Consultation response form

Please complete this form in full and return to IHconsultation@ofcom.org.uk.

Consultation Title	**Protecting people from illegal harms online**
Your Full Names	**Sally Broughton Micova, Andrea Calef, Bryn Enstone**
Your Contact Phone Number	**07904852037**
Representing (Self or Organisation only)	**Organisation:** Centre for Competition Policy (however this response has been drafted by the academic members of the Centre named above who retain responsibility for its content)
Organisation Name (if applicable)	**Centre for Competition Policy**
Email Address	ccp@uea.ac.uk S.Broughton-Micova@uea.ac.uk a.calef@uea.ac.uk T.Enstone@uea.ac.uk

Confidentiality

Is your name confidential? (please enter **yes** or **no** only)	**No**
Is your organisation name confidential? (please enter **yes** or **no** only)	No
Can Ofcom publish a reference to the contents of your response? (please enter **yes** or **no** only)	Yes
Please indicate if your full response is confidential. Partly confidential responses can be indicated under each question. (please enter **yes** or **no** only)	Not Confidential

We ask for your contact details along with your response so that we can engage with you on this consultation. We will keep your contact number and email address confidential. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

Response: We welcome Ofcom's acknowledgements of the interlinkages between smaller services and larger services and of the way which illegal content can spread between services. Our research has found that these interlinkages, which can take the form of functionalities, common users, or shared reliance on assets (for example: hash databases or third-party moderators) are fundamental to understanding the proliferation of harm[1]. We also recognise and appreciate Ofcom's acknowledgement that functionalities as not inherently harmful, and moreover that functionalities should treated as a factor in the assessment of risk.

One thing that may merit further consideration in Ofcom's understanding of the impact of illegal harms is the potential for pollution-type effects. These effects are often long term and inherently affect individuals that are not the direct target of the illegal content, or in some cases, are not even directly exposed to illegal content. These are often the result of accumulation of harm over time in online spaces.[2]

Section 6E on harassment could include consideration of the harm to individuals who are not the immediate object of the abuse. In 6E.21 Ofcom notes that some harassment and abuse is visible to users which are not the immediate victim or abuser. For example, public or semi-public humiliation can be an objective of harassment and/or abuse. This leads to harm not only to the user or users who is/are the object of the abuse but also can influence others to harass users and may contribute to the normalisation of such behaviour, essentially polluting the communication space created by online services. Polluting effects have been shown to have a negative effect on the civility of discourse and participation of women and minorities.[3] Some of the research cited by Ofcom in 6E.23 provides evidence that voices are silenced out of fear among those who only witnessed abusive behaviour. Research by the Organization for Security and Co-operation in Europe (OSCE) has shown this to be particularly prevalent among female journalists.[4]

In the analysis of the risk of harassment, Ofcom might encourage services to consider the harm that can arise from witnessing abuse and the effects this can have on communication

[1] Broughton Micova, S. & Calef, A. (2022) *Elements for Effective risk Assessment under the DSA* https://cerre.eu/publications/elements-for-effective-systemic-risk-assessment-under-the-dsa/

[2] For elaboration of the notion of the accumulation of harm leading to pollution-like effects on services that function as public spaces see Broughton Micova, S. (2021) *What's the harm in size?* https://cerre.eu/publications/what-is-the-harm-in-size/

[3]; Moore, M. (2018) *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*

[4] Désir, H. (2019). Communiqué by the OSCE Representative on Freedom of the Media on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online. OSCE Representative on Freedom of the Media. https://www.osce.org/representative-on-freedom-ofmedia/411917

spaces. This may mean examining not only the overall incidence of harassment and which people subject to harassment, but also the duration of incidence of harassment and whether it is concentrated in certain communities or groups of users that are connected through online services. There are some indications that the design and functionalities of services, such as the way content is presented or how comments are organised can contribute to normalisation or secondary negative effects on other users.[5] The inclusion of social media as a service type of particular risk in relation to harassment is appropriate, but video-sharing platforms might also be included, as they often allow comments and reactions to content. It might also be useful to note in the section on functionalities where "posting" is being discussed in 6E.71 & 7. the public nature of the posts and factors that influence the potential reach of the abusive content, such as the use of popular hashtags, cross-posting across services, or screen sharing functionalities.

Hate speech provides another example of polluting effects. The use of hateful speech in online communities has been shown to normalise language and narratives linked to hate.[6] As Ofcom points out in 6F.31 & 32 there can be interlinkages between larger services, probably with better detection and mitigation mechanisms, and less moderated smaller services. These interactions can be a two-way and dynamic. The consequence of these interlinkages are that hateful or 'borderline' content, language, and narratives can develop and move back and forth between services with greater and lesser reach. While it may not be proportional to place addition requirements on smaller platforms that otherwise might be classified as low risk, some 'free riding' could be encouraged in which smaller platforms can make use of the insight from content moderation done by larger services, for example where common users have been blocked or identified as frequent perpetrators by the larger services. Even if short term or long term competition aspects are not considered in this consultation, it is worth keeping in mind the potential consequences of the requirements made to large and small platforms with the aim to avoid that the latter exit the market, due to excessive regulation which can translate in disproportionate costs to them. On the contrary, free riding between large platforms should be avoided, as it may eventually become a source of competitive advantage for one of them, potentially leading to a significant change in the market structure. Both cases would have straightforward impacts for consumer protection.

Ofcom considers the business model of services as a risk factor across the offences. Ofcom appropriately highlights that business models which rely on engagement with content can contribute to the spread or amplification of hate speech. It is also recognised that models that rely on advertising can be a factor contributing to risk where advertising can be misused by perpetrators. For example, in relation to sexual exploitation and trafficking offences Ofcom notes that advertisements can be used to lure victims, and classified the type of sales that can be used to entice buyers. Ofcom also notes that advertisements, particularly dark posts and highly targeted political ads, can be used by foreign interference operations. However, Ofcom could also consider in its understanding of the sources of risk the relationship that the advertising business model has with the volume of content and traffic. Advertising can also be sold around content that is generated by bots, which Ofcom rightly noted is especially relevant to FIO and false communication

[5] Maddocks, S. & Parfaite, F. (2021) "Watch me pretend to punch my girlfriend": exploring youth responses to viral dating violence, *Feminist Media Studies* Volume 24, 2024 - Issue 1

[6] Mathew, B., Illendula, A., Saha, P., Sarkar, S., Goyal, P., & Mukherjee, A. (2020). Hate begets hate: A temporal study of hate speech. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), 1–24.

offences. Therefore, the fact that the advertising business model can incentive allowing bots and automatically generated content is also worth highlighting.

The risk of harm to individuals' freedom of expression from over-removal or over-blocking is not sufficiently acknowledged in volume 6, which is a crucial expression of Ofcom's understanding of risk and will set the framework and expectations for the regulated services. It is particularly important that this risk be identified in relation to the understanding of risks stemming from governance arrangements. Throughout section 6U the only risk mentioned is exposure to illegal content, however in this section in particular the risk to users' freedom of expression (FoE) through ineffective mitigation measures should also be acknowledged.

For example, 6U.13 states that "Users may be more likely to be exposed to illegal content where there is insufficient oversight and scrutiny of risk management activities." Users are also at higher risk of being harmed by disproportionate restrictions on their FoE through misidentification or imprecise measures to combat illegal content. The same holds true for instances of "poor content moderation" addressed in 6U.29, where over-removal and over-blocking is also a risk. There is a growing body of evidence that over-removals in content moderation can further marginalise minority groups and can negatively affect the reporting of human rights abuses by activists[7] content related to asylum seekers rights or protections. This risk should also be acknowledged in this section to establish a thorough understanding of the risks associated with illegal content and to underpin the approach to performance targets taken in the draft Codes of Practice.

Corporate governance is a key factor to be considered when assessing risk management activities within financial corporations. It is good that the distinction between executive directors and non-executive directors is mentioned, however other features have been found relevant, such as age, background, gender of directors as well as board's size and compensation schemes.[8] Moreover, a key focus needs to be placed on the risk management team itself. The recent bank run of Silicon Valley Bank is a reminder that having a Chief Risk Officer in place is not optional[9] and auditors are required to deliver periodic checks within their "reasonable assurance"'s remits.

Corporate governance should also consider the shareholder's structure of each large platform as well as whether there are common shareholders across platforms. Some digital platforms may have a single shareholder that is able to control their board of directors, while some others are known as "public companies", i.e., their shareholder structure is fractioned among many small shareholders with no clear "shareholders of

[7] See for example: Haimson, O.L., Delmonaco, D., Nie, P. and Wegner, A., (2021) Disproportionate removals and differing content moderation experiences for conservative, transgender, and black social media users: Marginalization and moderation gray areas. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), pp.1-35 https://dl.acm.org/doi/abs/10.1145/3479610; Gorwa, R., Binns, R. and Katzenbach, C., (2020) Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1) https://journals.sagepub.com/doi/abs/10.1177/2053951719897945

[8] The literature is vast. See: Carter, D. A., Simkins, B. J., & Simpson, W. G. (2003). Corporate governance, board diversity, and firm value. *Financial review*, *38*(1), 33-53. Ali, M., Ng, Y. L., & Kulik, C. T. (2014). Board age and gender diversity: A test of competing linear and curvilinear predictions. *Journal of Business Ethics*, *125*, 497-512. Kang, H., Cheng, M., & Gray, S. J. (2007). Corporate governance and board composition: Diversity and independence of Australian boards. *Corporate governance: An international review*, *15*(2), 194-207. Sarhan, A. A., Ntim, C. G., & Al-Najjar, B. (2019). Board diversity, corporate governance, corporate performance, and executive pay. *International Journal of Finance & Economics*, *24*(2), 761-786.

[9] See Fortune (2023).

control". Even though the last case may not seem potentially problematic, it may become so if there exists some common shareholders in multiple digital platforms ("common ownership"), being able to nominate directors in these corporations. "Common ownership" may lead to coordinated decisions, which may affect consumer protection[10] as well as the level of risk mitigation.
ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: See Above
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 2:
i) Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
Response: Yes, please see response to question 1.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

[10] See, for example, Azar, J., Schmalz, M. C., & Tecu, I. (2018). Anticompetitive effects of common ownership. *The Journal of Finance*, *73*(4), 1513-1565. Also, Schmalz, M. C. (2018). Common-ownership concentration and corporate conduct. *Annual Review of Financial Economics*, *10*, 413-448.

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response:	In volume 3 there is a lack of recognition of the harm that inadequate governance and accountability measures can pose from undue restrictions on FoE, over-collection or misuse of personal data, and other harms that are not from exposure to illegal content. For example, in 8.92 (page 22), Ofcom notes that the internal assurance and compliance functions will be crucial to preventing exposure to illegal content or the use of the services for its dissemination. However, as discussed in our answer to 6.1, these are also crucial to ensuring that mitigation measures are proportionate and do not result in over-blocking, over-removals and that redress mechanisms are sufficient. The expectations for these systems set out here will serve to establish the service providers' design and direction of their assurance and compliance functions so it is vital that these other concerns, or purposes for these functions, be noted. We welcome the proposed options for staff incentives, especially the option of providing adequate training on compliance and 'risk culture' training. It is important that this includes imparting understanding of the fundamental rights that are balanced within the risk management process. Remuneration incentives in the financial sector operate in systems in which the costs of poorly managed risk or non-compliance are easily calculated (losses or fines)[11]. For online harms the situation is more nuanced. KPIs should be varied and aimed at achieving effective and proportionate mitigation. There will also likely be a learning process as Ofcom's supervision of regulated services results in generating new knowledge on what constitutes effectiveness in relation to the various illegal harms. Therefore, we support Ofcom's decision not to include a remuneration related measure in this first Code of Practice.
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

[11] The literature is vast. Please see: Bolton, P., Mehran, H., & Shapiro, J. (2015). Executive compensation and risk taking. *Review of Finance*, *19*(6), 2139-2181.
Dittmann, I., Yu, K. C., & Zhang, D. (2017). How important are risk-taking incentives in executive compensation?. *Review of Finance*, *21*(5), 1805-1846.
Cheng, I. H., Hong, H., & Scheinkman, J. A. (2015). Yesterday's heroes: compensation and risk at financial firms. *The Journal of Finance*, *70*(2), 839-879.
Guo, L., Jalal, A., & Khaksari, S. (2015). Bank executive compensation structure, risk taking and the financial crisis. *Review of Quantitative Finance and Accounting*, *45*, 609-639.
Tao, N. B., & Hutchinson, M. (2013). Corporate governance and risk management: The role of risk management and compensation committees. *Journal of Contemporary Accounting & Economics*, *9*(1), 83-99.

Response: See Above
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 4:
i) Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: Yes, we agree that governance and accountability measures are particularly important for large firms that are dominant in the market and have the greater potential to impact users. Failure to effectively mitigate risk in these services can have significant impact on users and on the rest of the market. Parallels, albeit an imperfect ones, can be made with other sectors. The Arthur Andersen/Enron scandal (2001) and bank run on Silicon Valley Bank (2023) are just two examples that highlight the key importance of corporate governance, internal and external auditing and risk management procedures, and need to monitor and review periodically. The outcome of the Arthur Andersen/Enron scandal was not just the default of a key energy firm (Enron), but also the end of one of the then-Big 5 auditing companies (now known as the Big 4), leading to a more concentrated financial auditing reporting market. The latter, Silicon Valley Bank's default, together with the follow-on defaults of First Republic and Signature Bank, demonstrated the contagion effect on the other banks. US authorities (The Federal Reserve, FDIC, and US Treasury) bailed out these banks. However, this led to more "moral hazard", which ultimately increased banks' risk-taking appetite, making the banking system more prone to a future systemic crisis. How would this translate in the world of digital platforms and Online Safety? Failures to mitigate risk on the scale of services that are used by large numbers of the population can have significant effects on both users and ancillary services, as well as put added pressure on the regulator testing the whole system. There is also credible evidence of cross-platform contagion effects of illegal and harmful content.[12] Therefore, poor governance and accountability in large services can affect the circulation of such content on smaller services and makes them less resistant to contagion from such services. Larger firms also can play a standard setting role. Overly burdening smaller services can also have detrimental impact on consumer welfare, innovation levels, media pluralism.
ii) Please explain your answer.
Response: See above
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

[12] Ng, L. H. X., Cruickshank, I. J., & Carley, K. M. (2022). Cross-platform information spread during the January 6th capitol riots. *Social Network Analysis and Mining*, *12*(1), 133. ; Zannettou, S., Caulfield, T., De Cristofaro, E., Kourtelris, N., Leontiadis, I., Sirivianos, M., Stringhini, G., & Blackburn, J. (2017). *The web centipede: Understanding how web communities influence each other through the lens of mainstream and alternative news sources*.

Question 5:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?

Response: We believe that implementation of independent audit of illegal harm mitigation systems is feasible, but it would require the creation of a new market – a market for online safety act audits. As we are not currently aware of any evidence on the effectiveness of external audit in manging illegal content risks therefore, we agree that Ofcom should not aim to create this market at this stage.

However, Ofcom should monitor developments in the European Union. The European Commission is creating a similar market (the DSA audit market) and it is possible that other jurisdictions may follow suit. Evidence for the creation of an online safety audit market in the UK may arise in the future. We now explain why we support Ofcom's decision in more detail below.

As highlighted above, a key difference between the online safety Act (OSA) and its European counterpart, the digital services act (DSA) is that the DSA obligates very large service providers (VLOPs and VLOSEs) to conduct independent audits of their illegal harm risk mitigation and management systems.

The OSA does not. Whilst large multi risk service providers must still conduct independent monitoring and assurance this can be conducted internally and reported to a governance body.

Ofcom is yet to publish a list of *'large multi-risk services'* however it defines a service as *'large'* if it has over 7 million average monthly users. Approximately equivalent to 10% of the UK population. The DSA defines a service as *'very large'* if it has more than 45 million users per month. Again, approximately equivalent to 10% of the European Union population.

Although the two list of services will undoubtably differ it is worth highlighting that the European Commission has published its list of *'very large'* service providers.[13] The OSA list is unlikely to be an order of magnitude different and many services will be on both lists. Data on the average number of monthly users is currently available for 19 out of 22 of services designed as *'very large'* by the European Commission.

Notably:

- 18/19 of these (94.74%) were at least twice the *'very large'* threshold;
- 12/19 (63.19%) were at least triple the *'very large'* threshold;

[13] As of the 31ST of January 2024 these providers are, with their number of services in brackets: Alibaba (1), Amazon Services Europe S.a.r.l (1), Apple Distribution International Limited (1), Alyo Freesites Ltd (1), Booking.com BV (1), Google (5), LinkedIn (1), Meta Platforms (2), Mircosoft Ireland Operations limited (1), Pinterest Europe Ltd (1), Snap B.V. (1), Technius (1), Tiktok Technology Limited (1), Twitter International Unlimited Company (1), Webgroup Czech Republic (1), Wikimedia Foundation Inc (1), Zalando (1).

- 6/19 (31.58%) were at least five times the *'very large'* threshold, meaning that, in principle at least, these 6 are on average, used by over half the population of the European Union each month.

This trend is likely to be the same for services designated as U2U services and search services under the OSA. Many of the services which are well over the *'very large'* threshold for the purposes of the DSA are also heavily used in the UK and are household names.

The fact that most of these services are so comfortably over the *'very large'* threshold highlights the positions of great power and responsibility which relatively few digital platforms hold in the mitigation of the spread of illegal harm. Whilst this does not mean that smaller firms do not also have a significant role to play, we support Ofcom's decision to extend the obligations of large and multi-risk service providers, particularly the obligation for these entities to develop and maintain *'internal monitoring and assurance function to independently assess the effectiveness of measures to mitigate and manage the risks of harm'*.[14]

We also recognise and appreciate that Ofcom is assessing possible options for extending these obligations further such as the introduction of independent audit for large and multi-risk providers.

We foresee two interrelated issues with independent audit of illegal content reporting:

i) **Cost/Benefit Issue:** Is there any evidence that external audits would add societal value beyond the existing governance mechanisms within the OSB?

ii) **Implementation Issue:** How would the market for independent audit of illegal content reporting function? Is it possible for the firms conducting these audits to have the necessary capacities and independence to conduct them competently? Who would oversee the auditors? Would developing this new audit market possibly risk harm to existing audit markets?

Cost/Benefit Issue

Prior to the DSA we were not aware of a similar type of statutory obligation to introduce external audit of illegal harm mitigation measures to U2U services and search engines. However, the first DSA audits are due to be published by the end of August 2024. If a significant number of the VLOPs/VLOSEs fail their external audits yet pass internal compliance monitoring measures, then given the likely overlap between *'very large'* and *'large multi-risk providers'* arguably this would provide evidence that Ofcom should consider introducing external audits. We therefore recommend Ofcom follow the results of these audits carefully.

A possible exception to the need to adopt these audits in these circumstances would be if there was sufficient evidence that introducing external audits under the OSA had such a high financial cost associated with it that it had a material risk of causing very large multi risk U2U and search engine providers to be financially unviable in the UK market. Although given that they are carrying out their obligations to external audit under the DSA, this appears unlikely.

[14] See page 3 of Ofcom (2023) 'Consultation at a glance: our proposals and who they apply to'. Available at Consultation at a glance: our proposals and who they apply to (ofcom.org.uk)

Whilst failure of external audit by VLOPs and VLOSEs could provide definitive evidence Ofcom should introduce external audit the antithesis is not **necessarily** true.

The additional layer of oversight which DSA external audit provides may act as an incentive for service providers to improve their internal systems and control functions within the European Union and then they may not necessarily apply these changes to the UK. Equally, without external audit there may be a risk that harm mitigation systems in the UK have an increased chance of failure. Therefore, we recommend that the Ofcom conducts regular comparative analysis between the effectiveness of harm mitigation systems in the European Union and the UK once the obligations of the DSA and the OSA have both fully entered into force. This may reveal that there is benefit in introducing external audit in the future.

It is also worth highlighting that external audits could fail in their purpose. I.E., auditors fail to detect failure in internal monitoring functions of VLOPs/VLOSEs. This has happened in financial audit, and the industry has suffered several high-profile crises such as Author Andersons role in the Enron scandal[15]. More recently PwC was fined £1.8 million by the Financial Reporting Council (FRC) for failing to properly audit BTs accounts.[16]

Furthermore, financial audit markets are also fraught with audit quality issues and whilst financial audit quality in the UK is improving, the most recent figures available on audit quality only found that 77% of external audits of largest UK companies were of good quality[17]. As audit of illegal harms monitoring appears novel, it is likely that, at least to begin with, the quality of these audits would be lower than financial audits. As such the OSA should monitor the effectiveness of external audit under the DSA over a several years, as it may take time for these audits to become effective.

Implementation Issue

The service providers which would need auditing under the DSA have a gargantuan number of users and in some cases moderators.[18] It is likely that only the largest financial auditors (the so called 'big 4') have sufficient capacity and expertise to carry out audits of illegal harm mitigation systems whilst also maintaining necessary degree of independence to conduct these audits impartially to the required standard.

The other firms which may have the capacity to conduct these audits would be the tech firms themselves (i.e., they audit each other) but this is probably infeasible due to impartiality concerns. Large technological consultancy firms such as Accenture might have the technological knowhow to conduct these audits however are already involved in

[15] See Mark Maurer, Wallstreet Journal (2022) Arther Andresen's Legacy, 20 Years after its demise, is complicated' Available at " Arthur Andersen's Legacy, 20 Years After Its Demise, Is Complicated - WSJ" for additional information on this scandal.

[16] See Mark Swney, the Guardian (2020) PWC fined nearly £1.8 over BT fraud audit failures. Available at PwC fined nearly £1.8m over BT fraud audit failures | PwC | The Guardian

[17] See FRC (2023) Tier 1 firms – Overview: Audit Quality Inspection and Supervision Report. Available at Tier 1 Firms – Overview (frc.org.uk)

[18] For example, a BBC news article stated that Meta and Tiktok recently disclosed in a US senate hearing that they each had 40,000 moderators. See Meta boss Mark Zuckerberg apologises to families in fiery US Senate hearing - BBC News, Under the DSA, Meta disclosed that they have approximately 259 million average European Union users monthly and Tiktok disclosed that they have on average approximately 135 million.

content moderation, For example, a 2021 media article revealed that Facebook pays $500 million a year to outsource content moderation to Accenture.[19]

There is some evidence that the big 4 are building capacity in areas related to online harms audits due to their diversification into digital consulting. Media searches reveal that the big 4 audit networks made approximately 200 acquisitions between the 1st of January 2018 and the 31st of December 2023, 68% of these acquisitions had a digital/technological focus. Conversely the next largest 6 networks in terms of audit fee income made just 62 acquisitions with 34% having a digital/technological focus.[20]

Equally several of the big four firms have released press statements in 2023 on the DSA audits. Deloitte has encouraged large platforms to reach out them for further information these audits and another by PwC stated it planned to host a roundtable for its existing clients on the implications of the DSA.[21]

We therefore predict that the big four will conduct most of, if not all, the external audits required under the DSA and indeed this would likely be the same if external audit was introduced in the OSA and the market for OSA audits would likely be highly concentrated.

In a recent consultation response[22], Broughton Micova and Calef argued that the concentration in the provision of DSA auditing would put significant standing setting power in the hands of a few large audit networks. These entities would gain a first mover advantage in terms of establishing standards, defining concepts, benchmarks and language used in relation to policy goals. This would likely be the same if a market was immediately developed for OSA audit. This would mean that DSA auditing market would automatically be rather concentrated. Moreover, as mentioned above, this feature would be exacerbated by the legal incompatibility of providing other types of auditing services, such as financial and sustainability reporting.

Equally they cautioned there may be an increased risk of collusion as the big 4 would now be competing in both the DSA audit market and the financial audit market for same firms. This increases their potential gains from collusion. Furthermore, due to the small number of firms, the normal rules on limiting financial auditors from conducting other services could lead to the creation of timed monopolies.

Another issue is that if Ofcom was to create a market for independent audit of illegal harms mitigation, then this market would require regulatory oversight. This is the issue of '*who audits the auditor?*'. In this circumstance it would probably fall on Ofcom to do this itself, which would impose another duty and cost upon Ofcom, at a time, when as a consequence of the OSA, its regulatory duties are already expanding significantly.

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

[19] See Rob Litterst (2021) 'Facebook is paying Accenture $500m a year to moderate content on its platforms, the Hustle. Available at Facebook is paying Accenture $500m a year to moderate content on its platforms - The Hustle.

[20] This data is available on request.

[21] See The path to audit for very large online platforms and search engines | Deloitte UK 2023. Deloitte state that their team has 'extensive experience helping firms gain comfort over complex regulation, algorithms, and AI. If you would like to discuss any aspects of DSA audit-readiness, please feel free to get in touch'.

[22] Broughton Micova, S. and A. Calef, (2023). Feedback on draft EU Delegated Regulation Ares (2023) 3171302 on the Performance of Audits of Very Large Online Platforms and Very large Search Engines, Centre for Competition Policy, University of East Anglia, June 2023.

Response: No

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service's risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response: Ofcom's four step process for risk assessment is clear and in line with experience from other sectors. We particularly appreciate that Ofcom has made very clear that its risk profiles are presented as starting points, and that services should not be limited by these. Our research[23], which examined the experience of risk assessment in the financial services sector and the existing evidence of harm from online services suggests that services should account for the role of their interlinkages with other services, such as through functionalities or shared assets or user groups in their estimation of the potentiality and impact of illegal content offences. This will necessarily be service specific. Ofcom's Guidance in annex 5 section 2.1 that services should consider "any additional characteristics" should be able to encompass these considerations, though it might be useful to foreground them as well in Volume 3. In addition, our research suggested that external shocks may be relevant to the potentiality and impact of harm, such as the outbreak of new conflict as we saw with the events in Gaza and the Covid-19 pandemic. Risk assessment mechanisms should take into account such eventualities and model "what if…" scenarios that might suddenly affect the circulation of illegal content. This could be reflected both in Volume 3 and the Guidance. Other research by our team has also suggested that an important consideration in terms of assessing harmful impact will also be time.[24] The accumulation of harm from content over time can increase the impact as well as result in the secondary or pollution-type effects discussed in our answer to section 6.1. This could be reflected in the Guidance in list of key judgements for assessing impact in A5.65 and other areas.	

[23] Broughton Micova, S. & Calef, A. (2022) *Elements for Effective risk Assessment under the DSA* https://cerre.eu/publications/elements-for-effective-systemic-risk-assessment-under-the-dsa/

[24] Broughton Micova, S. (2021) *What's the harm in size?* https://cerre.eu/publications/what-is-the-harm-in-size/

Ofcom's decision not to opt for risk profiles based on service type seems appropriate. As our research demonstrated, there can be strong interlinkages among services of different types, especially with part of the same corporate ecosystem or relying on shared assets as part of their business model or for mitigation mechanism[25]. Maintaining separate risk profiles may discourage service providers from considering the way these interlinkages may increase or decrease levels of risk. It also would make it difficult for the framework to adapt to new types of services that may combine or push the boundaries of the existing type categories as defined.

Ofcom's decisions not to opt for individualised risk profiles for the 15 priority harms. We view this also as an appropriate decision, not just for the reasons noted in 9.81 (page 62) and table 9.3, but also because some of the priority harms can easily be interlinked or have exacerbating effects on one another. Research we are currently conducting on risks to electoral process has uncovered evidence of links among what could be considered illegal hate offences, false communication offences and FIO, for example.

We appreciate Ofcom's high level approach to the core inputs to risk assessment set out in table 9.4. Especially useful is the general category of relevant data that the service already holds. One of the greatest hurdles to overcome in the area of digital services or platform regulation is the information asymmetry between the services on the one side and the regulators, researchers and civil society organisations on the other. This is a clear finding already evidenced in research we are currently conducting related to the implementation of the EU's Digital Services Act. Only the individual services know exactly what data they are collecting and holding on to, so trying to require specific types that Ofcom is already aware of would have been quite limiting. This more general approach to this core input, combined with Ofcom's investigatory powers and the dialogue it aims to maintain with the regulated services should encourage the inclusion of a greater and consistently growing evidence base on the risks.

Ofcom has produced a commendable and appropriate list of enhanced inputs. We suggest one additional enhanced input, **consultation with other service providers** for inclusion in Volume 4 and Annex 5. Some inputs in this category already exist due to collaboration on some priority offences, particular CSEA and Terrorist content, that are happening at the transnational level. Shared insight on sources of risk and the effectiveness of certain measures is being or can be generated through these. As we have previously argued, due to the multi-homing of users, common interlinkages with third parties, reliance on common assets and other factors there could be significant value in communication and sharing of insight among services[26]. Rather than seeing this as collusion in a competition sense, this should be viewed as responsible corporate behaviour to mitigate harm to individuals and society. Many services have common users, similar user bases, and similar functionalities. Examination of combined data may give different insight as to the level of risks posed by certain functionalities or the effectiveness of certain mitigation measures.

Ofcom's guidance on conducting risk assessments set out in Annex 5 is generally thorough and clear. It is commendable that the guidance repeatedly encourages services to not be limited by the Risk Profiles or core inputs suggested, and to bring as much evidence to

[25] See Broughton Micova, S., & Calef, A. (2023). Elements for Effective Systemic Risk Assessment under the DSA. Available at SSRN 4512640. Available at CERRE-DSA-Systemic-Risk-Report.pdf

26 See Broughton Micova, S., & Calef, A. (2023). Elements for Effective Systemic Risk Assessment under the DSA. Available at SSRN 4512640. Available at CERRE-DSA-Systemic-Risk-Report.pdf

bear as possible. The guidance also appropriately points out in A5.46 that services should take "reasonable and proportionate" approaches to non-priority illegal content such as false and threatening communication. Our research[27] supports Ofcom's decision to include business development related changes in the list of design and operational changes (A5.135) that should be considered significant enough to merit additional risk assessment. As noted, certain acquisitions, changes in ownership or revenue models, as well as changes in growth strategy can affect the levels and nature of risk in various ways and should trigger assessments.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See Above
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:
i) Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response:
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

[27] See Broughton Micova, S., & Calef, A. (2023). Elements for Effective Systemic Risk Assessment under the DSA. Available at SSRN 4512640. Available at CERRE-DSA-Systemic-Risk-Report.pdf

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response:	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: Ofcom might consider whether 5 years is sufficient time to require records be kept given the planned supervision approach and level of learning that needs to take place on both sides. In the UK accounting records must be held for 6 years for the purposes of auditing. The difference is not great, so the 5 year limit is largely in line with records for other purposes, however it might be worth raising it to 6 or 7 in this early stage.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: Yes, as with financial records and others required of any firm there seems no justification to exempt at this time. Given the potential for rapid growth of services in this area, it seems prudent that they should keep records from the start in case they need to be referred to later as risk levels increase.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:
i) Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: We commend Ofcom on its overall approach to developing the Code and the way in which the topics to be covered were broken down. We note the reservation with which Ofcom approaches areas where the body of evidence to support a particular measure or practice is not yet developed. We can also see a precautionary approach being taken in relation to CSEA, which is appropriate given the nature of the harm. As Ofcom notes, some of the same measures are used by services in relation to terrorist content, namely those relying on hash databases. We agree that Ofcom is right not to require such measures at this time and appreciate Ofcom's recognition that an ecosystem of larger and smaller services, and sophisticated networks, can be involved in this offence. There are also greater risks to freedom of expression from misidentification of terrorist content. However, Ofcom might suggest that large services participate in collaborative efforts to identify trends and specific sources of risk such as radicalisation pathways enabled by interlinkages among services, dissemination networks for legal yet extremist content, or common practices that might be identified as grooming for terrorist purposes. It also might suggest that services engage in specific data gathering in order to begin to establish an evidence base on the effectiveness of measures. Wherever performance targets are discussed in Volume 4 in relation to U2U and Search content moderation, Ofcom makes very clear that such targets should be based on both speed and accuracy and not speed alone. This approach seems to be aimed at mitigating the risk of over-removals or over-blocking, which can have a stifling effect on freedom of expression and other fundamental rights. This is a welcome approach. As has been argued, there are commercial incentives to standardise, automate and centralise content moderation in larger services, which can remove it from context and result in being overly cautious in some grey areas.[28] It might be helpful in this section to give some indications of how accuracy should be determined to ensure this is a useful measure. It could be suggested that the data on complaints made and upheld might be useful indicators and that input from external organisations can be useful to regularly test content moderation systems. Such an approach has been used since 2016 for monitoring the implementation of the Code of Conduct on Countering Illegal Hate Speech Online[29] and many of the large services are already familiar with the process. We also welcome Ofcom's consistent recognition of the importance of language capabilities throughout its approach. Initial findings from research we are currently

[28] Caplan R. (2019). *Content or context moderation? Artisanal, community-reliant, and industrial approaches*. Data & Society Research Institute. https://datasociety.net/library/content-or-context-moderation/

[29] See information on the monitoring rounds: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#monitoringrounds

conducting has already flagged up this as critical to efforts to combat harmful content and to adequately protect freedom of expression. Ofcom has appropriately highlighted capacity in the diversity of languages used in the UK in the section on resources and capabilities for content moderation (V4, 12.148). Though a decision was made not to require specific language use, attention was drawn to language in recommending that services consider the nature of their user base when designing complaints systems (V4, 16.48).

We generally agree with Ofcom's approach to measures related to complaints handling, which are generally in line with instruments in other jurisdictions. Ofcom rightly notes that rather than negatively impacting freedom of expression, these measures should help to ensure it is protected. We also believe that it is not useful at this stage to require complaint tracking or responses in a specific timeframe. However, we are somewhat concerned with Ofcom's attribution of the human right to freedom of expression rights to the services themselves in its discussion of the impact on rights in paragraph 16.112. Requiring service providers to provide information that is relevant to consumer protection is normal across sectors and crucial to the exercise of regulation.

We appreciate and agree with Ofcom's decision to limit prescriptions in the Code on blocking users' access to when CSEA has been disseminated and to terrorist groups proscribed by the UK government. Given the severity of the harms in question the precautionary principle should apply and these measures included in the Code despite the lack of definitive evidence on effectiveness. As long as the elements covered in the complaints handling part are also in place, there should be effective recourse for those who feel unjustly blocked.

We agree with Ofcom's reasoning and approach on the use of schemes that purport to verify identity (notable user and monetised schemes) and its choice to not require identify verification as a measure for mitigating harms. Transparency and appropriate internal policies are especially important when services offer monetised labelling schemes that can be easily manipulated to deceive users. The option of anonymity, especially on major services that act as public spaces, remains important for preserving freedom of expression and the practice of journalism. We look forward to future consultation on age verification measures.

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 13:	
i)	Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?

Response: Yes. Illegal content offences can be perpetrated on smaller, niche services, and often these are used for some of the most egregious ones in order to avoid detection. However, size in the form of reach and market power do matter when it comes to harmful impact due to reach, the often public nature of the dissemination, and the potential for contagion.[30] In addition, research that we are currently undertaking has already collected evidence from monitors on the dynamics of FIO and false communication offences that

[30] Broughton Micova, S. (2021) *What's the harm in size?* https://cerre.eu/publications/what-is-the-harm-in-size/

indicates that the large popular services can be gateways to the less-moderated smaller or private services, or used for fishing. For example, links shared on popular social media that do not meet the threshold for actionable content, and may be bot-generated, are used to entice users into Telegram groups, or other closed spaces. Mitigation measures taken at the level of the larger services can still help mitigate these risks.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 14:
i) Do you agree with our definition of large services?
Response: Yes, as discussed in question 5 it appears that the 10% threshold appears suitable as most of the platforms on the '*very large*' list are comfortably over the threshold, a trend which is likely to be similar in the UK's '*large*' list. Therefore, most of the largest services should be captured by the 10% threshold. Equally, we support Ofcom's suggestion that having the same methodology for designating a service as large under the OSA or very large under the DSA should reduce the burden on services. The notion that once as firm is designated as large that it cannot drop below the large threshold unless it registers average monthly users below the threshold for 6 months appears reasonable, as if a firm is very close to the threshold and goes over it/under it on a monthly basis then a prudent approach seems appropriate.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 15:	
i)	Do you agree with our definition of multi-risk services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?
Response: The draft Codes reflect the approach described in volume 4 so the comments in response to those questions generally apply. One specific thing we noticed with appreciation is that measure 5E(i) in both draft Codes makes it clearer than volume 4 did that performance targets on both speed and accuracy are expected for complaints and appeals as well as for content moderation processes. This is an important clarification that can help counterbalance the incentives of the services. We also note that measure 4E makes it clear that language should be a consideration in how services take into account the nature of their user base for the purpose of resourcing. This is in line with our response above.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 17:	
i)	Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Content moderation (User to User)

Question 18:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.

Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:	
i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response:	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response:	

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response:	
ii)	What are the underlying arguments and evidence that inform your view?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:
i) Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response: We recognise the approach described in volume 6 as in line with Ofcom's approaches to regulated services in the other sectors it oversees. This demonstrates coherence and will likely allow Ofcom to leverage its experience in dealing with audiovisual media services, video-sharing platforms, telecommunications providers, and others. Ofcom rightly adopts a broad understanding of appropriate sources of information and lists in paragraph 28.55 several sources including "other bodies, such as other regulators, MPs or consumer organisations." Given that the EU's Digital Services Act enables special access to vetted researchers, there is potential for significant growth in the research conducted by academic institutions and civil society organisations on the risks and harms associated with online services and mitigation measures relevant to the illegal content offences covered by the OSA. Given constraints on capacity and funding, not all of the insight gained will be quickly published. We suggest therefore that is worth mentioning academic institutions and wider civil society organisation (in addition to consumer ones) to highlight that information channels beyond publicly available ones will be open. It also might be useful in relation to information sources to specifically mention Ofcom's special relationship with the ICO and the CMA through the Digital Regulation Cooperation Forum. These would fall into the category of other regulators, but the DRCF will be a UK specific source of information and a forum in which information gathering priorities can be set leveraging the powers of each of the three UK regulators. Information from regulators from other jurisdictions, such as those designated as digital service coordinators in the EU and other members of the Global Online Safety Network, will certainly also be very useful but will we expect will play a different role in Ofcom's work. The importance of the Supervision approach outlined by Ofcom in Volume 6 should not be understated. Though it is not stated in the document, the "understanding phase" is in fact a necessary first step in correcting the information asymmetry that currently exists. To make effective use of information gathering and investigative powers, Ofcom will need to learn in this phase what information is generated by the services' processes and what gaps might exist in data to evidence the nature and scale of risks and effectiveness of mitigation. It would be therefore advisable that the supervisory strategy focus set out in paragraph 30.16 also include a point on understanding the data and information generated by processes.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See Above

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response:	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	