RUTGERS LAW RECORD

Volume 53

Issue II: Spring 2026

BEYOND SELF-REPORTING: VERIFYING PLATFORM TRANSPARENCY UNDER THE EU DIGITAL SERVICES ACT

Alessia Zornetta[1*]

Table of Contents

INTRODUCTION **240**

I. THE RELIABILITY PROBLEM AND THE DSA'S VERIFICATION FRAMEWORK **244**

A. RELIABILITY CHALLENGES IN TRANSPARENCY REPORTING 244
B. THE DSA'S ASYMMETRIC TRANSPARENCY OBLIGATIONS 247
C. THE DSA DATABASE AS VERIFICATION TOOL 249

II. DSA ARTICLE 37 AND THE DELEGATED REGULATION **251**

A. LEGAL BASIS 251
B. SCOPE OF AUDITABLE TRANSPARENCY OBLIGATIONS UNDER THE DSA 255
C. AUDITOR INDEPENDENCE 257

III. AUDITS AS VERIFICATION MECHANISMS **258**

A. METHODOLOGY AND OVERVIEW 259
1. Who are the auditors? *259*
2. Audit Approaches and Assurance Standards *261*
B. GENERAL AUDIT FINDINGS 263
C. FINDINGS ON TRANSPARENCY COMPLIANCE 265
1. Transparency Reporting Findings (Article 15, 24.1) *268*
2. Statements of Reasons and the DSA Transparency Database (Article 24.5) *271*
3. Human Resources Involved in Content Moderation (Article 42.2) *273*

IV. ENHANCING THE VERIFICATION FRAMEWORK **275**

[1*] Alessia Zornetta, Independent Researcher, UCLA Institute for Technology, Law, and Policy; S.J.D. UCLA School of Law. I thank John Villasenor, Sarah T. Roberts, Yuan Tian, and Michael Karanicolas for their advice and support.

[**] This Article was accepted for publication in August 2025. The views expressed are solely those of the author.

A. Improving Auditing Requirements.....275
B. Bridging Transparency Mechanisms.....277
C. Beyond VLOPs.....279

Conclusion.....281

Introduction

The European Union's Digital Services Act (DSA) represents an ambitious attempt to improve the oversight of digital platforms through a multi-layered transparency framework. At its core, the regulation aims to increase platform accountability through strict transparency obligations and independent verification mechanisms. This article examines a key element of this framework: the role of independent auditors in verifying platform transparency and how it functions alongside other DSA transparency tools to address the reliability problem. While the DSA introduces various tools to improve platform oversight, the auditing requirements under Article 37 represent one of its most significant innovations in addressing the longstanding challenge of unverifiable platform disclosures.

For transparency to be truly meaningful in platform governance, it must be both reliable and independently verifiable.[2] Platform transparency reports have long faced criticism for serving more as public relations tools than genuine accountability mechanisms, with their accuracy

[2] Alessia Zornetta, *Clearing the Haze: Is the EU Digital Services Act Finally Forcing Platforms to Open Up About Content Moderation?*, 6 Notre Dame J. On Emerging Tech. 1 (2025); *see also* Amitai Etzioni, *Is Transparency the Best Disinfectant?*, The Geo. Wash. Univ. (2016), https://papers.ssrn.com/abstract=2731880; Mikkel Flyverbom, *Sunlight in cyberspace? On transparency as a form of ordering*, 18 Eur. J. of Soc. Theory 168 (2015); Nicolas P. Suzor, et al., *What Do We Mean When We Talk About Transparency? Toward Meaningful Transparency in Commercial Content Moderation*, 13 Int'l. J. of Comm'n. 18 (2019).

and completeness frequently called into question.[3] This reliability problem has led to sustained calls for the development of verification mechanisms for platform data.[4]

This article provides, to the best of the author's knowledge, the first academic analysis of the recently published DSA audit reports, contributing insights on how the auditing mechanism is functioning in practice. Through an examination of the audit reports from nineteen Very Large Online Platforms and Search Engines, the article reveals significant challenges in the verification of transparency practices, identifying patterns across different platforms that have not previously been documented in academic literature. While some initial blog posts and analyses have highlighted selected aspects of these reports, this article offers a systematic examination of how auditors approached transparency verification, what compliance issues they identified, and what these findings tell us about the reliability of platform transparency more broadly.

The underlying assumption driving demands for verification is that transparency reports could become effective tools for public policy decisions about platforms' abilities to limit online harm, but only if there exists a reliable way to verify the platforms' representations of their

[3] Ben Wagner, et al., *Auditing Big Tech: Combating Disinformation with Reliable Transparency*, ENABLING DIGIT. RTS. & GOVERNANCE, at 20 (Feb. 2021), https://enabling-digital.eu/wp-content/uploads/2021/02/Auditing_big_tech_Final.pdf; Ben Wagner & Lubos Kuklis, *Establishing Auditing Intermediaries to Verify Platform Data, Regulating Big Tech* (Nov. 2021), https://doi.org/10.1093/oso/9780197616093.003.0010 (explaining that "Private companies' voluntary provision of data in transparency reports is problematic not just because that data is unverified but also because their own presentation of categories and standards for transparency data allow them to shape the dimensions of the debate extensively."); *see also* Mikkel Flyverbom, *Transparency: Mediation and the Management of Visibilities*, 10 INT'L. J. OF COMMC'N 110 (2016); Oana Brindusa Albu & Mikkel Flyverbom, *Organizational Transparency: Conceptualizations, Conditions, and Consequences*, 58 BUS. & SOC. 268 (2019).

[4] Wagner, et al., *supra* note 2, at 13 (on the need for such body to be independent and not housed within regulatory bodies).

content moderation efforts accurately reflect reality.[5] The role of auditors in the financial sector is often pointed at as an example of what should happen with online platforms.[6] Just as financial auditors examine banks' procedures for monitoring suspicious activities rather than reviewing each transaction, platform auditors could verify content moderation transparency by evaluating the processes that generate reported outcomes. However, unlike financial auditing, which operates within well-established standards and methodologies developed over decades, platform auditing has emerged in a regulatory vacuum where platforms use different reporting formats and metrics, making meaningful cross-platform comparison and verification quite challenging.[7]

The Digital Services Act attempts to respond to these demands for independent verification through Article 37, which establishes a framework for platform auditing.[8] Under this provision, Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) must undergo annual independent audits to assess compliance with two distinct sets of obligations. First, auditors must verify platforms'

[5] Wagner, et al., *supra* note 2 ("Using 'auditing intermediaries' limits challenges associated with privacy and data protection, as it can ensure that a more limited subset of verified data is provided to both regulators and the general public." And "[e]nsuring that regulators remain within the scope of their mandate is particularly important given the diversity of regulators interested in regulating online platforms and the considerable power that can be drawn from access to their data"); *see also* Wagner & Kuklis, *supra* note 2, at 169–71; Flyverbom, *supra* note 2.

[6] *See generally* Wagner & Kuklis, *supra* note 2; Joint Statement, *A diverse auditing ecosystem is needed to uncover algorithmic risks*, ALGORITHM WATCH (June 5, 2023), https://algorithmwatch.org/en/diverse-auditing-ecosystem-for-algorithmic-risks/; Rogier Deumes, et al., *Audit Firm Governance: Do Transparency Reports Reveal Audit Quality?*, AUDTING, A J. OF PRAC. & THEORY (2012), https://papers.ssrn.com/abstract=1847924; Jenny de Fine Licht, *The role of transparency in auditing*, 35 FIN. ACCOUNT. & MGMT. 233 (2019).

[7] Wagner, et al., *supra* note 2, at 15.

[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, 2022 O.J. (L 277/1), art. 37(1) [hereinafter DSA] (Platforms are required to commission and fund the auditing process); *see* Claire Pershan, *Cutting Through the Jargon - Independent Audits in the Digital Services Act*, MOZILLA FOUND. (Jan. 30, 2023), https://foundation.mozilla.org/en/blog/cutting-through-the-jargon-independent-audits-in-the-digital-services-act/ (distinguishing between "adversarial" and "cooperative" audits and explaining that the DSA requirements are "specifically for a cooperative audit, commissioned and paid for by the company").

compliance with all obligations set out in Chapter III of the DSA, which encompasses the complete range of transparency and accountability requirements including risk assessments, risk mitigation measures, transparency reporting, content moderation resources, recommender systems, and advertising transparency.[9] Second, auditors must assess platforms' adherence to any voluntary commitments they have undertaken through the DSA's codes of conduct and crisis protocols. This means auditors must evaluate not only mandatory regulatory requirements but also platforms' self-imposed obligations, creating a verification framework that extends beyond basic statutory compliance.[10]

To enable meaningful oversight, the provision establishes substantial independence requirements for auditors, including prohibitions on conflicts of interest, requirements for technical expertise, and restrictions on long-term auditing relationships with the same platform,[11] while requiring platforms to provide auditors with necessary access to data and premises while maintaining appropriate confidentiality safeguards.[12] The resulting audit reports must detail methodologies, findings, and, where necessary, specific recommendations for addressing compliance gaps.[13] Through these requirements, Article 37 represents the first major regulatory attempt to systematically verify platform transparency through independent third-party assessment.

This article examines how the DSA's auditing framework attempts to address the reliability problem in platform transparency. Through analysis of both the legal requirements and early implementation challenges, it demonstrates that while Article 37 creates important verification mechanisms, significant obstacles remain in ensuring meaningful oversight of platform practices.

Beyond assessing the role of auditors, the article shows

[9] DSA, art. 37(1)(a).
[10] *Id.*, art. 37(1)(b) (referencing commitments under Articles 45, 46, and 48).
[11] *Id.*, art. 37(3).
[12] *Id.*, art. 37(2).
[13] *Id.*, art. 37(4).

how the findings from the first rounds of DSA audits substantiate the existence of the reliability problem even when platform transparency is mandated by law.[14] The audit results reveal significant discrepancies in how platforms implement transparency requirements, providing empirical evidence of the challenges in verifying the accuracy and completeness of platforms' disclosures. These findings reinforce the argument that mandatory transparency alone, without effective verification mechanisms, cannot fully address the reliability issues that have historically undermined platform accountability.

The article proceeds in four parts. Section I examines the historical context of platform transparency and the reliability challenges that prompted calls for independent verification. Section II analyzes the legal framework established by Article 37 and its implementing regulations, focusing on how the provisions attempt to enable meaningful oversight. Section III explores the challenges and concerns that have emerged in early implementation, particularly around the assessment of compliance with transparency obligations. Section IV provides recommendations on how to improve the DSA transparency framework to address the reliability problem.

I. THE RELIABILITY PROBLEM AND THE DSA'S VERIFICATION FRAMEWORK

Platform transparency suffers from a fundamental reliability problem that hinders its effectiveness as an accountability mechanism. Despite significant evolution in transparency reporting practices over the past decade, the inability to verify platforms' disclosures creates an inherent asymmetry where companies retain complete control over what information becomes public. The Digital Services Act attempts to address this challenge through a multi-layered framework combining mandatory transparency reports, a centralized Database of Statements of Reasons, and

[14] Alessia Zornetta, *The DSA Database as a Tool for Transparency Accountability*, UNIV. ILL. J. OF L. TECH. & POL'Y (2025).

independent audits. Together, these mechanisms create a complex system with varying obligations based on platform size and classification. This section examines how the historical limitations of voluntary transparency initiatives have shaped the DSA's approach, explores the asymmetric obligations imposed on different types of platforms, and analyzes how the EU Database of Statements of Reasons could theoretically function as a verification tool despite current structural limitations that limit its potential.

A. Reliability Challenges in Transparency Reporting

Platform transparency has evolved substantially over the past decade, yet it continues to suffer from a reliability problem.[15] The historical evolution of transparency reporting presents persistent challenges that weaken its effectiveness as tools for meaningful accountability. Understanding these issues requires looking at the development of transparency practices and their limitations.

Platform transparency reports emerged in the early 2010s as voluntary initiatives primarily focused on providing information on government surveillance and data requests to users across the world. This initial wave of disclosures was largely reactive, triggered by revelations about governmental surveillance programs that threatened public trust.[16] Online platforms used these reports to strategically distance themselves from government actions and rebuild user trust. Google pioneered this approach in 2010 with other platforms following suit, establishing what would become an industry-standard practice for selective disclosure[17]

The scope of transparency disclosures expanded

---

[15] Zornetta, *supra* note 1.

[16] Robert Gorwa & Timothy Garton Ash, *Democratic Transparency in the Platform Society, in* Soc. Media and Democr., The State of the Field and Prospects for Reform 286 (Nathaniel Persily & Joshua A. Tucker eds., 2020) (tracking the evolution of transparency reporting).

[17] David Drummond, *Greater Transparency around Government Requests*, Google Blog (Apr. 20, 2010), https://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html (announcing Google's first transparency report).

significantly following the Cambridge Analytica scandal in 2016, which shifted public attention towards platforms' own content moderation practices.[18] By 2018-2019, major platforms began publishing their community standards and detailed enforcement reports, marking a new phase in voluntary transparency reporting.[19] Nevertheless, this apparent progress hid continuing limitations in the reliability and comprehensiveness of the information provided.

Indeed, voluntary transparency efforts consistently fell short due to the inability to verify their information. Despite a decade of evolution, the reports remain impossible to authenticate, creating a reliability problem. The issue manifests across multiple dimensions of transparency reports, from the absence of standardized metrics preventing meaningful cross-platform analysis to inconsistent categorization schemes and selective disclosure of favorable statistics without proper context, ultimately concealing potential failures.[20] These inconsistencies give platforms considerable discretion in

---

[18] The Cambridge Analytica scandal exposed how Facebook had allowed a political consulting firm to collect data from millions of users without informed consent and exploiting it for political advertising during the 2016 US presidential election and the Brexit referendum. *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, THE NEW YORK TIMES, (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html; Ben Gilbert & Alexandra Ma, *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now.*, BUSINESS INSIDER (Aug. 23, 2019), https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3; Julia Carrie Wong, *Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports*, THE GUARDIAN (July 12, 2019), https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations; *see also* Robert Gorwa, et al., *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, 7 BIG DATA & SOC. (2020) (analyzing how the Cambridge Analytica scandal shifted the focus of transparency to platforms' own content moderation practices).

[19] Amanda Reid, et al., *Transparency reports as CSR reports: motives, stakeholders, and strategies*, 20 SOC. RESP. J. 81 (2023); Gorwa & Ash, *supra* note 15.

[20] Daphne Keller & Paddy Leerssen, *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation, in* SOC. MEDIA AND DEMOCR., THE STATE OF THE FIELD AND PROSPECTS FOR REFORM 286 (Nathaniel Persily & Joshua A. Tucker eds., 2020).

how they present their content moderation practices, allowing them to highlight successes while ignoring problematic patterns.[21]

The verification challenge extends beyond mere inconsistency. Without access to underlying data, observers cannot validate whether platforms' disclosures accurately represent their practices.[22] This creates a scenario where platforms maintain complete control over what information becomes public, effectively functioning as both the subject of oversight and the gatekeeper of evidence needed for that oversight. Even when platforms disclose large volumes of statistics, the inability to verify these numbers against original data sources renders the transparency efforts largely performative rather than meaningful.[23] This verification gap persists regardless of the comprehensiveness of disclosures, as even detailed statistics remain unverifiable claims rather than authenticated facts.

Attempts to establish voluntary verification mechanisms have proven insufficient. Independent initiatives like the Santa Clara Principles established baseline standards for transparency but lacked enforcement mechanisms to ensure compliance.[24] Even more structured oversight approaches, such as Meta's Oversight Board, examine only a minuscule fraction of content moderation decisions, leaving the vast majority of platform operations beyond independent scrutiny.[25] These initiatives are certainly a step forward in addressing individual high profile cases but cannot overcome the broader verification problem inherent in platform-controlled disclosure.[26] Without

---

[21] Aleksandra Urman & Mykola Makhortykh, *How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms*, 47 Telecomm. Pol'y. 102477 (2023) (discussing how terminological inconsistencies prevent meaningful cross-platform comparisons).

[22] Wagner, et al., *supra* note 2.

[23] Zornetta, *DSA Database*, *supra* note 13; *see also* Reid, et al., *supra* note 18; Urman & Makhortykh, *supra* note 20.

[24] Chapeu, *The Santa Clara Principles on Transparency and Accountability in Content Moderation* (last visited Feb. 19, 2024), https://santaclaraprinciples.org/.

[25] *See, e.g.,* David Wong & Luciano Floridi, *Meta's Oversight Board: A Review and Critical Assessment*, 33 Minds & Machines 261 (2023).

[26] Suzor, et al., *supra* note 1 (explaining how transparency without verification fails to

external independent verification means, voluntary transparency frameworks cannot authenticate the information upon which their oversight function depends.

The persistent verification problem demonstrates that meaningful transparency requires not just disclosure requirements but also verification mechanisms that can authenticate platforms' claims independently.[27] This fundamental gap between disclosure and verification created the need for regulatory frameworks like the Digital Services Act, which attempts to address this problem through complementary tools that could potentially work together to enable verification of platforms' transparency claims. The DSA's approach specifically addresses these shortcomings through a complex structure of tiered obligations.

B. The DSA's Asymmetric Transparency Obligations

The Digital Services Act establishes a multi-layered transparency framework that aims to address limitations in platform accountability. Building on previous transparency initiatives, the DSA introduces four interconnected components: mandatory transparency reports, a Database of Statements of Reasons, independent audits, and researcher access.[28] Together, these mechanisms create a system of disclosures that varies significantly by platform size and classification.

Asymmetry forms the core principle of the DSA's transparency architecture.[29] The regulation imposes increasingly stringent requirements based on platform classification, creating substantial disparities between Very Large Online Platforms (VLOPs) and smaller online platforms. All intermediary services must publish annual transparency reports covering government orders, notice-and-action submissions, own-initiative content

---

achieve meaningful accountability).

[27] Wagner, et al., *supra* note 2; Suzor, et al., *supra* note 1; Gorwa & Ash, *supra* note 15; Flyverbom, *supra* note 2.

[28] DSA,,arts. 15, 17, 24, 40, 42.

[29] *Id.*, Recitals (13), (40)-(41) (explaining the logic behind asymmetric regulation).

moderation, user complaints, and automated systems.[30] Online platforms must additionally report on dispute resolution and provide user counts by Member State.[31] VLOPs and VLOSEs face the most extensive obligations, including biannual reporting and detailed disclosures about content moderation personnel, training protocols, and accuracy metrics.[32] Even though this asymmetrical approach is informed by platforms' varied societal impact, it still creates an uneven transparency landscape with substantially different accountability expectations.

The Database of Statements of Reasons (DSA Database) is one of the most innovative components of this transparency framework. Unlike other DSA mechanisms that scale with platform size, this centralized repository applies broadly to all online platforms regardless of their user base.[33] The Database collects individual content moderation decisions in a standardized format that documents violation types, enforcement actions, and detection methodologies. As discussed below, this repository, now exceeding nine billion entries, theoretically provides the granular evidence necessary to substantiate platforms' broader statistical claims.[34] The Database's structured attributes could enable systematic comparison between individual decisions and the aggregated metrics found in transparency reports, potentially addressing the long-standing verification gap in platform transparency.[35]

On the other hand, independent audits constitute the most asymmetrically applied element of the DSA's transparency framework. While all platforms must submit transparency reports and Database entries, only VLOPs and

---

[30] *Id.*, art. 15.

[31] *Id.*, art. 24.

[32] *Id.*, art. 42.

[33] *Id.*, arts. 17, 24(5) (requiring submission of statements of reasons to the Database from all online platforms).

[34] Zornetta, *supra* note 1; *Overview Documentation*, *Explanation of the information held in the DSA Transparency Database*, DSA Transparency Database (last visited Oct. 23, 2024), https://transparency.dsa.ec.europa.eu/page/documentation; *API and Schema*, DSA Transparency Database (last visited Feb. 5, 2025), https://transparency.dsa.ec.europa.eu/page/api-documentation#creating-a-statement.

[35] Zornetta, *supra* note 1.

VLOSEs undergo annual audits that evaluate compliance with their broader regulatory obligations.[36] These assessments specifically include verification of transparency disclosures, where auditors are required to evaluate the accuracy of reported metrics and the underlying systems that produce them.[37] The complete absence of equivalent verification mechanisms for smaller platforms creates a bifurcated system where only the largest services face external scrutiny of their transparency claims. This significant discrepancy extends the reliability issues that have undermined platform transparency efforts, particularly for services that fall below the VLOP/VLOSE threshold.

While the DSA's asymmetric framework creates a set of transparency obligations, uncertainties remain about how these parallel mechanisms should interact with one another to address the reliability problem. The potential strength of the DSA's approach lies, indeed, in the complementary nature of its transparency mechanisms. However, their effectiveness depends on cross-integration that facilitates verification between parallel disclosure requirements. Currently, the DSA mandates each transparency tool separately without establishing clear connections between them, creating a fragmented framework with limited verification potential. This structural separation between transparency mechanisms represents a significant missed opportunity in the DSA's approach. The following subsection explores how the Database could specifically function as a verification tool within this framework, examining it from both a theoretical perspective and the practical limitations that currently prevent it from fulfilling this role.

C. The DSA Database as a Verification Tool

The Digital Services Act's Database of Statements of

[36] DSA, art. 37; Commission Delegated Regulation (EU) 2024/436 of 20 Oct. 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines, 2023 O.J. (L 2024/436) [hereinafter DRA].

[37] *See* Section III.

Reasons represents the first regulatory tool that requires platforms to share granular data about content moderation practices. Since February 2024, this centralized repository has collected over nine billion copies of individual content moderation decisions from platforms operating in the EU.[38] While primarily designed as a documentation tool for individual content moderation actions, the Database architecture contains the theoretical foundations for a more ambitious function: verifying the accuracy of platforms' broader transparency claims.[39]

Three design features give the Database verification potential. First, its standardized submission format requires platforms to use consistent categories when documenting content moderation decisions, addressing a longstanding issue of varying metrics and terminology in voluntary transparency reporting.[40] Second, the Database offers unprecedented visibility into individual moderation actions, theoretically enabling observers to reconstruct aggregate claims from granular data.[41] Third, the mandatory fields could counteract selective disclosure by ensuring documentation of all content moderation aspects, including problematic areas platforms might otherwise minimize in transparency reports.

This verification ability extends beyond numerical validation to create meaningful connections between individual decisions and aggregate statistics. By bridging granular data and high-level reporting, the Database could provide a solution to unreliability concerns around platforms' self-disclosures.[42] For example, researchers could determine whether a platform's claimed enforcement rates for a specific category of infringement align with the volume and nature of individual decisions for such category documented in the Database, exposing any

---

[38] *Welcome to the DSA Transparency Database*, DSA Transparency Database (last visited Mar. 23, 2025), https://transparency.dsa.ec.europa.eu/?lang=en.

[39] Zornetta, *supra* note 1.

[40] *Id.*

[41] *Id.*

[42] *Id.*

discrepancies between public claims and actual practices.[43]

Such cross-verification would address three persistent transparency challenges. First, it could limit platforms' ability to curate disclosures by requiring consistency across parallel reporting mechanisms. Second, it could systematically identify mismatches between platforms' public statements and actual practices without depending on extraordinary events like whistleblower revelations. Most importantly, it could establish an ongoing verification system that continuously validates the accuracy of platforms' transparency reporting.[44]

However, significant structural limitations currently prevent the Database from effectively becoming an accountability tool. The template for statements of reasons fails to capture moderation complexity, often reducing nuanced enforcement to standardized options. Moreover, the Database's rigid architecture cannot accommodate decision updates or track appeal outcomes, creating an incomplete picture of content moderation processes.[45] Perhaps most critically, the mismatch between platforms' internal categorization systems and the Database's standardized framework makes establishing reliable verification controls exceptionally difficult. Empirical analysis comparing Database entries with transparency reports shows systematic discrepancies across all major platforms, with platforms often reporting content categories in one mechanism while completely omitting them from the other.[46]

For non-VLOP platforms specifically, the challenges may be amplified by the asymmetric transparency obligations. While these platforms must submit statements of reasons to the Database, their transparency reporting requirements

---

[43] *See, e.g.,* Amaury Trujillo, et al., *The DSA Transparency Database: Auditing Self-reported Moderation Actions by Social Media*, CORNELL UNIV. (Feb. 7, 2025), https://arxiv.org/abs/2312.10269.

[44] Zornetta, *supra* note 1.

[45] *API and Schema*, *supra* note 33; *DSA Transparency Database, supra* note 33; Zornetta, *supra* note 1.

[46] Zornetta, *supra* note 1; Trujillo, et al., *supra* note 42.

are less extensive than those for VLOPs.[47] This asymmetry creates a verification gap where Database entries exist without corresponding detailed transparency reports against which to verify them. Additionally, medium-sized platforms often lack the technical infrastructure and dedicated compliance teams that larger platforms can rely on, potentially affecting the quality and consistency of their Database submissions.

These limitations represent a limitation in the DSA's transparency framework. While mandating both detailed transparency reports and documentation of individual decisions, the regulation provides no mechanism to ensure consistency between these parallel requirements. Without structural improvements enabling cross-verification, the Database remains just another layer of procedural transparency that fails to deliver on its accountability potential. For VLOPs and VLOSEs, however, the DSA introduces an additional verification mechanism: independent audits. These audits could fill the gap left by the disconnect between the Database and transparency reports by providing external validation of platforms' transparency claims.

II. DSA Article 37 and the Delegated Regulation

The DSA establishes a framework for independent auditing of VLOPs and VLOSEs, creating an additional accountability mechanism. Article 37 forms the legal foundation for this auditing requirement, while the subsequent Delegated Regulation on Auditing (DRA) provides operational details on implementation.[48] This section examines the legal basis and scope of this auditing framework, analyzing how it structures verification of platforms' compliance. Although audits represent a significant advancement in enhancing the reliability of platform disclosures, the current framework contains significant weaknesses. Understanding these constraints is crucial for evaluating whether DSA audits can effectively

[47] DSA, art. 24.
[48] DRA.

verify platform transparency and where complementary mechanisms might be needed.

A. Legal Basis

The Digital Services Act establishes a two-tiered legal framework for platform audits. At its foundation, Article 37 creates the basic requirement for VLOPs and VLOSEs to undergo annual independent audits.[49] However, this primary legislation provides only minimal guidance on audit implementation, establishing core obligations while leaving the implementation and operational details unspecified. Article 44 fills this gap by granting the European Commission authority to issue Delegated Regulations that clarify specific aspects of the DSA's requirements.[50]

In October 2023, the Commission exercised these powers to adopt a Delegated Regulation on Auditing, following extensive public consultation with stakeholders including civil society organizations, academics, auditing companies, and platforms themselves.[51] The DRA aimed to "set out the necessary rules for the procedures, methodology and templates used for the audits."[52] It embodies the deliberate regulatory flexibility that the EU regulators embedded in the DSA's design. The approach to place operational and implementation details in delegated acts rather than in the primary legislation allowed EU regulators to create an adaptable framework that can respond to technological developments without requiring the traditionally cumbersome amendment process of the main regulation. This regulatory design enables the Commission to revise technical specifications through a simplified procedure, bypassing the political complexity and time constraints that typically characterize legislative modifications.

---

[49] DSA, art. 37.

[50] DSA, art. 44.

[51] *Digital Services Act – Conducting Independent Audits*, EUROPEAN COMM'N (2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en.

[52] *Id.*; DRA.

To structure the audit process, the DRA requires platforms and auditors to establish written agreements detailing the scope of audited obligations, access procedures, and timelines.[53] Yet even these procedural requirements maintain flexibility. While mandating documentation of the audit approach, they do not prescribe specific methods for verifying transparency claims. The DRA establishes a three-tier classification system for evaluating platform compliance. For each audited obligation, including transparency requirements, auditors must reach one of three possible conclusions: "positive," "positive with comments," or "negative."[54] These individual conclusions then determine the overall audit opinion. A single negative conclusion for any obligation triggers a negative overall opinion, while any "positive with comments" conclusion results in a qualified opinion unless another obligation received a negative assessment.[55] This approach means that even minor issues with transparency reporting could affect the platform's overall audit outcome. When auditors cannot reach a conclusion with reasonable assurance about any aspect of transparency compliance, they must explain in detail why such assurance could not be achieved.[56]

The regulation requires detailed documentation of findings through standardized templates. Audit reports must include specific sections addressing each audited obligation, with particular attention to areas where auditors identify concerns.[57] When issuing recommendations, auditors must explain how their suggested improvements would affect the materiality threshold of their conclusions.[58] However, without defined standards for materiality in

---

[53] DRA, art. 7(1). These agreements must be annexed to the final audit report. *See* DRA, art. 7(2).

[54] DRA, art. 8(1). A positive conclusion indicates compliance has been verified with reasonable assurance. A positive with comments indicates compliance but includes either remarks about the platform's benchmarks or recommendations for non-substantive improvements. A negative conclusion signifies non-compliance.

[55] *Id.*, art. 8(6).

[56] *Id.*, art. 8(8).

[57] *Id.*, art. 6(1).

[58] *Id.*, art. 8(3).

transparency reporting, auditors must rely on professional judgment to determine when discrepancies or omissions warrant criticism.[59]

The DRA creates specific requirements for platforms that receive non-positive audit opinions. When auditors identify issues with transparency compliance, platforms must prepare an audit implementation report within one month detailing their response to the auditors' recommendations.[60] This report must follow a standardized template provided in Annex II of the regulation, ensuring consistent documentation of remedial measures across platforms.[61] According to the DSA, platforms retain some flexibility in how they address audit findings. If a platform disagrees with specific recommendations regarding its transparency practices, it can propose alternative measures to achieve compliance.[62] However, the platform must explicitly justify its decision to deviate from the auditors' recommendations and demonstrate how its alternative approach will address the identified compliance gaps.[63]

Although the DRA establishes common frameworks for conducting audits, it also intentionally avoids prescribing rigid methodologies, instead allowing auditors to develop appropriate approaches based on platform-specific characteristics.[64] The regulation introduces specific requirements for how auditors must evaluate platforms' compliance. Audits must be performed in a manner that enables auditors to assess compliance with all obligations at

---

[59] Ben Wagner, Comment on *Digital Services Act—conducting independent audits*, EU COMM'N (2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits/F3423998_en.

[60] DRA, art. 8(2).

[61] *Id.*, art. 6(2).

[62] DSA, art. 37(6).

[63] *Id.*

[64] Anna Morandini, *DSA Audits: Procedural Rules Leave Some Uncertainties*, DSA OBSERVATORY (Nov. 28, 2023), https://dsa-observatory.eu/2023/11/28/dsa-audits-procedural-rules-leave-some-uncertainties/ (explaining that the Commission's vision "is to create a range of suitable approaches by providing 'sufficient flexibility for the development of good practices'").

a "reasonable level of assurance" - defined as a high but not absolute level of certainty based on sufficient evidence.[65] To achieve this standard, platforms must provide auditors with comprehensive access to internal controls, risk analyses, decision-making structures, relevant algorithmic systems, and all other necessary resources including "data, documentation, information on procedures and processes, and to the information technology systems, testing environments, personnel and premises of that provider, and any relevant sub-contractors."[66]

The final text of the DRA, nevertheless, fails to address some of the concerns raised during the stakeholder consultation. Most critically, the regulation deliberately avoids establishing standardized definitions, methodologies, or benchmarks for evaluating compliance. This omission represents a significant departure from conventional auditing practices in other regulated fields, where auditors typically apply established criteria rather than developing their own.[67] During the consultation process, major auditing firms themselves explicitly expressed concerns about this approach, arguing that leaving criteria definition to auditors would diminish comparability across platforms and potentially undermine the independence of the auditing process.[68]

Indeed, section IV of the DRA is quite general and only

---

[65] DRA, arts. 3(1) & 2(13) (explaining that "'reasonable level of assurance' means a high but not absolute level of assurance, which allows the auditing organisation to assert in its audit opinion and audit conclusions whether the audited provider complies with the audited obligations or commitments, based on sufficient and appropriate evidence").

[66] *Id.*, art. 5.

[67] Morandini, *supra* note 63.

[68] Pablo Zalba, Comment on *Digital Services Act—conducting independent audits*, EU COMM'N (2023), https://ec.europa.eu/info/law/better-regulation/have; Andrew Hobbs, Comment on *Digital Services Act—conducting independent audits*, EU COMM'N (2023), https://ec.europa.eu/info/law/better-regulation; Jacomien van den Hurk, Comment on *Digital Services Act—conducting independent audits*, EU COMM'N (2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits/F3424073_en; Aliya Bhatia & Asha Allen, *Auditing in the Dark: Guidance Is Needed to Ensure Maximum Impact of DSA Algorithmic Audits*, CTR. FOR DEMOCRACY AND TECH. (Nov. 20, 2023), https://cdt.org/insights/auditing-in-the-dark-guidance-is-needed-to-ensure-maximum-impact-of-dsa-algorithmic-audits/.

clarifies that auditors are expected to use "appropriate auditing methodologies to reduce the assessed audit risks,"[69] without specifying exactly what methodology should be followed. Auditors hold significant discretion in designing and applying the chosen methodology.[70] This methodological ambiguity creates particular challenges for verifying transparency obligations. Without shared definitions or standardized assessment frameworks, each auditing firm must develop its own approach to evaluating whether platforms have met their transparency requirements under Articles 15, 24, and 42. This creates a patchwork verification landscape where conclusions about compliance become highly dependent on which firm conducted the audit and what criteria it chose to apply. Ultimately, auditors are placed in the position of both establishing evaluation standards and then applying them.[71] Methodologies developed in silos without multi-stakeholder consultations and input could undermine their findings' reliability and consistency, and overall trust.[72]

The regulation only introduces procedural safeguards through sampling requirements. When audit evidence relies on data sampling, auditors must select sample sizes and methodologies that ensure representativeness while considering factors like changes to platform services, algorithmic personalization, and impacts on vulnerable groups.[73] Platforms are explicitly prohibited from interfering with sampling decisions.[74] However, without standardized benchmarks for determining appropriate sample sizes or evaluating representativeness, auditors retain significant freedom in how they implement these

[69] DRA, art. 10.

[70] On the contrary, the DRA sets out significant details on how to conduct audits related to the obligations under articles 34, 35, and 36 of the DSA. *See* DRA, arts. 13-16.

[71] Morandini, *supra* note 63; Bhatia and Allen, *supra* note 67.

[72] Jason Pielemeier, et al., *Ensuring Digital Services Act Audits Deliver on Their Promise*, TECH POL'Y PRESS (Feb. 19, 2024), https://techpolicy.press/ensuring-digital-services-act-audits-deliver-on-their-promise.

[73] DRA, art. 12(2).

[74] *Id.*, art. 12(1).

requirements. Furthermore, the vagueness around the methodology in the DRA has the result of not only asking auditors to establish the evaluation standards, but also to allow companies to set their own benchmarks. This results in companies being able to virtually provide their own "answer key against which auditors will grade their homework."[75]

The DRA provides some guidance on audit evidence and quality standards, even while leaving methodological choices to auditors. Audit conclusions must be based on evidence that is both "relevant and sufficient to reduce audit risks" and "reliable, according to the auditing organisation's professional judgment and scepticism."[76] When auditing transparency reports, auditors must specifically assess whether the reported information is "free from material error or omission which might otherwise render them misleading."[77] However, the regulation does not define what constitutes a material error or provide standards for making this assessment, leaving the definition to auditor's discretion.[78] Overall, the DRA failed to provide auditing guidelines that will make the resulting audits difficult to compare, less rigorous, and at risk of failing to meet the regulators' goals.[79]

B. Scope of Auditable Transparency Obligations Under the DSA

Article 37 of the DSA requires VLOPs and VLOSEs to be subject to independent auditing for what concerns their compliance with the obligations set out in Chapter III of the DSA. For the scope of this article, the relevant obligations are articles 15 (transparency reports), 17 (statements of reasons), 24, and 42 (human resources involved in content moderation).

The core transparency obligations subject to

[75] Pershan, *supra* note 7.

[76] DRA, art. 11.

[77] *Id.*, art. 10(6).

[78] Wagner, *supra* note 58.

[79] Pielemeier, et al., *supra* note 71; Bhatia & Allen, *supra* note 67; Morandini, *supra* note 63.

independent auditing include four interconnected components. Article 15 establishes baseline transparency reporting requirements that apply to all intermediary services, mandating annual reports on content moderation actions, government orders, and automated decision-making systems.[80] Article 17 complements these aggregate reports by requiring individual statements of reasons for each content moderation decision, which must be submitted to the centralized Database of Statements of Reasons.[81] For online platforms, Article 24 adds further transparency obligations concerning dispute resolution mechanisms and user counts.[82] Finally, Article 42 imposes enhanced reporting requirements on VLOPs and VLOSEs, demanding greater detail on their content moderation workforce, internal processes, and risk mitigation measures.[83]

The independent audit requirement serves as a verification mechanism for this layered transparency framework. Auditors must not only confirm that platforms publish the required reports and submit statements of reasons, but also verify that these disclosures accurately represent the platforms' actual practices.[84] This verification function is particularly important given the historical challenges with reliability in platform transparency, where self-reported information often lacks independent confirmation.[85] Audits have the potential to fill the verification gap that has hindered previous transparency initiatives by evaluating both the presence and accuracy of disclosures.

However, the design of the audit mechanism is limited

---

[80] DSA, art. 15.

[81] *See* DSA, arts. 17, 24(5) (mandating that online platform "provide a clear and specific statement of reasons" for content moderation decisions); *see also* DSA, art. 24(5) (requiring platforms to submit these statements to the EU Commission).

[82] DSA, art. 24.

[83] *Id.*, art. 42.

[84] This verification function is implied in DSA, art. 37(4)(g), which requires the audit report to include "an audit opinion on whether the provider of the very large online platform or of the very large online search engine subject to the audit complied with the obligations and with the commitments referred to in paragraph 1."

[85] Suzor, et al., *supra* note 1; Gorwa & Ash, *supra* note 15.

by the fact that it applies exclusively to VLOPs and VLOSEs.[86] This limited application creates a two-tiered verification system within the DSA's transparency framework. On one hand, smaller platforms must comply with transparency obligations under Articles 15, 17, and 24, but on the other, their disclosures remain unverified through formal auditing processes. This gap is particularly problematic for platforms that fall just below the VLOP threshold but still have substantial user bases and societal impact.[87] The absence of verification requirements for these platforms perpetuates the reliability concerns for a significant portion of the digital world, potentially limiting the overall effectiveness of the DSA's transparency objectives.

Ultimately, the asymmetric approach to verification reflects the DSA's broader strategy of imposing proportionate obligations based on platform size and risk.[88] Yet this design choice creates a scenario where the statements and reports most likely to receive independent verification are those produced by platforms with the greatest resources to ensure compliance, while smaller platforms with potentially limited compliance capacity operate with less oversight.

This asymmetry is further compounded by the fact that larger platforms typically attract greater regulatory attention and public scrutiny independent of formal auditing requirements.[89] VLOPs and VLOSEs operate in the spotlight of media coverage, academic research, and civil society monitoring, creating additional incentives for transparency compliance. Conversely, smaller platforms may operate with minimal external oversight despite potentially significant impacts on specific communities or

---

[86] DSA, art. 37.

[87] The 45 million user threshold for VLOP/VLOSE designation creates a bright line that excludes platforms with substantial but smaller user bases from the audit requirement. *See* DSA, art. 33(1).

[88] *Id.*, recital 13.

[89] Natascha Just & Florian Saurwein, *Enhancing Social-Media Regulation through Transparency? Examining the New Transparency Regime in the EU*, Univ. Zurich (2024), https://www.zora.uzh.ch/id/eprint/257668.

contexts, allowing transparency gaps to persist unnoticed and unaddressed. This difference raises questions about the effectiveness of the DSA "transparency machine" across the entire digital services landscape.

C. Auditor Independence

Both Article 37 of the DSA and the DRA establish guidelines on which organizations can be in charge of performing the auditing process. The main objective of such limitations is to ensure auditors' independence and attempt to obtain as much of an unbiased opinion as possible.

The independence framework sets explicit prohibitions against conflicts of interest. Auditors must not have provided non-audit services to the platform being audited during the preceding twelve months.[90] The DSA further prohibits auditing organizations from performing audits when fees are contingent on the audit results, eliminating potential financial incentives that could compromise objectivity.[91]

Beyond conflict of interest prohibitions, the framework requires specific qualifications for organizations performing audits. These entities must demonstrate "proven expertise in the area of risk management, technical competence and capabilities" relevant to evaluating systemic risks.[92] This expertise requirement prevents platforms from selecting technically unqualified but potentially more favorable auditors while also ensuring the audit process can meaningfully examine complex content moderation systems. The DRA clarifies that while independence requirements must be met individually by each entity involved in the audit, expertise requirements can be fulfilled jointly, allowing for specialized knowledge to be contributed by different entities.[93]

---

[90] DSA, art. 37(3). This prohibition extends to "legal entities belonging to the same network, association, or group of undertakings," preventing platforms from circumventing independence requirements through corporate arrangements. *See* DRA, art. 4(2)(a).

[91] DSA, art. 37(3)(a)(iii).

[92] *Id.*, art. 37(3)(b).

[93] DRA, art. 4(2)(b).

To prevent audit capture, the independence framework restricts long-term relationships between platforms and auditors.[94] Article 37(3)(a)(ii) prohibits auditors from providing services to the same platform "during a period longer than 10 consecutive years." This mandatory rotation disrupts the potential development of overly familiar relationships that might compromise objectivity.

Nevertheless, the effectiveness of the independence framework is potentially limited by the constrained pool of eligible auditors. The DSA demands expertise in risk management, technical systems, and "the subject-matter of [the DSA] and, in particular, the systemic societal risks referred to in Article 34."[95] This combination of specialized knowledge, which would ideally include familiarity with established methodologies like human rights impact assessments, significantly narrows the field of qualified candidates.[96] The strict independence requirements further restrict this already limited pool of potential auditors.

For what concerns the information to be accessible by auditors performing the audits, article 37 requires platforms to provide auditors with all necessary access while also subjecting the auditors to strict confidentiality requirements. To address concerns around a potential tension between protecting legitimate platform interests and ensuring meaningful audits, the DSA further specifies that the confidentiality requirement “shall not adversely affect the performance of the audits.”[97]

III. Audits as verification mechanisms

This section analyzes the first nineteen DSA audit reports published in late 2024, revealing significant insights about both the verification framework and platforms' compliance patterns. By reviewing the publicly available versions of these reports, this analysis identifies patterns in transparency compliance, verification approaches, and

[94] Algorithm Watch, *supra* note 5 (discussing the risk of audit capture).
[95] DRA, recital 9.
[96] *See also* Pielemeier, et al., *supra* note 71; Bhatia & Allen, *supra* note 67.
[97] DSA, art. 37(2).

challenges in the independent assessment of platform accountability.

The analysis serves a dual function in understanding platform transparency under the new regulatory framework. First, the audit reports provide concrete evidence of the reliability problem, as auditors identified material inaccuracies in transparency disclosures across nearly all platforms examined. Despite facing professional auditing requirements, VLOPs still produced flawed transparency reports, with systematic gaps in reporting practices and inconsistencies between different transparency mechanisms.

Second, these findings demonstrate the need for integrated verification approaches across the DSA's transparency framework. If VLOPs struggle to meet reporting obligations under formal audit scrutiny, platforms not subject to Article 37's audit requirements almost certainly face greater challenges in producing reliable disclosures. This gap in the verification framework highlights why the Database of Statements of Reasons should be enhanced to serve as a complementary verification tool for all platforms, particularly those without audit requirements. Only by connecting these transparency mechanisms, rather than treating them as isolated compliance exercises, can the DSA effectively address the reliability problem across its tiered regulatory structure.

A. Methodology and Overview

This analysis examines the first round of independent audit reports submitted by the 19 VLOPs and VLOSEs designated under the Digital Services Act. The audit reports cover each platform's compliance with their respective obligations under the DSA, including the transparency provisions that are the focus of this article.

1. Who Are the Auditors?

As had been anticipated during the initial DSA discussions, the audit landscape was significantly concentrated among a small number of professional

services firms.[98] Ernst & Young (EY) was the dominant auditor, conducting nine of the nineteen audits (47%), including those for Apple, Meta, Alphabet, Pinterest and Snapchat. Deloitte conducted four audits (21%), serving Microsoft's Bing, Booking.com, LinkedIn, and Zalando. KPMG performed three audits (16%), including those of the Amazon Store, AliExpress, and TikTok. The two remaining platforms selected different firms, with X choosing FTI Consulting, and Wikipedia selecting Holistic AI.

This concentration reinforces concerns about audit independence and effectiveness, especially given that many of these accounting firms had pre-existing business relationships with the platforms they were auditing.[99] The reliance on dominant traditional accounting firms, while bringing established audit methodologies, also raises questions about whether these organizations possessed the specialized expertise needed to meaningfully evaluate platform governance and content moderation practices, areas that differ substantially from traditional financial auditing.[100]

The predominance of large accounting firms may also explain methodological limitations observed throughout the reports. Most audits heavily relied on platforms' existing processes and internal documentation to verify compliance, with limited evidence of independent testing or verification beyond what platforms themselves provided.[101] This reliance on company-provided information creates a fundamental weakness in the verification framework, as auditors may lack both the

---

[98] *See, e.g.,* Bhatia & Allen, *supra* note 67.

[99] Pielemeier, et al., *supra* note 71 (explaining that the DSA creates an extremely limited pool of eligible auditors by requiring expertise in risk management, technical systems, and "the subject-matter of [the DSA] and, in particular, the systemic societal risks referred to in Article 34." These stringent qualifications, coupled with the DSA's independence requirements, severely restrict the number of organizations capable of conducting such audits).

[100] *See* Section II.C.

[101] Mark Scott, *5 Things to Know about the Digital Services Act's First Risk Assessments and Audits*, TECH POL'Y PRESS (Dec. 11, 2024), https://techpolicy.press/5-things-to-know-about-the-digital-services-acts-first-risk-assessments-and-audits.

technical means and incentives to challenge platforms' representations about their compliance.[102]

The selection of smaller, specialized firms like Holistic AI for Wikipedia's audit represents an alternative approach that may bring platform-specific expertise, but these cases remained exceptions rather than the norm. As the DSA's audit framework continues to mature, the ability of traditional accounting firms to serve as appropriate entities to verify compliance with new platform governance requirements will need ongoing assessment. At this early stage, the DSA audits represent an important first step toward enhancing platform accountability, but they fall short of providing the in-depth independent verification needed to fully respond to reliability concerns.[103]

2. Audit Approaches and Assurance Standards

The auditing approaches used were substantive testing, control-based verification, and mixed approaches. Substantive testing tends to involve a direct examination of samples or outcomes to verify compliance, such as reviewing a selection of content moderation decisions to determine if they followed required procedures. Control-based verification, by contrast, evaluates the systems and processes designed to ensure consistent compliance, such as examining whether platforms have implemented effective approval workflows, monitoring systems, and quality checks.

The reports analyzed showed a significant predominance of substantive testing over control-based

[102] *Id.* (explaining that X's case exemplifies how these limitations lead to contradictory assessments. "FTI Consulting explicitly stated that, based on its review of the company's internal processes, Elon Musk's platform was compliant with its DSA obligations to provide outside researchers with real-time access to its public data. That, however, was in direct contradiction to preliminary charges filed by the European Commission, which accused X of failing to comply with such outsider data access." Such discrepancies raise critical questions about the rigor of these audits and their reliability as verification mechanisms). *See also* Pielemeier, et al., *supra* note 71 (explaining how the scarcity of auditors is problematic in view of how much auditors have to rely on companies to identify relevant systems, provide access to necessary data, and explain technical complexities).

[103] Bhatia & Allen, *supra* note 67 (arguing that the value of the first audit reports lies primarily in establishing a baseline for future improvement rather than in resolving longstanding challenges in verifying platform disclosures).

approaches, potentially indicating uncertainties around DSA compliance frameworks in place at platforms. This pattern signals that auditors relied primarily on sampling and individual compliance instances instead of looking at whether platforms had (or lacked) sufficient governance mechanisms to ensure compliance up front.

For transparency obligations specifically, most auditors employed a combination of documentation review, interviews with relevant personnel, and sample testing of published transparency reports against supporting evidence such as internal data repositories. However, few auditors conducted systematic cross-verification between transparency reports and Database entries, limiting their ability to detect inconsistencies across transparency mechanisms. This methodological imbalance is particularly problematic because rather than evaluating whether platforms have reliable systems to ensure accurate reporting across all transparency mechanisms, auditors often resorted to checking individual disclosures or reports. This approach cannot verify the consistency between different transparency tools, which is precisely the verification tool needed for meaningful transparency.

A significant limitation was the lack of standardized reporting periods, making cross-platform comparisons virtually impossible.[104] This inconsistency in temporal scope, combined with variations in audit methodology and depth, has created a fragmented landscape where each platform's compliance is evaluated in isolation. Without standardized approaches, these audits serve more as individualized compliance checks than as components of a cohesive regulatory framework that enables meaningful comparisons across platforms.[105]

For what concerns the "reasonable assurance" standard, most auditors relied on the ISAE 3000 assurance standard, except for Wikipedia and X. The ISAE 3000 is an in

[104] Scott, *supra* note 100; Chris Powers, *DSA audit scorecard: How Are Big Tech platforms complying with the EU's landmark legislation?*, EURACTIV (Dec. 2, 2024), https://www.euractiv.com/news/dsa-audit-score-card-how-are-big-tech-platforms-complying-with-the-eus-landmark-legislation.

[105] *See* Section II.B.

international standard which provides a framework for assurance in context that does not involve financial information.[106] The standard establishes guidelines for planning, evidence collection, and reporting. For the DSA, the standard might have been selected by most auditors for two main reasons. First, the auditing firms used by the companies are also involved in other auditing services in other markets and therefore might have been familiar with the tool in other parts of their practice. Second, it establishes evidence standards and ensures consistent quality control procedures, a gap left by the EU regulator in the DRA.

However, this standard creates significant hurdles when applied to platform transparency verification. The DRA's lack of benchmarks and methodologies for auditing created ambiguities that auditors had to clarify independently.[107] At the same time, requiring "reasonable assurance" imposes a remarkably high standard for verification, requiring auditors to affirmatively confirm that information is materially correct rather than simply noting the absence of material misstatements.[108] There are few precedents of applying such a rigorous standard to qualitative corporate systems, even in areas like environmental, social, and governance matters.[109] The DSA demands evaluation of substantially more complex technical systems and internal controls, yet requires reasonable assurance without establishing standards or benchmarks. This lack of shared understanding makes determining "reasonable assurance"

---

[106] INT'L AUDITING AND ASSURANCE STANDARDS BD., INT'L INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3000 REVISED, ASSURANCE ENGAGEMENTS OTHER THAN AUDITS OR REVIEWS OF HISTORICAL FINANCIAL INFORMATION, (2013), https://www.iaasb.org/publications/international-standard-assurance-engagements-isae-3000-revised-assurance-engagements-other-audits-or.

[107] *See ECG responds to the EC call for feedback on the Digital Services Act audit methodology draft delegated regulation*, EUROPEAN CONTACT GRP. (July 4, 2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits/F3424074_en.

[108] Pielemeier, et al., *supra* note 71 (explaining that "reasonable assurance effectively requires the auditor to be confident affirmatively stating that the information they are attesting to is materially correct (as opposed to 'limited assurance,' which requires a negative determination that no evidence of material misstatement has been found)").

[109] *Id.*

an effectively impossible task, particularly for transparency verification.[110]

Furthermore, the absence of this standard in the reports of Wikipedia and X creates an issue for cross-comparability of the reports.[111] Without a common standard, the rigor of verification procedures may vary significantly across platforms, the interpretation of "reasonable assurance" becomes ambiguous, and the criteria for issuing various conclusions lack uniformity.[112] In cases where alternative standards were used, reports provided no clear explanation of what framework guided the assessment, making it almost impossible to evaluate whether these approaches offered equivalent scrutiny.

Overall, these variations create challenges for the DSA's compliance assessment. Rather than establishing a consistent foundation for meaningful oversight, the current approach still allows platforms significant discretion in how their compliance is evaluated and presented. This discretion risks undermining the very accountability the audit system was designed to ensure.

B. General Audit Findings

The audit reports reveal widespread compliance challenges across platforms, with variances in both the nature and severity of identified deficiencies. These findings provide a window into platforms' implementation of DSA obligations and highlight specific areas where transparency requirements face the greatest obstacles. The

---

[110] *Id.*; Asha Allen, Comment on *Digital Services Act—conducting independent audits*, EUROPEAN COMM'N (June 2, 2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits/F3424081_en (arguing that the Commission should have clarified what is required under "reasonable assurance); Zalba, *supra* note 67 (arguing that the Commission should have replaced "reasonable assurance" with "limited assurance").

[111] *See* Independent Audit, FTI CONSULTING (Aug. 27, 2024), https://transparency.x.com/content/dam/transparency-twitter/dsa/dsa-audit/TIUC-DSA-Audit-Report-2024-08-27.pdf; *Wikipedia DSA Audit Report*, WIKIMEDIA FOUND. (last visited Feb. 19, 2025), https://foundation.m.wikimedia.org/wiki/File:Wikipedia_DSA_Audit_Report_2023-24_Public.pdf.

[112] EUROPEAN CONTACT GRP., *supra* note 106; Pielemeier, et al., *supra* note 71.

pattern of exceptions and disclaimers suggests systemic issues in the transparency framework rather than isolated compliance failures.[113]

The DSA's audit framework requires auditors to issue one of four conclusion types: positive (indicating full compliance), positive with comments (suggesting improvement areas while confirming basic compliance), negative (indicating non-compliance), or disclaimer of opinion (where insufficient evidence prevents an assessment). The analysis of these conclusions across the nineteen reports highlights a concerning trend: all reports except Wikipedia contained substantive remarks or exceptions, indicating broader challenges in meeting DSA obligations.

Platform	In compliance	Partly compliant	Not compliant	No verdict as under investigation	Inconclusive	N/A
Alibaba AliExpress	40	19	0	19	0	100
Amazon Store	69	8	4	0	0	98
Apple Appstore	77	2	2	0	0	98
Bing	26	0	3	0	3	147
Booking.com	33	0	17	0	30	99
Facebook	47	5	0	14	0	113
Google Maps	70	4	0	0	0	105
Google Play	58	5	1	0	0	115

[113] Disclaimers occur when auditors state they cannot form an opinion on compliance because they lack sufficient evidence to reach a conclusion. When multiple auditors issue disclaimers for similar obligations across different platforms, this creates a pattern suggesting that certain aspects of the framework may be inherently difficult to verify.

Google Search	32	1	1	0	0	145
Google Shopping	62	2	0	0	0	115
Instagram	50	4	0	14	0	111
LinkedIn	46	17	2	0	4	110
Pinterest	61	4	0	0	0	114
Snapchat	64	3	0	0	0	112
TikTok	53	11	0	6	0	109
Wikipedia	77	0	0	0	0	102
X	72	0	9	0	2	96
YouTube	62	3	0	0	0	114
Zalando	64	5	0	0	18	92

(Table 1 – Auditing conclusions by platform and by conclusion type)

The data in Table 1 demonstrates striking variations in compliance patterns across platform types, with several platforms showing distinctive compliance profiles. Wikipedia stands alone in achieving full compliance with all 77 applicable DSA requirement, a record that distinguishes it from every other audited platform.[114] At the opposite end of the spectrum, Booking.com demonstrates significant compliance challenges, meeting only 33 out of 80 applicable requirements.[115] Even more concerning is Booking.com's high rate of negative findings (17 non-compliant requirements) and inconclusive results (30 requirements). Meta's audits reflect the regulatory scrutiny affecting both companies which have identical numbers of provisions where auditors could not reach a verdict due to ongoing European Commission investigations.[116] X exhibits

[114] WIKIMEDIA FOUND., *supra* note 110.

[115] *Booking.Com B.V. DSA Assurance Report*, DELOITTE (Aug. 28, 2024), https://q-xx.bstatic.com/data/mobile/2f26af50-3773-4484-a693-4ca3c78dede3.pdf [hereinafter Deloitte Booking.com Report].

[116] *Independent Audit on Instagram*, ERNST & YOUNG (Aug. 28, 2024), https://scontent-lga3-3.xx.fbcdn.net/m1/v/t0.84174-6/An8wBbgR2Nf3CEJJEGIroggiLDQHftp15y40nSuNb6k0nQ5xivPA56RNc0l-zIb2dznp9JI8LgmUfPh16KyWLR5kxJUcSjat7Dul98WISuHSpG3Y_bUTc6bYkn4Mx_48BrifhA7E?_n [hereinafter EY Instagram Audit]; *Independent Audit on Facebook*, ERNST & YOUNG (Aug. 28, 2024), https://panoptykon.org/sites/default/files/2024-11/ocena-ryzyka-dsa-2024_facebook.pdf [hereinafter EY Facebook Audit].

an "all-or-nothing" compliance profile. Despite having the third-highest number of compliant requirements (72), X also has one of the highest non-compliance counts (9), while showing zero partially compliant requirements.[117] AliExpress presents yet another unique compliance profile with the highest number of partially compliant requirements (19) and requirements under investigation (19).[118] In contrast, app stores demonstrate consistently strong compliance, with Apple App Store implementing 77 out of 81 applicable requirements and Google Play implementing 58 out of 64.[119]

This quantitative evidence confirms the performance disparity between content-focused and other platform types. Social media platforms not only received more negative conclusions but also faced more instances where auditors could not reach a verdict due to ongoing investigations. This pattern could suggest that content-moderation-intensive platforms face not only more complex compliance challenges but also greater regulatory scrutiny.

The distribution of "partly compliant" findings further illustrates implementation challenges. Platforms with the highest partial compliance counts included AliExpress (19), LinkedIn (17), and TikTok (11), potentially indicating that these services struggled to fully implement certain requirements despite avoiding outright non-compliance. Most concerning are the instances of "inconclusive" verdicts, where auditors could not form an opinion due to evidence limitations rather than regulatory investigations. Zalando had 18 such instances—the highest among all platforms—indicating verification challenges even in the

---

[117] FTI CONSULTING, supra note 110.

[118] *Independent Audit of AliExpress*, FTI CONSULTING (Dec. 2025), https://www.aliexpress.com/p/transparencycenter/auditReport.html.

[119] Cathy Kearney, et al., *Independent Audit of the App Store,* APPLE DISTRIBUTION INT'L LIMITED (last visited Feb. 19, 2025), https://www.apple.com/legal/dsa/20242708_app-store_reasonable-assurance-report_non-confidential.pdf; *Independent Audit on Google Play*, GOOGLE IRELAND LTD. (2024), https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-google-play_2023-8-28_2024-5-31_en_v1.pdf .

absence of regulatory action.

C. Findings on Transparency Compliance

While the overall pattern of audit conclusions shows important compliance disparities across platforms, transparency requirements require specific analysis given their centrality to the DSA's accountability framework. The audits present significant patterns in platforms' compliance with DSA transparency obligations. While certain obligations appear to be straightforward for platforms to implement, others highlight consistent challenges across the digital ecosystem.[120] The analysis below examines these patterns, focusing on three key areas: compliance with basic transparency reporting requirements, challenges in implementing the statements of reasons mechanism, and platforms' adherence to enhanced transparency obligations around human resources involved in content moderation.

[120] The compliance rate decreases progressively from general transparency obligations (Article 15.1, with 12 compliant platforms) to specific content moderation transparency (Article 24.5, with 10 compliant platforms) to risk assessment transparency (Article 42.2, with 10 compliant platforms).

Table 2 – Audit Reporting Findings for Transparency Obligations

DSA Article	15.1	15.2	15.3	24.1	24.2	24.3	24.4	24.5	24.6	42.1	42.2	42.3	42.4	42.5
AliExpress	In compliance	N/A	N/A	In compliance	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	In compliance	N/A	N/A
Amazon Store	In compliance	N/A	N/A	In compliance	In compliance	In compliance	N/A	In compliance	N/A	In compliance	Partly compliant	In compliance	In compliance	N/A
Apple App Store	In compliance	N/A	N/A	In compliance	In compliance	In compliance	N/A	Partly compliant	N/A	In compliance	In compliance	In compliance	N/A	N/A
Booking.com	Not compliant	N/A	N/A	Inconclusive	In compliance	In compliance	N/A	Not compliant	N/A	In compliance	Not compliant	Inconclusive	N/A	N/A
Facebook	Partly compliant	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	Under investigation	N/A	In compliance	Partly compliant	In compliance	N/A	N/A
Google Play	In compliance	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	In compliance	N/A	N/A
Google Maps	In compliance	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	In compliance	N/A	N/A
Google Shopping	In compliance	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	In compliance	N/A	N/A
Instagram	Partly compliant	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	Under investigation	N/A	In compliance	Partly compliant	In compliance	N/A	N/A
LinkedIn	Inconclusive	N/A	N/A	Inconclusive	In compliance	In compliance	N/A	Partly compliant	N/A	In compliance	Inconclusive	In compliance	N/A	N/A
Pinterest	In compliance	N/A	N/A	In compliance	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	Partly compliant	N/A	N/A
Snapchat	Partly compliant	N/A	N/A	In compliance	In compliance	In compliance	N/A	In compliance	N/A	In compliance	Partly compliant	In compliance	N/A	N/A
TikTok	In compliance	N/A	N/A	In compliance	In compliance	In compliance	N/A	In compliance	N/A	In compliance	In compliance	In compliance	In compliance	N/A
Wikipedia	In compliance	N/A	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance	In compliance
X	Not compliant	N/A	N/A	Not compliant	In compliance	In compliance	N/A	In compliance	N/A	In compliance	Not compliant	In compliance	N/A	In compliance
YouTube	In compliance	N/A	N/A	Partly compliant	In compliance	In compliance	N/A	Partly compliant	N/A	In compliance	Partly compliant	In compliance	N/A	N/A
Zalando	Not compliant	N/A	N/A	In compliance	In compliance	Inconclusive	N/A	Partly compliant	N/A	In compliance	In compliance	Partly compliant	In compliance	Inconclusive
Bing	In compliance	N/A	N/A	N/A	Inconclusive	In compliance	N/A	N/A	N/A	In compliance	N/A	Inconclusive	N/A	N/A
Google Search	In compliance	N/A	N/A	N/A	In compliance	In compliance	N/A	N/A	N/A	In compliance	N/A	In compliance	N/A	N/A

1. Transparency Reporting Findings (Article 15, 24.1)

Article 15(1) establishes the foundational transparency reporting requirements for all intermediary services covered by the DSA. Compliance with these basic reporting requirements varies substantially across platforms, with a third of audited platforms falling short of full compliance. The most common deficiencies relate to the documentation of own-initiative content moderation and the reporting on automated means used for content moderation. Article 24(1) adds additional requirements for online platforms, mandating disclosures about out-of-court dispute resolutions and account suspensions for manifestly illegal content or unfounded notices and complaints.

Auditors' findings revealed particular compliance issues among social media platforms. Both Facebook and Instagram received "partly compliant" assessments, with auditors citing incomplete transparency over monetization restrictions and inadequate breakdowns of moderation measures for non-organic content.[121] The audit report specified that Meta's platforms "did not report on the monetization restrictions as required" and only provided breakdown by violation types and detection methods for "organic content, but did not provide such breakdown for non-organic content (e.g., business entities)."[122] The auditor further noted that Meta's platforms "did not report the content moderation measures by type of violation nor detection method applied" in their transparency reports for certain content categories.[123] Snapchat similarly received a "partly compliant" determination for failing to provide "meaningful and comprehensible information about the content moderation engaged in at the providers' own initiative, including the number of content categorized by the type of restriction applied."[124]

---

[121] EY Facebook Audit, *supra* note 115, at 19–23; EY Instagram Audit, *supra* note 115.

[122] EY Facebook Audit, *supra* note 115, at 19–23; EY Instagram Audit, *supra* note 115.

[123] EY Facebook Audit, *supra* note 115, at 19–23; EY Instagram Audit, *supra* note 115.

[124] *Independent Audit on Snapchat*, Ernst & Young (Aug. 26. 2024), https://assets.ctfassets.net/kw9k15zxztrs/5CrFmNWQztRkDcvhZ8TwyC/6014cd3df6544a2a68a56dfad1712b56/DSA_Independent_Audit_Report_-_Snapchat_-_August_2024.pdf

The most concerning compliance failures occurred with Booking.com, Zalando, and X, all receiving "not compliant" assessments for Article 15(1) obligations. X's audit revealed the platform excluded the basis for complaints from its report, claiming this omission stemmed from the variety of reasoning in complaint fields. The platform also failed to include error rates or safeguards for automated systems.[125] Booking.com's non-compliance stemmed from material deficiencies in documentation retained by the company for control purposes. The auditors note that they were "unable to place reliable of controls to gain reasonable assurance over the subject matter information." Furthermore, the auditors noted that the transparency report contained inaccuracies over the number of total member state orders received for unsafe and/or illegal products and the breakdown by each member state, and that "the number of actions taken on the basis of the terms and conditions missed disclosure details for the Notice and Action Mechanisms."[126] For Zalando, auditors applied the platform's own methodologies to internal data sets and found numbers that differed from those published in the transparency report, concluding the platform had presented incorrect information.[127]

LinkedIn represents a unique case with an "inconclusive" assessment, reflecting the inability of auditors to verify the accuracy of self-reported information when platforms provide limited access to underlying data. LinkedIn lacked documented inventories of processes and systems used in producing transparency reports, and the complexity of these undocumented systems prevented auditors from designing alternative verification procedures.[128] This

[hereinafter EY Snapchat Audit].

[125] FTI CONSULTING, *supra* note 110, at 88–89.

[126] Deloitte Booking.com Report, *supra* note 114, at 28–29.

[127] *Independent Practitioner's Assurance Report on Zalando SE's Compliance with the Digital Services Act*, DELOITTE (Aug. 23, 2024), https://corporate.zalando.com/sites/default/files/media-download/Zalando-SE_DSA_Independent-Practitioners-Assurance-Report.pdf [hereinafter Deloitte Zalando Report].

[128] *LinkedIn's Digital Services Act (DSA) Report*, DELOITTE (Aug. 23, 2024), https://content.linkedin.com/content/dam/help/tns/en/2024_LinkedIn_DSA_Redacted_Report_NON-CONFIDENTIAL.pdf [hereinafter Deloitte LinkedIn Report].

limitation stresses a fundamental tension in the DSA's verification framework, where auditors must often rely on the same self-reported data that the transparency mechanism aims to make more reliable.

These findings further sustain the reliability problem in platform transparency.[129] When discrepancies exist between platforms' internal data and public disclosures (e.g., Zalando), and when factual inaccuracies appear in mandatory reporting (e.g., Booking.com), it becomes clear that transparency reports cannot be relied upon even when legally mandated and backed by significant penalties. The audit findings show that when platforms control both the production and documentation of transparency data without meaningful interconnected verification mechanisms, the resulting disclosures remain inherently unreliable. The fact that auditors themselves could not verify information for some platforms underscores how deeply embedded this reliability problem remains despite the DSA's ambition to become a "transparency machine".[130]

Notably, no platforms were assessed for compliance with Article 15(2), as the provision only applies to hosting services that are not online platforms. Only Wikipedia was assessed for compliance with Article 15(3), which requires companies to follow the implementing act laying down templates for transparency reports.[131]

Article 24(1) compliance findings further confirm the disconnect between different transparency mechanisms under the DSA. Over half of platforms failed to achieve full

---

[129] *See supra* Section I.

[130] Alessia Zornetta, *Is The Digital Services Act Truly A Transparency Machine?*, TECH POL'Y PRESS (July 11, 2024), https://www.techpolicy.press/is-the-digital-services-act-truly-a-transparency-machine/; *See* Mathias Vermeulen (@mathver), X (Nov. 4, 2023, 7:43 AM), https://x.com/mathver/status/1720768618328162375 ("The Digital Services Act is a transparency machine. Platforms have to submit every 6 months a report describing their content moderation activities in the EU. The first reports are in and there's a wealth of information in there. Thread).

[131] Wikipedia's assessment is curious since the platform was found in compliance despite the fact that the implementing act establishing standardized templates had not yet entered into force at the time of the audit. This outcome highlights a fundamental inconsistency in the audit process, where platforms may be evaluated against requirements that have been legislated but not yet operationalized through implementing acts.

compliance with requirements to report on out-of-court dispute resolutions and account suspensions. This high rate of deficiency reinforces the inability to verify platforms' broader transparency claims. Most concerning are the findings for X, which was deemed "not compliant" because its transparency report completely omitted references to unfounded notices or complaints.[132]

Meta's platforms (Facebook and Instagram) failed to accurately report suspensions for manifestly illegal content based on their own methodology and definitions under Article 23.[133] Google's services (Play, Maps, Shopping, and YouTube) did not properly specify which suspensions for unfounded complaints pertained to each specific service, instead presenting consolidated figures across multiple platforms.[134] For Booking.com, auditors were unable to design appropriate tests to verify suspension records, citing insufficient documentation and evidence to form a conclusion about compliance.[135] The findings appear to signal that platforms tend to separate their compliance with different transparency provisions, treating each as a distinct obligation rather than components of an interconnected framework. This approach significantly hinders cross-verification between different transparency provisions.

2. Statements of Reasons and the DSA Transparency Database (Article 24.5)

Audit findings for Article 24(5), requiring platforms to

[132] FTI CONSULTING, *supra* note 110, at 179.

[133] EY Facebook Audit, *supra* note 115, at 41-43; EY Instagram Audit, *supra* note 115, at 40-42.

[134] Kearney, et al., *supra* note 118 at 68–69; *Independent Audit on Google Maps*, ERNST & YOUNG (Sept. 27, 2024), https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-google-maps_2023-8-28_2024-5-31_en_v1.pdf; *Independent Audit on Google Shopping*, ERNST & YOUNG (Sept. 27, 2024), https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-google-shopping_2023-8-28_2024-5-31_en_v1.pdf; *Independent Audit on Youtube*, GOOGLE IRELAND LIMITED (2024), https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-youtube_2023-8-28_2024-5-31_en_v1.pdf [hereinafter Google Youtube Audit].

[135] Deloitte Booking.com Report, *supra* note 114, at 67.

submit copies of statements of reasons to the Commission's Database, revealed compliance challenges for seven out of the seventeen platforms assessed.[136] This high rate is particularly concerning given the Database's potential role in enabling verification of broader transparency claims. The most prevalent patterns of partial and non-compliance relate to delayed submissions, technical implementation failures, and incomplete data transmission.

Booking.com received a "not compliant" assessment after self-identifying instances where the platform failed to send Statements of Reasons to both users and the European Commission when content was rejected. Auditors concluded that "the controls to meet the audit criteria were inappropriately designed and implemented" due to insufficient documentation and lack of controls over data completeness and accuracy.[137] Booking.com implemented the required functionality in phases from August 2023 to April 2024, meaning they "did not enable the functionality to send SORs to the European Commission for specific content items from the day the restriction was imposed."[138] This implementation gap reinforces the importance of transforming the Database into a real-time verification tool, as these temporal blind spots in the record of content moderation decisions prevent comprehensive oversight of platform practices.

Technical issues prevented several platforms from achieving full compliance. Apple App Store received a "partly compliant" assessment because of a bug in the system which prevented "several SOR emails, related to review takedowns from the App Store during a period from September 2023 to October 2023" from being transmitted to the Transparency Database.[139] LinkedIn's self-reported partial compliance stemmed from delayed integration with the Database for advertisements and profile-related moderations, which weren't fully implemented until March

[136] The provision is not applicable to Bing and Google Search.
[137] Deloitte Booking.com Report, *supra* note 114, at 71.
[138] *Id.*
[139] Kearney, et al., *supra* note 118, at 73-74.

and May 2024 respectively, creating category-specific gaps in their submissions.[140]

Timeliness of submissions represented another significant compliance challenge. While Article 24(5) requires platforms to submit statements "without undue delay," auditors found that YouTube failed to submit 14% of its total statements within their four-day operational benchmark.[141] Zalando similarly received a "partly compliant" assessment because several moderation decisions were transmitted to the Database "several weeks after" they occurred.[142] Zalando's auditor explicitly noted that such delayed transmission cannot be considered timely or "without undue delay."[143] Zalando also had documentation problems, with some moderation decisions showing API transmission numbers not found in the Database and others lacking any transmission details despite being required under Zalando's own methodology.[144] These discrepancies between Zalando's internal records and Database submissions further demonstrate why transforming the Database into a verification tool is essential as such inconsistencies could be systematically identified through automated cross-referencing between platforms' internal systems and their Database submissions.

Surprisingly, X was found in full compliance with Article 24.5, despite evidence from other research showing clear discrepancies between X's transparency report and Database submissions during the audit period. As highlighted in mine and others' previous work, X's transparency report disclosed 19,828 actions taken through automated content moderation for terms of service violations, yet the Database contained no statements of

---

[140] Deloitte LinkedIn Report, *supra* note 127, at 70–71.

[141] Google Youtube Audit, *supra* note 133, at 72–74. It is also interesting to note that the Commission has not precisely defined "without undue delay". This lack of definitional clarity potentially illustrates how auditors end up filling regulatory gaps with their own interpretive standards.

[142] Deloitte Zalando Report, *supra* note 126, at 69–70.

[143] *Id.*

[144] *Id.*

reasons where X reported using automated means.[145] This inconsistency raises questions about the thoroughness of the audit methodology, as the auditor appears to have focused on whether X submitted statements rather than the accuracy or completeness of those submissions relative to the platform's broader reporting.

These compliance challenges directly reinforce the arguments about the Database's structural limitations. The delayed and incomplete implementation of Database submission mechanisms across multiple platforms limit the Database from serving as a real-time verification tool. Technical issues and delays in submission further undermine the Database's potential to document individual content moderation decisions. Most importantly, the absence of systematic verification between platforms' transparency reports and their Database submissions allows discrepancies to persist unchallenged.

The findings demonstrate how the current implementation of the Database maintains rather than solves the reliability problem in platform transparency. Without systematic cross-referencing between transparency reports and Database entries, platforms can continue providing inconsistent information across different transparency mechanisms without consequence. The inconsistencies revealed by the audits highlight the need to transform the Database from an isolated documentation tool into an integrated verification mechanism that works in concert with transparency reports to enable meaningful oversight of platform practices.

3. Human Resources Involved in Content Moderation (Article 42.2)

Very Large Online Platforms and Search Engines face enhanced transparency obligations under Article 42, which mandates detailed reporting on human resources dedicated

[145] *See, e.g.*, Zornetta, *DSA Database*, *supra* note 13; Charis Papaevangelou & Fabio Votta, *What Platform Observability Have You given Us? A First Look into the Statement of Reasons Database*, DSA OBSERVATORY (2024), https://dsa-observatory.eu/the-dsa-and-platform-regulation-conference-2024/; Trujillo, et al., *supra* note 42.

to content moderation. This mandate attempts to clear the haze over the often opaque workforce behind content moderation decisions, requiring platforms to disclose information about moderators' qualifications, linguistic expertise, and accuracy rates broken down by each official language of EU Member States.

The audit findings highlight compliance issues across platforms, with almost half of the VLOPs failing to fully meet the requirements. The patterns of non-compliance highlight both deliberate resistance to transparency and technical difficulties in gathering and reporting the required information. Three differing compliance issues appear from the analysis of the reports: inadequate disclosure of moderator qualifications, failure to provide language-specific accuracy metrics, and systemic issues in data collection.

X and Booking.com present cases of outright non-compliance. X demonstrated active resistance to verification, with auditors noting that the platform "declined to engage in a live discussion on qualifications and linguistic expertise."[146] This refusal to cooperate fundamentally undermines the audit process and raises serious questions about the platform's commitment to transparency. Similarly, Booking.com failed to disclose moderator qualifications, and omitted accuracy rates for five official EU languages in its transparency reports.[147] The auditors determined these omissions were "material" enough to halt further testing procedures, suggesting the deficiencies substantially compromised the reliability of the platform's transparency disclosures.[148]

Even platforms deemed "partly compliant" demonstrated significant shortcomings. Amazon Store, for instance, organized its human resources and accuracy data by store rather than by language, creating a mismatch with the DSA's requirements.[149] Meta's platforms failed to

[146] FTI CONSULTING, *supra* note 110, at 307.

[147] Deloitte Booking.com Report, *supra* note 114, at 127.

[148] *Id.*

[149] *Amazon DSA Assurance Report*, KPMG at 94–95 (Aug. 29, 2024), https://trustworthyshopping.aboutamazon.com/attachment-file-eu-dsa-audit-report-amazon.

provide language-specific accuracy indicators and self-reported miscalculations in their moderator metrics for both their October 2023 and April 2024 transparency reports.[150] Similarly, Snapchat and YouTube failed to provide the language-specific accuracy metrics required under Article 42.2, with YouTube being specifically criticized for inconsistencies across reporting periods.[151]

In addition to compliance issues, auditors struggled to reach a conclusion for LinkedIn, citing the platform's lack of sufficient controls over information preparation as the primary obstacle. The auditors noted an absence of "documented inventory/listing of all of the steps that take place before the information is ready to be used in the Transparency Reports," indicating fundamental gaps in LinkedIn's transparency infrastructure.[152] This finding shows how inadequate documentation of internal processes can undermine transparency efforts, as auditors cannot verify information without understanding how it was produced.

These patterns of non-compliance with Article 42.2 signal a broader challenge in the DSA's transparency framework. While platforms are generally willing to provide aggregate information about their content moderation workforce, they demonstrate significant resistance to the more granular, language-specific disclosures that would enable meaningful assessment of their content moderation abilities across the EU's diverse linguistic landscape. This resistance, whether manifested through outright refusal, incomplete reporting, or technical obstacles, undermines the DSA's goal of providing insight into platforms' actual capacity to moderate content effectively across all EU languages and territories.

Overall, the audit findings analyzed in this section highlight a trend that goes beyond mere compliance failures with individual provisions of the DSA. What

[150] EY Facebook Audit, *supra* note 115, at 72-73; EY Instagram Audit, *supra* note 115, at 71-72.

[151] EY Snapchat Audit, *supra* note 123; Google Youtube Audit, *supra* note 133.

[152] Deloitte LinkedIn Report, *supra* note 127, at 123–124.

appears is a fragmented approach to transparency, where platforms treat the DSA requirements as isolated obligations rather than linked components. This fragmentation is particularly evident in how platforms like Meta can submit statements of reasons to the Database while reporting contradictory information in transparency reports, or how LinkedIn can produce public disclosures without maintaining the documentation necessary for auditors to verify their accuracy. The inconsistencies across transparency mechanisms demonstrate that the current framework, despite its ambitious scope, fails to create the accountability system needed to avoid selective disclosure.

These issues point to the need for structural changes that would strengthen the connections between the DSA's various transparency tools. The verification difficulties identified by auditors cannot be addressed through stricter enforcement alone. Rather, they require rethinking how different transparency mechanisms interact. The next section examines specific improvements that could enhance the verification framework.

IV. Enhancing the Verification Framework

Despite the DSA's ambition to transform platform accountability through transparency requirements, the first round of audits demonstrates that platforms continue to provide inconsistent information across different transparency mechanisms without facing meaningful consequences. This section proposes specific improvements to strengthen the connections between the DSA's parallel transparency mechanisms and transform them from isolated compliance requirements into a verification system. These recommendations focus on three complementary approaches: improving the auditing process itself, bridging the disconnect between transparency reports and the Database of Statements of Reasons, and leveraging the Database's potential to fill the verification gap for platforms not subject to auditing requirements. Together, these improvements would

address the systemic weaknesses identified in previous sections while creating a more effective framework for ensuring the reliability of platform transparency.

A. Improving Auditing Requirements

The first round of DSA audits represents a significant step towards addressing the reliability problem for VLOPs and VLOSEs, yet their full potential remains unrealized due to fundamental weaknesses in the current auditing framework. The limitations discussed in Section II and their manifestation shown in Section III reveal a critical design flaw: the absence of established assessment criteria allows platforms to define their own standards for compliance, with auditors left to develop methodologies around these platform-defined benchmarks.

This approach effectively enables platforms to provide the answer against which their performance is assessed.[153] The flexibility left to auditors and platforms in the DRA perpetuates the ineffectiveness of transparency practices by enabling platforms to main their selective approach while still complying with audit requirements. The widely varying audit methodologies across platforms and the inconsistent treatment of similar transparency obligations demonstrate how this approach undermines rather than enhances accountability.[154] This pattern of inconsistency across platforms proves that the current framework partially fails to establish the oversight needed to ensure meaningful transparency.

Developing standardized auditing methodologies and criteria through a multi-stakeholder process would address these challenges. Unlike the current approach, standardization would establish clear benchmarks against which platforms' transparency disclosures could be measured and compared. This approach aligns with established practices in financial and environmental auditing where regulators provide the assessment

[153] Pielemeier, et al., *supra* note 71.

[154] The audit findings analyzed in Section III demonstrate this problem across multiple platforms, with issues ranging from insufficient documentation at LinkedIn to deliberate resistance to verification at X.

standards. Having uniform benchmarks would also enable the Commission to conduct meaningful cross-comparisons of audit reports across platforms, allowing for evaluation of compliance patterns and identification of issues across the board.[155] Such comparative analysis is currently particularly challenging given the fragmented methodologies and platform-specific criteria used in the first round of reports.[156]

Additionally, the "reasonable assurance" standard in the DRA could be further clarified. At present, auditors are required to affirmatively state that information is materially correct, without having specific guidance for what "materially correct" means in the context of platform compliance.[157] This vagueness coupled with the lack of agreed upon benchmarks makes it particularly challenging to assess complex platform systems. The audit reports analyzed in Section III reflect this difficulty, with multiple auditors issuing disclaimers of opinion due to insufficient evidence or uncertainty about verification standards.[158]

Beyond procedural clarifications, technical improvements to platforms' internal documentation and control systems are also needed for addressing the reliability problem. The first audits revealed widespread difficulties in platforms' ability to trace and verify the information in their transparency reports.[159] As shown in Section III, even platforms assessed as "compliant" often lacked systems to ensure consistency across their transparency mechanisms.[160] Platforms should be required to implement standardized record-keeping practices and

---

[155] Magdalena Jóźwiak, *The Wait is (almost) over! First risk assessment and audit reports – what will be published, when, and the way forward*, DSA Observatory (Nov. 22, 2024), https://dsa-observatory.eu/2024/11/22/the-wait-is-almost-over-first-risk-assessment-and-audit-reports-what-will-be-published-when-and-the-way-forward/.

[156] Bhatia & Allen, *supra* note 67; Morandini, *supra* note 63.

[157] Pielemeier, et al., *supra* note 71; Morandini, *supra* note 63.

[158] *See* Section III.C. LinkedIn's auditors, for instance, could not reach a conclusion on transparency compliance due to "insufficient controls or processes over the preparation of that information and underlying systems."

[159] *See* Section III.

[160] *See* Section III.C.

develop systems specifically designed to verify the consistency between statements of reasons submitted to the Database and aggregated statistics in transparency reports.[161] Such systems would directly address the cross-mechanism verification failures discussed in Section II.

These improvements would transform the DSA auditing framework from a set of inconsistent methodologies and platform-defined benchmarks into a more effective verification system that meaningfully addresses the reliability problem in platform transparency.

B. Bridging Transparency Mechanisms

The Digital Services Act's transparency framework suffers from a fundamental disconnect between its parallel mechanisms: transparency reports and the Database of Statements of Reasons. This disconnection perpetuates the weaknesses of platform transparency. Despite mandating comprehensive disclosure requirements, the DSA does not establish systematic connections between these transparency tools, allowing platforms to technically comply with each obligation while presenting inconsistent information across different mechanisms.

The first round of DSA audits confirms this disconnect. While auditors assessed compliance with individual transparency requirements, they rarely evaluated consistency across parallel reporting mechanisms. Most audit reports focused narrowly on whether platforms published transparency reports and submitted statements of reasons without systematically examining whether the information in these disclosures aligned. This siloed approach to verification fails to address the reliability problem, as platforms can present contradictory information across different transparency mechanisms without triggering compliance concerns.

To transform the DSA's transparency framework from disconnected disclosure requirements into an integrated verification system, three specific improvements are

[161] Zornetta, DSA Database, *supra* note 13.

necessary. First, the EU Commission should establish mandatory cross-reference documentation requirements.[162] Platforms should be required to explain in their transparency reports how their aggregate statistics correspond to the individual moderation decisions documented in their Database submissions. This documentation should identify the specific categories and measurement methodologies used to generate aggregated figures, enabling verification of whether the statistics presented in transparency reports accurately reflect underlying individual decisions.

The audit findings underscore the urgency of this requirement. For instance, Zalando's auditors discovered that "by applying the determined methodologies on the data sets provided, [they] derived differing numbers than those that were published in the transparency report," resulting in an "incorrect representation in the published transparency report."[163] Even LinkedIn's auditors couldn't form a conclusion about compliance because "there was no documented inventory/listing of all of the steps that take place before the information is ready to be used in the Transparency Reports nor that of the relevant systems that are relied upon in producing the Transparency Reports."[164] These examples demonstrate how the absence of cross-reference documentation undermines the verification potential of the DSA's parallel transparency mechanisms.

Second, auditors should be explicitly required to verify consistency between transparency reports and Database submissions as part of their assessment.[165] The current DRA provides minimal guidance on cross-mechanism verification, allowing auditors to evaluate each transparency mechanism in isolation. Future iterations should include specific requirements for auditors to examine whether platforms' Database submissions substantiate their

[162] *Id.*

[163] Deloitte Zalando Report, *supra* note 126, at 69–70.

[164] Deloitte Linkedin Report, *supra* note 127, at 70-71.

[165] Zornetta, *DSA Database*, *supra* note 13; Trujillo, et al., *supra* note 42 (identifying discrepancies between platforms' transparency reports and their Database submissions that remained unaddressed in audit reports).

transparency report claims and to identify any material discrepancies between parallel transparency mechanisms. This verification should extend beyond simply confirming the existence of disclosures to evaluating their substantive consistency and accuracy across mechanisms.

These improvements would fundamentally transform the relationship between the DSA's transparency mechanisms. Rather than functioning as separate compliance requirements, transparency reports and the Database would become complementary verification tools that enable systematic authentication of platforms' claims. By creating clear connections between individual decisions and aggregate statistics, this integrated approach would strengthen the reliability of platform transparency while providing regulators, researchers, and the public with more accurate information about content moderation practices.

The absence of such integration in the current framework represents a significant missed opportunity in the DSA's approach to platform accountability. As the European Commission continues refining the DSA's implementation through delegated acts and enforcement actions, addressing this disconnect should be a priority for enhancing the effectiveness of the regulatory framework. Without systematic bridges between transparency mechanisms, the reliability problem will remain even in a highly regulated environment, limiting the transformative potential of the DSA's transparency provisions.

C. *Beyond VLOPs*

While the DSA establishes comprehensive auditing requirements for VLOPs and VLOSEs, the vast majority of online platforms fall outside this enhanced oversight framework. This creates a significant gap, as several platforms must comply with transparency requirements without being subject to independent audits. The Database of Statements of Reasons offers a potential solution to this gap, presenting an opportunity to establish automated verification capabilities for platforms of all sizes.

Non-VLOPs face the same fundamental transparency

reliability challenges as their larger counterparts but without the external verification that audits provide. The audit findings discussed in previous sections identified significant compliance issues even among heavily scrutinized VLOPs, suggesting that reliability concerns may be even more acute among platforms with fewer resources and less regulatory attention. When platforms subject to rigorous auditing requirements show material discrepancies in their transparency reporting, it raises concerns about the reliability of disclosures from platforms operating with reduced oversight.

The Database could serve as an automated verification tool for platforms of all sizes if properly integrated with transparency reporting requirements. By enabling systematic cross-referencing between aggregate statistics in transparency reports and individual decisions documented in the Database, regulators could identify discrepancies without requiring resource-intensive audits. This approach would be particularly valuable for non-VLOPs, which collectively moderate vast amounts of content but individually lack the scale that would trigger auditing requirements under the DSA.

For example, if a medium-sized platform reports in its transparency disclosure that it removed 10,000 instances of hate speech content during a reporting period, with 80% detected through automated means, these claims could be automatically verified by querying the Database for entries from that platform categorized as "illegal or harmful speech" and filtered by "automated detection: yes." Such a verification mechanism would quickly identify cases where the number of Database entries significantly differs from the reported aggregate statistics, flagging potential accuracy issues for further investigation.

Similarly, if a platform reports that it primarily restricts violating content through content removal rather than demotion, regulators could verify this claim by analyzing the distribution of "decision visibility" values in the platform's Database entries. A predominance of "content removal" entries would confirm the platform's claim, while

a significant number of "demotion" entries would raise questions about the correctness of its transparency reporting.

Several specific improvements would be necessary to realize this potential. First, standardized mapping between platforms' internal content categories and Database classifications would facilitate automated verification of content moderation statistics. When platforms report removing specific amounts of content in particular violation categories, these claims could be automatically verified against the corresponding Database entries. Second, introducing mandatory cross-reference documentation in transparency reports would create clear connections between aggregated statistics and Database entries. Platforms would need to explain any numerical discrepancies between their Database submissions and transparency reports, addressing variations stemming from technical limitations, counting methodologies, or other factors.

The case of X highlights the importance of such cross-verification even for platforms subject to audits. Despite being found in full compliance with Article 24.5, X's transparency report disclosed 19,828 actions taken through automated content moderation for terms of service violations while the Database contained no statements of reasons where X reported using automated means.[166] This evident discrepancy went unaddressed in the audit, potentially highlighting how even audit processes may miss inconsistencies that could be systematically identified through automated cross-verification.

For smaller platforms with more limited resources, the Database could provide an automated compliance option. If properly structured, the Database could allow non-VLOPs to generate their transparency reports directly from their Database submissions, ensuring consistency between individual statements of reasons and aggregated statistics. This approach would not only reduce compliance

[166] *See* Section III.C.2; *see also* Zornetta, *DSA Database*, *supra* note 13; Trujillo, et al., *supra* note 42; Papaevangelou & Votta, *supra* note 144.

burdens but also guarantee alignment between different transparency mechanisms, addressing the reliability problem.

Digital Services Coordinators (DSCs), tasked with overseeing DSA compliance, could also benefit from this approach. By using automated cross-verification between transparency reports and Database entries, DSCs could efficiently identify platforms with significant reporting discrepancies, focusing their limited resources on cases where reliability problems appear most significant. For example, a DSC could implement automated checks to flag platforms whose Database entries show patterns inconsistent with their transparency reporting, such as claiming minimal use of automated detection while Database entries indicate widespread automation. This mechanism would enhance the effectiveness of DSA enforcement while recognizing the resource constraints of overseeing thousands of platforms across the European Union.

The current implementation of the DSA misses this opportunity by treating the Database primarily as a documentation repository rather than a verification tool. Transforming the Database from an isolated compliance requirement into an integrated verification mechanism would address the reliability gap for non-VLOPs while strengthening the overall effectiveness of the DSA's transparency framework.

Conclusion

The Digital Services Act's framework for addressing the reliability problem in platform transparency establishes important verification mechanisms but remains fundamentally incomplete. As demonstrated through analysis of the first nineteen audit reports, VLOPs and VLOSEs continue to provide inconsistent and sometimes inaccurate information across different transparency mechanisms despite facing independent audits. These findings confirm that mandatory transparency obligations

alone, without effective verification systems, cannot solve the longstanding challenges of platform accountability.

Three key limitations prevent the DSA from fully addressing the reliability problem. First, the auditing framework lacks standardized methodologies and assessment criteria, allowing platforms to effectively define their own benchmarks for compliance. Second, the disconnection between transparency reports and the Database of Statements of Reasons creates opportunities for platforms to present contradictory information across parallel disclosure requirements without consequences. Third, the asymmetric application of verification mechanisms leaves thousands of non-VLOP platforms subject to transparency obligations without independent verification, perpetuating reliability issues across much of the digital services landscape.

Transforming the DSA's transparency framework from disconnected requirements into a cohesive accountability system requires specific improvements. Standardizing auditing methodologies through multi-stakeholder processes would prevent platforms from defining their own compliance standards. Establishing mandatory cross-reference documentation between transparency reports and Database submissions would create automated processes for verifying platforms' claims. Most importantly, enhancing the Database's verification tools would address the reliability gap for platforms not subject to auditing requirements, creating a more comprehensive framework for platform accountability.

The DSA's approach to platform transparency represents a significant advancement compared to previous regulatory frameworks, particularly through its combination of mandatory reporting, granular documentation, and independent verification. However, its siloed implementation prevents it from fully realizing the potential of this multi-layered approach. Strengthening the connections between parallel transparency mechanisms can enable the DSA to effectively address the fundamental reliability problem and facilitate meaningful oversight of

platform governance.