Your response

Question	Your response
Question 1: Do you have any views on our audit-based assessment, including our proposed principles, objectives, and the scoring system? Please provide evidence to support your response	Consultation 4.22 P31 Proposed objectives: Technical Performance; For the testing of technical performance to be effective, technologies need to be tested against real CSEA material datasets. If datasets are to be representative of the harm being detected (CSEA), then there should be expanded reference to the management of illegal material. There should be further guidance on the considerations required to include staff welfare, security, re-victimisation, offences committed in creation and distribution of indecent images of children unless a legal agreement with guardrails, checks and balances have been put in place. Consultation 4.30 P31 Proposed objectives: Robustness; 'Developed in a secure environment'. The terminology seems vague and publishing of more detailed agreed standards would be beneficial. There are likely published government standards available. This will ensure the data's security guardrails are consistent across technology developers. Consultation 4.33 P31 Proposed objectives: Robustness; In terms of ensuring a reliable operation, there should be the ability to 'scale up' to cope with large demand of CSEA content scanning. This will ensure both large and small online service providers can utilise the accredited technology. Consultation 4.34 P31 Proposed objectives; Robustness, Detection and Mitigation of Threats. Technologies have to be able to adapt to tradecraft of offenders. Offenders will circumvent measures which will erode the trust, integrity and accuracy of the accredited technology. Ability for this constant evolution to keep ahead of offender's methodology is essential. Consultation 4.40 P32 Proposed objectives: Maintainability: There should be established procedures for the non-emergency updating of software to avoid it becoming

Question	Your response
	obsolete and incompatible with latest infrastructure changes. For example, online service providers might update their core infrastructure quicker than the accredited technology can be upgraded. Annex 11 A13.4 P8 Illegal and benign data: There should be an explicit ratio of the split of benign vs illegal data required to be used in the testing of the minimum standards of accuracy. The use of predominantly benign data will lead to a vast disparity in accuracy between datasets and undermine the accuracy of accreditation. Companies will need to be informed that it is illegal in the UK and other jurisdictions to create or distribute CSAM for this purpose without specific legal agreements and controls in place. [redacted] Annex 14 4.7 P15 Technical Information, Application form; Privacy and legal considerations) It would be beneficial to additionally know what if any data sharing agreements the applicant organisation has in place for the legal use of CSEA data.
Question 2: Do you have any views on our proposals for independent performance testing, including the two mechanisms for setting thresholds; the approach to testing technologies in categories against particular metrics; and data considerations? Please provide evidence to support your response.	Consultation 4.50 P36 Prescribed vs benchmarked thresholds. We agree that benchmarked thresholds offer the flexibility compared to prescribed thresholds but we need to be cautious that benchmarks don't degrade over time. Benchmarks should drive technology up not the other way around. Benchmarks are more appropriate for CSEA content as this will limit the amount of different illegal content datasets that will need to be acquired, reducing the legal administrative burden. Consultation 4.66 P39

Question	Your response
	It should be ensured that the testing of text, images and video should be effective for synthetic, partially-synthetic, indeterminate and real images. There should also be effective mechanisms to ensure that each type has a marker for flag to differentiate it and help assess risk.
Question 3: Do you have any comments on what Ofcom might consider in terms of how long technologies should be accredited for and how often technologies should be given the opportunity to apply for accreditation? Is there any further evidence we should consider?	General themes: Effectiveness of accreditation Technology development could easily outpace the accreditation process, leaving it unattractive for firms to invest in accredited technology as it is outdated. We want this to be avoided as investment not only spurs innovation, but leads to better online safety outcomes. Careful consideration will need to be made over the length of time it would take to accredit and then re-accredit to ensure effectiveness. General themes: Multiple tools/processes required It is unlikely that part 3 services will use one tool in isolation to combat Image, URL, Video instances of CSEA material. Likely that peripheral tooling and human moderation in addition to increase accuracy. This could make accreditation complex to administer for in house solutions. General themes: Flexibility There needs to be flexibility with accreditation and the context of the company the technology that it is being applied to. End to end processes may need to be assessed in their entirety, to ensure that accuracy is effectively tested, as multiple tooling could impact results. General themes: Global Consistency There could be greater adoption and engagement with online service providers there is global consistency with accredited technology. There will need to be alignment with other online harms regulators who adopt similar accreditations for the same technologies. Services will want to avoid having to use different tech in different regions. Consultation Measure could be stronger The consultation does not identify specific technologies that prevent CSEA in a particular environment only where it is technically feasible. This needs to be

Question	Your response
	strengthened to say that if it is not technically feasible then the onus is on the company to prove it can't be done, by providing detailed rationale under an agreed feedback framework explaining why it is not feasible. This would then allow Ofcom to see where companies can adapt to make things possible or where it is genuinely not feasible. This puts greater responsibility on the company and also gives Ofcom greater insights as to how to develop regulation to have greater impact in specific areas. Consultation Further explanation Best endeavours' definition needs to be clear as they are primarily subjective which could lead to differing standards across technologies Consultation Consistency of accreditation If 3rd party companies are accrediting technologies on behalf of Ofcom, it must be ensured that they are all consistently accrediting to the agreed standards, where the technologies will be complex and innovative and require a high level of expertise. Consultation 3rd party organisation standards If 3rd party partners are used in the accreditation process, there needs to be clear ethical boundaries in place. There should be appropriate checks and balances put in place to ensure issues of impartiality, suitability and conflicts of interest are discovered and appropriately dealt with in a transparent manner.
Question 4: Do you have any views on how to turn these proposals into an operational accreditation scheme, including the practicalities of submitting technology for accreditation? Is there any additional evidence that you think we should consider? Please provide any information that may be relevant.	Consultation Testing accuracy Technology companies applying for audit-based assessment will need to test their tech against real CSAM to ensure accuracy. Who will supply the test data, who will assure it (including ensuring it stays reflective of real-world conditions), who will store it and will there be assurances against prosecution for each company? To have an effective accreditation scheme, the ability to trust the assessment and performance testing results is critical. This can be achieved by using the same testing datasets across technologies and ensuring test data

Question	Your response
	replicates real world application of the technology, i.e. real CSAM.
Question 5: Do you have any comments on our draft Technology Notice Guidance?	There should be specific guidance for technology companies on how they navigate legislation when creating, testing and distributing material connected to child abuse. Clear instructions here are important to enable companies to operate in this space safely and legally and help avoid blockers from the outset.

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