Supervision of Digital Services: Large Online Platforms versus Smaller Services

A Risk Assessment Framework for Intermediary Services under the DSA

August 2026

Digital Services Supervision
do@rpms.sk

Council for Media Services
Palisády 36
811 06 Bratislava
Slovakia

Supervision of Digital Services: Large Online Platforms versus Smaller Services

A Risk Assessment Framework for Intermediary Services under the DSA

Under the Digital Services Act, obligations placed on regulated services scale primarily with their economic size and user volume, focusing attention on Very Large Online Platforms. However, from a national enforcement perspective, reliance on such indicators alone risks overlooking services with limited user bases but significant risk factors. To address this gap, we propose an operational framework aiming to support supervisory prioritization under limited regulatory capacity and without access to platform-side data. We construct a scalable composite risk index that evaluates intermediary services across two dimensions: traffic and design-and-content risk. Applied to the Slovak national market dataset, the framework reveals a weak association between the dimensions, indicating that low-traffic services can exhibit relatively high risk driven by design- and content-related factors. By demonstrating how national authorities can systematically profile and prioritize services, the paper provides a decision-support framework for proportionate, evidence- and risk-based enforcement. The paper was presented at the DSA Platform and Regulation Conference 2026 held by the DSA Observatory at the Amsterdam Law School.

#DIGITAL SERVICES ACT

#RISK ASSESSMENT

#COMPOSITE INDICATOR

#DIGITAL REGULATION

#NATIONAL ENFORCEMENT

Table of Contents

I. Introduction

The Digital Services Act (DSA), Regulation (EU) 2022/2065, introduces a comprehensive regulatory framework for intermediary services in the European Union. Much of the scholarly and policy debate concerning the risks associated with intermediary services has focused on very large online platforms and very large online search engines (VLOPSEs), reflecting both their perceived systemic importance (Efroni 2021) and the additional risk-assessment and risk-mitigation obligations imposed on them under Articles 34 and 35 of the DSA. However, the DSA's regulatory framework extends beyond VLOPs and VLOSEs to other intermediary services, including hosting services and smaller online platforms.

The main goal of this paper is to introduce a framework for a data-driven, risk-based prioritisation tool that enables comparison within a given dataset of intermediary services falling under the scope of the DSA. Since the societal impact of such services varies significantly — a recipe blog and an adult content platform being clear extremes — we introduce a risk index, a composite indicator that assigns each service a level of potential risk. This enables a consistent ranking of services according to their potential negative societal impact and supports the Digital Services Coordinator (DSC) in prioritizing supervisory activities and allocating regulatory +resources efficiently. This is grounded in Article 50 of the DSA, which lays out the requirement for DSCs to perform their tasks in an impartial, transparent, and timely manner, including adequately supervising all providers of intermediary services falling within their competence. Ultimately, the proposed framework offers insights into how national-level implementation can complement and extend EU-level oversight, while opening further research questions.

As the proposed framework is applicable to datasets of intermediary services, we apply it at the Slovak national level. It relies on a dataset of intermediary services compiled through a market mapping initiated by the Slovak DSC (Council for Media Services, CMS) in spring 2025 and refined throughout the year, with primary data collection executed in Q3 and Q4 of 2025.

This paper is structured as follows. First, in *Section II,* we present the theoretical background and conceptual foundations of the risk index and its two dimensions. In *Section III,* we then turn to the design of the framework, where these theoretical concepts are operationalized into a data-driven tool based on measurable variables. Next, we present the main results of applying the framework to the Slovak dataset. Finally, we conclude by discussing the key takeaways in *Section V*.

II. Conceptual Background

For the purpose of this framework, a risk can be understood broadly as "adverse events that may occur in the future" (Baldwin & Black 2016, p. 566). The value of measuring such risk lies in its capacity to make uncertain and potentially harmful future developments more intelligible, comparable, and actionable for regulatory decision-making. Risk assessments are conducted to understand and characterize risk and in this way support decision-making on the choice of alternatives and measures. This is particularly relevant in the context of intermediary services under the DSA, where regulatory attention and enforcement resources must often be allocated across different types of intermediary services. A risk index can therefore function not as a substitute for legal assessment, but as a structured, evidence-based method for identifying, comparing, and prioritizing services that may warrant closer regulatory scrutiny (OECD 2018, p. 7).

Prioritization frameworks based on risk are implemented throughout diverse domain-specific models, as mentioned by Scheuerman et al. (2021, p. 6). Examples include law-enforcement triage, where tasks are prioritized according to strict risk hierarchies focused on immediate danger to human life rather than on a "first come, first served" basis. A further example is mental-health triage, where severity is assessed by reference to the duration, frequency, and physical threat posed by symptoms or behaviours.

A classical quantitative approach to measuring risk can be found in Kaplan and Garrick (1981, p. 11). The authors frame risk as a "set of triplets" that identifies scenarios, their probability, and their resulting consequences. This definition aligns with comprehensive risk assessment frameworks, such as the ISO 31000:2018 standard, which provides a generalized international framework for managing risks internally across any organization, regardless of the sector (ISO 2018). This approach is also reflected in EU digital legislation beyond the DSA, notably in Article 3(2) of the Artificial Intelligence Act, Regulation (EU) 2024/1689, which defines “risk” as “the combination of the probability of an occurrence of harm and the severity of that harm.”

Current risk assessment frameworks utilised by legislators in the field of digital safety, such as the European Union’s DSA, or those implemented by the UK’s Ofcom (2024) and the Australian eSafety Commissioner (2024), rely on internal risk assessments performed by service providers. Under Articles 34 and 35 of the DSA, systemic risk assessment and mitigation obligations for VLOPSEs are predicated on this internal model, subject to direct oversight by the European Commission. These methodologies rely on providers’ access to detailed internal data and complete analytics, including moderation outputs, internal safety documentation, and specific user behaviour metrics that are not available to the public.

The methodology presented in this paper, in contrast, is designed as an external risk assessment conducted by a third party, i.e. a DSC. This framework differs from the models mentioned above as it relies exclusively on publicly available data to capture and quantify

the risks posed by intermediary services. For such an external approach to be valid, it must be effective, objective, and replicable, ensuring that regulatory oversight remains robust despite the lack of access to internal data.

Within the proposed framework, the overall level of risk associated with each service is captured by a composite indicator called the risk index, built according to OECD's *Handbook on Constructing Composite Indicators* (2008). The risk index considers two dimensions — *traffic* and *design & content* (see *Table 1*), and it is defined as a combination of indicators representing these dimensions (see *Section III*).

Table 1. Overview of the conceptual approach to constructing the risk index (Source: CMS)

Traffic		**Design & Content**
How many users, how often, or for how long do they use the service?	vs.	What risk factors arising from the design and content do the users encounter while using the service?

We note that the proposed dimensions do not account for the economic strength of intermediary service providers. This is a deliberate methodological choice, reflecting the logic of the DSA. The Regulation already differentiates between categories of providers by imposing distinct tiers of obligations according to their role, scale, and economic significance. However, designation as a VLOPSE is not contingent on the economic size of the provider. Accordingly, even micro and small enterprises, within the meaning of Articles 2 and 3 of the Commission Recommendation 2003/361/EC, which may otherwise be exempt from certain obligations, are not excluded from designation as a VLOPSE. Once designated, such providers are subject to the full scope of VLOPSE obligations, including the systemic risk assessment and mitigation obligations laid down in DSA Articles 34 and 35.

1. Risk Index Dimension: *Traffic*

In this framework, we chose to use *traffic* as one dimension of the risk index, assuming that greater service traffic increases the probability that a user is exposed to design features or content with a potentially negative impact, and that services attracting more users are more likely to expose a larger number of individuals to negative consequences linked to harmful interface design or content-related factors. Moreover, existing research indicates that exposure to harmful online content or online threats is associated with a range of adverse offline behaviour (Branley & Covey 2017, p. 283). *Traffic* is therefore a proxy measure intended to capture the likelihood of a service's potential negative impact on society.

The DSA itself reflects the assumption that platform reach is relevant to risk, insofar as it reserves the full set of obligations, including risk assessment and mitigation obligations, for services with the number of average monthly active recipients exceeding 45 million,

which is equivalent to 10% of the European Union population. However, the relationship between a service's traffic and its overall level of risk remains insufficiently explored and requires further empirical analysis. It remains an open question whether, in terms of societal impact, traffic alone can determine a service's overall level of risk.

Website traffic, however, is generally difficult to measure accurately (Prantl & Prantl 2018), especially without access to provider-side data. In principle, traffic can be estimated based on the number of responses exchanged between a server and a client, but the decentralised nature of the internet makes access to such data inherently difficult (Jansen et al. 2022). Measurement is further complicated by the inconsistent definition and lack of standardisation of the metrics being tracked, which reduces accuracy even further. Article 33(3) of the DSA empowers the Commission to adopt delegated acts laying down the methodology for calculating the number of average monthly active recipients of the service in the Union. As of July 2026, no delegated act laying down that methodology had been adopted. In the absence of such an act, the Commission has provided non-binding guidance on the identification and counting of active recipients (European Commission 2023).

2. Risk Index Dimension: *Design & Content*

The second risk index dimension aims to capture the risks related to a service's design and intended content focus. This approach is based on the review-level research suggesting that risk assessment frameworks should take into account multiple dimensions beyond mere traffic or exposure metrics. For example, the theoretical framework for assessing the severity of harmful online content proposed by Scheuerman et. al. (2021) identifies nine dimensions relevant to evaluating the potential impact of content, only one of which relates to scale, while others include factors such as urgency, vulnerability, medium, or the sphere in which harm occurs. Recent research also suggests that the effects of social media use on the well-being of adolescents depend not only on the extent of use, but also on the services' content and design (Sala et al. 2024). Recent policy-oriented research published by the Institute for Strategic Dialogue (Katzy-Reinshagen et al. 2026) on systemic risks under the DSA similarly proposes that risk assessments should account for factors such as content moderation practices, recommender systems, and content-dynamics metrics, in addition to scale-based indicators.

Under Article 34 of the DSA, providers of VLOPSEs are required to carry out annual assessments of systemic risks across four categories: the dissemination of illegal content, negative impacts on fundamental rights, adverse effects on democratic processes and public security, and risks to public health and well-being. While this categorization has faced criticism (Griffin 2025), the regulatory framework also identifies examples of contributing risk factors, such as the design of recommender systems, content moderation practices, advertising selection systems, and the enforcement of terms and conditions. Furthermore, the first and second report of the European Board for Digital Services (2025, 2026),

issued pursuant to Article 35(2), identify additional recurrent risk factors, including monetisation policies.

The proposed framework builds on this logic by identifying a broader set of risk factors applicable to the wider intermediary services landscape, including providers operating below the VLOPSE designation thresholds. These factors form the basis for measuring the *design & content* dimension of the risk index (see *Section III*).

III. Framework Design: Risk Index

In this section, we describe the basis for the prioritization — a composite indicator called risk index, calculated for each service. The construction of the risk index follows the methodology outlined in OECD's *Handbook on Constructing Composite Indicators* (2008).

The risk index is constructed from indicators representing the dimensions *traffic* and *design & content*, with weights w_1 and w_2, respectively (see *Figure 1*). We apply geometric aggregation to combine the two dimensions. In contrast to arithmetic aggregation, geometric aggregation assigns higher risk index values to services with balanced risk levels across both dimensions, since the index increases most when both dimensions are simultaneously high. This reflects the assumption that risk arises from the interaction between traffic-related metrics and service-design characteristics, rather than from either dimension alone.

$$\text{Risk index} = \text{traffic}^{w_1} \times \text{design \& content}^{w_2}$$

$$\text{traffic}, \text{design \& content} \in [1,2]$$

$$w_1 + w_2 = 1 \qquad w_1, w_2 \geq 0$$

Figure 1. Risk index structure (Source: CMS)

Based on the categories defined in the DSA, the framework distinguishes between the following service categories and assigns each service to one of them:

- *Mere conduit* as defined in Article 3(g)(i) DSA;
- *Caching* as defined in Article 3(g)(ii) DSA;
- *Hosting* as defined in Article 3(g)(iii) DSA, that does not fall within the subcategory of online platforms defined below;
- *Online platform* as defined in Article 3(i) DSA, that does not fall within the subcategory of *online platform — marketplace* defined below;

- *Online platform — ancillary feature*, which means a hosting service that would otherwise qualify as an online platform pursuant to Recital 13 DSA, i.e. the dissemination to the public constitutes only a minor and purely ancillary feature of another service, or a minor functionality of the principal service, which cannot be used independently;
- *Online platform — marketplace*, by which is understood an online platform allowing consumers to conclude distance contracts with traders as defined in Article 3(l) DSA.

1. *Traffic* Indicator Selection

Traffic- and exposure-related metrics can be defined in various ways, including by reference to the number of unique users, the number of visits, or the amount of time users spend on an online service. In this framework, traffic was measured using Similarweb.com, which provides data on both monthly visits and monthly users. However, because monthly user data were unavailable for a substantial number of services, the *average monthly number of visits* per service URL was selected as the indicator representing the *traffic* dimension.

a. Key Limitations

Compared to the preferred indicator *of average monthly number of users*, the *average monthly number of visits* represents a qualitatively different measure, as visits do not correspond to unique users. Individual users may generate multiple visits, resulting in substantial disparities between the most and least visited services and consequently producing a highly skewed distribution.

Additionally, Similarweb relies on the triangulation of multiple data sources, which should, in principle, produce more accurate estimates than reliance on a single source. Nevertheless, the traffic data used in this framework should be understood as an approximation. This is due both to the broader measurement problems described in section *Risk Index Dimension: Traffic*, and to the fact that Similarweb does not disclose its methodology in full detail. As a result, it is currently not possible to estimate website traffic with full accuracy.

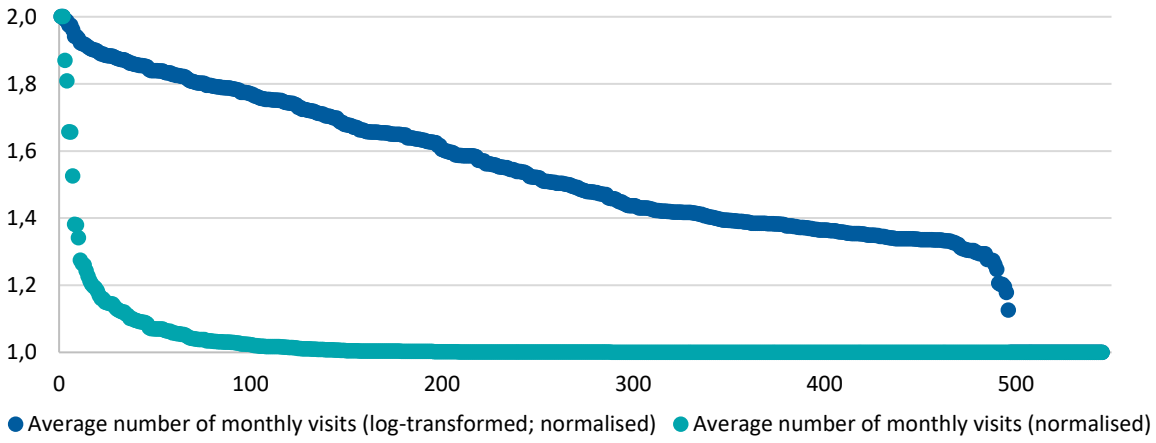
Furthermore, the number of visits obtained through Similarweb is particularly limited as a proxy for service traffic in the categories of *mere conduit* and *caching* intermediary services. Users of such services may not visit the service's website, while website visitors may not necessarily use the underlying intermediary service. Accordingly, the number of website visits does not necessarily correspond to the number of users. Nevertheless, we assume that services with higher website-visit volumes are likely to be used by a larger number of people than services with lower website-visit volumes. Therefore, despite its limitations, the average number of website visits was used as a proxy measure for these categories of services.

Another limitation is that Similarweb does not account for mobile app users, which may create a significant measurement gap for some service categories.

b. Methodological Adjustments

The use of data on average monthly visits requires a methodological adjustment, since visit-based traffic data may amplify differences between services with different levels of repeat use and produce substantial disparities between the most and least visited services. In the dataset, this results in a highly skewed, long-tail distribution (see *Graph 1*).

For this reason, the average monthly visits indicator is log-transformed prior to normalisation. The purpose of this transformation is to reduce the influence of extreme values arising from the visit-based metric and to enhance comparability across services, while preserving their relative ordering. The transformed indicator is then normalised by rescaling it to the interval [1, 2] for the purposes of constructing the risk index. For services lacking Similarweb traffic data, missing values are imputed using the minimum value of the normalised scale.



Graph 1. Long-tail distribution of average monthly visits and the effect of log transformation (Source: CMS, 2025)

2. *Design & Content* Indicator Selection

Unlike the *traffic* risk index dimension, which is represented by a single indicator, the *design & content* dimension is measured with a dedicated composite indicator. For the purpose of this framework, risk factors are defined as the design- and content-focus-related features and attributes of a service that may influence the types of risks present on that service. To ensure the replicability of the framework, the risk factors were selected based on the following key considerations, which also define their inherent limitations:

- **Data availability** — Unlike internal assessments conducted by services using detailed operational data, the risk factors in our framework are assessed externally and therefore rely on publicly available data.
- **Efficiency** — The data collection process is designed to be time-efficient.
- **Objectivity** — Manual data collection is structured to produce relatively objective results and to minimise assessor bias.
- **Adaptability** — The framework is designed to be applicable across different datasets, including at the Member State market level.

To ensure data availability and process efficiency, all risk factors are defined as binary indicators and therefore share the same measurement unit, taking values of either 0 or 1.

The selected risk factors are organized into four groups:

1. *Financial and Business Aspects;*
2. *Content Format and How It Is Shared;*
3. *Risk Mitigation Mechanisms;*
4. *Content Focus.*

1. Financial and Business Aspects

The first group comprises three risk factors: *presence of financial transactions, user content monetisation,* and *presence of dark patterns* (see *Table 2*). The associated risk of harm to consumer protection is also classified as a systemic risk under the DSA, as detailed in Recital 81 and Article 34(1)(b). We note that this group also covers the key objectives of the Digital Fairness Act (European Commission 2025), the proposed legislation designed to protect consumers in the digital environment. Specifically, its objectives include tackling unethical techniques and commercial practices related to financial transactions through regulations on unfair marketing related to pricing and issues with digital contracts, user content monetisation regarding the disclosure of commercial influencer marketing, and the presence of dark patterns used to manipulate or deceive consumers.

Table 2. Risk factors, data collection methodology, and identified risk types within the Financial and Business Aspects group (Source: CMS)

Risk factor	Data collection methodology		Risk types
Presence of financial transactions	Does the use of the service potentially involve financial transactions between users, for example marketplaces, classifieds for goods and services, real estate listings, dating services, or between the user and the service, where such transactions relate primarily to user content, for example in-app purchases or purchases of virtual items?	Yes = 1; No = 0	Risk of financial loss; risk of fraud, such as misuse of payment data; increased risk for minors and vulnerable groups.
User content monetisation	Does the service allow users to earn money directly from their own content by offering content monetization tools, for example tools for partner commissions, affiliate programmes for the influencer ecosystem, remuneration of content creators with credits or virtual currency, or subscriptions to user content?	Yes = 1; No = 0	Risk of financial loss; risk of user manipulation; risk to consumer protection, since rewarded user activities may constitute commercial communication that must be clearly labelled.
Presence of dark patterns	Does the service display dark patterns that may lead to user manipulation, i.e. design and interaction elements of the service that may manipulatively influence the user's decision-making, in accordance with Recital 67 and Article 25 DSA?	Yes = 1; No = 0	Risk of financial loss; risk of user manipulation; increased risk for minors and vulnerable groups.

2. Content Format and How It Is Shared

The second group, *Content Format and How It Is Shared*, contains four indicators: *interaction between users, images, videos, live streaming* (see *Table 3*). The *interaction between users* indicator includes both public and private forms of interaction, reflecting Scheuerman et al.'s (2021, pp. 23, 24) distinction between the spheres in which harm may occur. Similarly, the *images*, *video*, and *live streaming* indicators correspond with the eighth dimension from that same framework — the medium through which harmful content is disseminated (Scheuerman et al. 2021, p. 23). Within this dimension, the authors highlight the heightened underlying risks associated with visual and real-time content compared to traditional text-based formats.

Table 3. Risk factors, data collection methodology, and identified risk types within the Content Format and How It Is Shared group (Source: CMS)

Risk factor	Data collection methodology		Risk types
Interaction between users	Does the service allow communication between at least two arbitrary users, for example the ability to reply to comments, use chat, or the presence of a discussion section?	Yes = 1; No = 0	Increased risk for minors and vulnerable groups; private interaction — risk of isolation and vulnerability, bullying, harassment, and potentially stronger psychological impact if it takes place privately, as problems are more difficult to detect and address; public interaction — risk of reputational harm, social pressure, chilling effect, and a persistent digital footprint.
Images	Does the service allow users to add content in the form of images, either directly or by embedding?	Yes = 1; No = 0	Increased risk for minors and vulnerable groups; risk of stronger emotional harm compared with text, as images cannot be "unseen"; risk of sharing illegal visual content, for example child sexual abuse material, terrorist content, or memetic hate speech.
Videos	Does the service allow users to add content in the form of video, either directly or by embedding?	Yes = 1; No = 0	Increased risk for minors and vulnerable groups; risk of stronger emotional harm compared with text and images, as video also includes audio and motion, for example child sexual abuse material or terrorist content.

Live streaming	Does the service allow live video broadcasting through the service's native functionality? *Note: Services that allow users to view video by embedding are not included here, as the risk of this aspect is already covered by the "Videos" indicator.*	Yes = 1; No = 0	Increased risk for minors and vulnerable groups; risk of immediate emotional harm, i.e. awareness that harmful content is happening "here and now"; more difficult content moderation.

3. Risk Mitigation Mechanisms

The third risk factor group, *Risk Mitigation Mechanisms*, contains three indicators: *missing contact point*, *missing terms and conditions*, and *missing notice and action mechanism* (see *Table 4*). These indicators signal possible non-compliance with Articles 12, 14, and 16 of the DSA, respectively.

Table 4. Risk factors, data collection methodology, and identified risk types within the Risk Mitigation Mechanisms group (Source: CMS)

Risk factor	**Data collection methodology**		**Risk types**
Missing contact point	Is there no contact point indicated on the service's website in accordance with Recitals 42 and 43 DSA and Articles 11 and 12 DSA?	Yes = 1; No = 0	Possible non-compliance with Article 12 DSA; reduced availability of assistance in the event of harm to the user's rights; increased risk for minors; risk of communication exclusively through automated tools.
Missing terms and conditions	Are terms and conditions concerning user content, or the part of the service involving user content, missing from the service's website in accordance with Recitals 45 to 48 and Article 14 DSA?	Yes = 1; No = 0	Possible non-compliance with Article 14 DSA; lack of predictability and legal certainty; increased risk of unfair treatment by the provider; increased risk for minors; insufficient transparency of algorithmic decision-making.

Missing notice and action mechanism	Is there no notice and action mechanism on the service's website in accordance with Recitals 50 to 57 and Article 16 DSA?	Yes = 1; No = 0	Possible non-compliance with Article 16 DSA; risk of financial loss; reduced safety and protection against harmful conduct; increased risk for minors; insufficient ability to respond to violations of one's rights, for example in the case of copyright; increased risk of unfair treatment by the provider.

4. Content Focus

The final risk factor group, Content Focus, differs from the preceding groups because its indicators are not assessed directly at the level of each individual service. Instead, they are assessed through a preliminary classification of services according to their *technical and thematic purpose*. This classification was developed to capture the provider's intended content focus in a systematic and replicable manner (see *Table 5*).

Table 5. Examples of service classification by technical and thematic purpose (Source: CMS)

Service category	**Technical purpose**	**Thematic purpose**
Online platform — ancillary feature	Reviews	general; architecture; financial services and products; hobby (photography); hobby (gaming); hobby (hunting and guns); music; humour; lifestyle; maternity; property; recipes; sex; news reporting; betting; weddings; sport; education; health; auctions; travel; company directory; events; jobs; second-hand; healthcare services; dating; crowdfunding; taxi; tickets; discounts
	Discussion forum	
Online platform	Blog platform	
	Search engine	
	Listing service	
	Video sharing platform	
	Q&A service	
	Social network	
	Discussion forum	
Online platform — marketplace	Marketplace	

Note: The list of examples of technical and thematic purposes stems from the application of the framework to the dataset of intermediary services in Slovakia (see Section IV) and may therefore be expanded when applying the framework to a different set of services.

Note 2: The classification by technical and thematic purpose partially corresponds to Ofcom's (2024) risk profiles.

On the basis of this classification, the *Content Focus* risk factors are assessed at the level of *technical and thematic purpose*, rather than separately for each individual service. By assessing these broader purposes rather than individual instances, we can more effectively collect data that reflects the inherent risk profile of a service's functional design and topical orientation (see *Figure 2*).

Step 1: adding the *technical and thematic purpose*

Service name	Service category
service_1	Online platform
service_2	Online platform
service_3	Online platform - ancillary feature

1.1 →

Service name	Service category	Technical purpose
service_1	Online platform	Listing service
service_2	Online platform	Social network
service_3	Online platform - ancillary feature	Discussion forum

1.2 →

Service name	Service category	Technical and thematic purposes
service_1	Online platform	Listing service - financial services and products
service_2	Online platform	Social network - general
service_3	Online platform - ancillary feature	Discussion forum - maternity

Step 2: *Content Focus* indicator assessment

Technical and thematic purposes	Potentially problematic content	Health-related content	Political content	Financial content	Content risky for minors
Listing service - financial services and products	1	0	0	1	0
Social network - general	1	1	1	1	1
Discussion forum - maternity	1	1	0	0	0

Figure 2. A visualisation of the Content Focus risk factor group assessment process (Source: CMS)

The final risk factor group contains indicators for *potentially problematic content, financial content, political content, health-related content,* and *content risky for minors* (see *Table 6*). This group distinguishes between specific and general content intermediary services, where the content is accessible at the request of a recipient (i.e. *online platform — ancillary feature*, *online platform*, and *online platform — marketplace*). For example, it differentiates between a recipe blog and a general social network platform, or, drawing a finer line, between a gambling discussion forum and a discussion forum dedicated to photography hobbyists. Our framework operates on the hypothesis that services with either a general focus or a specific high-risk content focus (e.g., adult content) exhibit a higher likelihood of disseminating problematic or potentially illegal content to the public, with illegal content constituting the first category of systemic risks under the DSA (DSA, Recital 80; Art. 34(1)(a)). We acknowledge that these relationships are currently based on expert judgement and require further empirical research to determine whether, and under what conditions, causal links can be established.

Table 6. Risk factors, data collection methodology, and identified risk types within the Content Focus group (Source: CMS)

Risk factor	Data collection methodology		Risk types
Potentially problematic content	Does the *technical* and *thematic purpose* of the service imply a higher likelihood that potentially illegal content may be made publicly available through the service, i.e. content available at any time?	Yes = 1; No = 0	Emotionally charged or sensitive topics; risk of dissemination of illegal content and related negative impacts; increased risk for minors and vulnerable groups; risk of misuse of the service for criminal activity.
Financial content	Does the *technical* and *thematic purpose* of the service imply a higher likelihood of the presence of content focused on financial products (e.g., topics such as investing, cryptocurrencies, debt enforcement, or gambling)?	Yes = 1; No = 0	Emotionally charged or sensitive topics, for example economic anxiety and stress; risk of financial loss; risk of fraud.
Political content	Does the *technical* and *thematic purpose* of the service imply a higher likelihood of content focused on political topics such as elections, discussions about political parties, and political actors?	Yes = 1; No = 0	Emotionally charged or sensitive topics; risk of user and public-opinion manipulation; risk of threats to democratic and electoral processes; risk of increased polarisation and social tension.
Health-related content	Does the *technical* and *thematic purpose* of the service imply a higher likelihood of the presence of content that may have a negative impact on mental health, such as advice on physical health, mental health, sexual and reproductive health, guidance on treatments and medications, or advertising of healthcare services and facilities?	Yes = 1; No = 0	Emotionally charged or sensitive topics; increased risk for minors; risk of negative impact on users' health, for example the sale of unverified supplements, products or medicines, inappropriate advice, dietary advice, or non-professional treatment procedures.

Content risky for minors	Does the *technical* and *thematic purpose* of the service imply a higher likelihood of the presence of content risky for minors, such as services with a thematic focus on gaming or adult-oriented topics (i.e., content intended for users above a certain age, such as 15+ or 18+), including gambling and betting, pornography and sexual content, addictive substances such as alcohol, tobacco, or weapons?	Yes = 1; No = 0	Increased risk for minors; risk of privacy violations or inappropriate sharing of personal information; emotionally charged topics or the addictive nature of content; potential negative impact on mental health.

a. Applicability of *design & content* risk factors for service categories

Given the functional diversity of the intermediary service landscape, not all *design & content* risk factors are applicable to every service. For example, risk factors in the *Content Focus* group only apply to services that, at the request of a recipient of the service, store and disseminate information to the public (see *Table 7*).

Table 7. Applicability of design & content risk factors by service category. A = Applicable; N/A = Not applicable (Source: CMS)

Risk factor group	**Risk factor**	**Applicability for service categories**		
		Online platform; Online platform — marketplace; Online platform — ancillary feature	**Hosting**	**Cashing; Mere conduit**
Financial and Business Aspects	Presence of financial transactions	A	A	A
	User content monetisation	A	N/A	N/A
	Presence of dark patterns	A	A	N/A
Content Format and How It Is Shared	Interaction between users	A	N/A	N/A
	Images	A	N/A	N/A
	Videos	A	N/A	N/A
	Live streaming	A	N/A	N/A

Risk Mitigation Mechanisms	Missing contact point	A	A	A
	Missing terms and conditions	A	A	A
	Missing notice and action mechanism	A	A	N/A
Content Focus	Potentially problematic content	A	N/A	N/A
	Health-related content	A	N/A	N/A
	Political content	A	N/A	N/A
	Financial content	A	N/A	N/A
	Content risky for minors	A	N/A	N/A

b. Key Limitations

The limitations of the *design & content* composite indicator stem from the same methodological choices that make the framework replicable and scalable. In particular, the reliance on publicly available data, the use of manual data collection, and the prioritization of efficiency over granularity necessarily shape the scope and precision of the assessment.

First, unlike internal assessments conducted by services using proprietary operational data, this framework relies on publicly available information. This creates an inherent selection bias, as the framework is necessarily weighted toward risks that are visible from the outside. Consequently, several potentially significant risk factors were excluded because they could not be reliably captured as binary indicators without access to internal platform systems. This is particularly relevant for risk factors such as the design of recommender systems, which may require access to internal data or more resource-intensive auditing methods.

Second, the framework was applied and tested on the Slovak intermediary services market (see *Section IV*). While it is designed to be adaptable, applying it to different datasets or national markets may require adjustments to account for additional or less relevant risk factors.

Third, the data were collected manually, which introduces potential collection bias and subjective interpretation. To mitigate this, we used standardized definitions and data collection questions for each indicator.

Finally, the data collection process was intentionally designed to be time-efficient. This reflects a methodological choice in favor of breadth and scalability rather than depth and granularity. As a result, the framework may overlook risks that would only become visible through a more detailed, longitudinal audit of individual services.

c. Methodological Adjustments

To construct the *design & content* composite indicator, the following methodological adjustments were applied. First, where data could not be collected due to registration requirements or restricted access, missing values were imputed using the mean value calculated within the respective service category. In case of non-applicability (see *Table 7*), a value of 0 was assigned instead of N/A, as the associated risk is not expected to occur.

For the purposes of this analysis, all *design & content* risk factors were assigned equal weights, indicating no preference among them. However, if regulatory priorities so require, the weights assigned to specific *design & content* risk factors may be adjusted. For example, during a financial crisis, greater weight can be assigned to the *financial content* indicator, while in a pandemic, indicators related to *health content* can be prioritized. The nature of the harm, together with the vulnerability of certain user groups and public sensitivity, can thus serve as a key driver of risk prioritization (Baldwin & Black 2016, p. 580). Alternatively, weights may be derived from statistical methods that capture the underlying structure of the data, such as principal component analysis or factor analysis.

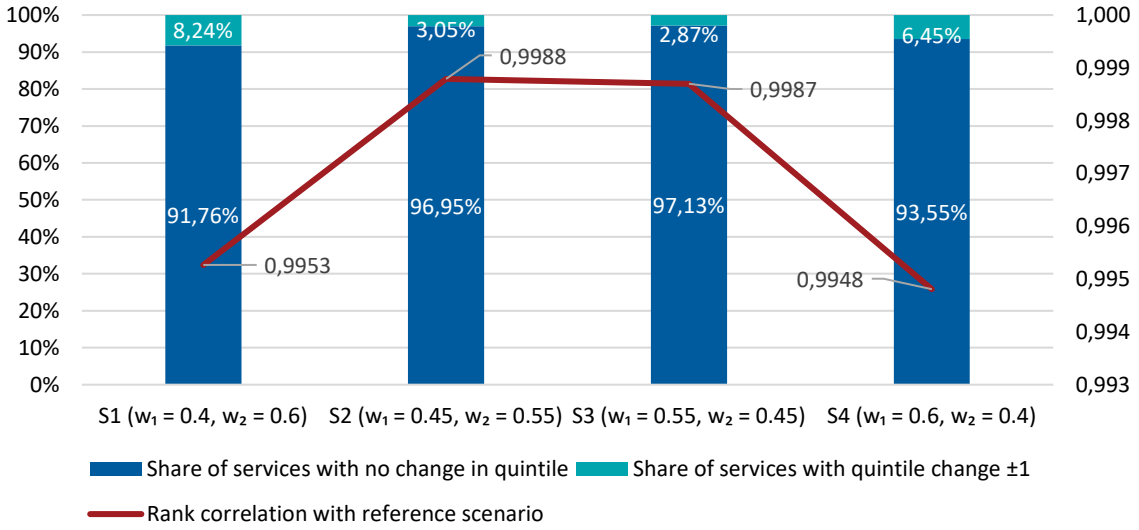
Lastly, linear aggregation was used to combine the design and content indicators into a single composite indicator representing the *design & content* dimension. The resulting composite indicator was then rescaled to the interval [1, 2] to ensure consistency.

3. Risk Index Robustness Check

The correlation analysis of *design & content* risk factors indicated predominantly low to moderate associations between the given binary risk factors, ranging from −0.29 to 0.75, which also supports the assumption that the variables capture distinct, albeit partially overlapping, factors of service-design and content-related risk. Negative correlations are generally weak and do not indicate systematic inverse relationships between indicators. Stronger correlations were observed mainly among variables in the *content focus* group, particularly *health-related, political*, and *financial content* (0.63–0.75). This likely reflects the structure of the classification: general-content services tend to score positively on several *Content Focus* indicators, whereas specialised services are more likely to score positively only on the indicator corresponding to their specific thematic focus. At the same time, most other correlations remained substantially lower, generally below 0.4, indicating limited redundancy across the broader set of indicators.

The robustness of the risk index was assessed through a sensitivity analysis of the dimension weights w_1 and w_2 defined in *Section III*. Four weight scenarios with uniform spacing were tested, with the reference scenario using equal weighting of $w_1 = w_2 = 0.5$. The stability of the results was evaluated by analysing correlations between risk index values and service rankings under the tested scenarios and by comparing the number of services that remained in the same risk quintile. The results confirmed low sensitivity to changes in

weights. More specifically, the risk index values and service rankings showed high correlations above 0.99 between the tested weight scenarios and the reference scenario. Most services also remained in the same risk index quintile across all weight scenarios. The share of services with no change in risk index quintile ranged from 91.76% to 97.13%, while a change of one quintile occurred in only 2.87% to 8.24% of services (see *Graph 2*). These results demonstrate high stability and robustness of the composite risk index with respect to variations in dimension weights.

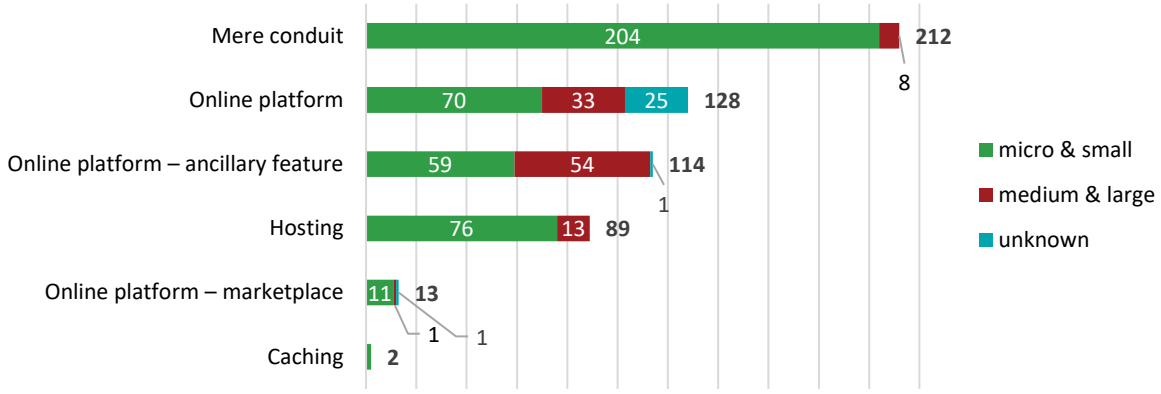


Graph 2. Sensitivity analysis of the risk index to changes in dimension weights (Source: CMS, 2025)

IV. Application of the Framework on the Slovak Intermediary Services Market

1. Intermediary Services in Slovakia

As of December 2025, the CMS has 558 active intermediary services provided by 455 entities with establishment in the Slovak Republic in evidence. Most of these providers qualify as micro or small enterprises within the meaning of Articles 2 and 3 of the Annex to Commission Recommendation 2003/361/EC. Hence, 75.63% of the intermediary services are subject to a limited scope of obligations, in accordance with Articles 15(2), 19, and 29 of the DSA. Moreover, almost half of the regulated services are in the *mere conduit* category, while only 2 services fall into the *caching* category. In terms of services that have full obligations stemming from Sections 3 and 4 of the DSA, only 34 such services are present in the dataset (see *Graph 3*).

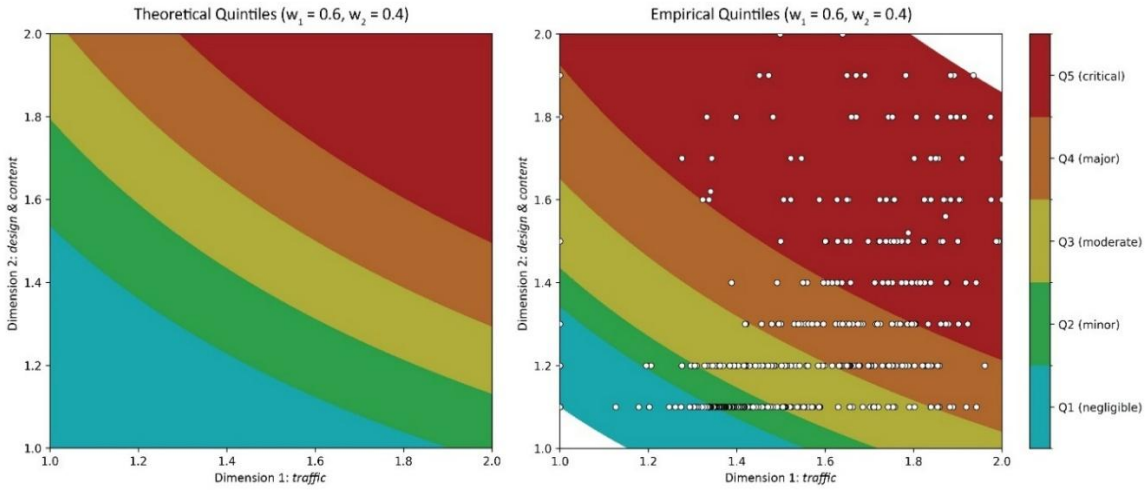


Graph 3. Structure of the Slovak intermediary services dataset by DSA category and provider size (Source: CMS, 2025)

2. Results and Discussion

The overall level of service risk, as expressed by the risk index and its two dimensions, is illustrated in the risk matrix (see *Graph 4, Empirical Quintiles*). The matrix classifies services into quintiles representing five risk levels: negligible, minor, moderate, major, and critical. Each point represents one service, while the background colour indicates the corresponding risk index quintile, ranging from Q1 (negligible, blue) to Q5 (critical, red).

Compared with the illustrative risk matrix based on a theoretical uniform distribution of dimension values, the empirical matrix shows that fewer intermediary services in Slovakia fall into areas combining high *design & content* scores with lower *traffic*. Many services are instead concentrated in the lower and middle regions of the matrix. This pattern is largely due to a substantial share of services classified as *mere conduits* (see *Graph 3*), for which only a limited number of *design & content* risk factors are applicable (see *Table 7*), resulting in lower scores on the *design & content* dimension. The spatial concentration of points highlights that services with high traffic often have low to medium *design & content* risk.

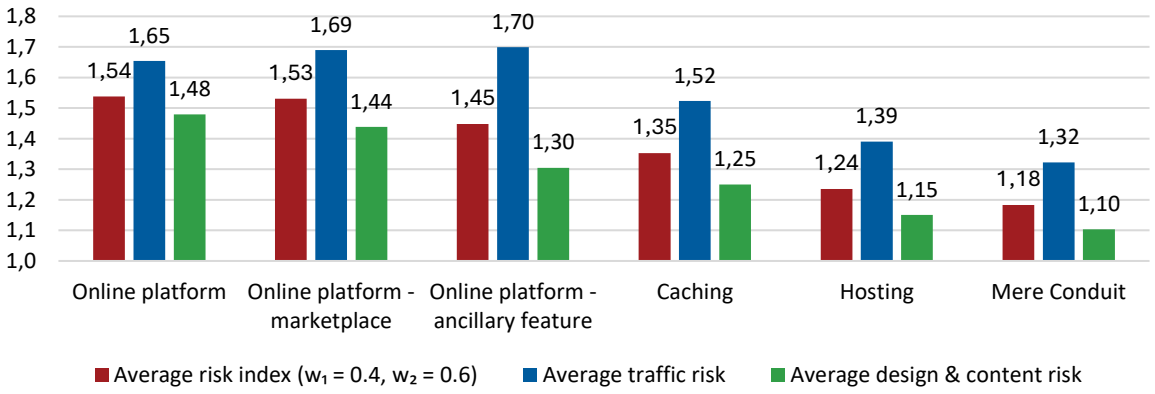


Graph 4. Theoretical and empirical risk index matrices for intermediary services in Slovakia (Source: CMS, 2025)

Note: The left panel shows quintiles based on a theoretical uniform distribution of dimension values, while the right panel shows empirical risk index values and quintiles.

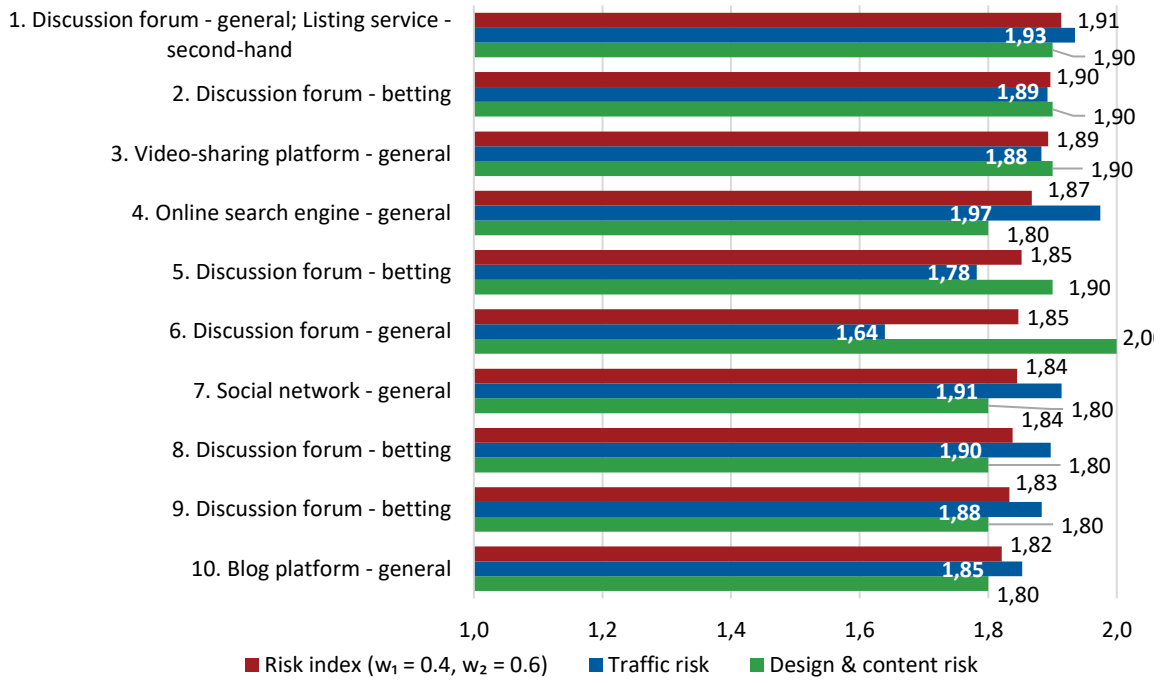
The correlation between the risk index dimensions was analyzed for 255 services for which all *design & content* risk factors were applicable (see *Table 7*). *Traffic*-related risk and *design & content*-related risk were found to be largely independent, with a Pearson correlation of r = 0.022 (t = 0.351, p = 0.726). When considering the rank ordering of services, a slight positive association emerges, though with a limited effect size, with the Spearman rank correlation of r = 0.136 (t = 2.179, p = 0.03), suggesting a weak but statistically significant association. This suggests that services with higher *traffic* may be marginally more likely to rank higher on *design & content* risk, but the relationship remains weak. These results indicate that the two dimensions capture largely distinct aspects of risk and that the observed rank-based association warrants further examination using additional datasets of intermediary services.

The combined risk index balances the two dimensions of *traffic* and *design & content*. On average, the categories *online platform* and *online platform — marketplace* exhibit the highest overall risk levels (1.53–1.54). By contrast, the *hosting* and *mere conduit* categories display the lowest overall risk levels (1.18–1.24), reflecting both lower *traffic* and *design & content* risk. *Caching* services exhibit slightly higher average risk levels (1.35), however, this category is represented by only two services in the dataset. Overall, the results indicate that *traffic* risk, measured as the log-transformed average monthly visits, tends to be higher than *design & content* risk across all service categories (see *Graph 5*).



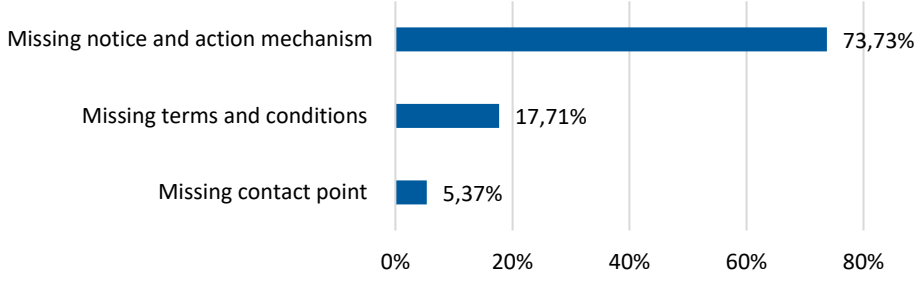
Graph 5. Average risk levels by service category and risk index dimension (Source: CMS, 2025)

The ten services with the highest risk index scores are all classified as *online platforms*. The maximum risk index observed is 1.91 for a service with both *discussion forum — general* and *listing service — second-hand* technical and thematic purposes, with the two risk index dimensions showing similarly high levels: *design & content* risk at 1.9 and *traffic* risk at 1.93. This indicates that this platform combines both extensive user exposure and potentially harmful design or content features, making it one of the highest-priority services from a regulatory perspective. The results also show that not all services in the top 10 list are equally risky across both dimensions. For example, number 6, a general discussion forum, exhibits a *design & content* risk of 2 and a *traffic* risk of 1.64, resulting in an overall risk index of 1.85 (see *Graph 6*).



Graph 6. Ten services with the highest risk index score, named by their technical and thematic purposes and rank (Source: CMS, 2025)

Besides the risk index calculations, the framework also enables more targeted analysis that may support regulatory and policy decisions. For example, the results relating to risk factor group *Risk Mitigation Mechanisms* provide insight into the extent to which intermediary services have implemented basic DSA-related compliance mechanisms. Although the assessment carried out within this framework does not have legally binding significance and serves only as a risk signal, it may help regulators identify areas where compliance support, monitoring, or enforcement priorities could be needed. The results for the Slovak intermediary services market suggest a moderate level of implementation of such mechanisms. Contact information was generally available, with only 5.37% of services lacking a contact point. Terms and conditions were also mostly present, although 17.71% of services were found to be missing them. However, their substantive quality was not assessed, and further legal analysis could reveal deficiencies. In contrast, notice and action mechanisms were considerably less common, with data indicating that such mechanisms were absent in nearly three-quarters of services (see *Graph 7*).



Graph 7. Share of services with missing risk mitigation mechanisms (Source: CMS, 2025)

V. Key Takeaways

This paper has proposed and tested a risk-index-based framework for assessing and comparing risks across different types of intermediary services within the scope of the DSA. Despite the functional diversity of these services, the framework demonstrates that a unified approach to comparative risk assessment is possible, provided that the assessment is structured around measurable and consistently applied indicators.

However, data availability constitutes a key limitation. External assessment does not provide access to internal platform data, and the manual collection of *design & content*-related risk factors introduces constraints related to subjectivity, time intensity, and potential inaccuracies. These limitations can be partially mitigated through clear indicator definitions, illustrative examples, and peer review processes. Nevertheless, compared with approaches relying on internally available platform data, the proposed framework is inherently less precise, as it depends on approximations and manually collected or secondarily processed information. *Traffic* data availability presents an additional constraint.

Importantly, the findings suggest a substantial degree of independence between *traffic* and *design & content*-related risks, with limited correlation between the two dimensions. This indicates that services with low traffic may still pose significant risks to users, underscoring the need for supervisory approaches that extend beyond traffic-based prioritization.

The assessment further highlights gaps in DSA implementation. Many services lack established compliance mechanisms, and awareness of DSA obligations appears to be particularly limited among smaller providers. This underscores the need for national-level communication and outreach activities aimed at improving awareness and compliance. At the same time, the results may help identify sectors or categories of intermediary services where additional guidance, monitoring, or awareness-raising efforts are most needed.

From a methodological perspective, the framework is designed to be applicable across different datasets, including at the Member State market level, and adaptable to evolving service landscapes. Its modular design allows the set of *design & content* risk factors to be expanded or reduced without affecting its underlying logic.

Overall, the framework supports evidence-based prioritization of supervisory activities by DSCs, enabling a more efficient allocation of regulatory resources. Its repeated application may also allow monitoring of market-wide compliance trends and the effectiveness of regulatory interventions.

These findings also point to avenues for further specialised research. Such research could deepen understanding of the risks associated with intermediary services and contribute to more effective DSA implementation and supervision.

References

Baldwin R, Black J (2016) Driving Priorities in Risk-based Regulation: What's the Problem? *Journal of Law and Society* 43, 565–595.

Branley DB, Covey J (2017) Is exposure to online content depicting risky behavior related to viewers' own risky behavior offline? *Computers in Human Behavior* 75, 283–287.

Efroni Z (2021) The Digital Services Act: risk-based regulation of online platforms. *Internet Policy Review*. https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606.

eSafety Commissioner (2024) Assessment tools. https://www.esafety.gov.au/industry/safety-by-design/assessment-tools.

European Board for Digital Services (2025) *First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures*. European Commission, Brussels https://digital-strategy.ec.europa.eu/en/news/digital-services-act-report-lays-out-landscape-systemic-risks-online.

European Board for Digital Services (2026) *Second report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risk as well as mitigation measures*. European Commission, Brussels https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services.

European Commission (2023) *Questions and Answers on identification and counting of active recipients of the service under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers.

European Commission (2025) *Proposal for a Directive/Regulation of the European Parliament and of the Council on strengthening consumer protection in the digital environment (Digital Fairness Act)*. Directorate-General for Justice and Consumers, Brussels https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:Ares%282025%296333296.

Griffin R (2025) Governing platforms through corporate risk management: the politics of systemic risk in the Digital Services Act. *European Law Open* 4, 223–253.

ISO (2018) ISO 31000:2018 Risk Management—Guidelines.

Jansen BJ, Jung S, Salminen J (2022) Measuring user interactions with websites: A comparison of two industry standard analytics approaches using data of 86 websites (H Suleman, Ed). *PLOS ONE* 17, e0268212.

Kaplan S, Garrick BJ (1981) On The Quantitative Definition of Risk. *Risk Analysis* 1, 11–27.

Katzy-Reinshagen A, Beyer J, Saab B et al. (2026) *Bridging Policy and Research under the DSA: A Structured Research Agenda for Identifying Systemic Risks*. Institute for Strategic Dialogue, Berlin https://www.isdglobal.org/publication/bridging-policy-and-research-under-the-dsa-a-structured-research-agenda-for-identifying-systemic-risks/.

OECD (2018) *OECD Regulatory Enforcement and Inspections Toolkit*. OECD Publishing https://www.oecd.org/en/publications/oecd-regulatory-enforcement-and-inspections-toolkit_9789264303959-en.html.

OECD, European Union, Joint Research Centre - European Commission (2008) *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD https://www.oecd.org/en/publications/handbook-on-constructing-composite-indicators-methodology-and-user-guide_9789264043466-en.html.

Ofcom (2024) *Risk Assessment Guidance and Risk Profiles*. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/risk-assessment-guidance-and-risk-profiles.pdf?v=390984.

Prantl D, Prantl M (2018) Website traffic measurement and rankings: competitive intelligence tools examination. *International Journal of Web Information Systems* 14, 423–437.

Sala A, Porcaro L, Gómez E (2024) Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports* 14, 100404.

Scheuerman MK, Jiang JA, Fiesler C, Brubaker JR (2021) A Framework of Severity for Harmful Content Online. *Proceedings of the ACM on Human-Computer Interaction* 5, 1–33.

Laws cites

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) (2003) http://data.europa.eu/eli/reco/2003/361/oj.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (2022) http://data.europa.eu/eli/reg/2022/2065/oj.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) (2024) http://data.europa.eu/eli/reg/2024/1689/oj.