GLOBAL NETWORK INITIATIVE

Implementing risk assessments under the Digital Services Act

REFERENCE MATERIAL

MAY 2023

Digital Trust & Safety Partnership

Purpose of discussion and objectives

Risk assessments are an important part of the DSA, but the form they will take is still yet to be fully defined. Both risk assessment best practices and Recital 90 of the DSA highlight the importance of engaging independent experts and civil society, among others, in order to draw on the best available insights about systemic risks, online platforms, and the European context.

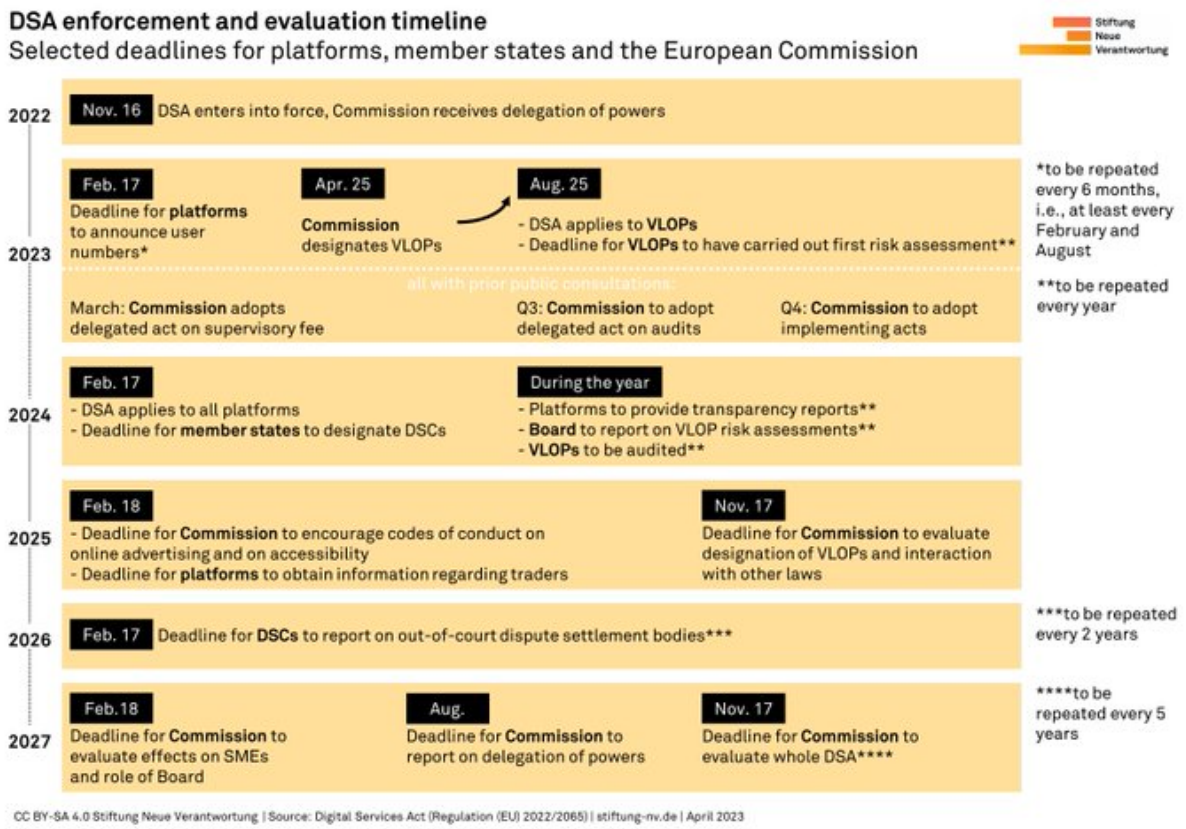
This discussion will help to inform the first DSA systemic risk assessments by facilitating stakeholder discussion on the structures and processes of risk assessments, as well as on macro questions, issues, and understandings relating to the systemic risk areas outlined in the DSA.

Conditions of discussion

The workshops will be held under the Chatham House Rule. After the event, the convenors will publish a report summarising key topics, observations, and recommendations, consistent with the Chatham House Rule. Participants must agree to be listed, by affiliation, in the event report, which will make clear that participation does not imply endorsement of the report content.

Timeline for DSA enforcement

The DSA will be implemented over time. Stiftung Neue Verantwortung (SNV) has produced the useful graphic below, and the DSA Observatory has also published a timeline here.



Assessing systemic risk under the DSA

The role of risk assessments

In public discussions accompanying the passage of the DSA, several senior members of DG CNECT compared the DSA to banking regulation, in the sense that the banking system performs such a vital role in society that maladministration creates "systemic risk". Recital 76 of the DSA reflects this framing, noting that "[o]nce the number of active recipients of an online platform or of active recipients of an online search engine … reaches a significant share of the Union population, the systemic risks the online platform or online search engine poses may have a disproportionate impact".

Article 34 of the Digital Services Act (DSA) requires "very large online platforms" and "very large online search engines" to undertake systemic risk assessments of their services in the European Union. The Article 34 obligation requires providers to "diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services." The deadline for completing systemic risk assessments is 25 August 2023.

While the broader obligation is to identify and assess "any systemic risks", four categories of risk are specifically identified. These are:

a. Dissemination of illegal content.
b. Actual or foreseeable negative effects on the exercise of fundamental rights, with specific fundamental rights being identified in Article 34.
c. Actual or foreseeable negative effects on civic discourse, electoral processes, and public security.
d. Actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

Other articles relevant to identification of systemic risk

Methods for identifying and mitigating the impact of providers' activities on systemic risk feature throughout the DSA, and there are an interconnecting range of articles in play beyond Articles 34 and 35, including:

- Transparency reporting requirements pursuant to Articles 15 (here) and 42 (here) specifically, as well as Article 24 (here).
- Audit obligations under Article 37, including the methods and frameworks for auditing risk assessments and mitigations as set out in the draft delegated act on Article 37 audit.
- The ability to develop and promote codes of conduct under Article 45 for dealing with systemic risk.
- The promotion of voluntary standards by "relevant European and international standardisation bodies" under Article 44. While Article 34 is not mentioned specifically, various factors and mechanisms relevant to risk assessments are

mentioned (including Article 37 audits, application programming interfaces for Article 40, advertising repositories, and standards related to disclosure of the key parameters of recommender systems pursuant to Article 38).
- The "compliance function" obligation (Article 41) that imposes an obligation on providers to nominate and support a person or group with adequate resourcing and qualifications to monitor systemic risk, audit frameworks, and risk assessment and mitigation, with direct access to a service's managing body.
- Obligations on the Commission to proactively identify emerging systemic risk across the Union in Article 64(2).

While risk assessments are a core feature of this broader approach, the purpose and orientation of the risk assessment obligation cannot be comprehensively understood without this broader framework.

Mitigating systemic risk (Article 35)

The purpose of identifying systemic risks is so that those risks can be mitigated. Article 35 obliges providers to "put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights."

The Commission's role in mitigating systemic risk

The Board and Commission will publish annual reports identifying the "most prominent and recurrent systemic risks" reported by VLOPs and VLOSEs, or identified through other means (such as Articles 39 (here), 40 (here) and 42 (here)). The reports will also include "best practices" for providers to mitigate systemic risks. Following public consultations, the Commission can also issue guidelines on how mitigation measures identified in Article 35(1), summarised below, can be used to mitigate systemic risks.

Examples of risk mitigations identified in the DSA

By way of summary, the kinds of risk mitigation measures identified in Article 35(1) include:

- Adapting the design, features or functioning of their services, including their online interfaces;
- Adapting their terms and conditions and their enforcement;
- Adapting content moderation processes;
- Testing and adapting their algorithmic systems, including their recommender systems;
- Adapting their advertising systems;
- Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk;
- Modifying trusted flagger arrangements, or the way out-of-court dispute settlements are implemented;
- Modifying or initiating codes of conduct and crisis protocols for collaboration with other providers;
- Increasing disclosure of relevant information to users, or raising awareness through online interfaces;

- Introducing parental control tools, age verification measures, or reporting mechanisms for minors;
- Labelling synthetic media or enhancing complaints processes about synthetic media.

A human rights approach to risk mitigation

Article 35 and supporting recitals place significant emphasis on requirements of necessity, proportionality and reasonableness. These requirements can be seen as a direct incorporation of human rights frameworks and principles, and are a likely response to concerns raised by civil society organisations and others during the drafting and negotiation of the DSA about unjustifiable risk mitigations.

Recital 86 of the DSA lists some of the relevant factors to consider when assessing proportionality, reasonableness, and the level of diligence required in devising and implementing risk mitigations. Notably:

- Providers should "deploy the necessary means to diligently mitigate the systemic risks identified in the risk assessments, in observance of fundamental rights."
- Risk mitigation measures should "be reasonable and effective in mitigating the specific systemic risks identified."
- Economic proportionality in light of the capacity of the specific provider, as well as the potential for risk mitigations to infringe negatively on fundamental rights. Freedom of expression is identified specifically as a right requiring close attention.

Process for conducting risk assessments

How frequently will risk assessments be conducted?

The first risk assessments are due on 25 August 2023. They must be completed "at least once every year thereafter". The delegated act on audit at Recital 5 indicates this is intended to fit with the yearly cycle of Article 37 audits. Risk assessments must also be conducted "prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to" Article 34. Methods of identifying functionalities that may contribute to systemic risk are an expected component of Article 37 audits of risk assessments.

It is clear that risk assessment is an ongoing process that is engaged particularly on the deployment of new functionality. Recital 88 states providers "may need to reinforce their internal processes or supervision of any of their activities, in particular as regards the detection of systemic risks, and conduct more frequent or targeted risk assessments related to new functionalities." Recital 88 also anticipates that systemic risk may be "shared across different online platforms or online search engines", and that this may require them to "cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures." Short of these codes of conduct or other measures, more limited actions such as "awareness-raising" may be appropriate, "in particular where risks relate to disinformation campaigns."

Codes of conduct for risk assessments

Civil society and others may be invited to contribute to voluntary codes of conduct, "taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks" (Article 45(1)). When developing codes of conduct (Article 45(3)), the Commission "shall aim to ensure that the codes of conduct clearly set out their specific objectives, contain key performance indicators to measure the achievement of those objectives and take due account of the needs and interests of all interested parties, and in particular citizens, at Union level."

Who is responsible for risk assessments? (The Article 41 "compliance function")

Risk assessment obligations are accompanied by "compliance function" obligations under Article 41. These outline the key features of a "compliance function" which must be established by the management body of VLOPs and VLOSEs, with specific requirements on how that compliance function must operate.

Management body must support compliance function

The management body for a VLOP/VLOSE must implement "governance arrangements that ensure the independence of the compliance function. … the prevention of conflicts of interest, and sound management of systemic risks identified pursuant to Article 34". At least annually, the management body must approve and review "the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34".

The DSA imposes obligations on the management body to "devote sufficient time to the consideration of the measures related to risk management." It must be "actively involved in the decisions related to risk management, and shall ensure that adequate resources are allocated to the management of the risks identified in accordance with Article 34."

Compliance function key obligations and requirements

The compliance function set up by the management body must conform to several detailed requirements. Key features include:

- Being "independent from [a provider's] operational functions";
- Having "sufficient authority, stature and resources";
- Having "access to the management body" and "shall report directly to the management body";
- Having obligations "to monitor the compliance of that provider";
- Having necessary "professional qualifications, knowledge, experience and ability";
- Being able to "raise concerns and warn [the management] body where risks referred to in Article 34" are implicated;
- "Ensuring that all risks referred to in Article 34 are identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures are taken pursuant to Article 35";

- "Organising and supervising the activities of the provider of the very large online platform or of the very large online search engine relating to the independent audit pursuant to Article 37".

The compliance function is also accountable for ensuring that Article 37 audits take place under the required conditions, including that auditors are given access to relevant materials, and that staff comply with auditors' requirements.

As a result of these comprehensive requirements on the compliance function, it has been suggested that risk assessments should include information on the role that platform governance decisions can present for systemic risk. Risk assessment reports could also include elements of a provider's organisational chart and reporting structure, outlines of decision-making authority, and descriptions of other internal governance structures and processes that could impact product, policy, and assessment outcomes. Even if these are not disclosed publicly, they will be necessary for the conduct of Article 37 audits.

Documentation requirements

Providers must preserve documentation supporting assessments for three years "[i]n order to make it possible that subsequent risk assessments build on each other and show the evolution of the risks identified, as well as to facilitate investigations and enforcement actions," (Recital 85). Recital 85 also anticipates the retention of "all supporting documents relating to the risk assessments that they carried out, such as information regarding the preparation thereof, underlying data and data on the testing of their algorithmic systems."

Compliance with documentation requirements, as well as the comprehensiveness and suitability of that documentation, will be audited under Article 37. Supporting documentation for risk assessments will be used in audits under Article 37. Compliance with documentation requirements is a specific obligation imposed on the compliance function (Article 41).

Indications about process from the delegated act on audit

Article 37 audits are intended to fit in with the yearly Article 34 risk assessment cycle. Recital 34 of the delegated act acknowledges that, given the uncertainty in how risk assessments might be performed, methods for auditing those risk assessments require clarification (in the delegated act). The draft delegated act on audit generates several insights into how risk assessments may be conducted (Article 13 of the delegated act).[1] Auditors will be required to assess, and providers must therefore have provided for, the following:

- The adequacy of methods for identifying relevant risks, and their suitability;
- Methods of accounting for regional and linguistic aspects of service usage in individual member states when assessing systemic risk;
- Methods of assessing the probability and severity of identified risks;
- How the "factors" influencing risk were identified, and whether the identification of specific factors in relation to types of systemic risk was appropriate;

[1] Article 14 of the delegated act relates to risk mitigations, but does not differ in any notable ways from Article 13 related to risk assessments. Our analysis here therefore equally applies to Articles 13 and 14 of the delegated act.

- What sources of information were used to identify and assess systemic risk, and how that information was collected;
- How information on scientific and technical insights relevant to the comprehensive identification of systemic risk was collected;
- How providers tested any assumptions involved in their risk assessments with groups most affected by provider influence on systemic risks;
- How relevant functionalities of a service presenting systemic risk were identified;
- Compliance with supporting documentation preservation requirements, and completeness of that documentation.

Because the delegated act is oriented toward Article 37 audits, it is also apparent that the implementation of systemic risk assessment obligations will include the following:

- Internal controls for monitoring the performance of risk assessments for each "factor" related to the types of systemic risk identified in Article 34(2);
- The use of "substantive analytical procedures" for internal controls;
- Tests of whether those internal controls are "reliable and diligently conceived, executed and monitored";
- An assessment of how the compliance function in Article 41 implemented internal controls, and the interactions between the compliance function and the management body;
- Tests by auditors of algorithmic systems in situations where substantive analytical procedures and internal controls leave the auditor with reasonable doubts.

The kinds of information auditors will use to assess the adequacy of risk assessments

Article 13 of the delegated act also sets out the kinds of information auditors must analyse to audit risk assessments. This provides compelling insights into the way that risk assessments must be conducted, and the methods available to auditors and others for assessing the adequacy of those assessments. Relevant sources of information include:

- The risk assessment report itself, including any confidential information included in the non-published risk assessment report, and any supporting documents;
- Any previous risk assessment reports from the provider, and supporting documents from those assessments;
- Any other information from the audited provider;
- All Article 15 transparency reports from the provider, which presumably also include any relevant Article 24 and 42 transparency reports;
- Any information provided to the auditor in responses to written or oral questions of the provider, which could include test results, documentation, evidence, or statements;
- Any observations made by the auditor on premises;
- "Other relevant evidence, including based on information made available by the audited provider" (it is not clear what this refers to);
- Article 35 risk mitigation reports and any guidelines issued by the Commission on the DSA.

Notably, it is anticipated that auditors will be able to rely upon information disclosed by **other providers** under Article 42(4), which would include other providers' risk assessments. Auditors can also rely on research published by researchers following Article 40 data requests.

Components of a risk assessment

> Recital 79. In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact.

Platform components ("factors") that "influence" systemic risks

Risk assessments must assess "whether and how the following factors influence any of the systemic risks". The list of "factors" provides a useful framework and it includes:

- Recommender and algorithmic systems
- Content moderation systems
- Terms and conditions, and enforcement of those terms and conditions
- Advertising systems
- Practices related to data

The delegated act on audit indicates auditors will be called upon to assess the methods used to identify these factors and how they may influence systemic risk as part of the risk assessment.

Intentional manipulation

A necessary part of Article 34 risk assessments is to "analyse whether and how" any of the systemic risks described in Article 34(1) "are influenced by intentional manipulation of their service". Two types of intentional manipulation are specifically identified:

- "inauthentic use or automated exploitation of the service";
- "the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions".

The assessment shall take into account specific regional or linguistic aspects associated with the influence of identified "factors" on systemic risk, including "when specific to a Member State".

What are the types of systemic risk?

Article 34 seems to require analysis of "any systemic risks", as well as several specifically identified types of systemic risks. These "shall include" the following specific "systemic risks":

(a) the dissemination of illegal content through their services;

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;

(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;

(d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

Conducting risk assessments requires identification of risk, as well as severity and likelihood of risk. In this regard, it may be worth noting that paras (b), (c) and (d) require attention to the "actual and foreseeable negative effects" on specific matters, whereas para (a) refers to the actual dissemination of illegal content. This may indicate a qualitatively different assessment is required when it comes to considering the nature, probability, and severity of each of the four types of systemic risk.

Systemic risks are identified not only through Article 34, but also through the researcher-access-to-data mechanisms under Article 40, with systemic risk being identified specifically in Article 40(4) and (12). The role of vetted researchers in improving understanding and identification of systemic risk is also reflected in Recitals 96 and 98.

Further insights: Illegal content

Recital 80 provides examples of the kinds of illegal content anticipated by risk assessment obligations. Specifically identified categories include:

- dissemination of child sexual abuse material;
- dissemination of illegal hate speech;
- other types of misuse of their services for criminal offences;
- the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products, or illegally-traded animals.

Recital 80 seems to anticipate that one incident where dissemination of illegal content occurs does not meet the threshold of "systemic risk", but the rapid and wide spread of illegal content through accounts with wide reach or via significant amplification may be.[2]

Further insights: Fundamental rights

Specific fundamental rights are identified in Article 34, however the DSA provides other indications that all fundamental rights are relevant to risk assessments. The Article 34 obligation is to assess "any actual or foreseeable negative effects for the exercise of fundamental rights" followed by a list of fundamental rights to be considered "in particular". The fundamental rights specifically identified in Article 34 and Recital 81 include:

- **Human dignity:** the fundamental rights to human dignity enshrined in Article 1 of the Charter,
- **Private and family life:** to respect for private and family life enshrined in Article 7 of the Charter,
- **Personal data protection:** to the protection of personal data enshrined in Article 8 of the Charter,
- **Freedom of expression and information, including freedom and pluralism of the media:** to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter,
- **Non-discrimination:** to non-discrimination enshrined in Article 21 of the Charter,
- **Rights of children:** to respect for the rights of the child enshrined in Article 24 of the Charter and
- **Consumer protection:** to a high-level of consumer protection enshrined in Article 38 of the Charter.

Recital 81 supports a reading that all fundamental rights are relevant, despite the identification of specific rights in Article 34. Providers must assess the risk of "actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, **including but not limited to** human dignity, freedom of expression and of information, including media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection."

Transparency of risk assessments

Civil society involvement in risk assessment and mitigation

Recital 90 on stakeholder engagement emphasises that stakeholder engagement with civil society and with specifically affected groups is an essential part of ensuring risk assessments and mitigations are based on "the best available information". In particular, any assumptions about systemic risk must be tested with groups most impacted by those risks, and the delegated act on audit indicates this is a specific area of emphasis for Article 37 audits of risk assessments.

[2] "For example, such dissemination or activities may constitute a significant systemic risk where access to illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification."

90. Providers of very large online platforms and of very large online search engines should ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights and that **they test their assumptions with the groups most impacted by the risks and the measures they take**. To this end, they should, where appropriate, **conduct their risk assessments** and **design their risk mitigation measures** with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations. They should seek to **embed such consultations** into their **methodologies** for assessing the risks and **designing** mitigation measures, including, as appropriate, **surveys, focus groups, round tables, and other consultation and design methods**. In the assessment on whether a measure is reasonable, proportionate and effective, special consideration should be given to the right to freedom of expression.

Documentation requirements

See above under "Process for conducting risk assessments".

Transparency reporting obligations around risk assessments

Recital 100 acknowledges that there are "additional transparency requirements" on VLOPs and VLOSEs, and these include to "report comprehensively on the risk assessments performed and subsequent measures adopted". Article 42 describes the more comprehensive transparency reporting obligations on VLOPs/VLOSEs (layered onto Article 15 (here) and 24 (here), where appropriate). It requires the disclosure of specific internal and external assessments required by the broader DSA, once they have been audited by an independent auditor under Article 37. In particular, Article 42(4) requires VLOPs and VLOSEs to make the following reports both publicly available and available to the Commission and Digital Services Coordinators after they have been audited:

1. A report on the results of any Article 34 risk assessment;
2. A description of some kind of the specific mitigation measures put in place under Article 35 in response to the Article 34 risk assessment;
3. The audit report itself (conducted under Article 37);
4. The audit implementation report (conducted under Article 37(6));
5. Information that describes the consultations conducted by the VLOP/VLOSE in support of the risk assessment process, and the design of any risk mitigation measures.

The information and reports at points 1-5 immediately above can be redacted, or information removed from publicly available reports if publication might:

- Result in the disclosure of confidential information of the provider;
- Result in the disclosure of confidential information of users;

- Cause significant vulnerability for the security of the service, undermine public security, or harm “recipients” (understood to be users of the service, not recipients of the reports).

If information is to be removed from the reports prior to publication, the full report without redactions must be sent to the relevant Digital Services Coordinator and the Commission, along with a statement of reasons justifying the removal of the information from public reports. The delegated act on audit anticipates that, in the course of their audits, auditors can reference risk assessments conducted by other providers and published under Article 42(4) transparency reporting requirements.

Broader approaches to risk assessment

Beyond the DSA

In addition to resources on risk assessment under the Digital Services Act, respondents also drew attention to the broader legislative landscape in Europe and in other jurisdictions. Some legislative proposals impose comparable risk assessment requirements, and entities looking to implement risk assessment frameworks will be influenced to some extent by these developments. Useful resources include the following:

- BSR’s analysis of the “state of play” on human rights due diligence in the technology industry, available here.
- BSR has identified some of the overlaps between DSA’s risk assessment provisions with three other incoming EU regulations: the EU Corporate Sustainability Due Diligence Directive, the EU Corporate Sustainability Reporting Directive, and the AI Act, available here.
- The Danish Institute on Human Rights has published a report titled, “How do the pieces fit in the puzzle? Making sense of EU regulatory initiatives related to business and human rights,” available here.
- The UN B-Tech Project has published a series of papers, including on “Addressing Business Model Related Human Rights Risks,” “Identifying Human Rights Risks Related to End-Use,” and “Taking Action to Address Human Rights Risks Related to End-Use,” available here.
- Ofcom has published an explanation of how they are approaching online safety risk assessments, available here.
- Ofcom has published a report on their first year of regulating video sharing platforms, available here.
- The Australian eSafety commissioner’s report on industry responses to the first mandatory transparency notices, available here.

Risk assessment frameworks

The Action Coalition on Meaningful Transparency has collated a range of risk assessment frameworks identified by ACT members in its draft briefing on risk assessments. These include risk assessment frameworks for broader human rights obligations, as well as assessing AI systems.

The Integrity Institute has recently released a framework for assessing election integrity (dated 17 May 2023, available here).

Potential areas for future collaboration

Throughout the workshops, we will be monitoring for areas of potential multi-stakeholder collaboration that may render risk assessment frameworks more effective and meaningful for all parties. At the outset, we anticipate the following will be useful areas of focus.

Provider confidentiality and engagement with civil society organisations

How to navigate confidentiality and sensitivities associated with risk assessment obligations and Article 37 audits, while also enabling participation by civil society organisations in the design and conduct of risk assessments, as anticipated by Recital 90.

Unintended cross-jurisdictional impacts

The Digital Services Act will have impacts outside the EU, and many of these may be positive and intended. However, with the DSA mandating risk assessments in Europe and no equivalent legislation in other jurisdictions, there is a risk that companies will focus their resources on evaluating and mitigating risks in Europe to the detriment of their activities elsewhere. It will require coordinated effort to mitigate the risk that DSA implementation in Europe does not come at the expense of similar efforts in other jurisdictions.

Development of codes of conduct (Article 45)

Article 45 anticipates the development of voluntary codes of conduct to support DSA implementation, including in relation to Article 34 risk assessments and the identification of systemic risk. There could be substantial benefit to formulating frameworks that enhance the consistency, certainty and transparency of risk assessment processes. Relevant questions here include:

- What might be done to foster the development of codes of conduct?
- When will it be appropriate to initiate these processes?
- What areas in particular might benefit from consolidated codes of conduct?

Measurability and performance over time

A theme from ACT respondents focused on the importance of measurability in risk assessment. Auditors will rely on risk assessments from others, and previous risk assessments by platforms. Contributions to the ACT briefing note on risk assessments covered the following points:

- Risk assessments should include, insofar as possible, clear measurements, benchmarks, or estimations to quantify existing risks and harms. These measurements are important for ongoing monitoring of risk, as well as measuring variations in risk over time, including in response to changing contexts and internal decision-making.

- There is merit to both qualitative and quantitative assessments, but there should be justifications offered for why particular qualitative or quantitative measures and approaches have been adopted, with some accounting for tracking qualitative measurements over time.
- Risk assessment processes and reports should include clearly recorded and auditable plans and processes for the ongoing monitoring and management of risks, including based on measurable thresholds for action.
- Methods of measurement incorporated into risk assessment methods and implementation can benefit from independent expert involvement. Initial methods can be tested with external parties to suggest more concrete benchmarks for measuring change over time, including by comparison of assessment reports. The Code of Practice on Disinformation was identified as an example of a structure that lacks benchmarks, and therefore presents opportunities for improvement.
- One respondent suggested that, over the next 3-10 years, DSA risk assessment could aim for standardised “systemic risk statements”, with a similar look and feel to “enterprise risk statements” included in United States Security and Exchange Commission Form 10-K reports (under Item 1A: Risk Factors).

Conclusion

While risk assessments under Article 34 of the DSA present a high profile area of focus, they sit within a broader network of obligations, all of which require careful implementation. Risk assessments and other methods of monitoring systemic risk will require multi-stakeholder engagement in the way they are designed, implemented, and reviewed over time.

As such, these initial workshops are the starting point for what will inevitably become a wider pattern of engagements between various stakeholder groups. The organisers will be identifying further opportunities for collaboration and support for such initiatives and thank you for your time and participation.