

How Ofcom is approaching online safety risk assessments

The [Online Safety Bill](#) is passing through Parliament, and Ofcom is continuing preparations as the future regulator. Risk assessments will be a fundamental part of the new regime and will require online platforms and search services to have a clear understanding of risks of harm to users and effective risk management processes. Here, we explain our proposed approach to risk, and how we intend to support services in carrying out their assessments.

At the time of writing, the Online Safety Bill has reached Committee Stage in the House of Lords. Many details of the legislation – including proposed amendments – are still being debated, meaning that future regulatory requirements for online services are still liable to change. However, it is clear the future online safety regime will require regulated services to better understand the risk that users will encounter illegal content or content harmful to children online.

The Bill will require all firms in scope of regulation to do a risk assessment of illegal content that may appear on their service, ranging from online fraud to terrorism. Services that are likely to be accessed by children will also have to do a risk assessment looking at content which is harmful to children. This is likely to include material such as pornography and content which promotes eating disorders. Ofcom will produce guidance to help services meet these requirements.

As a cornerstone of the regime, it will be important for regulated services to understand what good practice looks like for risk assessment and risk management. While it will be up to services to do their own assessments, our role as the future regulator is to provide guidance to services, helping them focus on illegal content and content that is harmful to children, explain how this content might appear on their service, and promote good practice around risk management as a fundamental part of service design and organisational culture.

A good risk assessment should help a service anticipate and address the ways in which their users could be exposed to greater risks of harmful content. They should ask questions like:

- How does the service's user base affect this risk; for example, do large numbers of child users in the UK increase the risk of exploitation?
- How do the functionalities of the service affect risk; for example, does offering stranger pairing increase the risk of romance fraud?
- What effect does the service's business model have; for example, how can a service's financial incentives under a given revenue model increase the risk of hosting harmful content?

With Ofcom's help, services can answer these questions and prepare to comply with the safety duties under the Bill and to use Ofcom's Codes of Practice.

Once the Bill passes, we will consult on our approach to risk assessments. This will be an opportunity for services and other stakeholders to review our plans in full and provide feedback. We are committed to providing comprehensive guidance to services about what risks they need to look out for; how they should assess them; and what they should do about them. In addition to our

engagement with industry and civil society organisations, we hope that early indications of our proposed approach will be instructive for services preparing for the new regulatory requirements under the Online Safety Bill.

Improving online safety through better risk management

Good risk management is key to ensuring positive outcomes for online safety. In practice, risk management is not a single process or activity, but a broader approach by companies that puts risk-awareness at the forefront of decision-making, operations and organisational culture.

Ofcom is focused on risk management because it can increase the likelihood of an organisation achieving its objectives, improve decision-making and accountability, and boost confidence and trust among stakeholders, among other benefits. In the online environment, where harms and potential measures to address them are constantly evolving, a risk management-focused approach can help organisations be proactive, responsive and agile to protect their users.

We have learned from our review of best practice and industry standards that good risk management relies on a culture of risk awareness and risk prioritisation by all teams across an organisation. In internationally recognised standards (e.g. [ISO 31000](#) and the [Three Lines Model](#), both widely adopted in corporate risk governance) this risk-focused culture is framed as a fundamental part of governance and leadership within an organisation, whose key objective should be to define the vision, mission, values and appetite for risk.

Having appropriate and well-developed risk assessment processes is a central feature of good risk management. Under the video-sharing platform (VSP) regime, Ofcom already regulates UK-based video-sharing platforms. While the VSP regulations do not require risk assessments, we strongly encourage VSP providers to put a process in place to assess and manage risk. We know some services have already developed such systems. As such, we have first-hand experience of the role that risk assessments can play in helping services understand and respond to harms to users, and the challenges that a lack of attention to risk can present. In the context of the Online Safety Bill, responses to our [call for evidence on illegal content](#) highlighted the role that risk assessment plays in improving firms' awareness of illegal and harmful content as it arises on a service.

As such, a key aim for Ofcom when we assume our responsibilities as the online safety regulator will be to promote good risk assessment practices and to advocate for strong governance and risk management more broadly. In practice, this will mean that our proposed approach to risk across the regime will be framed to achieve the following outcomes:

- That risk assessments are an **integral part of broader risk management processes** and embedded within an organisation's existing risk management structures.
- That **responsibilities** for risk management are clearly specified and **owned** at the most senior levels.
- That risk management activities are **regularly reported** to senior decision-makers, and **independently scrutinised** where possible.
- That risk controls are **assessed for effectiveness**, and emerging risks are monitored.

How risk assessments will work in the diverse world of online services

We recognise that a huge range of services will be in scope of the regime, from one-person microbusinesses to global tech giants. While all services must complete risk assessments, it will not be proportionate to set the same regulatory expectations for everyone. We have reviewed a broad range of literature on best practice in governance including the [Digital Trust & Safety Partnerships Safe Framework](#), [HM's Orange Book](#) and Ofcom's commissioned research by Milliman into best practice in risk management and organisational governance. This has highlighted the following:

- Most industry guidance on governance structures is principles-based, reflecting the diversity of organisations and their operations, and recognition that good governance is more dependent on effective communication and oversight than resource or capacity.
- Nevertheless, there is recognition that size and capacity of an organisation may have an impact on how detailed and comprehensive risk management and governance processes are.

To reflect this, Ofcom will publish **risk assessment guidance**, setting out how all services can meet their obligations under the regime and how to complete a suitable and sufficient assessment. We propose that what is suitable and sufficient will vary service by service; some services will be able to rely heavily on resources provided by Ofcom and information from users, while others will need to do much more work to assess risks accurately and adequately.

Ofcom will publish a sector-wide **register of risk** assessing the risks of harm presented by illegal content on user-to-user and search services, and **risk profiles** which will set out key risk factors services should take account of when they conduct their risk assessment. We will also produce Illegal Content Judgements Guidance to explain the offences covered by the Bill and help services make judgements about whether content is illegal content for the purpose of the online safety regime.

Our expected approach to risk assessment guidance is to outline a four-stage and repeatable process for assessing risk. We will consult on this once the Bill has passed. This approach aligns the regulatory requirements under the Online Safety Bill with best practice frameworks in risk management. There is no one-size-fits-all approach, but we consider that the following four steps are likely to be relevant to any robust risk assessment and can be applied by services of all types and sizes.



Based on our literature review, there is significant consensus around best practice and the key principles of risk management. The literature emphasises the need for risk assessments to be conducted in stages, and as part of a cyclical process of evidence-gathering, evaluation and review. Our four-step process reflects these principles. We have corroborated this best practice approach with evidence from industry, including as part of Ofcom's work with VSPs and our Call for Evidence last year. We will therefore propose that all services should engage in each step of the process, noting that the level of detail they should go into, and the amount of time and resources required for each step will vary significantly depending on the size, capacity and risk factors of the service.

To this end, our guidance will also cover the kind of evidence we think services should consider in their risk assessments to ensure it is suitable and sufficient. At a minimum, we would expect services to consider the types of information they are required to collect as part of online safety regulation, as well as any other relevant data they hold. We are also currently considering which other inputs to a risk assessment would be reasonable to expect of all services, and which do not place an unnecessary burden on smaller or less-resourced businesses.

Some services are likely to be better placed to draw on a broader evidence base for their risk assessments and may already have well-developed measures and metrics for assessing risks of harm to users and the effectiveness of their protections for users. Depending on the size and complexity of a service, it may be necessary for an organisation to consider a range of sources of evidence to inform their risk assessments. As such, we propose to outline in our guidance an additional set of evidence inputs for these services, which they can consult to ensure their assessment meets the required standard for a robust and accurate risk assessment.

We are also aware that services will need to comply with obligations in different legal jurisdictions; for instance, the largest services will also conduct a risk assessment under the EU's Digital Services Act. We are working with services and our international regulatory counterparts to share insights, best practices, and to work towards international coherence around the novel regulatory approach that is risk assessments for online safety.

We anticipate that our guidance on appropriate metrics, measurements and inputs to develop a robust risk assessment will evolve as the regime develops and risk assessment becomes more embedded among regulated services.

Next steps

As set out in Ofcom's 2022 [roadmap to regulation](#), we will launch our first consultation on our approach to illegal content risk assessments as soon as we can after our powers commence. This will include consultation on our risk assessment guidance, register of risk and risk profiles for illegal content. A separate consultation on children's risk assessments will follow.

Once we have completed the consultation process on the illegal content duties, we will issue a statement to finalise our first set of risk assessment guidance. Services will be required to carry out their first illegal content risk assessments within three months of Ofcom publishing this guidance.

We will be providing further detail of our proposals in the consultation. We welcome feedback and engagement with services on our approach to risk assessment and our guidance for services as part of that process.