025-10.pdf.

[15] *Costanza-Chock* et al., Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem, Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574 (2022); *Gerdemann*, Konformitätsbewertung als Kernpflicht der KI-Verordnung, NJW 2024, 2209, 2212; *BeckOK KI-Recht/Schefzig/Kilian*, KI-VO Art. 43 no. 20 (Last updated 4.11.2025); *Mökander/Floridi*, Ethics-Based Auditing to Develop Trustworthy AI, 31 Minds & Machines 323 (2021); *Raji* et al., Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 33 (2020) (available at: https://arxiv.org/abs/2001.00973).

[16] *Infra* II.1.; this terminology does not imply that an AI is doing the gatekeeping work.

for instance data protection laws[17] or sectoral laws on health,[18] finance,[19] employment,[20] advertising,[21] or deceptive commercial practices[22] cover situations that are now shaped by AI. For AI-providers and users this implies a challenge: Novel AI-processes must be designed so as to ensure compliance with „old" laws. Additionally, some jurisdictions have passed laws such as the EU AI Act[23] or AI-related state laws in the U.S. that specifically target the development or use of AI. I call these *designated AI laws*. They follow various regulatory strategies. Some are sectoral and address the use of AI in, for instance, health care, employment or finance. Others are categorical, for example targeting the use of certain high-risk AI. Yet others are situational, for instance by stipulating rules on mass-surveillance in public places. Many laws follow a mixed approach, for example by imposing rules for certain categories of AI, such as „high-risk", if they are used in a specific sector, for example in health care.

The paper starts with an overview on what established gatekeeper theory on financial markets was designed to achieve. It moves on to introduce the three groups of AI-gatekeepers mentioned above: established auditors, new entrants, and publicly accredited gatekeepers. Then, the paper describes designated AI-laws and designated AI-gatekeepers, both optional and mandatory. It concludes with a preliminary roadmap for regulating AI-gatekeepers.

The paper makes three contributions to the debate. First, it shows why a transplant of the proposal to introduce a version of strict gatekeeper liability from the financial-market setting is inadequate for AI-gatekeepers. Second, it suggests a

---

[17] For instance: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation – GDPR), OJ 2016 L 119/1, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[18] For instance: Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, available at: https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[19] For instance: Equal Credit Opportunity Act, 15 U.S.C. §§ 1691–1691 f., available at: https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap41-subchapIV.htm; Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., available at: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act; Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers (Consumer Credit Directive), OJ 2023 L 2023/2225, available at: https://eur-lex.europa.eu/eli/dir/2023/2225/oj/eng.

[20] For instance: Age Discrimination in Employment Act of 1967, 29 U.S.C. SEC. 621–634, available at: https://www.eeoc.gov/statutes/age-discrimination-employment-act-1967; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ 2000 L 303/16, available at: https://eur-lex.europa.eu/eli/dir/2000/78/oj/eng.

[21] For instance: New York State Law requiring advertisements to disclose the use of a synthetic performer, available at: https://www.nysenate.gov/legislation/bills/2025/A8887/amendment/B.

[22] For instance: *Meuti/Jarzyna*, FTC´s Operation AI Comply, available at: https://www.beneschlaw.com/resources/one-year-in-ftcs-operation-ai-comply-continues-under-new-administration-signaling-enduring-enforcement-focus.html.

[23] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), OJ 2024 L 2024/1689, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

two-layer transparency regime: aggregate disclosure of testing methodologies and standards, combined with compact certifications or scores at the individual level. Third, the paper proposes *ex ante* governance requirements operating at two sites: At the gatekeeper itself, through accreditation and independence requirements modelled on the EU's notified-body regime.[24] Additionally, at the interface of the gatekeeper with the client, through institutional structures analogous to the audit committee but designed for the interdisciplinary translation problem that distinguishes AI-compliance review from classical audit.

I. The Anatomy of Gatekeeping

Traditional gatekeepers on financial markets have been described as private parties who are able to disrupt misconduct by withholding cooperation from their clients. Scholars are split on what best incentivizes gatekeepers to fill this role. There is broad agreement that reputational capital, which gatekeepers built up across many engagements, is one important element.[25] Auditors and similar gatekeepers are repeat players whose accumulated reputational capital, built across many engagements, exceeds the one-time gain they could realize from misrepresenting any single client's situation.[26] However, critics have pointed out that several preconditions for this mechanism can fail. For many gatekeeper categories, the market is not able to reliably observe gatekeeper failure ex post.[27] Important fees from a single client can come to outweigh the broader reputational stake. Additionally, reputational capital can be a remote factor, and it can be rational for gatekeeper firms or individuals inside the firm to market themselves as flexibly accommodating management, especially if they face an end-game situation.[28] This risk is especially acute where gatekeeper fees are paid for consulting, rather than auditing services.[29] The value of reputational capital is context-dependent, it can be volatile during times of market euphoria, and is costly to assess after an injury.[30]

---

[24] *Infra* III.3.b. on notified bodies.

[25] Paradigmatic Judge *Easterbrook* in DiLeo v. Ernst & Young, 901 F.2d 624, 629 (7th Cir. 1990); see further: *Kraakman*, 2 Journal of Law, Economics & Organization 53, 70 (1986); on reputational cost: *Karpoff/Lee/Martin*, The Cost to Firms of Cooking the Books, 43 Journal of Financial and Quantitative Analysis 581 (2008).

[26] See *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 10; *Coffee*, 84 Boston University Law Review 301, 308 (2004); however, at (2001) 1, 12 also stressing the importance of the relationship with individual managers for auditors, see *infra* I.1.

[27] *Partnoy*, 79 Washington University Law Quarterly 491 (2001); *Partnoy*, How and Why Credit Rating Agencies Are Not Like Other Gatekeepers, in Fuchita/Litan (eds.), Financial Gatekeepers: Can They Protect Investors?, 2006, p. 59 questioning this especially as to credit rating agencies.

[28] *Kraakman*, 93 The Yale Law Journal 857, 893 (1984); *Kraakman*, 2 Journal of Law, Economics & Organization 53, 63 (1986); *Langevoort*, Where Were the Lawyers? A Behavioral Inquiry Into Lawyers' Responsibility for Clients' Fraud, 46 Vanderbilt Law Review 75, 76, 98 et seq. (1993); *Partnoy*, 79 Washington University Law Quarterly 491, 502 et seq. (2001).

[29] *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 27 et seq.

[30] *Coffee*, 84 Boston University Law Review 301, 310, 328 et seq. (2004).

Faced with the drawbacks of relying on reputational capital, less common ground exists when considering if and how gatekeeper liability should complement this mechanism. Some acknowledge that liability sharpens the cost of reputational failure but claim that it should still be based on negligence standards only, with governance and public oversight as additional disciplining elements.[31] Auditors are their paradigm case, a category of gatekeeper that has long been strictly regulated and supervised.[32] Others bemoan the inadequacy of negligence as the standard for liability. They point to the failure of credit rating agencies during the financial crisis of 2008 as their prime illustration, a time when these faced less regulation[33] and when several laws had built-in mechanisms invoking credit rating agencies' scores.[34] Against this background, strict gatekeeper liability is advocated, with modifications such as caps and conditions on client fees.[35]

1. Gatekeepers and Liability

Following classical law and economics theory, strict liability of gatekeepers towards third parties should produce optimal incentives:[36] Strategies such as

---

[31] *Coffee*, 84 Boston University Law Review 301 (2004); *Coffee*, Gatekeepers: The Professions and Corporate Governance, 2006; *Jackson*, 66 Southern California Law Review 1019, 1050 et seq. (1993).

[32] *Coffee*, 84 Boston University Law Review 301 (2004).

[33] Note that this has changed after 2008, in the U.S. through Title IX of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (expanding SEC supervisory oversight, internal control requirements, conflicts of interest rules, disclosure of performance statistics for ratings; lowering the pleading standard for private securities-fraud claims (which turned out to be limited in practice)). In the EU, Regulation (EC) 1060/2009 has required registration with ESMA, mandates disclosure of methodologies, addresses conflicts of interest, requires EU and MS institutions to not trigger "sole or mechanistic reliance" on credit ratings (Art. 5b, 5c), and established potent supervisory powers at EU level (followed by amending regulations in 2011 and Regulation (EU) 462/2013 with certain mandatory rotation requirements, and a civil liability regime for intentional/grossly negligent CRA misconduct (Art. 35a CRA III)).

[34] *Partnoy*, 79 Washington University Law Quarterly 491, 509 et seq., 513 et seq. (2001) for Section 11 of the 1933 U.S. Securities Act ("regulatory licence"). Note that some of this, too, has changed after 2008, in the U.S. through Title IX of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Section 939A removing certain references to CRAs from federal agency regulation). However, the Basel framework continues to use some external credit ratings, market practice and contractual reliance on credit rating agencies is still strong, and the oligopolistic market structure has remained essentially unchanged, as has the issuer-pays model. See *Coffee*, Ratings Reform: The Good, the Bad, and the Ugly, 1 Harvard Business Law Review 231 (2011); *Partnoy*, What's (Still) Wrong with Credit Ratings?, 92 Washington Law Review 1407 (2017); *White*, Credit Rating Agencies: An Overview, 5 Annual Review of Financial Economics 93 (2013).

[35] *Partnoy*, 92 Washington Law Review 1407 (2017); *Partnoy*, 84 Boston University Law Review 365 (2004); *Hamdani*, 77 Southern California Law Review 53, 65, 68 (2003): only under the assumption that risk-shifting is costless and gatekeeper liability still necessary, see p. 84 for negligence as optimal if regulators are perfectly informed. See *Coffee*, 84 Boston University Law Review 301, 350 et seq. (2004) for critique, advancing his own modified proposal for strict liability.

[36] See discussion at *Hamdani*, 77 Southern California Law Review 53, 57 (2003); *Partnoy*, 79 Washington University Law Quarterly 491, 540 et seq. (2001); *Tuch*, 96 Virginia Law Review 1583, 1584, 1605 et seq. (2010); *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 492 et seq. (2024) on

waiving claims or negotiating away liability are not available, because claimants come from beyond the two-party relationship. Third parties can be more willing to sue than the gatekeeper's client, who might prefer to spare its accomplice. Courts are relieved from the burden of identifying standards of reasonable care which are often context-dependent. Legislators receive support in defining and enforcing strict liability standards.[37] A standard example is the near-strict liability of underwriters under Section 11 of the U.S. Securities Act.

Critics of strict gatekeeper liability have stressed several limits of this model. The „expectations gap" regarding auditors is one. The public might expect auditors to detect any errors in the company's financial statements. However, neither their contractual mandate nor their lack of investigative powers provides a solid basis for these expectations.[38] Adding to that, there is the risk of opening the floodgates to uninsurable[39] exposure „in an indeterminate amount for an indeterminate time to an indeterminate class".[40] Reacting to such risks can lead auditors to propose inefficient overinvestments in compliance.[41]

Additionally, litigation has been viewed as a costly remedy, that can fail if gatekeepers lack the capacity or information to react. The risk that individuals within the firm are not sufficiently deterred can remain high.[42] Where accounting principles leave considerable discretion to management, which auditors cannot fully control, auditors are not always the cheapest cost avoider, contradicting the assumption of classical law and economics.[43] Even worse, in that model, adverse selection looms. If auditors cannot distinguish between honest and fraudulent clients, they

doctrinal challenges for non-contractual parties to claim damages (scienter, proportionate liability, in pari delicto).

[37] *Shavell*, Strict Liability versus Negligence, 9 Journal of Legal Studies 1 (1980); An additional assumption is that strict liability will have gatekeepers tailor their fees to the expected liability they incur. Clients, so the theory goes, will internalize the fee increase until it becomes too costly, *Hamdani*, 77 Southern California Law Review 53, 66 et seq. (2003).

[38] *Kraakman*, 2 Journal of Law, Economics & Organization 53, 57, 76 (1986); *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 481 et seq. (2024).

[39] *Uhlmann*, Interessenkonflikte bei Wirtschaftsprüfern und Ratingagenturen, ZHR 185 (2021), 669, 715; for attorneys see *Jackson*, 66 Southern California Law Review 1019, 1070 et seq. (1993).

[40] *Cardozo* in Ultramares Corp. v. Touche, 174 N.E. 441, 444 (N.Y. 1931).

[41] *Kraakman*, 93 The Yale Law Journal 857, 892 (1984); *Kraakman*, 2 Journal of Law, Economics & Organization 53, 57 (1986); critical: *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 515 (2024).

[42] *Kraakman*, 2 Journal of Law, Economics & Organization 53, 56, 69 (1986); *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 6, 11 et seq.; *Coffee*, 84 Boston University Law Review 301, 318, 346 et seq. (2004); *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 490 (2024) on the small chances that management sues its gatekeeper.

[43] *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 7 footnote 11.

will end up charging fees that reflect the average likelihood of fraudulent behavior.[44] This, in turn, can distort market-entry decisions by law-abiding clients.[45]

Neither U.S. nor German law has embraced strict auditor liability towards third parties on financial markets,[46] even though – with Wirecard and Enron – both faced serious accounting fraud scandals which could have made a forceful case for auditor liability to damaged investors.[47] Germany focused on tightening the liability of auditors toward the company that retained them. A new law increased liability caps and removed them entirely for cases of gross negligence.[48] But the law did not create a private right of action for third parties.[49] Plaintiffs were left to navigate tort law while due-care obligations were limited to direct contractual relationships. Additionally, the Court of Justice of the European Union (CJEU) confirmed the exclusion of state liability of BaFin, Germany's financial markets supervisor, for implausibly upholding a short-sale ban. The Court reasoned that the EU Short Sale Regulation did not create private rights of action; its purpose was to create stable and efficient markets.[50] This roughly aligns with the U.S.

---

[44] *Hamdani*, 77 Southern California Law Review 53, 72 et seq., 93 et seq. (2003) on three potential outcomes of adverse selection in this situation: strict liability may (i) drive out law-abiding clients and leave intact the number of wrongdoers, (ii) lead to an unraveling of the market, or (iii) may have no impact on the market 103 et seq.; but see *Partnoy*, 79 Washington University Law Quarterly 491, 545 (2001).

[45] See *Hamdani*, 77 Southern California Law Review 53, 106 (2003).

[46] On limiting penalties for gatekeepers *Kraakman*, 2 Journal of Law, Economics & Organization 53, 79 (1986). But see critical on German law: *Heukamp*, Brauchen wir eine kapitalmarktrechtliche Dritthaftung von Wirtschaftsprüfern?, ZHR 169 (2005), 471, 483 et seq.; *Doralt*, Die Haftung des gesetzlichen Abschlussprüfers – Mitverschulden, Ansprüche Dritter und Wege der Haftungsbegrenzung, ZGR 2015, 266, 292 et seq.; *MüKoBGB/Wagner*, § 826 BGB no. 182, for more forceful liability in other European countries; for an overview on product liability laws see the country reports in *Fairgrieve*, Product Liability in Comparative Perspective, 2009.

[47] Under German law see *Canaris*, Schutzwirkungen zugunsten Dritter bei "Gegenläufigkeit" der Interessen, JZ 1995, 441; *Canaris*, Die Haftung des Sachverständigen zwischen Schutzwirkungen für Dritte und Dritthaftung aus culpa in contrahendo, JZ 1998, 603; *Ebke*, Die Haftung des Abschlussprüfers in: Krieger/Schneider (eds.), Handbuch Managerhaftung, 2010, § 11; *Grigoleit*, Haftung des Wirtschaftsprüfers aus § 826 BGB gegenüber Dritten, ZIP 2024, 1293; *Lechner*, Der BGH und die spezialgesetzliche Prospekthaftung im (ehemals) "Grauen Kapitalmarkt", WM 2024, 536; *Möllers*, Bestätigungsvermerk des Wirtschaftsprüfers und KapMuG, BKR 2022, 339; *Schmidt*, Aktuelle Entwicklungen im Bereich der Dritthaftung aus Beratungsverträgen, GWR 2024, 155; *Uhlmann*, ZHR 185 (2021), 669; *MüKoBGB/Wagner*, § 826 BGB no. 172, 181 et seq.; *Wagner*, Marktaufsichtshaftung produktsicherheitsrechtlicher Zertifizierungsstellen, JZ 2018, 130, 135 (narrow tortious liability, no quasi-contractual liability); monograph treatment by *Büttner*, Umfang und Grenzen der Dritthaftung von Experten, 2006.

[48] See § 323 (2) HGB.

[49] *Homborg/Landahl*, FISG – Ist die Verschärfung der Abschlussprüferhaftung die richtige Antwort auf den Wirecard Skandal?, NZG 2021, 859, 864; *Nietsch*, Abschlussprüferhaftung nach Wirecard, WM 2021, 158; *Poelzig*, Die Haftung der Abschlussprüfer börsennotierter Gesellschaften für Anlegerschäden vor und nach dem FISG, ZBB 2021, 73 (doubtful on deterrent effects of liability); *Lenz*, Haftung und Strafbarkeit des Abschlussprüfers im FISG-RegE, BB 2021, 683; *Uhlmann*, ZHR 185 (2021), 669, 707 (hopeful as to deterrence).

[50] § 4 (4) FinDAG; *Gansmeier/Splinter*, Leerverkaufsbeschränkungen und Amtshaftung, WM 2025, 1445, 1454; *Goldmann*, Amtshaftung für Aufsichtsfehler oder Europäisierung der Finanzaufsicht? Konsequenzen aus dem Wirecard-Fall, EuR 2022, 569; *Renner*, Staatshaftungsrechtliche Implikationen des Wirecard-Skandals, ZBB 2021, 1.

experience under Sarbanes-Oxley.[51] The Act created the PCAOB, transferred control and supervision of auditors to the audit committee, and – recognizing conflicts of interest – barred auditors from providing various consulting services, but Sarbanes Oxley did not fundamentally reform auditor liability.[52] U.S. courts have been only marginally more willing to hold auditors accountable than German courts.[53] Both jurisdictions have relied on structural reform not on an expansion of strict liability.

2. Gatekeepers and Governance

Complementing the debate around strict liability, scholars have explored further market mechanisms that can discipline gatekeepers. This was accompanied by broadening the term 'gatekeeper' far beyond its initial focus as reputational intermediary on financial markets. Third parties whose services are optional, for instance lawyers, investment banks, rating agencies, and securities analysts have all been framed as gatekeepers.[54]

Beyond external gatekeepers, scholars have expanded the term to include agents inside the company that are considered to fulfill gatekeeping roles.[55] One illustration are board members, for instance if they must agree to a transaction.[56] Internal „deal teams" or compliance officers who can block entering a certain market or engaging in certain activities qualify, too.[57]

---

[51] For a detailed analysis of decreasing litigation prior to Sarbanes Oxley see *Coffee*, 84 Boston University Law Review 301, 318 et seq. (2004) and Sarbanes Oxley at 336 et seq.; *Tibbets*, Tarnished Reputations: Gatekeeper Liability After Janus, 20 Fordham Journal of Corporate & Financial Law 745 (2015).

[52] *Hamdani*, 77 Southern California Law Review 53, 56 (2003).

[53] See, e.g., the decision In re Enron Corp. Securities, Derivative & ERISA Litigation, 235 F. Supp. 2d 549 (S.D. Tex. 2002), but then Regents of the University of California v. Credit Suisse First Boston, No. 06-20856, 482 F.3d 372 (5th Cir. 2007); Stoneridge Investment Partners, LLC v. Scientific-Atlanta, Inc., 522 U.S. 148 (2008); Janus Capital Group, Inc. v. First Derivative Traders, 564 U.S. 135 (2011).

[54] *Jackson*, 66 Southern California Law Review 1019 (1993); *Kraakman* 93 The Yale Law Journal 857, 890 (1984); details at *Partnoy*, 79 Washington University Law Quarterly 491, 517 et seq. (2001); Very broad *Hamdani*, 77 Southern California Law Review 53, 56 et seq. (2003) who includes "any party, who sells a product or provides a service that is necessary for clients wishing to enter a particular market or engage in certain activities". This definition embraces any causal element such as internet service providers, handgun manufacturers or electronics retailers selling radar detectors (at p. 56, 64).

[55] Critique at *Coffee*, 84 Boston University Law Review 301, 309 footnote 14 (2004); see *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 519 (2024) on internal gatekeepers performing "cosmetic compliance".

[56] *Kraakman*, 2 Journal of Law, Economics & Organization 53 (1986); *Laby*, 1 Brook. J. Corp. Fin. & Comm. L. 119, 123 (2006); *Coffee*, 84 Boston University Law Review 301, 308 footnote 14 (2004): "some form of monitoring function".

[57] *Nili*, 72 Emory L.J. 91 (2022); *Tuch*, 96 Virginia Law Review 1583, 1597 (2010).

Where internal agents are included in the gatekeeper definition, the argument moves away from third party enforcement towards classical corporate governance.[58] Governance effects are strongest if involving the board is legally required. Examples under German law include the approval of financial statements,[59] certain major transactions,[60] or executive compensation.[61] Under Delaware General Corporation Law, examples for mandatory requirements to include the board are authorizing the issuance of stock[62] or approving mergers or certain fundamental transactions,[63] under SEC rules it must be involved in executive compensation.[64] The DGCL regulates some aspects of independence,[65] but mostly independence is required under listing rules, for instance of the NYSE or Nasdaq.[66]

Additionally, governance standards not only of the company but also at the gatekeeper have been suggested as an effective monitor for gatekeeper work. Larger audit firms have been said to be less corruptible by their wrongdoing clients, due to income sharing, joint liability, and internal governance structures across the firm.[67] Independent audit committees at the client firm have a specific role to play in monitoring wrongdoing, and auditors are expected to cooperate closely with them. Self-regulatory sanctions within the gatekeeper's industry are another example. Mandatory rotation or other forms of time limits for keeping the same gatekeeper can reduce the chances of auditors becoming too closely intertwined with their clients.[68]

II. Defining AI-Gatekeepers

Against the background of a comparatively fuzzy definition of what counts as a gatekeeper and which function a gatekeeper is supposed to fulfill, it seems useful to define this paper's terminology. „AI-Gatekeepers" is not an established term of

---

[58] *Kraakman*, 93 The Yale Law Journal 857, 891 (1984).
[59] § 172 AktG.
[60] See § 111 (4) AktG.
[61] § 87 AktG. Note, however, that under German law, there is no explicit requirement for *independent* directors in general corporation law. Under § 100 (5) *Aktiengesetz*, the supervisory board of certain public companies must include a minimum of two financial experts, § 107 (4) requires an audit committee, and C.6, C.7 of the German Corporate Governance Code includes recommendations on independent members, *Koch*, § 100 AktG no. 36.
[62] § 161 DGCL.
[63] §§ 251, 271 DGCL.
[64] NYSE Listed Company Manual 303A.05; Nasdaq Rule 5605(d).
[65] See for example § 144 DGCL; on EU recommendations see *Langenbucher*, Wettbewerbsverbote, Unabhängigkeit und die Stellung des Aufsichtsratsmitglieds, ZGR 2007, 571, 589.
[66] In both jurisdiction, proxy advisors tend to require some independence on boards, *Hopt/Leyens*, Der Deutsche Corporate Governance Kodex 2020, ZGR 2019, 929, 946; *Koch*, § 100 AktG no. 36.
[67] *Kraakman*, 2 Journal of Law, Economics & Organization 53, 72 (1986).
[68] On this strategy: *Coffee*, Columbia Law & Economics Working Paper No. 191, 2001, p. 7, 20 et seq. (these suggestions must be read in the context of 2001, i.e. before Sarbanes-Oxley, and the specificities of the U.S. broker-dealer self-regulatory framework that *Coffee* recommends as a model).

art. Here, it serves as a catch-all term for private actors that offer compliance monitoring services to providers or users of AI.[69] This covers established gatekeepers and new entrants, along with private firms operating under public accreditation.

1. Market Overview

Established gatekeepers, most notably auditors or law firms,[70] are well positioned to offer AI-compliance gatekeeping functions. This is most notable where international governance standards have emerged. ISO 42001[71] illustrates this by providing a global structured framework for AI-governance in firms. [72] Key elements include defining roles and responsibilities for AI oversight, conducting AI impact assessments, managing risks across the AI lifecycle, documenting policies for responsible use, and addressing concerns such as bias, transparency or data quality. At the time of writing, CEN/CENELEC JTC 21 have proposed prEN 18286, a European standard modelled on ISO 42001[73] and designed to eventually provide a presumption of conformity with Art. 17 AI Act.[74]

Additionally, a large market for new AI audits has been developing.[75] Some of these outfits offer for-profit services, others are civil-society oriented NGOs.[76] To name just a few companies engaged in private auditing: ORCAA, founded by Cathy O'Neil,[77] is an algorithmic auditing consultancy that serves private firms,

---

[69] *Infra* II.2.

[70] *Birhane* et al., AI auditing: The Broken Bus on the Road to AI Accountability, IEEE Conference on Secure and Trustworthy Machine Learning 612 (2024) offer an overview on law firms, consulting agencies, corporate audits, along with what might qualify as more remote gatekeepers, namely journalists and civil society organizations.

[71] The standards are available at: https://www.iso.org/standard/42001.

[72] Unlike NIST AIRMF, which is non-binding, voluntary guidance, and SOC2, which produces an attestation, not a certification, ISO 42001 is certifiable, i.e., an accredited auditor can assess and formally certify an organization's conformity. But see for shortcomings: https://technologyquotient.freshfields.com/post/102jcog/eu-ai-act-unpacked-10-iso-42001-a-tool-to-achieve-ai-act-compliance.

[73] https://www.schellman.com/blog/ai-services/how-pren-18286-aligns-with-iso-42001-for-eu-ai-act-compliance.

[74] https://jtc21.eu/pren-18286-reaches-enquiry-stage-a-milestone-for-ai-quality-management-in-europe/.

[75] *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574 (2022); *Gerdemann*, NJW 2024, 2209, 2212; BeckOK KI-Recht/*Schefzig/Kilian*, no. 20; *Mökander/Floridi*, 31 Minds & Machines 323 (2021); *Raji* et al., Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 33 (2020) (available at: https://arxiv.org/abs/2001.00973).

[76] For the latter see, for instance, https://ainowinstitute.org; https://www.ajl.org; https://www.mozillafoundation.org/de/; https://algorithmwatch.org/en/; https://algorithmaudit.eu; https://www.adalovelaceinstitute.org; https://www.turing.ac.uk; overview at *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574 (2022).

[77] *O'Neil*, Weapons of Math Destruction, 2016.

regulators and prosecutorial offices across industries.[78] Credo AI targets corporate compliance.[79] The company offers policy packs covering, for instance, the AI Act, the (non-binding) US National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), ISO 42001, and SOC2.[80] BABL AI offers similar services, including NYC's bias audit.[81] Monitaur specializes in governance software with a focus on financial industry, healthcare and insurance.[82] Luminos.law is a law firm that provides algorithmic audits.[83] Holistic AI, a UK firm,[84] the Swiss LatticeFlowAI,[85] and the EU-based fairnow[86] or eticas.ai[87] offer similar services.

Both groups of gatekeepers operate in the institutional space described earlier by financial-market gatekeeper theory:[88] privately retained intermediaries whose discipline runs primarily through reputation and liability.

A third group of gatekeepers is a familiar occurrence in product safety regulation. Gatekeepers in this group are public bodies or private firms operating under public accreditation. They validate or certify AI models against the requirements of designated AI laws. The AI Act's notified bodies are the paradigm case.[89] At the time of writing, the process of designating notified bodies is in the EU still ongoing. In France, public bodies seem to be in the run-up.[90] In Germany, the *Bundesnetzagentur* will be the notifying authority, and the TÜV has been one highly likely candidate for a notified body.[91] This suggests that Germany will follow a private-law based design for gatekeepers (even if some elements of the AI Act are hard to square with an entirely contractual approach).[92]

---

[78] https://orcaarisk.com.
[79] https://www.credo.ai.
[80] SOC2 is an auditing standard developed by the American Institute of Certified Public Accountants, originally for cloud services.
[81] https://babl.ai/ai-audits/; for the NYC law *infra* III.3.a.
[82] https://www.monitaur.ai.
[83] luminos law ai.
[84] https://www.holisticai.com.
[85] https://latticeflow.ai.
[86] https://fairnow.ai.
[87] https://www.eticas.ai.
[88] *Supra* I.1. on financial market gatekeeper theory.
[89] *Infra* III.3.b. on notified bodies.
[90] This goes, for instance, for LNE (Laboratoire National de Métrologie et d'Essais).
[91] See https://www.tuev-lab.ai; under Art. 6 (1), Annex I AI Act and the Machinery Regulation, TÜV Rheinland has been recognized by the EU Commission: https://www.tuv.com/press/en/press-releases/new-machinery-regulation-notified-body.html; TÜV Süd offers conformity certificates and additional services: https://www.tuvsud.com/en/newsroom/press-releases/2025/november/new-tuev-sued-services-for-efficient-implementation-of-the-eu-ai-act; for U.S. example see *Partnoy*, 79 Washington University Law Quarterly 491, 507 et seq. (2001).
[92] This is most notable for Art. 44 (3) AI Act. The rule applies if (i) a company decides to have a notified body issue the certificate on technical documentation according to Annex VII and (ii) that body later finds that the AI system no longer meets the relevant requirements. Art. 44 (3) AI Act sets out conditions for withdrawing the certification. Among these is observance of the principle of proportionality and a requirement to give reasons for the withdrawal decision. Additionally, Art.

2. The Three Groups of AI-Gatekeepers

Trusted traditional institutions, for instance auditors or lawyers, are a natural first group of gatekeepers.[93] Consider, for instance, a bank that uses an AI-enhanced credit-underwriting model. Its established gatekeepers might offer to test for discriminatory outcomes. In the U.S., the Equal Credit Opportunity Act provides the benchmark, an example of "old" law that is applied considering AI-supported decision-making. In the EU, the 2023 Consumer Credit Directive stipulates a similar rule. Additionally, an AI gatekeeper in the EU will monitor compliance with designated AI laws such as the 2024 AI Act, where AI-supported creditworthiness evaluation qualifies as a „high-risk AI system".[94]

A second group consists of specialist new entrants dedicated to AI compliance which, for now, lack the accumulated reputational capital of the incumbents. By way of illustration, consider a corporation that uses generative AI to draft marketing communications and engages a specialist start-up to audit the system for the inadvertent disclosure of material non-public information.[95] The start-up might offers domain-specific expertise in identifying what would qualify as insider information under the relevant securities-law regimes.

The third group, consisting of public bodies or private firms operating under public accreditation, is structurally different and has been less systematically addressed in the context of financial-market gatekeeper theory.[96] Instead, an important

---

44 (3) AI Act requires an appeal procedure against decisions of notified bodies, again, a legislative strategy that is more familiar from administrative law; see Martini/*Wendehorst-Gerdemann*, KI-VO, Art. 44 no. 34, 43-44, 48, noting that under the German approach of private notified bodies, the appeal procedure will be a private, not public law procedure, hence, must fall back on contractual arrangements. While this has been established practice in other areas such as product safety for medical drugs (on this see *Czettritz/Strelow* MPR 2022, 205 (207)), the author suggests for the legislator to use the framework of *Beleihung* for notified bodies under the AI Act.

[93] This first group, established gatekeepers, brings accumulated reputational capital from adjacent practices, but also conflicts of interest familiar from the post-Enron gatekeeper scholarship. See, for instance, *Coffee*, A Theory of Corporate Scandals: Why the US and Europe Differ in: Armour/McCahery (eds.), After Enron, 2006, p. 215; *Cox*, The Oligopolistic Gatekeeper: The US Accounting Profession in: Armour/McCahery (eds.), After Enron, 2006, p. 295; *Nolan*, The Legal Control of Directors' Conflicts of Interest in the United Kingdom: Non-Executive Directors Following the Higgs Report in: Armour/McCahery (eds.), After Enron, 2006, p. 367.

[94] *Langenbucher*, Consumer Credit in The Age of AI – Beyond Anti-Discrimination Law, 663/2022 ecgi Working Paper (2022) (available at: https://www.ecgi.global/publications/working-papers/consumer-credit-in-the-age-of-ai-beyond-anti-discrimination-law).

[95] On AI in corporate communication see *Bauer/Langenbucher, Corporate Communication, Agentic AI, and Prompt Injections* in Hacker (ed.), Oxford Intersections: AI in Society, 2026.

[96] But see *Choi*, Market Lessons for Gatekeepers, 92 Northwestern University Law Review 916 (1998); *Partnoy*, 79 Washington University Law Quarterly 491, 506 et seq. (2001); *Gilson/Kraakman*, 70 Virginia Law Review 549, 605 (1984) (on the Underwriter's Laboratory and the Good Housekeeping Seal); additionally, see *Hamdani*, 77 Southern California Law Review 53 (2003) for

strand of administrative law scholarship has focused on these actors, however, few apply the bonding logic of reputational capital[97] or consistently use the term 'gatekeeper'.[98] Gatekeepers in this third group are not immune to reputational capital or liability discipline. Their commercial standing depends on maintaining credibility and they can face tort exposure.[99] However, the primary disciplinary mechanism is *ex ante* public accreditation and ongoing supervisory monitoring, substituting regulatory oversight for purely market-based factors. To illustrate, return to the bank that uses an AI-supported credit underwriting tool. Instead of retaining its established auditor or lawyer, it could decide to ask a publicly accredited private body to validate or certify its AI. This gatekeeper would conduct a conformity assessment against the substantive requirements of a designated AI law – such as the EU AI Act – and could issue a certificate.

Public accreditation regimes also play a role for some of the established gatekeepers in the first group – most notably for auditors who are licensed and under regulatory oversight.[100] However, the focus of public accreditation differs: Auditor accreditation certifies the general fitness to perform audits whereas the notified-body designation under the AI Act[101] is tied directly to the regulatory regime whose standards are being assessed. In that way, one might conceptualize gatekeepers in the third group as sitting „within" the regulatory environment, as it were, while gatekeepers from the first group provide a purely private service which requires a license.

Against that background, the three forms of gatekeepers emerge as occupying positions on a spectrum of public-private hybridity. The first group combines purely private gatekeepers, for example lawyers, with gatekeepers that have significant public oversight, namely auditors. The second group of start-up gatekeepers is

---

qualifying certain manufacturer as gatekeepers; for compliance gatekeepers see *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 520 (2024).

[97] On AI regulation see *Coglianese/Crum*, Leashes, not guardrails: A management-based approach to artificial intelligence risk regulation, 45 Risk Analysis 4397 (2025); *Clark/Hadfield*, Regulatory Markets: The Future of AI Governance, 65 Jurimetrics 195 (2026), apply their "regulatory-markets"-framework specifically to AI safety; on regulatory intermediaries: *Abbott/Levi-Faur/Snidal*, Theorizing Regulatory Intermediaries: The RIT Model, The Annals of the American Academy of Political and Social Science 670 (2017), 14.

[98] This literature's central categories – for instance private regulators, third-party certifiers, or conformity assessment bodies – overlap with the gatekeeper concept but emphasize the regulatory design and standard-setting functions rather than focus on the disruption-of-misconduct of financial-market gatekeeper theory. See for instance *Clark/Hadfield,* 65 Jurimetrics 195, 197 (2026) with the term "independent sector of licensed private regulators". For the German equivalent of "*Beleihung*" see infra III.3.b.; see further *Coglianese/Crum,* 45 Risk Analysis 4397, 4401 (2025) with the term "third-party auditor"; but *Zaring*, Regulating by Repute, 110 Michigan Law Review 1003 (2012) for discussing reputation in a public agency context.

[99] Infra V.1. on tort exposure; see *Zaring*, 110 Michigan Law Review 1003, 1010 et seq. (2012), on gatekeeping in the administrative law context.

[100] In the U.S., the PCAOB supervises auditors; in the EU Regulation (EU) 537/2014 and directive 2014/56/EU establish a framework for national oversight bodies; the German equivalent is APAS.

[101] *Infra* III.3.b. on notified bodies.

usually purely private, with minimal public oversight. The third group displays important public elements which modify the classical tools of reputational bonds and liability discipline.[102]

III. Defining Designated AI Laws and Designated AI-Gatekeepers

Under U.S. federal law no designated AI law has been passed nor has any federal agency yet required any form of designated AI-gatekeeper.[103] Instead, AI-compliance is a matter of general compliance with „old" law in the U.S., while some agencies have started to work on developing guidance for selected issues.[104] This contrasts with U.S. state law and EU law, where a combination of „old" laws and new, designated AI-laws exists.[105]

1. „Old" Law and AI-Compliance

The introduction of AI into commercial activity does not suspend the legal frameworks that already govern that activity. By way of illustration, consider once again legislation such as Title VII of the Civil Rights Act of 1964, the Fair Housing Act (Title VIII of the Civil Rights Act) or the Equal Credit Opportunity Act that prohibit discriminatory practices in credit underwriting. If using an AI for recruiting employees or for evaluating creditworthiness, compliance checks must involve the question whether the AI and the AI-supported human discriminate against certain groups.[106] Another example is provided by bank supervisors. The OCC, the Federal Reserve and the FDIC apply Supervisory Guidance on Model Risk Management.[107] Following this guidance, banks must validate all models – including AI systems –

---

[102] See *Coglianese/Crum*, 45 Risk Analysis 4397 (2025); *Clark/Hadfield*, 65 Jurimetrics 195 (2026); for analogies: *Zaring*, 110 Michigan Law Review 1003, 1010 et seq. (2012).

[103] The Algorithmic Accountability Act of 2025 is a proposed federal bill which would require companies to perform impact assessments for bias, accuracy, and security. It has been introduced but not yet been enacted, https://www.congress.gov/bill/119th-congress/senate-bill/2164/text. Additionally, Executive Order 14110 had been passed under the Biden administration, revoked under the Trump administration by Executive Order 14179, which has issued its own executive orders.

[104] The FDA provides an example for a public agency that has worked out guidance on how AI-supported medical devices can comply under existing law , see https://www.fda.gov/media/145022/download?attachment; https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device.

[105] *Selbst,* An Institutional View of Algorithmic Impact Assessments, 35 Harvard Journal of Law & Technology 117, 139 et seq. (2021) gives an overview of a variety of algorithmic audits that have emerged in the U.S. under existing law; *Clark/Hadfield,* 65 Jurimetrics 195 207 et seq. (2026) give a broad overview on existing regulatory and voluntary standards in the U.S.

[106] See e.g. *Langenbucher*, Consumer Credit in The Age of AI – Beyond Anti-Discrimination Law, 663/2022 ecgi Law Working Paper (2023).

[107] SR-11-7 https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

according to supervisory standards.[108] Along similar lines, the FTC Act prohibits unfair and deceptive practices when companies transact with consumers. If they employ AI in reaching out to consumers, this standard must be met. More illustrations are provided by the Dodd-Frank and the Sarbanes-Oxley Acts, which – while not explicitly mentioning AI – indirectly set a baseline standard for what AI must achieve.[109]

Under EU and Member State law, similar old-law issues arise. The most evident illustration for pre-existing „old" law is the General Data Protection Regulation (GDPR),[110] which includes rules on, for instance, data minimization, consent, automated decision-making, and explainability. Compliance departments of companies that develop or use AI, just like their U.S. counterparts, must ensure that their AI-supported business practices do not violate such laws.

2. Designated AI-Law

Among the jurisdictions engaging explicitly with AI, U.S. states and the EU have been the most active, enacting sectoral, categorical, and situational laws,[111] or combinations of these, that this paper collectively terms „designated AI law.

a) U.S. State Law

U.S. states that have passed sectoral laws have often added situational and categorical elements.[112] To name just a few, California combines sectoral and situational approaches when it requires health insurers that use AI in specific situations, namely for utilization to approve or deny care, or to have a licensed physician oversee decisions.[113] Additionally, AI may not be the sole basis for denying coverage. Along similar lines, Illinois addresses the use of AI in health insurance

---

[108] See *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1575 (2022).
[109] *Cen/Alur*, From Transparency to Accountability and Back: A Discussion of Access and Evidence in AI Auditing, EAAMO: Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1, 4 (2024) (available at: https://arxiv.org/abs/2410.04772).
[110] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), OJ 2016 L 119/1.
[111] *Supra* introductory text before I. on sectoral, categorical, and situational laws.
[112] See https://corpgov.law.harvard.edu/2025/10/28/cyber-and-ai-oversight-disclosures-what-companies-shared-in-2025/ reporting that in 2025 state legislatures considered more than 1000 bills relating to AI, of those, 136 were signed into law in 40 states, most of them relating to deepfakes.
[113] SB 1120 (2024).

decision-making and requires human oversight.[114] Colorado regulates the use of AI and external data in insurance underwriting. The law prohibits the use of data that results in unfair discrimination, even if unintentionally done.[115] Several states have adapted their insurance codes to address algorithmic pricing tools.

In an employment context, the Illinois Artificial Intelligence Video Interview Act was one of the first laws in the country to require employers to notify applicants and seek consent when AI is used to analyze video interviews.[116] New York City Local Law 144[117] regulates the use of AI-based automated employment decision tools in hiring, requiring bias audits and disclosures.[118] Maryland restricts the use of facial recognition in job interviews without consent.[119]

Utah's ambitious AI-law is still pending.[120] Utah's Artificial Intelligence Amendments[121] combines sectoral and situational regulation. Certain occupations must prominently disclose when someone is interacting with a generative AI. California prohibits interactions with a bot with the intent to mislead about its artificial identity.[122] Texas regulates deepfake videos around elections.[123]

b) The EU AI Act

The EU AI Act[124] is currently the most comprehensive legislation that engages with AI. It combines categorical elements, distinguishing different types of risk, with a situational approach, singling out, for instance, the use of high-risk AI in credit underwriting or employment.[125] The Act applies to 'providers'[126], i.e.

---

[114] HB 3460.
[115] SB 169 (2023).
[116] Illinois Artificial Intelligence Video Interview Act, 820 ILCS 42/5.
[117] On bias audits: *Costanza-Chock*, Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574 (2022).
[118] *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1, 7 et seq. (2024); *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574 (2022).
[119] Md. Code, Labor & Employment § 3-717.
[120] https://commerce.utah.gov/ai/.
[121] S.B. 149, Gen. Sess. (Utah 2024).
[122] Cal. Bus. & Prof. Code § 17941.
[123] S. B. 751, 88th Leg., Reg. Sess. (Tex. 2023).
[124] Regulation (EU) 2024/1689.
[125] The AI Act does not follow a sectoral approach. However, at closer inspection it includes some sectoral elements. Art. 6 (1) AI Act refers to sectoral product safety regulation for qualifying an AI system as high-risk (see text accompanying footnote 134 et seq.). For the financial sector, Member States are encouraged to have financial institutions' supervisors to enforce compliance with the AI Act. Additionally, compliance with the AIA is possible through the existing EU banking supervisory law regime. The Colorado AI Bill includes a similar provision, see https://leg.colorado.gov/bills/sb24-205.
[126] Art. 3 (3) AI Act.

developers, of 'AI systems'[127] and to 'deployers',[128] who use them. What the Act expects depends on the intended use and on the person developing or (only) using the AI.

Some AI categories are entirely prohibited in certain situations, for instance manipulative or deceptive techniques, social scoring or certain emotion recognition systems in a workplace or educational setting.[129]

In addition to prohibited AI, the AI Act regulates a category it calls 'high-risk'.[130] It is important to note that the Act does not require the provider or deployer to decide what he considers high risk. Instead, the Act distinguishes between two well-defined high-risk AI categories.

The first high-risk category encompasses products such as certain machinery, toys, or medical devices,[131] that already fall under pre-existing, harmonized Union legislation and have been required to undergo a third-party conformity assessment under their respective „old" product safety legislation.[132] For this group, the existing conformity assessment will extend to certifying compliance with the AI Act. Traditional gatekeepers remain in charge.[133] These can be public or private bodies.

The second high-risk category under the AI Act groups together AI systems that the Act specifically designates as high-risk.[134] Whether an AI system qualifies as 'high-risk' depends on it being listed under Art. 6 (2) AI Act in conjunction with Annex III, and its being eligible (or not) for one of the exceptions of Art. 6 (3) AI Act.[135] Examples of high-risk AI systems include certain biometric categorization tasks, certain evaluation and assessment tools in employment, educational, or credit underwriting situations, certain law enforcement tasks or roles in the administration of justice. If an AI system qualifies as high-risk, Art. 8-15 AI Act require providers to observe product-design requirements such as risk management, data governance, transparency, and human oversight. Art. 16-25 regulate specific duties of providers of AI systems, for instance quality management, documentation

---

[127] Art. 3 (1) AI Act.
[128] Art. 3 (4) AI Act.
[129] Art. 5 AI Act.
[130] As of writing, the application of Art. 8-15 to high-risk systems is expected to be postponed under the Digital Omnibus on AI (COM(2025)1067 of Nov. 2025).
[131] For a full list see Annex I Nr. 1-20.
[132] Art. 6 (1) AI Act.
[133] If this is not the case (for instance where "old-school" laws lay down detailed rules instead of following the EU's new conformity assessment framework, e.g. for cars, planes, trains), these gatekeepers do not track compliance with the AI Act. Instead, these AI systems fall outside of the AI Act and await their own regulation, see *Denga*, Konformitätsbewertung von KI-Systemen, ZfPC 2023, 154, 156, 158.
[134] Art. 6 (2), Annex III AI Act. Exceptions apply if they do not pose a significant risk to health, safety or fundamental rights, Art. 6 (3) AI Act.
[135] These exceptions include the AI performing a narrow procedural task, improving the result of a previously completed human activity, pattern-detection without automatically replacing or influencing a previously completed human assessment, preparatory tasks. A counter-exception is added: Profiling is always considered high-risk.

or corrective actions. Art. 26-27 concern deployers, i.e. companies that use AI systems. These are, among other obligations, required to assign human oversight personnel, monitor input data quality, inform workers' representatives, and perform a human rights impact assessment. Additionally, providers of high-risk AI systems face post-market monitoring duties and must report serious incidents.[136]

A third category has been somewhat hastily added before the Act entered into force.[137] Providers of „general-purpose models" (large language models) that are not open source face additional requirements for, among other things, technical documentation, a policy on compliance with copyright laws and summary disclosure about the content used for training the model.[138] Developers of general-purpose models with systemic risk[139] must provide for model evaluation, market monitoring and cybersecurity protection.[140] Note that an AI general-purpose model does not in itself automatically qualify as an AI system. Instead, it is conceptualized as an essential component of an AI system, for instance after a user interface has been added.[141] This implies that the AI Act's compliance requirements are conditioned on providers placing on the market or putting into service or deployers using what counts as an AI „system".[142]

Outside of the prohibited and the high-risk category, the AI Act relies on situational elements. If an AI system is intended to interact directly with natural persons, providers must ensure that the AI is developed in such a way that these persons are informed that they are interacting with an AI or that certain content is AI-generated or manipulated.[143]

3. Designated AI-Gatekeepers

---

[136] Art. 72, 73 AI Act.
[137] With critique on legislators' instead of private standard-setting: *Muller/Yoo*, Taking Standards Seriously: The Case for a Private Standards-Based Approach to AI Governance, Wharton Accountable AI Forum (2026) (available at: https://www.accountableaiforum.com/p/taking-standards-seriously-the-case).
[138] Art. 53, Annex XI and XII AI Act.
[139] Art. 3 (65) AI Act.
[140] Art. 55 AI Act.
[141] The AI Act does not define what qualifies as AI model but integrates both terms and their relationship to each other in recital (97) AI Act; Martini/*Wendehorst-Wendehorst*, KI-VO, Art. 3 note 25-28; Martini/*Wendehorst-Bernsteiner-Schmitt*, KI-VO, Art. 51 note 12.
[142] Art. 3 (1) AI Act's broad and functionally indeterminate definition ("AI system means a machine-based system […]") is of little help in answering this question. Rather, it must be approached as an attempt to define which products and activities the AI Act wishes to target with specific duties. What is described as "AI system" faces the full list of requirements for high-risk systems described above, Art. 8-15 as to design, Art. 16-27 as to operation. What is described exclusively as "AI model" must meet the requirements of Art. 53 et seq., unless it is "specifically developed and put into service for the sole purpose of scientific research and development", Art. 2 Nr. 6 AI Act.
[143] Art. 50 AI Act.

Jurisdictions that have passed designated AI laws must decide on how to best enforce these laws. Public and private enforcement against a wrongdoer are evident choices, relying on fines and other sanctions as well as the threat of liability for damages. The New York Responsible Artificial Intelligence Safety and Education (RAISE) Act provides an example for public enforcement. It targets large-scale AI developers of frontier models and requires them to implement safety protocols. The Act creates an AI oversight office within the New York Department of Financial Services to monitor compliance, review safety incident reports, and adopt rules.[144] The New York Attorney General can bring civil actions against large frontier developers. Along similar lines, the EU AI Act mandates Member State public bodies to take care of market surveillance along product safety principles.[145]

a) AI-audits under U.S. State Law

Some designated U.S. state laws suggest or require designated AI-gatekeepers. These are conceptualized as private, not public bodies. New York City's Local Law 144 expects, for instance, a bias assessment for certain automated employment decision tools by an independent auditor.[146] The auditor may not be involved in the development of the AI and may not have a financial stake in the vendor or the employer. Employees of the company may not be bias auditors and the person performing the audit must be capable of exercising impartial and objective judgment. A New Jersey bill that mirrors the New York City law is pending.[147] The Colorado AI Act includes an audit requirement[148] as does the pending AB2930 in California which would require an annual bias audit for automated decision tools.[149]

---

144 Pozza/Scott/White, New York Finalizes RAISE Act for Frontier AI Models; Law Takes Effect January 1, 2027, Wiley Rein Alert, 3 April 2026, available at: https://www.wiley.law/alert-New-York-Finalizes-RAISE-Act-for-Frontier-AI-Models-Law-Takes-Effect-January-1-2027.

145 Art. 74 for GPAI see Art. 75, 88 et seq. AI Act.

146 Local Law 144 of 2021, Automated Employment Decision Tools, N.Y.C. Council Int. No. 1894-A (enacted 11 December 2021), codified at N.Y.C. Admin. Code §§ 20-870 to 20-874 (title 20, chapter 5, subchapter 25), available at: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9; https://fairnow.ai/guide/nyc-local-law-144/; on bias audits: *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571 (2022); on the relationship between AI audits and impact assessments: *Selbst*, 35 Harvard Journal of Law & Technology 117, 146 (2021)

147 New Jersey Assembly Bill A1021, 2026-2027.

148 Overview *see* Schellman/RockCyber, What You Need to Know About the Colorado AI Act, 26 February 2026, available at: https://www.schellman.com/blog/ai-services/what-you-need-to-know-about-the-colorado-ai-act.

149 California Assembly Bill 2930 (Bauer-Kahan), Automated Decision Systems, 2023–2024 Reg. Sess., as amended in Senate 28 August 2024 (failed to pass), available at: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2930.

b) Notified Bodies under the AI Act

The AI Act introduces its own designated AI-gatekeeper in the form of 'notified bodies'. These are a publicly accredited group of (mostly) private gatekeepers[150] who can assist providers of AI systems.[151] Like the manufacturer under traditional product safety laws, the provider of an AI system draws up an EU declaration of conformity[152] and a CE marking[153] under the AI Act. The notified body supports the provider with this task and can issue a certificate of conformity following a successful assessment procedure.[154]

Notified bodies are modelled after the EU's 'new legislative framework', a piece of product safety regulation.[155] Under this framework, manufacturers, as a general rule, not a public authority, carry out their own conformity assessments before[156] putting a product on the market.[157] A presumption of conformity applies, if so-called "harmonized standards" are followed.[158] For AI-compliance, the European Standardization Organizations[159] are in the process of developing these harmonized standards.[160] Providers of AI systems are free to enlist gatekeepers in the form of notified bodies to support them in assessing their products and monitoring compliance.

Under the AI Act, a notified body is an entity that must be equipped with legal personality under Member State law.[161] Moreover, it must pass the AI Act's

---

[150] *Supra* II.2. on the three groups of gatekeepers.
[151] See *Clark/Hadfield,* 65 Jurimetrics 195 (2026) for a functionally similar proposal of "licensed private regulators".
[152] Art. 47 AI Act.
[153] Art. 48 AI Act.
[154] Art. 44, Annex VII AI Act; *Denga*, ZfPC 2023, 154, 157; *Beyerbach*, Haftung der Benannten Stelle für Mängel in der Medizinprodukteherstellung? Überlegungen zum Vorlagebeschluss des Bundesgerichtshofs in der Rechtssache PIP vom 9.4.2015 (VII ZR 36/14), GesR 2015, 522, 525 on (mandatory) notified bodies for medical drugs.
[155] See *Selbst*, 35 Harvard Journal of Law & Technology 117, 154 et seq. (2021) on collaborative governance approaches in the U.S.
[156] *Denga*, ZfPC 2023, 154, 155.
[157] Art. 3 (22) AI Act; *Veale/Borgesius*, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97, 102; for a functionally similar management-based approach to AI-regulation: *Coglianese/Crum*, 45 Risk Analysis 4397, 4401-4402 (2025) ("the regulated entity is required to develop an internal plan to identify and monitor risks, produce and implement protective measures, and document changes to address those risks").
[158] Art. 42 AI Act.
[159] CEN and CENELEC.
[160] Standard-setting is an established tool of EU product regulation. Laws provide a broad framework and standard-setting bodies work out details. Standards for AI, once developed, will play a core role on the EU. On this technique, combined with concerns of low democratic accountability, see *Denga*, ZfPC 2023, 154, 157; Martini/*Wendehorst-Gerdemann*, KI-VO, Art. 40 note 2, 6; *Veale/Borgesius*, CRi 2021, 97, 104 et seq.
[161] Art. 31 (1) AI Act.

notification procedure,[162] which is performed by a public „notifying authority".[163] There are certain institutional requirements to follow for a notified body in the EU. They must offer satisfactory organizational and quality management capabilities, including cybersecurity requirements.[164] A notified body must be independent from the provider it certifies,[165] may not be directly involved in the design of the relevant AI system,[166] and have competent personnel.[167] Notified bodies must take out appropriate liability insurance for their conformity assessments, unless liability is assumed by the Member State or the Member State is itself directly responsible.[168]

The AI Act is indifferent as to the body's private, public, or hybrid form.[169] Hybrid structures are a feature in some Member States where the gatekeeping entity is a private institution but disposes of specific public powers that have been delegated to it („*Beleihung*"). A classic example is the German TÜV where it performs official vehicle inspections. The decision to issue or deny the car inspection sticker implies a binding administrative law determination. The power to issue this administrative act is conferred to the TÜV by the relevant public authority.[170] By contrast, where the TÜV acts as a notified body under existing product-safety laws, for instance for medical products, no such delegation of public powers exists. Instead, the TÜV promises in a private contract to validate whether the product follows product safety laws.[171]

The closest analogue in U.S. practice might be nationally recognized testing laboratories which are certified to test products for workplace safety. In the U.S., the non-delegation and the state-action doctrine have created considerable ambiguity around the question whether, in that way, public functions are being privatized.[172] A similar debate, which is beyond the scope of this paper, has evolved in the EU. Scholars have been critically discussing whether standard-setting and notified bodies might imply an unconstitutional delegation of powers that violates subsidiarity and democratic principles. A core concern revolves around CJEU decisions that have required a precisely defined framework for delegating powers, that is justified (and limited) by technical expertise and subject to judicial review.[173]

---

[162] Art. 29-30 AI Act.
[163] See Art. 28 AI Act for supervision, Art. 29 et seq. for the procedure.
[164] Art. 31 (2) AI Act; Martini/*Wendehorst-Roth-Isigkeit*, KI-VO, Art. 31 no. 7 et seq., 10 et seq.
[165] Art. 31 (4) AI Act.
[166] Art. 31 (5) AI Act.
[167] Art. 31 (11) AI Act.
[168] Art. 31 (9) AI Act.
[169] Martini/*Wendehorst-Roth-Isigkeit*, KI-VO, Art. 31 note 5.
[170] BGHZ 49, 108 (117); BeckGK/*Teichmann*, § 675 BGB no. 134.
[171] For medical products see *Beyerbach*, GesR 2015, 522, 524-525; Clausen/Schroeder-Printzen-Friedrich, Münchener Anwaltshandbuch Medizinrecht, 2026, § 18 no. 497; for implications for liability see *infra* V. 1.
[172] *Van Loo*, The New Gatekeepers: Private Firms as Public Enforcers, 106 Virginia Law Review 467 (2020); *Clark/Hadfield,* 65 Jurimetrics 195, 214 (2026).
[173] CJEU case C 9-56, Meroni & Co ECLI:EU:C:1958:7; CJEU case C-270/12, UK Short Selling ECLI:EU:C:2014:18.

Traditional, purely technical product-regulatory standards have met these requirements. The AI Act, by contrast, involves some technical standards, but, at the same time, includes complex rights-based risk assessments and balancing exercises, for instance on bias, discrimination and fundamental rights.[174] It is doubtful whether the classic reasoning frictionlessly applies to these challenges.

IV. Mandatory and Optional AI-Gatekeepers

Currently, most AI-gatekeepers provide optional, not mandatory services to firms, supporting them in their compliance efforts. For instance, a start-up company can decide to hire an AI-audit consultancy or conduct the audit in-house. An established tech company can rely on its legal and compliance departments, especially in jurisdictions without designated AI-laws, or can engage an AI-auditor, particularly if the company operates in places where designated AI-laws apply.[175]

Where gatekeepers are optional, there is an obvious challenge for the disruption-of-misconduct function of financial-market gatekeeper theory:[176] Firms can choose not to engage external gatekeepers, losing the leverage that withholding cooperation would otherwise provide.[177] Still, it is submitted below that in practice there are good reasons for investor expectations regarding involvement of an AI-compliance gatekeeper to develop.[178]

A more nuanced picture concerns AI-compliance where consumers are involved. Arguably, market pressure to integrate a gatekeeper to alleviate specific consumer concerns can be less pronounced. Even on competitive markets it can be cheaper to offer a low-quality product that comes with *ex post* litigation risk, which can be

---

[174] *Ebers*, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 2021, 588, 593; *Gerdemann*, Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI, MMR 2024, 614, 619. More generally on non-delegation to notified bodies: *Falke/Joerges*, The "Traditional" Law Approximation Policy Approaches to Removing Technical Barriers to Trade and Efforts at a "Horizontal" European Product Safety Policy, 6 Hanse Law Review 289, 314, 331, 345 et seq. (2010); *Unger*, Herstellerbegleitung oder Marktüberwachung? Zur Haftung "benannter Stellen" im Medizinproduktrecht, EuZW 2017, 299, 301; *van Gestel/Micklitz*, European integration through standardization: How judicial review is breaking down the club house of private standardization bodies, 50 Common Market Law Review 145 (2013); On non-delegation in the context of algorithmic decision-making by public bodies: *Butler*, Algorithmic Decision-Making, Delegation and the Modern Machinery of Government, 45 Oxford Journal of Legal Studies 727 (2025).

[175] Alternatively, the company might expect designated AI legislation to be passed or potential tort litigation to gain steam, having judges, as it were, "fill in" for regulators, for an example, see: *Daniels*, Instagram Addiction Trial Shows How Juries Step Into Policy Void, Bloomberg Law (Legal Exchange: Insights & Commentary), 24 February 2026, available at: https://news.bloomberglaw.com/legal-exchange-insights-and-commentary/instagram-addiction-trial-shows-how-juries-step-into-policy-void.

[176] *Supra* I.1. on that theory.

[177] Compare, by contrast, *Clark/Hadfield*s, 65 Jurimetrics 195 (2026) regulatory markets theory, where "the targets of regulation […] are required by the government to purchase the regulatory services of appropriate licensed private regulators".

[178] *Infra* III.2.

priced by the wrongdoer, than involve a costly gatekeeper. Against that background, most jurisdictions have – already outside the AI territory – installed mandatory public bodies that assess product safety, for instance for food and drugs. Another reaction involves strengthening consumer rights for contractual or tortious liability, for example in AI-supported medical products, or transparency and explainability rights, for instance in credit underwriting.

The AI Act sticks with this general strategy. Where product safety bodies have been in charge, they now surveil compliance with the AI Act.[179] A combination of rules under the GDPR[180] and the AI Act[181] accounts for transparency and explainability rights. The Revised Product Liability Directive adjusts some principles of strict liability.[182]

1. Optional AI-Gatekeepers

Originally, EU lawmakers had aimed for closer control of high-risk AI systems through mandated requirements for notified bodies to assess compliance.[183] As the AI Act moved through its legislative process, the current regime emerged,[184] displaying a preference not to overburden Member States with developing notified AI bodies in a rush. The ensuing lack of an external verifying party, which necessarily characterizes self-validation, is a corollary that lawmakers have *nolens volens* accepted, at least for now.[185] A countervailing effort is *ex post* public enforcement via market surveillance bodies.[186]

The 'deployer'[187], i. e. the company using the AI system, never directly works with the Act's notified bodies.[188] While deployers have their own specific obligations to comply with under the AI Act, these do not include interacting with a notified body.[189]

Notified bodies are relevant for 'providers' of AI systems. They have a duty to ensure that their AI system meets compliance requirements, to draw up an EU

[179] *Supra* II.2.; for an example (medical devices) see https://eyreact.com/notified-bodies-ai-act/.
[180] See Art. 15, 22 GDPR.
[181] See Art. 86 AI Act.
[182] Directive (EU) 2024/2853.
[183] Recital (125); Martini/*Wendehorst-Gerdemann*, KI-VO, Art. 43 note 12, 28 with further sources.
[184] For critique see: *Veale/Borgesius*, CRi 2021, 97; *Ebers*, RDi 2021, 588.
[185] Some U.S. laws, for instance in Colorado, follow a similar approach, allowing for internal and external validation. Going forward, the EU Commission is entitled to broaden the requirement for external gatekeepers, Art. 43 (6) AI Act; Martini/*Wendehorst-Gerdemann*, Art. 43 n 2.
[186] Art. 72-94 AI Act.
[187] Art. 3 (4) AI Act.
[188] Art. 43 AI Act, Annex VI.
[189] See, however, for the risk of a deployer becoming a provider under the Act when the deployer rebrands the AI system or substantially modifies it so that it becomes a new system, Art. 25 (1) (b) AI Act.

declaration of conformity, and to affix a CE-marking to their AI system, required to place the devices on the EU market.[190] The general rule is for the provider to freely choose between self-validation and voluntarily involving a notified body.[191] If the provider opts for self-validation, he verifies the product's quality management system, assesses compliance of its technical documentation, design, development, and post-market monitoring.[192] If he chooses to avail himself of a gatekeeper,[193] the notified body supports the provider[194] and issues a certificate.[195]

Where companies are free to mandate a gatekeeper, naturally, this extends to the selection of the gatekeeper, except for two cases mentioned further below.[196] Institutions inside the firm[197] can fulfill gatekeeping functions as can external gatekeepers.[198]

2. The Exception: Required Audits

A mandatory requirement to involve a gatekeeper in validating AI-related compliance – in the way external auditors are legally mandated for periodic financial statements – is, for now, a relatively rare occurrence under the AI Act and under U.S. law.[199] One exception in the U.S. is New York Local Law 144 that mandates a bias audit for all automated-decision-making tools in the context of a hiring decision.[200] Under the EU AI Act, an exception concerns a provider of certain AI systems that use biometrics,[201] for instance facial recognition for building access.[202] If

---

[190] *Supra* II.2. For a comprehensive list see Art. 16 AI Act; *Denga*, ZfPC 2023, 154, 157.
[191] *Supra* IV.2. for the exception, see Art. 43 (1) subpara. (1) with Annex VI AI Act.
[192] Annex VI AI Act.
[193] Art. 43 (2) AI Act somewhat misleadingly seems to suggest that providers of certain AI high-risk systems (everything except biometrics, see Annex III Nr. 2-8) may not choose external validation. However, given that there is no good argument available for excluding the stricter standard, commentators agree that this option remains possible, Martini/*Wendehorst-Gerdemann*, KI-VO, Art. 43 no. 39.
[194] Art. 43 (1) subpara. (3) sentence 1 with Annex VII AI Act.
[195] Art. 44 AI Act.
[196] For exceptionally mandated AI-gatekeepers, see *infra* III.2.
[197] For internal teams, close cooperation between legal, compliance, and developer teams throughout the process of designing a product and releasing it to the market is core.
[198] *Supra* I.2. In that respect, a lively debate has investigated whether supervisory boards should include an IT or an AI committee or at least provide for enough board members that are knowledgeable in that area.
[199] See *Partnoy*, 79 Washington University Law Quarterly 491, 507 et seq. (2001) on monopoly property rights of regulatory requirements to involve certain gatekeepers.
[200] *Supra* III.2.b.; *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571 (2022).
[201] Annex III Nr. 1: certain remote biometric systems; biometric categorization according to protected characteristics; emotion recognition. Art. 3 Nr. 34 AI Act defines biometrics as personal data that relates to physical, physiological or behavioral characteristics of a natural person.
[202] eyreACT, Notified Bodies Under the EU AI Act: The Gatekeepers You Haven't Met Yet, 2 February 2026, available at: https://eyreact.com/notified-bodies-ai-act/.

either no harmonized standards or common specifications exist or if the provider has not fully applied these standards, a notified body must be involved.[203]

Generally, the provider of an AI system has under the AI Act the choice between all available notified bodies in his Member State. Exceptions concern Union institutions that employ an AI system and all Member State public authorities that put an AI system into service for law enforcement, immigration or asylum purposes. In all these cases, the relevant market supervisory body shall act as notified body. For Union institutions, this is the European Data Protection Authority, for Member State public authorities the designated market surveillance authority must be the notified body.[204]

3. The (likely) Rule: Market Expectations

Even without a legal requirement, a market for AI-gatekeepers has started to develop.[205] One incentive to involve gatekeepers is to signal a firm's credible commitment to AI-related compliance and, in that way, build trust for investors and consumers.[206] Companies that develop or use AI know that their investors and their professional or retail contractual partners must deal with important information asymmetries. AI systems are fast-moving and novel business strategies keep developing. Investors are largely ignorant about the efforts a firm puts into AI-compliance. Contractual partners face uncertainty about how a company will use AI in transactions. Opacity of black-box models creates additional risks where reasoned explanations for strategic behavior are not readily available. Gatekeepers, especially of the external kind, can help to overcome some of these concerns. With external validation and certification, AI-developing and AI-using companies signal that, as a minimum, they adhere to relevant laws, confirmed by a gatekeeper.[207] The more reputational capital the gatekeeper has at stake, the stronger the signal such certification sends.

---

[203] Art. 43 (1) subpara. 2 AI Act; *infra* III.3.
[204] Art. 43 (1) subpara (3), Art. 74 (8), (9) AI Act; Martini/*Wendehorst-Roth-Isigkeit*, KI-VO, Art. 43 note 32.
[205] *Supra* II.1.
[206] Advocating for required audits: *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, at 5.2 (2022); for product markets more generally: *Choi*, 92 Northwestern University Law Review 916 (1998).
[207] *Supra* III.2. and III.3.

Risk management is another incentive to seek the services of gatekeepers.[208] In the EU, measurement methodologies, secondary legislation,[209] and common specifications[210] shape the services AI-gatekeepers can offer. Once harmonized standards will have been fully developed, companies will wish to profit from the (optional) presumption of conformity that involving a gatekeeper brings.[211]

Shifting the burden of proof in product liability litigation can be yet another motivating factor for a company to look out for a gatekeeper.[212] Providers are liable to their contractual counterparty (the deployer) and, additionally, to consumers if they qualify as 'manufacturer' under product liability laws. In this situation, involving gatekeepers can help, for instance, to produce sufficient documentation to rebut presumptions and shift the burden of proof.[213] Additionally, a right of recourse against the gatekeeper may lie.[214] The same logic applies to deployers who voluntarily involve a gatekeeper to monitor their AI system.[215] Moreover, insurance companies might insist on external gatekeepers to lower their exposure.[216]

Additionally, designated AI-laws raise demand in the legal profession. The AI Act not only includes a large amount of vague legal and technical terms that await further development.[217] Additionally, its expectations go beyond purely technical expertise. Take, for instance, art. 27 AI Act, which requires certain deployers to perform a fundamental rights impact assessment before its first use, involving

---

[208] Martini/*Wendehorst-Roth-Isigkeit*, KI-VO, Art. 43 no. 25; *Denga*, ZfPC 2023, 154, 156; *Kilian/Denga*, Das Testen und Zertifizieren von KI-Systemen, NJW 2024, 2945 2947; *Denga*, Unternehmenshaftung für KI – zur Konformitätsbewertung in Permanenz, CR 2023, 277; *BeckOK KI-Recht/Kilian*, KI-VO Art. 43 no. 12; see generally *MüKoAktG/Spindler*, AktG § 93 no. 89 et seq. with further references.

[209] See, e.g., Art. 51 for quantitative thresholds for GPAI models, Art. 53 for measurement and calculation methodologies for training compute. Any model trained using $\geq 10^{25}$ FLOP is presumed to carry systemic risk which triggers the heaviest compliance obligations.

[210] Art. 41 AI Act: Common specifications are a default option before harmonized standards have been fully developed, primarily by CEN/CENELEC.

[211] See Art. 42 for the presumption, Art. 40 AI Act for the procedure.

[212] See BeckOK KI-Recht/*Schefzig/Kilian*, no. 18; *Kilian/Denga*, NJW 2024, 2945, 2947 for a requirement to integrate an external gatekeeper if the provider lacks technical expertise; see further *Denga*, ZfPC 2023, 154, 157; on buying plausible deniability: *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 489 et seq. (2024).

[213] See for instance the EU the Product Liability Directive (Directive (EU) 2024/2853). National courts are under the Directive held to presume defectiveness of a product or the causal link between the damage and defectiveness where it would be 'excessively difficult' for the claimant to prove either, Art. 10 (4) (a) PLDirective. The better a company's documentation, the higher the chances to rebut this presumption.

[214] Martini/*Wendehorst-Roth-Isigkeit*, KI-VO, Art. 43 no. 25; BeckOK KI-Recht/*Schefzig/Kilian*, no. 20.

[215] For a list of deployer duties see Art. 26 AI Act. Deployers are generally not considered manufacturers under the Product Liability Directive, but exceptions apply for deployers who make substantial modifications, apply their own name to the AI system, or substantially modify it, for instance through continuous AI-learning.

[216] *Denga*, ZfPC 2023, 154, 156.

[217] *Denga*, ZfPC 2023, 154, 156.

distinctly legal interpretation and balancing exercises.[218] Another illustration concerns deployers of AI systems that evaluate the creditworthiness of natural persons, establish their credit score, or are used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. Deployers must describe in detail how the high-risk AI system will be used, which categories of persons will be affected, and which specific risks of harm exist for these persons. Human oversight measures must be explained, internal governance and complaint mechanisms provided.[219] Gatekeepers with a legal background are likely to fill this role, supported by input from model developers who are informed on the AI's metrics, specifications for input data, and model performance on specific groups of persons.[220]

V. A Preliminary Roadmap for AI-gatekeepers

Traditional gatekeeper theory on financial markets has proposed a third-party enforcement tool where trusted gatekeepers can detect and disrupt misconduct.[221] In its most forceful version, it suggests a strict liability standard and a mandatory requirement to involve an external gatekeeper. This has held promises of access to information about wrongdoers at reasonable cost, where courts and regulators have struggled. The role of auditors on securities markets has been its paradigm example, mitigating information asymmetries between investors and issuers. Knowledgeable experts such as securities analysts, rating agencies or investment banks provide further illustration.

There are notable similarities between classical and AI-gatekeepers. This is most evident in that both respond to pronounced information asymmetries. Companies that produce or deploy AI know far more about their systems than the professional or retail counterparties affected by them. These can often not adequately verify product quality or the AI-supported decision affecting them. Signaling and third-party certification can mitigate this asymmetry.[222] External gatekeepers with domain-specific expertise have emerged to provide such services.

Additionally, just as public-company auditors that are mandatory for certain financial statements, several designated AI-laws now require third-party

[218] Relevant situations are the use of a high-risk AI system under Art. 6 (2), Annex III, except for digital infrastructure, see *supra* III.2.b.
[219] Exploration against his own suggestion of an algorithmic impact assessment at *Selbst*, 35 Harvard Journal of Law & Technology 117, 142 et seq. (2021).
[220] See in more detail Art. 13 (3) AI Act.
[221] *Supra* I.
[222] For AI audits as knowledge-producing see *Selbst*, 35 Harvard Journal of Law & Technology 117, 156 (2021).

assessments as a condition for market access[223] – and market expectations are likely to demand third-party assurance, even absent legal mandates.

At the same time, core differences exist between traditional and AI-gatekeepers along three dimensions: the regulatory environment, the institutional form of the gatekeeper, and the gatekeeper's reputational capital.

A first reason is conceptual fluidity. Core technical notions are contested within the AI research community and, even more, in the interdisciplinary discourse between AI scholars, legal academics, and policymakers. Consider how „fairness" or „explainability" lack anything close to the settled meaning of „materiality" or „going concern" a traditional auditor uses.[224] This conceptual fluidity is compounded by an interdisciplinary translation problem. While management is racing to develop an understanding for core concepts of AI,[225] appreciation of the vague world of legal terms might not come naturally to coders, used to precise, well-defined concepts.[226] For AI-gatekeepers this implies that mixed teams face the challenge of bridging a considerable cultural divide. Where classic auditors' main task is to detect flaws in compliance with a framework that both, auditor and auditee know very well, AI-gatekeepers must first build that common understanding.

A second difference, still concerning the regulatory environment, has to do with the rule-boundedness Coffee had identified as a characteristic gatekeeper feature.[227] AI laws are a recent phenomenon, their rules are preliminary, dynamic, or in flux, mostly vague, and in need of further guidance. They often involve delegated authority of public agencies and standard-setting bodies. Many rest on value-laden judgments such as balancing predictive power against discrimination. While accounting fraud scandals, a classical gatekeeper topic, have occasionally involved novel standards as well,[228] coping with broad innovation across almost all sectors of life is a characteristic challenge for AI-compliance laws. Established business practices have not yet been developed. Rather, there is a mix of laws, agency guidance, and private standard-setters, which gatekeepers must navigate. All of this implies that AI-gatekeepers take over various inherently prognostic, rather than more technical tasks. This can increase their „error" rate, given that benchmarks

---

[223] *Supra* III.2.

[224] See *Coglianese/Crum,* 45 Risk Analysis 4397, 4398 et seq. (2025) on regulatory guardrails as ill-fitted for overseeing a dynamic, heterogeneous technology such as AI; a similar point at *Clark/Hadfield,* 65 Jurimetrics 195, 212 (2026).

[225] See https://corpgov.law.harvard.edu/2025/10/28/cyber-and-ai-oversight-disclosures-what-companies-shared-in-2025/ for data on director bios listing AI (reporting a change from 26% in 2024 to 44% in 2025).

[226] See *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1581 (2022), who reports that internal teams are interested in producing plausible deniability.

[227] *Coffee*, 84 Boston University Law Review 301, 353 (2004).

[228] *Healy/Palepu*, The Fall of Enron, 17 Journal of Economic Perspectives 3 (2003); *Benston/Hartgraves*, The Crisis of the Ethics of Audit Profession: Collapse of Enron Company and the Lessons Learned, 21 Journal of Accounting and Public Policy 105 (2002).

for concepts such as „fairness" or „explainability" will, at best, be established *ex post*.

Third, there is no direct institutional analogue to auditors, the paradigm gatekeeper. Some AI-gatekeepers offer more traditional consultancy or audit services, others perform product-safety investigations. The former cover a much broader range than auditor certification of financial statements. Methodologically, they are more freewheeling. As to governance, there are no expectations of independence from the client who hires the consultant. By contrast, the product-safety gatekeepers such as notified bodies, often mitigate specific, but narrow asymmetries, for instance where they supply certifications. They are expected to work with a certain degree of independence from their clients – sometimes they are public bodies or endowed with delegated administrative-law rights. While this rule-bound approach of product-safety gatekeepers brings an element of auditor work to mind, their focus is much more limited. Auditor certification involves a fair representation of the entire corporation's financial standing. Product-safety gatekeepers are concerned with compliance of one good that the company produces.

Fourth, while both groups, classical and new, gatekeepers depend on reputational capital as their core asset, not all AI-gatekeepers have such capital to pledge. There is an interesting asymmetry as to the AI-gatekeeper community: Start-up gatekeeper firms, maybe with a focus on model development but little background in regulation, will need to build market recognition. While they do so, the reputational bond traditional gatekeeper theory had identified[229] does not yet exist and it might be rational to be a captured, rather than a strict auditor. By contrast, incumbent gatekeepers have reputational capital to pledge, yet, can face more severe conflicts of interest if they audit clients to whom they sell consulting services.

1. AI-Gatekeepers and Liability

Traditional gatekeeper theory was built around financial markets. Reputational bonds and (different versions of) liability were understood to discipline gatekeepers. For AI-gatekeepers, various new adverse selection and quality-sorting problems have spawned. Refined business standards have not yet developed which makes the market for gatekeepers opaque. Potential outcomes vary according to the relevant group of gatekeepers.[230] Incumbent gatekeepers, who add AI compliance to their portfolio of services, have considerable reputational capital to pledge, even if it stems from a different, not AI-related service. Market-entry gatekeepers, by contrast, must first build reputational capital. While this can lead to intense

[229] *Supra* I.1.
[230] *Supra* II.2. on the three groups of gatekeepers.

efforts for some, another likely outcome are rationally captured gatekeepers who try to gain a competitive edge by delivering overly positive certifications.

a) From Financial Markets to Products: Liability of Certifying Bodies

In contrast to traditional gatekeepers, (even modified) strict liability has rarely been advanced as a proposal for AI-gatekeepers. Instead, the debate has proceeded almost entirely on the *ex ante* accreditation side. The German TÜV illustrates the structural complexity. In some functions – car maintenance inspections under § 29 StVZO – it exercises delegated public authority.[231] Liability claims then run against the state under Art. 34 GG. In its product-safety role as notified body, by contrast, it acts as private contractor,[232] and the state-liability route is closed. Instead, the manufacturer and the notified body conclude a private contract concerning validation and – sometimes – certification. As to claims of third parties, when a faulty product was certified, strict product liability does not lie against the gatekeeper, because he is not the manufacturer of the product he certifies.[233] While this does not in principle rule out contractual third-party claims or liability in tort, a landmark decision of the European Court of Justice (CJEU) illustrates the challenges of establishing liability and the intricate interplay between European and national Member State law.[234]

In *Schmitt v. TÜV Rheinland LGA Products GmbH* the Court issued a preliminary ruling in response to questions referred by the German *Bundesgerichtshof* arising from the Poly Implant Prothèse (PIP) breast implant scandal. PIP, a French medical device manufacturer, had used low-grade industrial rather than medically approved silicone in its breast implants. TÜV had been appointed by PIP as notified

---

[231] For another example for public-law delegation, concerning oil tanks, see OLG Hamm, NVwZ-RR 2007, 315; for auditing in the U.S. car industry see *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1 (2024).

[232] BGH NVwZ-RR 2011, 566; BGH, NJW 1978, 2548 f.; LG München, BeckRS 2008, 07080; *Bieback*, Zertifizierung und Akkreditierung. 2008, p. 93, 247 f.; *Klindt*, Geräte- und Produktsicherheitsgesetz (GPSG), § 7 no. 14, 23; *Schmatz/Nöthlichs/Fähnrich/Weber*, Sicherheitstechnik, 2017, § 7 Anm. 3.2, 5. 1, § 11 Anm. 9; *Weiß*, Die rechtliche Gewährleistung der Produktsicherheit, 2008, p. 354 ff.; along those same lines: OLG Hamm, NVwZ 1990, 1105 f.; *Janiszewski*, GerätesicherheitsR, p. 116; *Klindt*, 30 Jahre Gerätesicherheitsgesetz -Schieflagen in der Praxis, NVwZ 1999, 1177, 1180; *Peine*, Gerätesicherheitsgesetz, 1997, § 9 no. 18 ff.; *Schmidt-Preuß*, Verpackungsverordnung und Kartellrecht, VVDStRL 1997, 160, 167 footnote 18; *Kollmer*, Die Unabhängigkeit von Prüf- und Zertifizierungsstellen nach dem Gerätesicherheitsgesetz, GewA 1999, 48, 51; critique at: *Scheel*, Geräte- und Produktsicherheitsgesetz, 2005, § 7 no. 10 ff.

[233] *Clausen/Schroeder-Printzen-Friedrich*, Münchener Anwaltshandbuch Medizinrecht, 2026, § 18 Nr 497; for an overview on liability against the provider and the user see *Spindler*, Neue Haftungsregelungen für autonome Systeme?, JZ 2022, 793.

[234] CJEU, judgment of 16 February 2017, Schmitt v TÜV Rheinland LGA Products GmbH, Case C-219/15, ECLI:EU:C:2017:128, NJW 2017, 1161; for liability of an outside product-safety gatekeeper see *Eckstein/Shapira*, 41 Yale Journal on Regulation 469, 487 (2024) discussing Marchand v. Barnhill, 212 A.3d 805, 807 (Del. 2019).

body to conduct conformity evaluations leading to a CE marking.[235] The plaintiff argued that TÜV had failed to adequately fulfill its obligations under the Medical Devices Directive, contending that no random, unannounced inspections were conducted. Additionally, a simple inspection of PIP's business records, for instance delivery notes and invoices, would have been sufficient to uncover the manufacturer's fraud. The plaintiff sought damages from TÜV. The CJEU held that, under the Directive, a notified body bears no general obligation to conduct unannounced inspections, examine individual devices, or review the manufacturer's business records. The Court further clarified that while the purpose of the duty of care is to protect end users of medical devices, the conditions under which a breach of its obligations may give rise to civil liability toward those end users are governed by national law, subject to the EU principles of equivalence and effectiveness.

The Court's decision, characteristically, implied construing the substantive duty under EU law while remitting the liability determination to Member State courts. EU product liability law often takes this route of setting quality standards at Union level while letting Member States decide on the liability consequences. The product-safety approach of the AI Act works along those same lines: There are no private rights of action for damages in the Act. Instead, the reformed Product Liability Directive redefines, among other things, what qualifies as a 'product' to include software and AI-integrated products. AI system providers are treated as 'manufacturers'. Claimants can sue for damages involving life, bodily harm or property, including data loss. Presumptions mitigate information asymmetry for plaintiffs.[236] By contrast, the AI Liability Directive, originally tabled in September 2022 to address fault-based non-contractual liability for AI-caused harm, has been withdrawn in October 2025,[237] which throws claimants back to Member State law.

Following the CJEU's ruling, German and French judiciaries reached diametrically opposed conclusions. In Germany, the *Bundesgerichtshof* found that TÜV had fulfilled its obligations as a notified body. It was held to be entitled to rely on documentation supplied by PIP and was under no duty to conduct unannounced factory inspections or independently verify the composition of the implants.[238] French courts, by contrast, reached the opposite conclusion applying their own tort

---

[235] Then under Council Directive 93/42/EEC on medical devices; see *Beyerbach*, GesR 2015, 522; *Brüggemeier*, JZ 2018, 191; *MüKoBGB/Wagner*, § 823 BGB no. 1062 et seq.

[236] *Wagner*, Produkthaftung für das digitale Zeitalter - ein Paukenschlag aus Brüssel, JZ 2023, 1.

[237] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive — AILD), COM(2022) 496 final of 28 September 2022, procedure 2022/0303(COD), withdrawn by the Commission on 6 October 2025 (OJ 2025 C/2025/5423); see for the legislative history European Parliament, Legislative Train Schedule, AI Liability Directive (as of 20 April 2026), available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive; *Wagner*, Die Richtlinie über KI-Haftung: Viel Rauch, wenig Feuer, JZ 2024, 123.

[238] BGH 22.6.2017 – VII ZR 36/14, NJW 2017, 2617; OLG Zweibrücken 30.1.2014 – 4 U 66/13, MPR 2014, 62; LG Frankenthal 14.3.2013 – 6 O 304/12, GuP 2013, 233; LG Nürnberg-Fürth 25.9.2013 – 11 O 3900/13, BeckRS 2014, 8646.

law framework, particularly the standard of *faute* (fault) under the *Code civil*. They found TÜV Rheinland liable in negligence for having issued CE conformity certificates without sufficient diligence, opening the door to compensation for thousands of victims.[239] The resulting legal divergence, exoneration in Germany, liability in France, for the same conduct by the same notified body under the same EU Directive, illustrates the fragmentation that flows from the CJEU's choice to leave civil liability entirely to national legal orders.[240] After these decisions, Annexes to the relevant EU Directives were passed, requiring unannounced visits by notified bodies in charge of product safety.[241] The German *Bundesgerichtshof* subsequently held that while third parties have no contractual claim against notified bodies (privity), tort claims may lie depending on the facts.[242]

The lesson from this example is that tortious liability, while generally available, very much depends on doctrinal details and legal culture.[243] State liability is a theoretical option where Member States choose public notified bodies, but this is rarely available in practice and in any event doctrinally demanding.[244] At first glance, the AI Act assumes that – as a minimum – notified bodies bear some form of liability: Art. 31 (9) AI Act requires notified bodies to take out appropriate insurance for their conformity assessment activities.[245] However, at closer inspection the Act does not make clear whether the insurance is to cover liability of notified bodies to the provider or to third parties.[246] Provider-facing coverage is more likely: The product-safety approach of the AI Act implies the lack of a private right of action for damages, which is channeled into the reformed Product Liability Directive.[247] This Directive expands the definition of 'manufacturer' and covers

---

[239] On the decision of Tribunal de commerce de Toulon 14.11.2013 – 2011F00517: *Beyerbach*, GesR 2015, 522; *Brüggemeier*, JZ 2018, 191, 196; *Rott/Glinski* ZEuP 2015, 192; on the decision of the Cour d'appel in Aix: Fröding, MPR 2015, 162; on the Cour de Cassation: Ernst, GPR 2019, 133.

[240] See OLG Frankfurt NJW 2019, 525 on a horizontal effect of Art. 18 TFEU (concerning liability of the French insurance company), denied in CJEU, judgment of 11 June 2020, RB v TÜV Rheinland LGA Products GmbH and Allianz IARD S.A., Case C-581/18, ECLI:EU:C:2020:453, NJW 2020, 2169, para. 29 et seq. with a case note by *Armbrüster*.

[241] Commission Implementing Regulation (EU) 920/2013; Medical Device Regulation 2017/745; see *Wagner*/Rehmann, MP-VO, Einf. no. 38.

[242] BGH NJW 2020, 1514 (§ 823 (2) BGB); see *Bellinghausen/Krause*, NJW 2020, 1480; *Beyerbach*, GesR 2015, 522; *Poelzig*, ZBB 2021, 73.

[243] See *Eckstein/Shapira* 41 Yale Journal on Regulation 469, 492 et seq. (2024) for the U.S.

[244] It is subsidiary to any other claim, for instance against an insurer, § 839 BGB, Art. 34 GG. Additionally, the relevant duty of care must have the specific purpose to protect third parties, which courts have often denied, for instance where more general concerns of capital markets or public traffic are at stake, see for instance BGH NJW 1973, 458, 459 (public traffic); CJEU, 12 October 2004 – C-222/02, Peter Paul, para. 25 et seq.; *Gansmeier/Splinter*, WM 2025, 1445, 1454 (Short selling).

[245] BeckOK KI-Recht/*Beck/Irskens*, KI-VO Art. 31 no. 52-55 (Last updated 4.11.2025); the same problem had surfaced in the PIP case, see *Brüggemeier*, JZ 2018, 191, 194; *Wagner*, JZ 2018, 130, 133.

[246] *Unger*, EuZW 2017, 299, 302.

[247] EU 2024/2853.

software, however, it does not cover gatekeepers, which are still not 'manufacturers'.[248] Under this reading, Art. 31(9) AI Act is a contractual risk-allocation device between notified body and provider, not a third-party protection mechanism. In sum, quality assurance under the AI Act operates through detailed *ex ante* selection and certification rules for notified bodies (Art. 28-31), rather than through *ex post* liability.[249]

b) From a Rule-Bound World to a State in Flux

Moving beyond notified bodies, we have seen above that strict gatekeeper liability is an already contested element of classical financial-market gatekeeper theory.[250] Arguably, in the AI-gatekeepers' realm, each of the standard objections apply with greater force to AI-gatekeepers.

Litigation – and insurance against it – have often been flagged as a costly strategy[251] and this is compounded by the current lack of clear, rule-bound standards in AI laws.[252] One reason for this is the „regulate-and-anticipate" strategy[253] that laws such as New York's Local Law 144 and Colorado's AI Act, both with bias audits, as well as the EU AI Act follow: These legislators have tried to foresee specific risks and embed them in a detailed legal framework. However, in an area as fast-moving as AI, the resulting norms are necessarily sometimes over-, sometimes underinclusive. Some risks that the legislator has anticipated can turn out neglectable while he is likely to overlook other risks. New York City Local Law 144's bias audit illustrates this point. Its impact ratio metric captures some forms of disparate impact but misses others. The law applies to „automated employment decision tools" which might be understood as overinclusive as to vendors, yet underinclusive as to what counts as automation. To cope with this challenge, designated AI-laws often employ vague legal terms such as „automation" and include broad delegation to standard-setting private or public bodies.[254] This is what makes litigation costly, and insurance expensive, because chances of success are hard to predict. Unwanted side-effects, for instance a tendency of risk-averse gatekeepers to lean towards overinclusive monitoring and recommend

[248] The withdrawn AI Liability Directive COM(2022) 496 would also not have covered gatekeepers.
[249] In the case of the AI Act, this is Art. 28-31.
[250] *Supra* I.2.
[251] *Supra* I.1.
[252] On this *supra* V., text before 1.
[253] On this approach see Jackson/Langenbucher, The Regulation of Technological Innovation in Financial Services: A Comparative Approach With Respect to Digital Assets and Artificial Intelligence, 88 Law and Contemporary Problems 77, 98 (2026) on anticipating risk and integrating them into a "seamless web" of law.
[254] See *supra* V., text before 1.

overcompliance,[255] add concerns of inefficiency of strict liability, inverting the classical law and economics view where strict liability furnishes optimal care.

The traditional expectation gap between what the public assumes gatekeepers verify and the narrower scope of their actual mandate is likely to widen in the AI-compliance setting. [256] Consumers and professional counterparties facing radical uncertainty will read any AI-compliance certification as a broad validation of the product, even though the gatekeeper's access to the underlying data and model is typically limited to a specific question such as bias, robustness, or documentation. Strict liability would target an actor who, by virtue of this limited access, is not the cheapest cost avoider

Another classical argument against strict liability are expectation gaps of the public. Arguably, for AI compliance gatekeepers, even more of these gaps will spawn. Faced with uncertainty about how their contractual counterpart uses AI systems, consumers and professionals of AI providers/deployers are likely to rely on AI compliance gatekeepers that can offer any signal of having validated or certified an AI product. However, just like traditional gatekeepers, AI-gatekeepers' mandates usually target select issues that require validation or certification. While they are prone to suggest that a product has been comprehensively tested, their access to data and model a company employ does not usually meet this expectation.

2. TRANSPARENCY

While strict gatekeeper liability does not provide a good fit for AI-gatekeepers, the overview on similarities and differences between traditional and AI-gatekeepers[257] suggests an alternative remedy. One core point highlighted above stressed that auditors, the paradigm gatekeepers, deliver well-defined signals based on solid and established rules. Product-safety certificates, for instance by the TÜV, are publicly available and contain explanations of what has been tested.[258] AI-gatekeepers, by contrast, must wrestle with conceptual fluidity of key terms and, even more, testing methods. For AI-compliance, audit outcomes or documentation of audit

[255] *Supra* I.1.
[256] *Supra* I.1.
[257] *Supra* V., text before 1.
[258] For databases of designated certification bodies see: for Germany, TÜV Rheinland, Certipedia – Zertifikatsdatenbank, available at: https://www.certipedia.com/?locale=de; for the EU, European Commission, New Approach Notified and Designated Organizations (NANDO), available at: https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies; for the U.S., UL Product iQ, available at: https://productiq.ulprospector.com/en, and OSHA, Current List of Nationally Recognized Testing Laboratories (NRTLs), available at: https://www.osha.gov/nationally-recognized-testing-laboratory-program/current-list-of-nrtls.

methods are rarely publicly shared.[259] Agreed-upon testing standards are in their infancy. Some laws require basic transparency. For instance, under the Colorado Bill, the deployer must disclose AI „impact assessments" to the consumer. [260] Another legislative example is provided by New York City Local Law 144 concerning bias audits for hiring decisions. „A summary of the results of the most recent bias audit" must be publicly available on the website of the employer or employment agency.[261] As to testing methodology, the law stipulates the bare minimum that sufficient historical data must be integrated to be statistically significant.[262] The AI Act provides more details, for instance on data and data governance, technical documentation, record-keeping, accuracy, robustness and cybersecurity and transparent operation.[263] However, these rules address the provider of an AI system and, at best, indirectly the gatekeeper who supports the provider. Hence, where the market largely knows how to read an auditor report, this is much less the case for the emerging field of AI-compliance validations and certificates.

Faced with opacity, transparency is the standard response. Applied to AI-compliance, this paper proposes a transparency regime combining individual audit outcomes with the testing standards and methodologies gatekeepers employ. This has the potential to fulfill three goals: Informing the public, helping AI developers to anticipate and mitigate harm, and allowing policymakers as well as competing auditors[264] to learn from each other and refine methodologies that, for now, are still in flux.[265]

The debate about what an auditor needs to conduct meaningful evaluation and what should eventually be disclosed to the public has only just begun. When debating how much of the target system the auditor should actually see, many scholars have suggested that auditors need „black-box-access", i.e. „the ability to observe

---

[259] Empirical evidence at *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1579 (2022), stressing that when asked to name "best in class", respondents identified auditors that tend to publish methodologies and results, and there is broad support for requiring audits and disclose key audit results, 1579-1580, 1583-1584.
[260] Senate Bill 24-205 p. 17, available at: https://leg.colorado.gov/bill_files/47770/download.
[261] Subchapter 25, Chapter 5, section 1 of title 20 of the administrative code of the City of New York.
[262] Section 1 Chapter 5, subchapter 25 of title 20 of the administrative code of the city of New York.
[263] Art. 10 et seq.
[264] On competition between what they call "private regulators" see *Clark/Hadfield,* 65 Jurimetrics 195, 198, 226 (2026).
[265] *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571 (2022); *Raji* et al., Outsider Oversight: Designing a Third Party Audit Ecosystem for AI Governance, AAAI/ACM Conference on AI, Ethics, and Society 557 (2022) (available at: https://arxiv.org/abs/2206.04737); *Birhane* et al., IEEE Conference on Secure and Trustworthy Machine Learning 612 (2024); *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1 (2024); AI Now Institute https://ainowinstitute.org/publications/algorithmic-accountability; *Chmielinski/Newman/Kranzinger et al.*, The CLeAR Documentation Framework for AI Transparency: Recommendations for Practitioners and Context for Policymakers, Shorenstein Center on Media, Politics and Public Policy Discussion Paper, May 2024, available at: , https://shorensteincenter.org/wp-content/uploads/2024/05/CleAR_KChmielinski_FINAL.pdf; *Selbst*, 35 Harvard Journal of Law & Technology 117 (2021).

a system's behavior on queries of the auditor's choice without examining the system's inner workings".[266] Others stress that black-box access is insufficient for rigorous auditing of frontier models, because important safety properties remain invisible.[267] White-box access would grant auditor full access to model weights, architecture, training data and procedures and the ability to run the model in a controlled environment – a structural analogy to the type of access a financial auditor gets. „Grey-box" access is a catch-all term for forms of access in between these two. Additionally, hypothesis testing has been recommended.[268] More concretely, access for auditors can come in the form of access to training data, to training procedures, to the model skeleton, or to the trained model.[269] It should include quantifiable information, but overall, interdisciplinary evaluation including technical and qualitative analyses is key.[270] Disclosure only of key metrics are one option, release of the full audit code, methodology, and outcomes another.[271]

Admittedly, it will be delicate to draw the line between providing transparency and, at the same time, respecting security and privacy concerns, as well as trade secrets and intellectual property of both, the gatekeeper's client and the gatekeeper itself.[272]

The CJEU has in its Dun&Bradstreet decision recognized the need to strike a balance between proprietary information and transparency when a plaintiff requested access to information under the GDPR's right to an explanation of the „logic involved" under Art. 15(1)(h).[273] The controller must provide information that is sufficient for the data subject to understand and contest the decision, but trade secrets and the rights of others can justify not disclosing the algorithm itself. For now, national courts arbitrate the balance. Along those lines, the proposal advanced in this paper operates on two levels. At the aggregate level, abstract and generalizable testing standards and methodology are disclosed publicly. At the individual level, a certification or a score communicates the outcome of an assessment, explaining *what* an auditor tests without disclosing *how* individual companies meet these requirements.

---

[266] *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1, 2 (2024).
[267] *Casper* et al., Black-Box Access is Insufficient for Rigorous AI Audits, FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency 2254 (2024).
[268] *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1, 13 et seq. (2024).
[269] *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1, 11 (2024).
[270] Empirical overview at *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1576, 1578 (2022).
[271] See empirical overview at *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1581 (2022).
[272] *Selbst*, 35 Harvard Journal of Law & Technology 158 (2021).
[273] CJEU, judgment of 27 February 2025, CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien, Case C-203/22, ECLI:EU:C:2025:117.

Trade-secret concerns are not only about the audited company but, increasingly, about the gatekeeper's proprietary methodology which may confer a competitive advantage. A mandate to disclose methodologies, as suggested in this paper, steps toward commoditization of the gatekeeper's service. This implies a distributional concern, namely that the gatekeeper's methodology becomes part of the public record. Additionally, it risks prematurely locking in standards of review. Arguably, this is a cost to be borne, balanced against the countervailing risk of gatekeepers offering opaque certifications in a world where wrongdoing by the audited company can be hard to detect and failure of the gatekeeper impossible to identify – the very observability condition on which classical gatekeeper theory's reputational-capital mechanism depends.

With this in mind, the triple goals listed above can still be met, even if the standard-setting process will take time and is likely to need various rounds of updates, responding to priorities and viewpoints of different communities:

The public receives information on who follows required laws, but the details of how the company ensures this remain with the gatekeeper. Some firms may wish to go beyond what is required, to gain trust of consumers or professional partners.[274] Voluntary certifications provide an established means towards that end. At the same time, tensions between corporate interests and stakeholders that represent civil society are likely to continue where the extent of access to information is concerned.[275]

For producers and users of AI systems, transparency of key audit results allows them to understand how testing methods and standards develop so they can adapt early on in their own product design process.

Along those same lines, policy-makers and auditors learn how methods develop and can react accordingly. Art. 57 AI Act anticipates some of this learning logic by requiring Member States to establish at least one regulatory sandbox. Sandboxes are meant to facilitate the involvement of various actors, including testing and experimentation facilities, research and experimentation labs, centers of excellence and individual researchers.[276] Their purpose is to foster a cooperative spirit between many actors, including but not limited to gatekeepers, to cope with the challenges of providing guidance in a world in flux.

---

[274] See *Selbst,* 35 Harvard Journal of Law & Technology 117, 169 (2021) on what he terms "beyond compliance behaviors"; *Cen/Alur,* Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1 (2024) on comparable behavior of car manufacturers in the U.S.

[275] *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1574, 1585 (2022) advocate for that broad stakeholder involvement; similar: *Selbst,* 35 Harvard Journal of Law & Technology 117 (2021); for explainability of individual decisions see *Bauer* et al., Expl(AI)n It to Me – Explainable AI and Information Systems Research, 63 Business & Information Systems Engineering 79 (2021).

[276] Art. 57 (2) f. AI Act; recital (165) AI Act.

2. Governance

Complementing transparency, a second take-away from classic gatekeeper theory concerns governance. It operates at two sites: At the gatekeeper itself, where governance requirements safeguard independence and competence, and at the interface with the client, where they enable effective monitoring across a disciplinary divide. Each requires its own institutional response. Along those lines, two features of classical auditor governance are particularly instructive for the AI-compliance context: independence from the client, [277] and the audit committee as an institutional interface between gatekeeper and management.

a) Gatekeeper Governance

Designated AI-laws have started to include some governance requirements for certain gatekeepers. In the U.S., New York City Local Law 144 is currently the only enforceable law that explicitly mandates an external audit. It defines a „bias audit" as „an impartial evaluation by an independent auditor".[278] This has been understood as the bias auditor being free from conflicts of interest. The auditor may not be involved in any part of the AI system's lifecycle, not have an active employment relationship with the employer or the AI system's developer, and have no financial interest in these parties.[279] However, no license or other form of credential is required from the bias auditor.

The Colorado AI Act requires an impact assessment for high-risk AI systems, however, the gatekeeper performing the assessment must not be external. „A deployer or a third party contracted by the deployer" can run the impact assessment.[280] The Colorado AG has rule-making authority under the Act, which may yield more detailed auditor qualification rules in implementation.[281]

---

[277] Paradigmatic: United States v. Arthur Young & Company et al. 465 U.S. 805; today see in the U.S. Rule 2-01 of Regulation S-X; in Germany §§ 319, 319a HGB; EU-Regulation 537/2014.
[278] Subchapter 25, Chapter 5, section 1 of title 20 of the administrative code of the City of New York.
[279] Lumenova AI, NYC Local Law 144 and Bias Audit Regulation, 16 May 2024, available at: https://www.lumenova.ai/blog/new-york-city-local-law-144-bias-audit-regulation/.
[280] Senate Bill 24-205, Consumer Protections for Artificial Intelligence (Colorado AI Act), 73rd Gen. Assembly, 2nd Reg. Sess. (Colo. 2024), enrolled bill p. 11, available at: https://leg.colorado.gov/bill_files/47770/download.
[281] Colorado AI Act, SB 24-205 (2024), available at: https://leg.colorado.gov/bills/sb24-205.

The AI Act stipulates broad-ranging requirements for one category of gatekeepers, the notified bodies,[282] which are publicly accredited and monitored.[283] This includes independence from the provider for whom they perform monitoring services. The Act adds independence from „any other operator having an economic interest in high-risk AI systems assessed, as well as of any competitors of the provider". Their personnel may not be involved in design, development, marketing or use of high-risk AI systems. They may not engage in consultancy services and similar activities that might conflict with their independence of judgment or integrity. Additionally, notified bodies must satisfy „organizational, quality management, resources and process requirements".[284]

All three regimes reflect a spectrum of internal governance rules for gatekeepers. Of course, not every gatekeeper is a notified body, nor does the AI Act mandate that notified bodies must be involved, Art. 43.[285] Where consultancy firms that have emerged on the AI-gatekeeper market support manufacturers in their self-validation, the requirements for notified bodies do not apply. In this way, the AI Act offers the developers of AI systems a choice between different signals, opening a market for certification quality. Engaging a notified body comes with enhanced credibility, given the public accreditation and monitoring of notified bodies, along with the extensive set of mandatory requirements. Alternatively, developers can opt for consultancy firms which might or might not follow governance requirements such as independence.

b) Interface Governance

The interface between AI-gatekeeper and client is a key place to facilitate effective monitoring by overcoming the problems of conceptual fluidity and interdisciplinary communication mentioned above.[286] For classic gatekeepers, audit committees have long played a core role. Audit committees insulate gatekeepers from direct management pressure, preserving their independence and objectivity. By providing a dedicated oversight body, ideally composed of independent directors, audit committees create a credible channel through which auditors can communicate and raise concerns without fear of retaliation from the executives whose work they scrutinize. This facilitates communication and strengthens accountability on both

[282] Art. 31 (4) AI Act.
[283] Art. 28 AI Act. *See Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1581 (2022) who report a lack of enthusiasm by respondents at the idea of accrediting AI-compliance auditors or certification of AI systems, but support for mandatory audits.
[284] Art. 31 (2), (10) AI Act.
[285] *Supra* II.2. and IV.1.
[286] *Supra* V.; *Costanza-Chock* et al., Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 1571, 1581 (2022) reporting lack of auditee buy-in as widespread.

sides: holding management to consistent reporting standards while monitoring the quality and rigor of the gatekeeper's own work.

Dedicated AI committees on corporate boards have started to develop but are not yet widespread – let alone mandated by law – although there is investor demand for it.[287] Many firms charge existing board-level committees with AI oversight responsibilities. Audit committees are one candidate,[288] as are technology or governance-focused committees.[289] Examples[290] include Meta, which has established a Privacy and Product Compliance Committee,[291] Citigroup, which entrusted AI oversight to its Technology Committee,[292] and Lockheed Martin, which designated different facets of AI-related oversight to three different committees, namely the audit, classified business and security, and governance committees.[293]

Learning from traditional gatekeeper theory, more thinking should go into creating a well-working interface between gatekeeper and audited firm. As explained above,[294] disciplinary background, conceptual fluidity, and methodological training of AI providers and data scientists differ from those of non-technical managers far more than the analogous gap between auditors and their corporate clients. At the same time, combining independence with AI literacy can be hard to find, which does not allow for a clean transplant of the classical audit committee model. Designated AI-committees, internal gatekeeper teams, or board members who function as a bridge between AI-gatekeeper and directors can act as a first step towards meaningful integrating AI oversight into routine corporate governance.

---

[287] See *Wenger*, US AI Oversight Through Three Lenses: Investor Expectations, the S&P 100 and Company-Specific Analysis, Harvard Law School Forum on Corporate Governance, 11 March 2026, available at: https://corpgov.law.harvard.edu/2026/03/11/us-ai-oversight-through-three-lenses-investor-expectations-the-sp-100-and-company-specific-analysis/#2b reporting that 65% of U.S. investors believe all companies should provide clear disclosure of board oversight on AI governance issues and 46% responding that the entire board or a committee should be tasked with AI oversight.

[288] *Niemann*, Cyber and AI Oversight Disclosures: What Companies Shared in 2025, Harvard Law School Forum on Corporate Governance, 28 October 2025, available at: https://corpgov.law.harvard.edu/2025/10/28/cyber-and-ai-oversight-disclosures-what-companies-shared-in-2025/ (reporting that in 2025 40% charge at least one board-level committee, a jump from 11% in 2024); for the European perspective *Çelikmen*, The Current State of Board AI Policies and Oversight in Europe in 2025, Glass Lewis, 11 December 2025, available at: https://www.glasslewis.com/article/the-current-state-of-board-ai-policies-and-oversight-in-europe-in-2025; on the broader oversight role *Schroeder* et al., The Expanding Role of the Audit Committee Chair, Harvard Law School Forum on Corporate Governance, 11 April 2026, available at: https://corpgov.law.harvard.edu/2026/04/11/the-expanding-role-of-the-audit-committee-chair/.

[289] *Niemann*, Harvard Law School Forum on Corporate Governance, 28 October 2025 (supra).

[290] *See Wenger*, Harvard Law School Forum on Corporate Governance, 11 March 2026 (supra).

[291] Meta Platforms, Notice of Annual Meeting and Proxy Statement 2025, available at: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/817c2e5b-b0be-40f5-8b52-4f5a0db288c5.pdf.

[292] Citigroup, 2025 Notice of Annual Meeting and Proxy Statement, available at: https://www.citigroup.com/rcs/citigpa/storage/public/citi-2025-proxy-statement.pdf.

[293] *Wenger*, Harvard Law School Forum on Corporate Governance, 11 March 2026.

[294] *Supra* V.

VI. Conclusion

AI-gatekeepers have begun to take on familiar functions: signaling quality through validation and certification, monitoring developers, and channeling information to markets, policy-makers, and standard-setting communities. In these respects they resemble the financial-market gatekeepers around whom classical gatekeeper theory was built. But the resemblance is incomplete in ways that matter for institutional design. AI-gatekeepers operate in a legal framework that is preliminary and fluid, not rule-bound. The technical concepts on which their work depends are contested even within the expert community. New entrants have no reputational capital to pledge and face the rational temptation to compete through lenient certification.[295]

These structural features argue against transplanting versions of strict gatekeeper liability into the AI-compliance setting. Instead, this paper has proposed a two-part response.

First, transparency should operate at the level of methodologies, standards, and individual audit outcomes in the form of a score or a certification. The public and the market need to understand what is being tested and how. This approach mitigates the observability problem on which the classical reputational-capital mechanism depends, without forcing disclosure of client-specific details.

Second, governance requirements should operate as an *ex ante* mechanism to ensure quality at the gatekeeper. This concerns both, the gatekeeper, through accreditation and independence requirements on the model of the EU's notified bodies, and the interface with the client, through institutional structures analogous to the audit committee but designed for the interdisciplinary translation problem that makes AI-compliance review distinctive.

Much remains open. Whether notified-body involvement should be required for a wider class of AI systems under the AI Act, how US state-level regimes will evolve alongside the emerging EU architecture, and how corporate governance will adapt to the translation problem invite fresh thinking. What the classical gatekeeper literature teaches is not a template, but an analytic apparatus: the reputational-capital mechanism, the disruption-of-misconduct function, and the *ex ante* alternative of public accreditation. Applied to the three groups of AI-gatekeepers identified here, and adapted to the distinctive features of the AI-compliance setting, that apparatus can guide the institutional choices the coming years will require.

[295] See *Clark/Hadfield,* 65 Jurimetrics 195, 236 (2026) on regulatory capture.

european corporate governance institute

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

www.ecgi.global

european corporate governance institute

ECGI Working Paper Series in Law

Editorial Board

Editor	Amir Licht, Professor of Law, Harry Radzyner Law School, Reichman University
Consulting Editors	Hse-Yu Iris Chiu, Professor of Corporate Law and Financial Regulation, University College London
	Martin Gelter, Professor of Law, Fordham University School of Law
	Geneviève Helleringer, Professor of Law, ESSEC Business School and Oxford Law Faculty
	Kathryn Judge, Professor of Law, Coumbia Law School
	Wolf-Georg Ringe, Professor of Law & Finance, University of Hamburg
Editorial Assistant	Asif Malik, ECGI Working Paper Series Manager

https://ecgi.global/content/working-papers

european corporate governance institute

Electronic Access to the Working Paper Series

The full set of ECGI working papers can be accessed through the Institute's Web-site (https://ecgi.global/content/working-papers) or SSRN:

Finance Paper Series	http://www.ssrn.com/link/ECGI-Fin.html
Law Paper Series	http://www.ssrn.com/link/ECGI-Law.html

https://ecgi.global/content/working-papers