Protecting people from illegal harms online

Annex 5: Service Risk Assessment Guidance

DRAFT FOR CONSULTATION

Published 9 November 2023
Closing date for responses: 23 February 2024

A5. Service Risk Assessment Guidance

Introduction

A5.1 This guidance aims to help services regulated by the Online Safety Act 2023 ('the Act') comply with the illegal content risk assessment duties. The purpose of the risk assessment is to improve your understanding of how risks of harm could arise on your service and what safety measures you need to put in place to protect users. It is essential that you complete an illegal content risk assessment to meet your duties under the Act.

A5.2 The guidance will help you understand what your obligations are and how you can fulfil them. You can navigate the guidance using the table of contents below. It includes four sections and two annexes:

- **i)** **Risk assessment guidance summary**: A summary of your legal duties and an introduction to how you can fulfil them.
- **ii)** **How to carry out a risk assessment – four-step methodology**: A step-by-step process for all services to follow, setting out how we recommend you carry out risk assessments in practice and how that process can help you meet other duties under the Act.
- **iii)** **What evidence to assess:** Guidance on the evidence that different services should consider when assessing risks. This is made up of core evidence which we believe all services should consider at a minimum and additional enhanced evidence which some services may need to consider to ensure their assessment is accurate.
- **iv)** **When to review or carry out a new risk assessment:** Guidance on how to keep a risk assessment up to date and the circumstances under which you need to carry out a new assessment.
- **v)** **Appendix A on Risk Profiles:** A series of tables which set out the risk factors (such as particular features and functionalities) that your service may have which are likely to lead to specific kinds of illegal harm.
- **vi)** **Appendix B on offences:** For reference, the list of illegal offences that are covered by the Act.

A5.3 This document provides a comprehensive explanation of Ofcom's recommended approach to the risk assessment duties, but we also provide supporting resources and tools on the Ofcom website to help you understand and meet your obligations. As well as covering risk assessments, our resources will help you decide if your service is regulated under the Act, how to fulfil your safety duties, and how to address other obligations you may have.

Contents

Risk assessment guidance summary

What are the illegal content risk assessment duties?

A5.4 If you provide a user-to-user ('U2U') or search service, you must carry out an illegal content risk assessment. This legal obligation requires you to assess the risk of illegal harms that your service presents. This guidance aims to help you meet your duties, and you can also consult the detailed research and analysis of the harms in our Register of Risks.

A5.5 The Act sets out the specific elements that an illegal content risk assessment needs to include. In particular, you need to take into account your service's characteristics – such as its user base and functionalities – and consider how they affect **the likelihood and impact** of each kind of illegal harm occurring on your service.

A5.6 Your risk assessment must also be **suitable and sufficient**, which we explain in more detail below.

A5.7 Once you have completed your first risk assessment, there are several duties relating to reviewing, updating or completing new risk assessments:

- You must take appropriate steps to keep your risk assessment **up to date**;
- You must update your risk assessment if Ofcom makes a significant **change to a Risk Profile** that relates to your service; and
- You must carry out a further risk assessment before making **any significant change** to any aspect of your service's design or operation.[1]

A5.8 You need to **keep a record** of each risk assessment you carry out. Alongside this document, we have published Record Keeping and Review guidance to help you.

A5.9 To help services meet all of these requirements, our guidance sets out a **four-step risk assessment process**. Following this process will help you comply with the illegal content risk assessment duties and the linked safety duty and record keeping duties.

What is a 'suitable and sufficient' risk assessment?

A5.10 Risk assessments must meet the requirements of the law, including being of a suitable and sufficient standard.

A5.11 To be suitable and sufficient, your risk assessment must include all the elements of a risk assessment specified in the Act (section 9(5) for U2U services and section 26(5) for search services). It should be **specific** to your service and **reflect the risks accurately**. It is important that you have an adequate understanding of those risks to **implement appropriate safety measures**.

A5.12 Following our four-step process is likely to be the most effective way to achieve this, but summarise the key legal duties below.

A5.13 Your assessment must:

- Assess all the relevant kinds of illegal harm**;**[2]
- Take into account a list of **risk factors** (such as features and functionalities) we have published, with an explanation of how they could increase the risk of harms

[1] We explain what a significant change may involve in A5.132.
[2] See A5.20.

covered by the Act (such as terrorism offences). These tables are called **Ofcom's 'Risk Profiles'** and are included in Appendix A;

Take into account the **characteristics** of your service, including its user base (e.g. user numbers, age, languages, groups at risk, groups increasing risk), functionalities, algorithmic systems (and how easily, quickly and widely they disseminate content) and the business model;

Take into account any other relevant aspects of your service's **design and operation**, including governance, use of proactive technology, measures to promote users' media literacy and safe use of your service, and other systems and processes;

Take into account **how your service is used** – for example, both the intended and unintended ways that people may use your service; and

Considering all this information, assess the risk of different kinds of illegal harm covered by the Act. This will require an assessment of the **likelihood** of each kind of illegal harm taking place, and the **impact** of that harm for users (its nature and severity).

A5.14 Our detailed guidance provides more information on how you should go about evaluating these factors and make a judgement about the risks on your service.

A5.15 Your judgements on risk should be based on **relevant information and evidence** as far as possible, so that they accurately reflect the risks of harm. What is suitable and sufficient will vary by the size and nature of the service, so different services will need to consider different types and levels of evidence and analysis. It's important that the information and evidence you use gives you a sufficient understanding to reach accurate conclusions about the level of risk presented by your service.

A5.16 Our guidance on evidence sets out:

The **core evidence** that all services should consider, including information on your service's characteristics and risk factors (from Ofcom's Risk Profiles), user complaints including user reports, relevant user data, and any other relevant information you already hold. Such information should be readily available to all services, and failing to consider it may mean that the risk assessment is not suitable and sufficient.

Where the core evidence is not sufficient to complete an accurate risk assessment, large services[3] and those operating in a more complex risk environment should consider additional **enhanced evidence.** This may include the results of product testing, content moderation, consultation with technical experts, consultation with users or research into users' behaviours and needs, views of independent experts, independent research, engaging representative groups, and/or external audit or other risk assurance processes. Large services or services which have identified several specific risk factors for a harm will typically need to include some or many enhanced inputs to improve the accuracy of their judgments on risk and ensure their risk assessments are suitable and sufficient.

How you can **decide what evidence you should collect and assess**. You can take an iterative process to assembling your evidence base. We expect that services to consider collecting the enhanced evidence if you are not confident that the core

[3] Large services are those with more than 7 million UK users.

inputs have given you a sufficient understanding to complete a robust, accurate assessment of the level of risk.

A5.17 Using Ofcom's Risk Profiles and the core and enhanced evidence will provide you with a good understanding of how the characteristics of your service increase the risk of illegal content being present on the service, or the service being used to commit or facilitate an offence. However, these resources are not exhaustive, and you should consider whether you need to assess any other characteristics or gather further information to ensure your risk assessment is suitable and sufficient.

When do you need to do a risk assessment?

A5.18 If your service is in operation when this guidance is published on 9 November 2023, you need to complete your first risk assessment **within three months** of this date.[4]

A5.19 If you start a new service or change an existing service so it falls within scope of the Act for the first time, you must complete your risk assessment within three months from starting your new service, or making the change to your existing service.

A5.20 If you are planning to make a significant change to an existing service, you need to carry out a risk assessment **before you make the change.**

What risks do you need to assess?

A5.21 You need to assess the risk of each kind of illegal harm set out in the Act. The priority illegal content defined by the Act includes many individual offences, and Ofcom has grouped these into **15 kinds of illegal harm.**[5] The priority and other offences which are grouped into each of these kinds of illegal harm are set out in Appendix B.[6]

Terrorism offences;
Child Sexual Exploitation and Abuse (CSEA) offences, including Grooming and Child Sexual Abuse Material (CSAM);
Encouraging or assisting suicide (or attempted suicide) or serious Self-Harm offences;
Harassment, stalking, threats and abuse offences;
Hate offences;
Controlling or coercive behaviour (CCB) offence;
Drugs and psychoactive substances offences;
Firearms and other weapons offences;
Unlawful immigration and human trafficking offences;
Sexual exploitation of adults offence;
Extreme pornography offence;
Intimate Image Abuse offences;
Proceeds of crime offences;
Fraud and Financial services offences; and

[4] Please note, this draft has been published for consultation; the three-month period begins when Ofcom publishes the final version of its guidance.
[5] These 15 kinds of illegal harm cover the priority offences, and the relevant non-priority self-harm offence, as explained further below. Other kinds of illegal harm referred to in Ofcom's risk assessment relate to other relevant non-priority offences.
[6] Services can find more information on each offence in Ofcom's Register of Risks, and guidance on 'illegal content' in Ofcom's illegal content judgements guidance.

Foreign Interference Offence (FIO).

A5.22 Our Register of Risks sets out detailed research and analysis on each kind of illegal harm which you can consult where helpful for your assessment.

A5.23 You must assess the risk of each kind of illegal harm occurring on your service. U2U services need to consider the risk of:

Illegal content appearing on the service – for example, content inviting support for a proscribed organisation (e.g. a terrorist group);

An offence being committed using the service – for example, a messaging service being used to commit grooming offences, in a situation where adults can use the service to identify and contact children they do not know; and

An offence being facilitated by use of the service – for example, the use of an ability to comment on content to enable harassment.

A5.24 You must assess the likelihood of these illegal harms taking place, and the potential impact (i.e. the nature and severity of harm to individuals).

A5.25 As long as you are covering all of the risks of harm to individuals, you can assess these three aspects together when you assess each kind of illegal harm.

A5.26 Search services need to consider the risk of users encountering illegal content and the nature and severity of the harm that may be suffered by individuals (but not the risk of an offence being committed or facilitated by use of the search service).

A5.27 All services also need to assess the risk of harm from **relevant non-priority offences** appearing on the service. This does not mean assessing the risk of every possible individual offence occurring on your service. However, if you have evidence or reason to believe that other types of illegal harm that aren't listed as priority offences in the Act are likely to occur on your service, then you should consider those in your risk assessment.

What does assessing each risk involve?

A5.28 You need to assess the level of risk presented by your service for each kind of illegal harm. This means evaluating the likelihood and the impact (i.e. nature and severity) of each kind of illegal harm. To do this, you must consider all of the characteristics covered above and should use evidence about your service to make your assessment. You can then assign a risk level for each kind of illegal harm: low, medium or high.

Table 1: Overview of risk assessments

What do you need to assess?	What should you take into account?	How do you make judgements about risk?
The **likelihood and impact** of each of the 15 kinds of illegal priority harm	Ofcom's Risk Profiles – which help you identify your **risk factors** – and any relevant **characteristics** of your service, including user base, functionalities, algorithmic systems, business model, any user protection or risk mitigation measures, and other relevant aspects of the service's design and operation, and the way the service is used	Review **evidence** about how harm could be experienced on your service and how your service's characteristics increase or decrease risks
Outcome: an assessment of low, medium, or high risk for each kind of illegal harm Our detailed guidance offers help on how to make this decision.		

Source: Ofcom analysis

How should you carry out a risk assessment in practice?

A5.29 We set out a four-step risk assessment process which Ofcom has designed based on best practice in risk management. Following this process will help you comply with the illegal content risk assessment duties, alongside other duties under the Act.

A5.30 To help you carry out your risk assessment, Ofcom has a duty to produce Risk Profiles. Risk Profiles are tables which set out the risk factors (e.g. features and functionalities) that are likely to lead to specific kinds of illegal harm. You should use the Risk Profiles to identify and record the relevant risk factors for your service. You must take the Risk Profile relevant to your service into account when you carry out your risk assessment. These are set out in Appendix A.

A5.31 Services can adopt their own risk assessment methodology, as long as they comply with the risk assessment duties. However, please note that some measures in Ofcom's Codes of Practice are linked to the outcome of your illegal content risk assessment, and are based on services reaching an assessment of whether they are medium or high risk for each kind of illegal harm. So a service that chooses to adopt the measures in the Codes of Practice to comply with its safety duties should ensure that its risk assessment methodology allows it to reach equivalent conclusions on its risk level for different kinds of illegal harm.

A5.32 There are also some measures in Ofcom's Codes of Practice which are targeted at mitigating harms related to CSEA and grooming. We provide detailed guidance on how U2U services can assess the level of risk related to these harms in A5.73.

Introduction to the four-step process for risk assessments

Step	Key activities	Outcomes
1. Understand the harms	• Identify the harms that need to be assessed (see list above); and • Consult Ofcom's Risk Profiles – these are a list of risk factors and the harms they are associated with. You should look at this list and consider which risk factors you have. This will help give an indication of what harms are more likely to occur on your service.	• You have **established the 15 kinds of illegal harm** that need to be assessed as part of a risk assessment; • You have understood the need to assess the **presence of illegal content** on your service and, if you are a U2U service, how your service may be used to **commit** or **facilitate** an illegal offence; and • You have **consulted Ofcom's Risk Profiles**, to identify the risk factors your service has for each kind of illegal harm.
2. Assess the risks of harm	• Consider any additional characteristics that may increase or decrease risks of harm on your service; • Assess the likelihood and impact of each kind of illegal harm; and • Assign a risk level for each kind of illegal harm, including (if you are a U2U service) by referring to our additional guidance on specific harms.	• You have **assessed the risks** of harm of the 15 kinds of illegal harm by considering the likelihood and impact of each, taking in to account the risk factors highlighted by Ofcom and your own evidence; • For **CSEA and grooming**, you have considered our additional guidance on assessing risk and assigned a risk level to each; and • You have assigned a level of risk of **low, medium or high** to each of the 15 kinds of harm.
3. Decide measures, implement and record	• Decide on the appropriate measures to reduce risk of harm to individuals, including by consulting Ofcom's Code of Practice; • Consider any additional measures that may be appropriate; • Implement all measures; and • Record the outcomes of the risk assessment	• You have **decided the measures** your service is going to implement to reduce the risk of harm to individuals by consulting Ofcom's Codes of Practice or by considering alternative ways to meet the safety duties; • You have **implemented** and made a record of these measures including how you think they meet the relevant safety duties; • You have made a **complete record** of your risk assessment, as per Ofcom's guidance on record keeping and review.

4. Report, review and update risk assessments	• Report on the risk assessment and measures via relevant governance channels; • Monitor the effectiveness of mitigation measures; and • Review your risk assessment.	• You have **reported your risk assessment findings** through appropriate governance channels; • You have established an **annual review** cycle for your illegal content risk assessments; and • You have **understood the triggers** set out in the Act for when you should review your risk assessment.

Source: Ofcom analysis

What happens if you do not complete a suitable and sufficient risk assessment?

A5.33 If we suspect your service has failed to carry out a suitable and sufficient risk assessment properly or at all, then we are able to take enforcement action. Any decision on whether to take enforcement action would be made in line with our **online safety enforcement guidance**.[7] Where appropriate, we may first engage with your service to ensure you understand what you need to do to meet the requirements of the law.

A5.34 In the event that we decide to open an investigation and find that your service has contravened its obligations, we have the power to impose a penalty of up to **10% of qualifying worldwide revenue or £18 million** (whichever is the greater) and require remedial action to be taken.

A5.35 As part of any remedial action, where we identify a **risk of serious harm which your service is not effectively mitigating or managing**, we can require that you comply with parts of the illegal content safety duties that require your service to mitigate and manage the risks identified in the relevant risk assessment despite the fact you did not identify the risk in your risk assessment (or failed to carry out a risk assessment at all). The intention is that your service will be required to mitigate the risk that we have identified despite you not having identified it in your own risk assessment.

[7] See Annex 11 (Enforcement guidance).

How to carry out a risk assessment: four-step methodology

A5.36 This methodology sets out a four-step process based on best practice in risk assessments:

i) **Understand the harms**

ii) **Assess the risk of harm**

iii) **Decide measures, implement and record**

iv) **Review, report and update**

A5.37 The way you fulfil these steps will vary based on the size and nature of your service. However, the guidance is intended to apply to all services.

A5.38 We expect the outcomes of risk assessments to differ from service to service. However, following the four steps we set out is likely to be the most effective way of ensuring that your assessments are suitable and sufficient and that you comply with the law.

A5.39 To confirm that your assessment meets this standard, you should check that your assessment meets all the elements of the risk assessment duty (section 9(5) for U2U services and section 26(5) for Search services), and that it reflects risks of harm accurately.

Step 1: Understand the harms

Outcomes and requirements of Step 1

You have **familiarised yourself with the 15 kinds of illegal priority harm** that need to be assessed as part of a risk assessment (1.1);

You have understood the need to assess **the presence of illegal content** on your service and, if you are a U2U service, how your service may be used to **commit or facilitate an illegal offence** (1.1);

You have **consulted Ofcom's Risk Profiles**, and identified the risk factors your service has for each kind of illegal harm (1.2).

What you should have recorded

Confirmation that your service has consulted **Ofcom's Risk Profiles**. You may do this by recording the outcomes of the Risk Profiles questionnaire (explained below)**;**

Any **risk factors** from Ofcom's Risk Profiles which are relevant to your service.

Supporting resources

Risk Profiles (Appendix A)
Register of Risks
Risk Glossary
Illegal Content Judgments Guidance

Source: Ofcom analysis

1.1 Identify the harms that you need to assess

A5.40 The Act specifies a range of priority offences which you need to address in your risk assessment. Ofcom has grouped these offences into **15 kinds of illegal harm** set out below. For full information on the specific offences, see Appendix B.

Table 2. Kinds of priority illegal harm

Kinds of priority illegal harm*
Terrorism offences Child Sexual Exploitation and Abuse (CSEA) offences ○ Grooming** ○ Child Sexual Abuse Material (CSAM) – U2U services should consider image based CSAM and CSAM URLs separately** Encouraging or assisting suicide (or attempted suicide) or serious self-harm offences[8]

[8] The new self-harm offence is not yet in force and is not a priority offence. However, we have included suicide and self-harm in the same kind of illegal harm. Most of our evidence base relates to both suicide and self-harm, so we have considered them together in our risk assessment. The evidence we analysed does not often distinguish between content that focuses solely on suicide, compared to content which focuses on self-harm that is potentially life-threatening. We also think that services may find it easier to consider these offences together, so have provisionally included it here and throughout this guidance, for consistency. For the avoidance of doubt however, services are not required to treat self-harm as a priority offence. We will keep our approach to self-harm under review when we finalise the guidance.

Harassment, stalking threats and abuse offences Hate offences Controlling or Coercive Behaviour (CCB) offence Drugs and psychoactive substances offences Firearms and other weapons offences Unlawful immigration and human trafficking offences Sexual exploitation of adults offences Extreme pornography offence Intimate image abuse offences Proceeds of crime offences Fraud and Financial services offences Foreign Interference Offence
* You can find more information about the detail of the corresponding offences (including relevant non-priority offences) in Ofcom's illegal content judgements guidance. ** Although these fall within CSEA, we recommend services assess the risks of harm from CSAM and Grooming separately; and within CSAM, U2U services should consider the risks of image-based CSAM and of CSAM URLs separately. Further guidance for U2U services on how you assess the risks of these two subsets of illegal harm is provided below.

Source: Ofcom

A5.41 Your risk assessment must consider the risk of i) **illegal content** appearing on your service, and – if you are a U2U service – the risk that your service could be used to ii) **commit** or iii) **facilitate** an offence set out in the Act.

i) **The presence of illegal content:** U2U services need to consider whether there is a risk of individuals encountering "illegal content" on their service. The Act defines "illegal content" as content that "amounts to an offence". An example of illegal content includes content sharing a terrorist publication or which invites users to support a proscribed organisation (e.g. a terrorist group).

Search services must consider the risk of individuals encountering "search content" that is illegal content. Search content is content that may be encountered in or via search results of a search service, i.e. content presented to a user of the service by operation of the search engine in response to a search request made by an individual.

To carry out your risk assessment, you will need a working understanding of what "illegal content" is, and what offences you must consider. The Act distinguishes between "priority" and other (i.e. non-priority) illegal content. All services are required to consider each kind of illegal harm separately in their risk assessments.

ii) **The commission of a priority offence:** U2U services are required to consider the risk of the service being used to commit a priority offence.

iii) **The facilitation of a priority offence:** U2U services are required to consider the risk of the service being used for the facilitation of a priority offence. This refers to content or behaviour that is not necessarily illegal, but which facilitates a priority offence.

Illegal content, and the service being used to commit or facilitate offences

In the risk assessment, the key objective is for you to consider in a broad way how your service may be used in a way that leads to harm.

The different elements of a risk assessment listed above are intended to help services be more comprehensive in how they identify and assess the risks of their service being used to host illegal content, or commit or facilitate priority offences. Your risk assessment should not be limited to an assessment of individual pieces of content, but rather consider how your service is used overall. In particular, the requirement to assess the risk of the service being used to commit or facilitate priority offences may mean considering a range of content and behaviour that may not amount to illegal content by itself.

We recognise that in practice the differences between illegal content and the commission and facilitation of offences will often be blurred. **For the purpose of your risk assessment, you can choose to make a single assessment of each kind of illegal harm that encompasses these three elements together.**

Ofcom's Register of Risks provides further context on how different kinds of illegal harm take place online and includes examples of how facilitation of an offence can happen.

A5.42 All services have a duty to assess each kind of priority illegal harm separately in their risk assessment. Some services may find it appropriate to further separate the kind of harms into subsets relating to specific offences, categories or manifestations of that harm on their service. An example may be highlighting evidence of specific types of fraud that disproportionately affect your service under the 'Fraud and Financial services' kind of illegal harm.

A5.43 If you choose to do this, you should still make a full assessment of each kind of illegal harm listed above. You can note any particular trends within the kind of illegal harm based on evidence you have consulted but should still assign an overall risk level to the kind of harm as a whole.

A5.44 You should also consider if you are aware of any **relevant non-priority illegal content** that may be present on your service.

A5.45 Some non-priority offences are described in the Act, such as false and threatening communications offences. These offences are not included in the 15 kinds of harm above, but they are addressed in Ofcom's Register of Risks.

A5.46 When assessing the risk of relevant non-priority illegal content, you should take a reasonable and proportionate approach based on your understanding of your service and any information you hold.

A5.47 We do not expect that services will necessarily consider every possible offence, but if you have any knowledge, experience, or evidence that illegal content may be present on your service (or at risk of appearing), then you should include this kind of illegal harm in your risk assessment. Unlike illegal content relating to priority offences (as set out in Table 2 above), you do not need to assess each kind of non-priority illegal harm separately.

1.2 Consult Ofcom's Risk Profiles

Consult the relevant Risk Profile

A5.48 Ofcom's Risk Profiles are a resource to consult when conducting your risk assessment. All services must take account of the relevant Risk Profile when conducting their own risk assessment.

A5.49 There is a Risk Profile for U2U services, and a Risk Profile for Search services. Each Risk Profile identifies risk factors associated with the priority offences based on the evidence in the Register of Risks. These risk factors are a selection of service characteristics (such as user base, business models and functionalities) that the evidence indicates are strongly linked to a risk of different kinds of priority illegal offence. We have grouped these into general risk factors, which all services should take account of, and specific risk factors, which are dependent on specific service characteristics.

A5.50 These risk factors are a good starting point for thinking about which harms could manifest on your service, and how. However, it is important to understand that the risk factors are not comprehensive and are context specific.

A5.51 To consult the Risk Profile, read the instructions in Appendix A. They will explain how you can identify which risk factors apply to your service. We provide a set of questions to help you do this.

Record your risk factors

A5.52 Record your risk factors. We suggest you do this by using the check boxes provided in the Risk Profiles in the section below. Each risk factor will be relevant to one or multiple kinds of illegal harm, which the Risk Profile will tell you.

A5.53 You should use these risk factors when assessing your risks of harm for the associated kinds of illegal harm in Step 2.

Step 2: Assess the risk of harm

Outcomes and requirements of Step 2

You have considered whether there are any specific **characteristics** (including functionalities) that apply to your service that may increase the risks of harm to individuals, but which are not covered in Ofcom's Risk Profiles (2.1);

You have assessed the risks of harm of the 15 kinds of illegal harm by considering the **likelihood and impact** of each, taking in to account the risk factors highlighted by Ofcom and **your own evidence** (2.2);

You have considered whether there are **other kinds of non-priority illegal harm** that you should assess, based on your knowledge and experience of your service (2.2);

You have assigned a level of risk of **high, medium or low** to each of the 15 kinds of harm (2.3);

For specific harms including the dissemination **of Child Sexual Abuse Material (CSAM) and Grooming**, you have considered our additional guidance on assessing risk (if you are a U2U service) and have assigned a level of risk for each (2.3).

What you should have recorded

Where applicable, a list of any additional **characteristics** (including user base, business models, functionalities, governance and systems and processes) you have considered alongside the risk factors identified in Ofcom's Risk Profiles in Step 1;

A list of the **evidence** that has informed the assessment of likelihood and impact of each kind of priority illegal harm;

The **level of risk** assigned to each of the 15 kinds of illegal harm and any relevant non-priority illegal harm, and **an explanation of the decision**. Where appropriate, this should also include the level of risk assigned to sub-categories of harm (including CSAM (U2U services should consider CSAM images and CSAM URLs separately) and Grooming).

Supporting resources

Risk Profiles
Register of Risks
Core and enhanced evidence inputs

Source: Ofcom analysis

2.1 Consider any additional characteristics that may increase or decrease risks of harm

A5.54 Using the information in Step 1 and your own evidence, you must now assess the risk of each kind of illegal harm. Your assessment must cover all the elements set out in sections 9 and 26 of the Act.

A5.55 Practically this means that when conducting your risk assessment, you should:

Consider if there are any **additional characteristics** that your service has which have the potential to increase risks of harm, but which may not be present in Ofcom's

Risk Profiles. For example, there may be a certain functionality or business model feature related to a new or emerging risk.[9]

Consult **your own evidence** when considering all risk factors to complete your risk assessment. This is because the riskiness of an individual risk factor will be influenced by various other elements, including how a service's functionalities, user base, business model and systems and processes in combination can serve to increase or decrease risks of harm.

2.2 Assess the risks of harm by considering evidence of likelihood and impact

A5.56 We recommend you assign a level of risk (high, medium or low) on your service for each of the kinds of illegal harm. The risk level that you assign to each harm will be important when considering which safety measures you need to implement as part of Step 3.

A5.57 To make the assignment of high, medium or low, you should consider the likelihood of each kind of illegal harm taking place on your service, alongside the potential impact on individuals.

A5.58 To help you with this, we have listed the sorts of evidence we recommend you consider when doing the assessment. We have divided the evidence into **core inputs** which all services should consider, and **enhanced inputs** which some services should consider gathering in addition. Large services or services which have identified several specific risk factors for a harm using the Risk Profile will typically need to include some or many enhanced inputs to improve the accuracy of their judgments on risk. We set out further guidance on which services we think should consider enhanced inputs in A5.104.

A5.59 We expect that the core and enhanced inputs will provide you with a good understanding of how the characteristics of your service increase the risk of illegal content being present on the service, or the service being used to commit or facilitate an offence. However, the list is not exhaustive, and services should consider whether they need to take any additional steps to ensure their risk assessment is suitable and sufficient.

Table 3. Types of evidence

Type	Overview of inputs
Core inputs	Risk factors identified through relevant Risk Profile (Step 1) User complaints and reports User data Retrospective analysis of incidents of harm Register of Risks (optional for user-to-user services) Other relevant information (including any other characteristics that apply to your service that may increase or decrease risks of harm)

[9] We are particularly aware of the debate around the potential risks that generative AI may pose. Given the pace of developments regarding generative AI and the fact that the evidence base in this area is still developing, we have not considered this technology in depth in this version of the Register and therefore it does not appear in Risk Profiles. We will return to consider it in more detail in the future.

Enhanced inputs	Results of product testing Results of content moderation systems Consultation with internal experts on risks and technical mitigations Results of previous interventions to reduce online safety risks Views of independent experts Internal and external commissioned research Outcomes of external audit or other risk assurance processes Consultation with users Results of engagement with relevant representative groups

Source: Ofcom analysis

Assessing likelihood of harm

A5.60 Likelihood refers to the chance that users will encounter illegal content on your service, and the chance of your service being used to commit or facilitate an offence.

A5.61 The risk factors you identified in Step 1 are an important starting point for identifying how harm could manifest on your service. These will give a good indication of which offences are most likely to occur on your service, and which risk factors play a role in increasing that likelihood.

A5.62 However, the risk factors that you identify from Ofcom's Risk Profiles do not provide a complete picture of likelihood. You should consider additional evidence, including:

Any other characteristics of your service that may increase or decrease the likelihood of harm, as outlined in step 2.1. This might include how the design of your service, including existing systems and processes, may increase or reduce the likelihood of certain kinds of illegal harm occurring.

Relevant core and enhanced inputs. Consulting these inputs will provide you with information about how the various kinds of illegal harm are experienced on your service specifically.

How the design of your service, including **existing systems and processes**, may increase or reduce the likelihood of the certain kinds of illegal harm occurring.

Ofcom's **Register of Risks**. The Register provides detailed evidence on risk factors that we have used to inform the Risk Profiles, organised by kind of illegal harm**.** It is **not essential** to consult the Register of Risks, but services can review the relevant sections of the Register to gain a better understanding of the dynamics and drivers of harm for each offence. For example, if you identify through Ofcom's Risk Profiles that your service has risk factors which increase the risk of Fraud, Grooming, and Hate offences, you may choose to review the corresponding chapters in the Register to gain a better understanding of how these offences happen, and how this could apply to your service.

For **search services,** Ofcom's Register chapter on search. We recommend that all search services consult this chapter to understand how harm may occur on your service.

A5.63 The table below provides guiding questions on what to consider when consulting your evidence. Answering these questions should help you reach a view on the likelihood of the risks you are considering.

Table 4. Guiding questions on likelihood

What to consider when assessing likelihood
• If your service is U2U, do your service's **risk factors** identified in Step 1 indicate that this kind of illegal harm is likely on your service? If so, how many risk factors do you have that are associated with the kind of illegal harm? Ordinarily, the larger the number of risk factors for a given harm, the higher the likelihood of that harm. If your service is a Search service, does the Register chapter indicate evidence that harm is likely to occur on your service? • Are there any other **characteristics** that apply to your service (including functionalities, user-base, business model and governance, systems and processes) that you have identified may make the kind of illegal harm more likely? • Is there any evidence that the kind of illegal harm is likely to occur on your service based on the information from your **core inputs**? You should consider: o Whether there is evidence of harm occurring based on user complaints and reports. For example, significant volumes of reports in relation to a particular harm could indicate a higher likelihood of that harm occurring; and o Whether there is any other relevant evidence and data which suggests there is a risk of the harm occurring on your service. • If you have consulted core evidence inputs and are still unsure about the likelihood of this harm, then consider any additional evidence based on the information from **enhanced inputs.** You may consider: o Whether there is any evidence from independent experts or externally commissioned research that highlights the potential for harm to occur; o Whether there is evidence based on results of product testing of the potential for harm to occur; and o Whether there is any evidence based on results of content moderation of harm occurring. • Are there systems or processes already in place that reduce the risk of harm occurring on your service? Can you demonstrate that these are effective in decreasing the risk of harm?

Source: Ofcom analysis

Assessing the impact of harm

A5.64 To make a judgement on impact, you need to consider the nature and severity of harm that your users or other individuals could experience (e.g. victims of crimes such as CSEA or fraud who may not be users of your service).

A5.65 Evaluating impact will be much more dependent on your understanding of the evidence about your own service. The key aspects of this judgement will be:

The reach of illegal content measured by numbers of users who could be affected and how content is shared and disseminated;
How different user groups (including vulnerable users) could be affected by harm; and
How users experience different harms on your service.

A5.66 To make this evaluation, you should consider:

The risk factors you identified in Step 1. Information regarding business models, recommender systems and user base demographics may help you understand how different user groups are impacted by the kind of illegal harm. For example, women and girls are disproportionately and differently impacted by certain kinds of illegal harm including intimate image abuse and controlling or coercive behaviour. You can also consult the relevant sections of the Register to gain a fuller understanding of how different users are impacted by harms.

Any other characteristics of your service that may increase or decrease the impact of harm.

Relevant core and enhanced inputs. Consulting these inputs will provide you with information about how the kind of illegal harm is experienced on your service specifically.

A5.67 The table below provides guiding questions on what to consider when consulting your evidence.

Table 5. Guiding questions on impact

What to consider when assessing impact

• What is the potential reach of illegal content on your service? Consider:
  ○ The number of users of your service. Typically**,** we would expect that the larger the number of users the greater the potential impact of any given harm; and
  ○ Whether the way that content is shared and disseminated, including through recommender systems and other algorithmic systems, could increase the number of users encountering illegal content.
 	
• How does your service's user base demographics influence the way harm is experienced on your service? Consider the information we provide in Risk Profiles and your own evidence. For example, women and girls are disproportionately and differently impacted by some kinds of illegal harm including Intimate Image Abuse, and you should take this into account when assessing these harms. You might consider:
  ○ What user data tells you about user base demographics (including age, gender and any vulnerable groups) on your service;
  ○ How user base demographics may affect the way in which users experience harm on your service; and
  ○ How different users on your service or third-party individuals may be impacted by harm.
 	
• How does your service's revenue model and commercial profile influence the way harm is experienced on your service. Consider the information we provide in Risk Profiles and your own evidence.
 	
• Are there any other characteristics that apply to your service (including functionalities, user-base, business model and governance, systems and processes) that you have identified may increase the impact of harm?
 	
• Is there any evidence from core inputs about the experience of harm and its impact? for example:
  ○ What user complaints and reports regarding the harm tells you about impact on users and other individuals.

- If you have consulted core evidence inputs and are still unsure about the likelihood of this harm, then consider any additional evidence based on the information from **enhanced inputs.** You may consider:
    - What user research and consultation with users tells you about impact on users and other individuals; and
    - What independent experts or research tells you about the impact of harm on a service of your type.

Source: Ofcom analysis

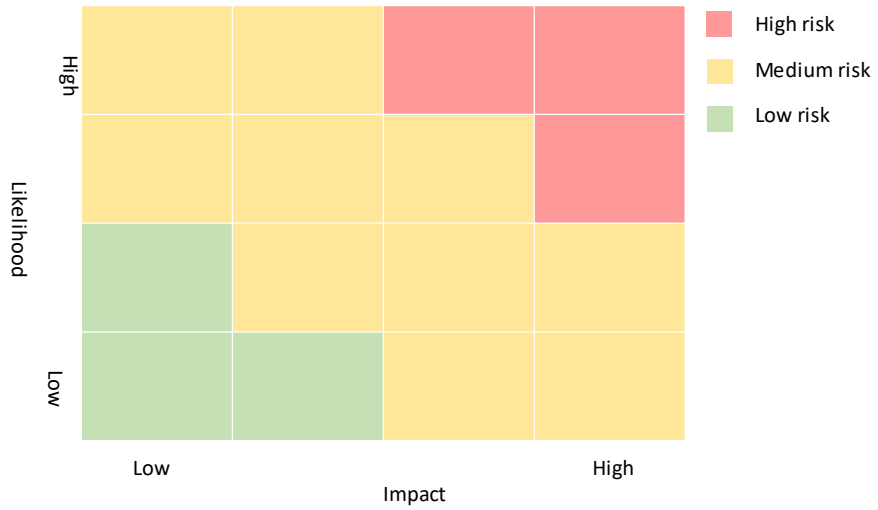
2.3 Assign a risk level to each kind of illegal harm

A5.68 Considering the relevant evidence, you should use your judgement to assign a **risk level** of high, medium or low to each of the 15 kinds of illegal harm (and CSAM – image-based and URLs separately – and Grooming). You should also assign a risk level to any non-priority illegal offences you have chosen to assess. If it is not possible for a harm to take place by means of your service, you may assess the risk as 'negligible'.

A5.69 The risk level that you assign to each harm will be important when considering which safety measures you need to implement as part of Step 3. Please note that certain measures listed in our Codes of Practice address specific kinds of illegal harm (image-based CSAM, CSAM URLs and Grooming). We provide further guidance on assessing risks related to these harms in A5.73.

A5.70 When it comes to assigning a risk level, you may find it easiest to use a **risk matrix** based on likelihood and impact. A risk matrix will help you in assigning a risk level based on the evidence you have consulted on the likelihood and impact of harm.

Figure 1 Illustrative risk matrix



Source: Ofcom

A5.71 To help services in making this judgement, we have created a Risk Level Table which sets out a high-level description of each risk level. This is a general overview of the factors that might inform different levels of risk based on information services will gain through Risk Profiles, evidence about how harm is experienced on your platform and how your service's characteristics increase or decrease risks.

A5.72 Most services will have at least one risk factor associated with each kind of illegal harm. We generally expect that the more risk factors a service has, the higher risk it is likely to be for the associated harm.

A5.73 **This table should not be read as a set of criteria that needs to be met in order for an assessed risk to be classified at these levels. It is intended to help inform your judgement on a risk level, rather than being a determination of risk levels across all harms**.

Table 6. Risk level table

Risk level	Description	Your service may decide on this risk level if some or all the following conditions are met
High risk	You assess that there is a high likelihood that the kind of illegal harm could occur on your service	• You have identified many[10] specific risk factors in the relevant Risk Profile* (Step 1) which increase the likelihood of harm occurring **and** there are no effective systems and processes in place to address this harm nor other factors which reduce risks to users and other individuals**;** • **Or** there is evidence that harm is very likely to occur on your service (for example evidence from external experts); • **Or** there is significant evidence of harm taking place on your service (for example from complaints).
	You assess that there is high impact to users of your service or other individuals from this illegal harm	• Based on your analysis of evidence, you make an independent judgement that the impact of the harm would be severe for your users or other affected parties. • **Or**there is broad scope for harm to impact users. This may apply if: o You have over 7 million monthly UK users**. o Content can be shared and disseminated in a way that has the potential to affect a significant number of users. • **Or** there is evidence of harm impacting a significant number of users. This may apply if: o There is evidence of harm impacting a significant number of all users. o There is evidence of harm impacting a significant number of vulnerable users (based on your understanding of user base demographics on your service). • **Or** there is evidence that the harm would impact a significant number of third-party individuals who may not be using the service. This may include, for example, individuals who are affected by harms such as Intimate Image Abuse but who are not users of your service.

[10] We consider 'many' to be a large number of risk factors as identified in Ofcom's Risk Profiles. You should be aware that a number of risk factors we have identified for different kinds of illegal harms varies in line with the evidence available and the way harm manifests. A kind of illegal harm which includes many different offences and behaviours may have more risk factors associated with it than one which is narrower.

Risk level	Description	Your service may decide on this risk level if some or all the following conditions are met
Medium risk	You assess that there is a moderate likelihood that this illegal harm could occur on your service	• You have identified several[11] specific risk factors in the relevant Risk Profile* (Step 1) which increases the likelihood of harm occurring **and** there are some systems and processes are in place to address this harm but you cannot demonstrate they are effective at reducing risks to users; **Or** one of the following applies: • There is evidence that harm is likely to occur on your service. • There is some evidence of harm taking place on your service**.**

	You assess that there is moderate impact to users of your service or third-party individuals from this illegal harm	• Based on your analysis of evidence, you make an independent judgement that the impact of the harm would be moderate for your users or other affected parties.
		• **Or** there is some scope for harm to impact a material number of users. This may apply if:
		  ○ You have between 700,000 and 7 million monthly UK users**.
		  ○ Content can be shared and disseminated in a way that has the potential to affect a material number of users or other individuals.
		• **Or** there is evidence of harm impacting a material number of users or third -party individuals.

Low risk	You assess that there is a low likelihood that this illegal harm could occur on your service	• You have identified no or few specific risk factors in the relevant Risk Profile* (Step 1);
		• **Or** one of the following applies:
		  ○ There are comprehensive and effective systems and processes in place, or other factors which reduce risks of harm to users.
		  ○ There is no evidence that harm is likely to occur on your service.
		  ○ There is no evidence of harm taking place on your service.

	You assess that there is limited impact to users of your service from this illegal harm	• There is limited scope for harm to impact users or other individuals; • **Or** there is no evidence of harm impacting users or other individuals**;** • **Or** there is evidence that harm impacts very few users or other individuals.
Negligible risk	If it is not possible for the harm to take place by means of your service, you may assess the risk of that harm as 'negligible'.	

[11] Some risk factors, while distinct, may have a similar effect on your service (such as a situation where your service has direct messaging as a functionality, and which is also a messaging service). In these situations, your service may choose to consider these risk factors together.

Risk level	Description	Your service may decide on this risk level if some or all the following conditions are met
*** Note that this condition is unlikely to apply to Search services. Instead, Search services should rely on information in the Register and their own evidence to make an assessment of likelihood.** **** In some instances, number of users may be a weaker indicator of risk level. You should consider this indicator alongside other factors listed in the relevant section.**		

Source: Ofcom

2.4 Guidance on assessing risks of certain harms for U2U services

A5.74 Certain measures listed in Ofcom's Codes of Practice address CSAM and grooming specifically. If you are a U2U service, we have provided further guidance on the elements you should consider to help you make an accurate assessment of the risks of these harms.

A5.75 **These tables should not be read as a set of definitive criteria that needs to be met in order for the risk of CSAM or grooming to be classified at these levels. It is intended to help inform your judgement on the risk level, rather than being a determination of risk level for CSAM or grooming.**

A5.76 We recommend services which find medium or high risks of harm of these offences to follow the corresponding measures laid out in our Codes of Practice. Further information on how services do this is provided in Step 3.

A5.77 If you are a search service, you can consider Table 6 above when assessing your level of risk for CSAM and grooming. You can also consider the additional guidance provided in Table 7 and Table 8 for high-level guidance on assessing risks of these harms but bear in mind that some of the criteria and risk factors listed are not applicable to search services. You are expected to determine your level of risk of CSAM but are not expected to consider it separately for image-based CSAM and CSAM URLs.

Child Sexual Abuse Material (CSAM)

A5.78 CSAM is a category of CSEA content, including in particular indecent or prohibited images of children (including still and animated images, and videos, and including photographs, pseudo-photographs and non-photographic images such as drawings). CSAM also includes other material that includes advice about grooming or abusing a child sexually or which is an obscene article encouraging the commission of other child sexual exploitation and abuse offences. Furthermore, it includes content which links or otherwise directs users to such material, or which advertises the distribution or showing of CSAM. The table below provides additional guidance on how U2U services can assess whether they are high, medium or low risk for CSAM.

A5.79 CSAM includes both image sharing (in the form of photographs, videos or visual images) and URL sharing[12], which have some distinct risk factors. You should consider both these aspects when making an overall judgment of the risk of CSAM on your service.

A5.80 It is important to understand that being low risk for one type of CSAM does not preclude your service from being high risk for the other. Ofcom's Codes of Practice recommend

[12] URL sharing refers to posting or sending content which contains a URL. This may be in the form of text or a hyperlink. "CSAM URL" means a URL at which CSAM is present, or which includes a domain which is entirely or predominantly dedicated to CSAM, (and for this purpose a domain is "entirely or predominantly dedicated" to CSAM if the content present at the domain, taken overall, entirely or predominantly comprises CSAM (such as indecent images of children) or content related to CSEA content).

different forms of automated content moderation technology to address the uploading and sharing of image-based CSAM and CSAM URLs. We therefore recommend that services which assess as high or medium risk adopt a form of content detection technology relevant to the type of CSAM sharing they are at heightened risk for.

Table 7. CSAM risk decision framework

Risk level	Decision framework	
	Image-based CSAM	CSAM URLs
High risk	Your service is likely to be high risk for image-based CSAM if your service allows images or videos to be uploaded, posted or sent; **And any** of the following applies: • Your service has systematically[13] been used by offenders to upload image-based CSAM; • Your service has a majority of relevant risk factors associated with CSAM in Ofcom's Risk Profiles[14], in addition to allowing images or videos to be uploaded, posted or sent; • Your service is a file-storage and file-sharing service;[15] • Your service is an adult service, or a service which allows pornographic content; • Your service allows users to post or send content without creating an account.[16]	Your service is likely to be high risk for CSAM URLs if your service allows text or hyperlinks to be posted or sent; **And any** of the following applies: • Your service has systematically been used by offenders to post or send CSAM URLs; • Your service allows users to post or send content without creating an account.

[13] This will be based on previous pattern of use by offenders to upload and share content. If there is some evidence of your service being used to share CSAM recently, you may choose to determine that it is medium risk. Possible indicators of this may be that there have been a small number of pieces of CSAM detected in recent years, though these may be irregular or in low volume, or if CSAM content is present in lower proportion compared to the total volume of content or total number of users. Where there is evidence of regular and consistent use of your service by offenders for this reason, or it is in higher proportion compared to the total volume of content or total number of users, it is more likely to fall into the 'high risk' category.

[14] Child users; social media services; messaging services; discussion forums and chat rooms; group messaging; direct messaging; encrypted messaging. This list excludes risk factors from the Risk Profiles which are indicated elsewhere the 'high risk' criteria. See Appendix A for further information.

[15] A U2U service type that enables users to upload, store, manage and distribute digital media. A key characteristic of file storage and file sharing services is the provision of link sharing, allowing users to generate and share unique URLs or hyperlinks that directly lead to the stored content. This encompasses sharing files and also embedding stored content (such as images and videos) into external services.

[16] This refers to services which allow users to post or send content without the need to register (for example with an email address) or to provide any log-in details; this can result in a user's identity being unknown (or partially unknown) to a service, as well as other users. This does not refer to 'pseudonymous' users, where a person registers for a service but does not necessarily use any personally-identifying information. This is also distinct from simply using a service without logging in (such as browsing a webpage), and specifically refers to the ability to post or send content on the service.

Risk level	Decision framework	
	Image-based CSAM	CSAM URLs
Medium risk	Your service is likely to be medium risk for image-based CSAM if your service allows images and videos to be uploaded posted or sent **and** does not meet the criteria for high risk; **And any** of the following applies: • There is evidence that your service has been used by offenders to upload, post or send image-based CSAM images recently; • Your service has two or more relevant risk factors[17] in the Risk Profiles associated with image-based CSAM, in addition to allowing images or videos to be uploaded, posted or sent.	Your service is likely to be medium risk for CSAM URLs if your service allows text or hyperlinks to be posted or sent **and** does not meet the criteria for high risk; **And any** of the following applies: • There is evidence that your service has been recently used by offenders to post or send CSAM URLs; • Your service has two or more relevant risk factors[18] associated with CSAM URLs in Ofcom's Risk Profiles, in addition to allowing text or hyperlinks to be posted or sent.
Low risk	Your service is likely to be low risk for image-based CSAM if your service allows images or videos to be uploaded, posted or sent; **And any** of the following applies: • Your service does not meet the criteria for high or medium risk for image-based CSAM; • Your service has adopted measures that demonstrably ensure that image-based CSAM is highly unlikely to occur on the service.	Your service is likely to be low risk for CSAM URLs if your service allows text or hyperlinks to be posted or sent; **And any** of the following applies: • Your service does not meet the criteria for high or medium risk for CSAM URLs; • Your service has adopted measures that demonstrably ensure that CSAM URLs are highly unlikely to be posted or sent on the service.
Negligible risk	Your service should only consider risks of image-based CSAM as negligible if you do not allow photographs, videos or visual images to be uploaded or posted or sent.	Your service should only consider risks of CSAM URLs as negligible if you do not allow text or hyperlinks to be posted or sent on the service.

[17] Child users; social media services; messaging services; discussion forums and chat rooms; user groups; livestreaming; direct messaging; encrypted messaging. This list excludes risk factors from the Risk Profiles which are indicated in the 'high risk' criteria. See Appendix A for further information.
[18] Child users; social media services; messaging services; discussion forums and chat rooms; user groups; direct messaging; encrypted messaging. This list excludes risk factors from the Risk Profiles which are indicated in the 'high risk' criteria. See Appendix A for further information.

Grooming

A5.81 The table below provides additional guidance on how U2U services can assess whether they are high, medium or low risk for grooming.

Table 8. Grooming risk decision framework

Risk level	Decision framework
High risk	Your service is likely to be high risk of grooming if it can be accessed by children **and** users are able to communicate one-to-one with child users (e.g. direct messaging); **And any** of the following applies: • Your service has been systematically used by offenders for the purposes of grooming children for child sexual abuse; • Your service has a majority of risk factors associated with grooming in Ofcom's U2U Risk Profile,[19] in addition to child users and direct messaging. • Your service includes child users when users are prompted to expand their networks, including through network recommender systems (e.g. network expansion prompts); • Your service allows users to view child users in the lists of other users' connections; • Your service has user profiles or user groups which may allow other users to determine whether an individual user is likely to be a child.
Medium risk	Your service is likely to be medium risk of grooming if your service does not meet the criteria for high risk, **and**: • It can be accessed by children; • **And** users are able to communicate one-on-one with child user (e.g. direct messaging). **And any** of the following applies: ○ Your service has recently been used by offenders for the purposes of grooming children for sexual abuse; ○ Your services two or more of the other risk factors associated with grooming in Ofcom's U2U Risk Profile,[20] in addition to child users and direct messaging.
Low risk	Your service is likely to be low risk of grooming if your service can be accessed by children; **And any** of the following applies: • Your service does not meet the criteria for high or medium risk; • Your service has adopted measures that demonstrably ensure that grooming is highly unlikely to occur on the service; • There is no evidence that grooming is likely to occur on your service, nor evidence of grooming taking place on your service. • Your service has less than 100,000 UK child users **and** your service does not meet the criteria for high risk;
Negligible risk	Your service should only consider risks of grooming as negligible if children are prevented from accessing the service.

[19] Social media services; messaging services; gaming services; livestreaming; encrypted messaging; commenting on content. See Appendix A for further information. This list excludes risk factors from the Risk Profiles which are indicated elsewhere in the 'high risk' criteria. See Appendix A for further information.
[20] Social media services; messaging services; gaming services; livestreaming; encrypted messaging; commenting on content. See Appendix A for further information. This list excludes risk factors from the Risk Profiles which are indicated in the 'high risk' criteria. See Appendix A for further information.

Step 3: Decide measures, implement and record

Outcomes and requirements of Step 3

You have **decided the measures** your service is going to implement to reduce risks of harm to individuals by **consulting Ofcom's Codes of Practice** or by considering alternative ways to meet the safety duties (3.1);

You have **considered any additional measures** that may be appropriate for your service to put in place that go beyond Ofcom's Codes of Practice (3.2);

You have **implemented and made a record of these measures** including why you think these measures meet the relevant safety duties (3.3);

You have made a **complete record of your risk assessment**, as per Ofcom's guidance on record keeping (3.4).

What you should have recorded

Any **measures from Ofcom's Codes of Practice** that have been or are planned to be implemented, and any measures that are not in use**;**

Any **measures that are alternatives** to those set out in Ofcom's Codes of Practice, with an explanation how the measures meet the relevant duties;

Other matters covered in our **guidance on Record Keeping and Review**.[21]

Supporting resources

Illegal Content Codes of Practice
Guidance on Record Keeping and Review.

3.1 Decide what measures you need to take to reduce the risk of harm

A5.82 You now need to decide what your service is going to do to reduce the risks of harm to individuals that you have identified.

A5.83 You should refer to Ofcom's Codes of Practice on illegal content. The list of recommended measures and which services they apply to is provided in our tear sheet, which is published alongside this consultation. We have also provided an example table below, which sets out the proposed U2U measures for governance and accountability, and which services we have proposed the measures apply to.

Table 9. The governance measures for U2U services in Ofcom's Codes of Practice for illegal content

	Proposed measures	**Smaller Services**			**Large Services**		
		Low risk	**Specific-Risk**	**Multi-Risk**	**Low risk**	**Specific-Risk**	**Multi-Risk**
Governance & Accountability							

[21] See Annex 6.

		Proposed measures	Smaller Services			Large Services		
			Low risk	Specific-Risk	Multi-Risk	Low risk	Specific-Risk	Multi-Risk
1	3A	Boards or overall governance bodies carry out an annual review and record how the service has assessed risk management activities in relation to illegal harms, and how developing risks are being monitored and managed				✓	✓	✓
2	3B	A named person is accountable to the most senior governance body for compliance with illegal content duties, reporting and complaints duties	✓	✓	✓	✓	✓	✓
3	3C	Written statements of responsibilities are provided to senior members of staff who make decisions related to the management of online safety risks			✓	✓	✓	✓
4	3D	Internal monitoring and assurance function to independently assess the effectiveness of the mitigations of illegal harms, reporting to a governance body						✓
5	3E	Evidence of new kinds of illegal content on a service, or increases in particular kinds of illegal content, is tracked and reported to the most senior governance body			✓	✓	✓	✓
6	3F	A Code of Conduct or principles provided to all staff that sets standards and expectations for employees around protecting users from illegal content risks			✓	✓	✓	✓
7	3G	Staff involved in the design and operational management of a service are sufficiently trained in a service's approach to compliance			✓	✓	✓	✓

A5.84 You can also choose to implement alternative measures to comply with the safety duty. Should you do so, you will need to record what measures you have taken and demonstrate how these measures achieve the safety duties. Further information is provided in A6.23 of in the guidance on Record Keeping and Review.

3.2 Consider any additional measures that may be appropriate

A5.85 For some services, Ofcom's Codes of Practice will not be comprehensive in addressing all risks identified in a risk assessment. Services may identify additional measures which go beyond the Codes that will help them to address any residual risk on their service. Some services may be better placed to identify additional effective measures or innovative approaches to preventing harm.

A5.86 We encourage services to consider such additional measures to manage or mitigate the risks they have identified. Good practice in risk management indicates that organisations are likely to be more effective at prioritising and managing adverse events when they have a good understanding of their residual risk levels (the risk that remains after controls are put

in place). Such measures may assist services overall to protect their users and others from harm.

A5.87 In addition, some services may be well placed to identify effective measures or innovative approaches to preventing harm as an alternative to those included in Ofcom's Code of Practice. If you choose to use alternative measures, you should be able to demonstrate that they will be effective. In these cases, you must record what measures you have taken and demonstrate how these measures achieve the safety duties (as described under section 3.1 of this guidance).

3.3 Implement all measures to mitigate and manage risk

A5.88 Once the measures have been decided, you should implement them.

A5.89 We recognise that it may take some time for your services to put all safety measures in place. Further information regarding our view on transition periods is covered in 30.11 in Chapter 30 regarding Ofcom's enforcement powers.

3.4 Record the outcomes of the risk assessment and how the safety duties have been met

A5.90 At this stage, you should ensure you have recorded the outcomes of the activities you carried out in Steps 1, 2 and 3. Further guidance in our guidance on Record Keeping and Review and summarised below.[22]

A5.91 When making a record of your risk assessment, you should include the information below. We consider that this will help you to demonstrate that your risk assessment is suitable and sufficient, that you have considered all of the elements of section 9 or section 26 (as applicable), and show the evidence you have relied on to assess the risks relevant to your service:

What service the risk assessment applies to;

The date the risk assessment was completed;

If applicable, the date the risk assessment was reviewed or updated;

Who completed the risk assessment;

Who approved the risk assessment;

Confirmation that your service has consulted Ofcom's Risk Profiles. You may do this by recording the outcomes of the Risk Profiles questionnaire, provided below (Appendix A)

A record of any risk factors from Ofcom's Risk Profiles which are relevant to your service;

If applicable, a list of any additional characteristics (including user base, business models, functionalities, governance and systems and processes) you have considered alongside the risk factors identified in Ofcom's Risk Profiles in Step 1;

[22] See Annex 6.

A list of the evidence that has informed the assessment of likelihood and impact of each kind of priority illegal harm;

The level of risk assigned to each of the 15 kinds of illegal harm and any relevant non-priority illegal harm, and an explanation of the decision. Where appropriate, this should also include the level of risk assigned to sub-categories of harm (including CSAM and Grooming);

Confirmation that the findings of the risk assessment have been reported through appropriate governance channels; and

Information regarding how your service takes appropriate steps to keep the risk assessment up to date (for example, a written policy).

Step 4: Report, review and update

Outcomes and requirements of Step 4
You have reported your risk assessment findings through **appropriate governance channels** (4.1); You have arrangements in place to **monitor the effectiveness of your safety measures** (4.2); You have established an **annual review cycle** for your illegal content risk assessments (4.3); You have **understood and act on the triggers** set out in the Act for when you should review or update your risk assessment or carry out a new one (4.4).
What you should have recorded
Confirmation that the findings of the risk assessment have been reported through appropriate governance channels; Information regarding how your service takes appropriate steps to keep the risk assessment up to date (for example, a written policy).
Supporting resources
Record Keeping and Review Guidance; Further guidance on keeping a risk assessment up to date.

4.1 Report on the risk assessment and measures via relevant governance channels

A5.92 Reporting on risk is a key element of good practice in risk management. Accurate and timely reporting through appropriate governance channels improves organisational oversight of risk and leads to better risk management outcomes.

A5.93 Where possible, we recommend that you consider reporting on your risk assessment outcomes and measures you plan to implement or have implemented.

A5.94 Smaller services are less likely to have formal organisational governance structure such as oversight boards or internal assurance functions. However, you can still improve the oversight of risks by reporting to a senior manager with responsibility for online safety duties on illegal harms.

4.2 Monitor the effectiveness of your safety measures

A5.95 Monitoring the effectiveness of the measures you implement is important for ongoing risk management. This will also help you keep your risk assessment up to date, as we explain in the section below on 'How to keep a risk assessment up to date'.

4.3 Review your risk assessment

A5.96 You will need to keep you risk assessment up to date. You should do this by **reviewing your illegal content risk assessment annually**. Services only need to review their risk assessment on an annual basis, rather than carrying out a new assessment. As we explain in the section below on 'How to keep a risk assessment up to date', a review requires you to check that the latest risk assessment still accurately reflects risks on your service. If there have been very few and minor changes to the design, operation and user base of your service since the last

risk assessment, there are unlikely to be substantial changes to your risk assessment findings.

A5.97 There are also triggers which will require you to review your illegal content risk assessment outside of an annual cycle, or to carry out a new assessment on your service. These are:

Review your assessment if Ofcom makes a **significant change to Risk Profiles**;
Carry out a new assessment before making a **significant change to the design or operation of your service**

A5.98 Further guidance on reviewing a risk assessment, including what constitutes a significant change, is provided in A5.132.

What evidence to assess

A5.100 This section of the guidance focuses on the different types of evidence that you should consider when assessing risks. It provides guidance on how to decide what evidence you need.

Why is evidence important?

A5.101 To be suitable and sufficient, your risk assessment needs to **reflect the risks on your service accurately**. It is important that you have an adequate understanding of the risks to **implement appropriate safety measures**.

A5.102 This means that your judgments on risk should be based on relevant information and evidence as far as possible.

A5.103 We understand that the appropriate level of evidence will vary based on the size and nature of the service. We provide advice on **core types of evidence** that all services should consider when assessing their level of risk for a kind of illegal harm. In some instances, the core evidence inputs will be insufficient to help a service reach an informed conclusion about the level of risk of a harm on their service, in these instances services should also consider which **enhanced types of evidence** will help them to accurately assign a risk level to a kind of illegal harm. We provide additional guidance below to help services understand which evidence inputs will be relevant to them.

How should you decide what evidence to collect?

A5.104 In step 2 (assess the risks), you should **review your evidence to assess the likelihood and impact of each kind of illegal harm.**

A5.105 The purpose of the risk assessment is to improve your understanding of how harm could take place on your service and what safety measures you need to put in place to protect users, especially children. The guiding principle when deciding what evidence to collect should be whether it will improve the accuracy of your risk assessment and your understanding of harm.

A5.106 For each kind of illegal harm, **you should consider all the core inputs and any other relevant information you already hold**. Then, at each stage of your analysis, you should consider whether you have sufficient information to reach accurate conclusions on the level of risk for that harm. If not, you should consider gathering additional evidence from the list of enhanced inputs.

A5.107 This can take place as an iterative process, with services collecting further information as needed until their evidence base and analysis can support a suitable and sufficient assessment.

A5.108 We expect you to use **only core inputs** if you are confident that they have given you an accurate assessment of the risk of an illegal harm on your service, this means:

- Ofcom's Risk Profiles identify no or very few risk factors relating to illegal harms (suggesting a potential lower level of risk on the service); or
- Evidence from the core inputs enables you to determine the likelihood and impact of a harm on your service and to use the Risk Level Table to assign a risk level this kind of illegal harm; or
- The enhanced inputs will be of limited value in assessing risk on your service.

A5.109 We expect that services should **consider the enhanced inputs** if you are not confident that the core inputs have given you an accurate assessment of the risk of an illegal harm to allow you to undertake a suitable and sufficient assessment. This is likely to be the case where:

- Evidence from the core inputs does not enable you to determine the likelihood and impact of a certain harm on your service, and therefore you are unable to assign a risk level for this kind of illegal harm using the Risk Level Table[23];
- You identify several risk factors for a certain harm which means you are more likely to need to consider enhanced inputs relating to understand that harm on your service;
- You are a larger service with the resources to undertake a more thorough assessment by including enhanced inputs. This is likely to materially improve the quality of your risk assessment. We would generally expect large services, those with more 7 million UK users, to use more than the core inputs.

A5.110 The following examples illustrate how we expect services to consider which inputs are appropriate for each harm they are assessing:

Using the Risk Profiles, **Service A** has identified several risk factors suggesting its service is high risk for a certain kind of illegal harm. **Service A gathers evidence from all the core inputs, but it finds very limited to no evidence of this harm occurring**, despite the Risk Profile indicating otherwise. There is therefore some ambiguity about how great the risk of that harm is, and the service is unable to determine accurately its likelihood or impact, and unable to assign a risk level using the guidance in the Risk Level Table. **Service A then consults the list of enhanced inputs** and selects inputs which will give more evidence relating to its risk factors to help it assign an accurate risk level and put appropriate measures in place.

Using the Risk Profiles, **Service B** has identified several risk factors suggesting its service is high risk for a certain kind of illegal harm. **Service B gathers evidence from all the core inputs and finds evidence of this harm occurring**. This means the service has sufficient evidence to assess the likelihood and impact of the harm occurring on its service, and therefore it is able to assign itself a risk level for this harm using the Risk Level Table without including additional evidence from the enhanced inputs.

Using the Risk Profiles, **Service C** has identified no additional risk factors which suggests it is not high risk for a certain kind of illegal harm. To assess whether this is correct, **Service C gathers evidence from all the core inputs and finds multiple sources of relevant evidence which shows it is not at high risk for this harm to occur on its service.** This means the service is able to determine the likelihood and impact of this harm occurring on its service and assign itself a risk level for his harm using the Risk Level Table without including additional evidence from the enhanced inputs.

A5.111 We expect that the core and enhanced inputs will provide services with a good understanding of risk. However, the list is not exhaustive, and services should consider

[23] This requires a good understanding of the specific context of the service, the combinations of risk factors present, and the effectiveness of any safety measures you currently have in place.

whether they need to take any additional evidence to ensure their risk assessment is suitable and sufficient.

What is a core input?

A5.112 Core inputs include information that all services can easily access, such as user complaints and Ofcom's Risk Profiles.

A5.113 The core inputs also include any information you already have which is relevant to your risk assessment. This includes any enhanced inputs (such as the results of testing or content moderation) that you already have and which do not require additional research or evidence gathering.

A5.114 Failing to consider this information may mean that the risk assessment is not suitable and sufficient.

Table 10. Core evidence inputs

Core inputs	Explanation
Risk Profile (and relevant parts of Ofcom's Register of Risks)	You have a duty to take account of the relevant Risk Profile as part of your risk assessment. The Register provides more detailed information on the characteristics of your service that may affect the level of risk. We encourage services to consult the relevant section of the Register. You can prioritise the most relevant parts of the Register of Risks once you have established your risk factors in Step 1. All the information presented in the Risk Profiles is based on the evidence in our Register. The Register looks at risks by offence grouping. Each chapter presents a summary box and full analysis of risk factors associated to an offence grouping. Consulting these resources **will help you understand the risk factors** you identified in the Risk Profiles so you can understand how they are likely to affect the risk of a harm on your service.
User complaints, including user reports	Under the Act, you are required to provide easy-to-access and use complaints procedures which allow complaints and reports to be made by users and for you to take appropriate action. You should consider any data from these complaints and reports when carrying out your risk assessment. If you have not collected this information before and set up a new user reporting function, you should consider any reports when you update your risk assessment. This could include, for example, the kind of illegal content being complained about, the accuracy of complaints and the length of time taken for an appropriate action to be taken. This input will help you understand the impact and frequency of a certain illegal harm on your service. **User complaints will help you assess the likelihood (how many user complaints) or impact (the nature of user complaints) of harm occurring on your service**.

Core inputs	Explanation
Where relevant, user data including age	By user data we mean data you hold that has been provided by users, including their personal data (for example, data provided when a user sets up an account), and data about users that you have created, compiled or obtained (for example, data relating to when or where users access a service or how they use it). You may already hold this kind of user data, for example for analysis via behaviour identification technology or user profiling technology. User data also includes any data held as a result of age assurance and age verification processes. Considering user data, in combination with other inputs into the risk assessment, will help you understand if any particular groups are at risk of certain kinds of illegal content on their service. This is relevant because, as set out in the Risk Profiles and Register of Risk, certain harms are disproportionately likely to affect certain demographic groups (e.g., women are more likely to experience harms like intimate image abuse and coercive and controlling behaviour than men). **User data will therefore help you determine the impact of each kind of illegal harm on your service.** When considering user data, you must also consider privacy rights and your duties under the UK GDPR. This is likely to be of greater consideration for age assurance and age verification measures, and any special category data that you may hold. We encourage you to consult the ICO's guidance on UK GDPR requirements[24] and The Age Appropriate Design Code.[25]
Retrospective analysis of incidents of harm	Following any significant incident of harm experienced on your service, you should undertake retrospective analysis or a 'lessons learned' exercise. This information should inform your risk assessment. A significant incident could include, for example, a major incident that causes serious harm, a prominent trend in illegal content, or an individual piece of content which becomes widely disseminated. **Retrospective analyses will help you assess the impact of different kind of illegal harm on your service, particularly those harms which are less common but high impact.** Such case studies may allow services to examine how particular aspects of the service's design (such as user characteristics, functionalities, recommender systems) may have played a role and where mitigating measures (such as content moderation, terms of service, user reporting) and associated processes could have been more effective.

[24] See the ICO's guidance and resources on the UK GDPR
[25] See the ICO's Children's code guidance and resources

Core inputs	Explanation
Other relevant information	If you hold any other relevant evidence or data which may help you improve your understanding of risk on your service, you should consider it as part of your risk assessment. This may include any existing harms reporting, published research, referrals you have made to law enforcement, reports provided to you by expert groups or by law enforcement agencies, data on user behaviour relating to harms, or the outcomes of product testing. **Any types of evidence listed below under Ofcom's enhanced inputs (e.g., the results of content moderation, the results of testing, any research commissioned) that the business already holds, and which are relevant to the online harms, should inform your risk assessment.**

What is an enhanced input?

A5.115 The enhanced inputs are types of evidence that some services should consider when reviewing the risk of a harm on their service to help them assign an appropriate risk level and achieve a suitable and sufficient risk assessment. Services considering enhanced inputs may wish to include some or all of the types of inputs suggested below.

A5.116 The type and number of enhanced inputs a service considers when assessing the risk of a particular kind of illegal harm is down to you. **This decision is likely to be informed by the risk factors you have identified in the Risk Profiles and the size of your service**. We provide descriptions of the different types of enhanced evidence below to help you decide if an input is relevant to your assessment of risk.

A5.117 Large services[26] or services which have identified several specific risk factors for a harm using the Risk Profile will typically need to include some or many enhanced inputs to ensure their risk assessments are suitable and sufficient. To illustrate this further please consider the examples above under 'How should you decide what evidence to collect?'.

A5.118 As noted above, many services will already hold evidence inputs which feature on the enhanced list. If so, you should include them in their risk assessment.

Table 11. Enhanced evidence inputs

[26] By a 'large service' we mean those with more than 7 million UK users per month.

Enhanced inputs	Explanation
Results of product testing[27]	To improve your understanding of risk on your service at a product level, you may consider running tests on individual products ahead of launching them on your wider services, in particular to understand how users behave and engage with the products and the potential impact of any behavioural biases. Evaluating data and insights gathered from these tests will improve your risk assessment because testing may indicate the effect of any product changes and whether they may increase or decrease the likelihood of illegal content appearing on or being disseminated by your platform, and its impact. For example, services running on-platform tests[28] of their recommender systems should include any additional safety metrics they gather as part of this routine testing to provide insights as to how minor changes may impact the risk of illegal content being disseminated on the service. Considering the results of product testing will help you understand certain risk factors which you may have identified in risk profiles, such as functionalities which allow users to find and encounter content, to communicate with one another, and/or to network.
Results of content moderation systems	Most services are likely to have a content moderation system in place, though the nature, scope and maturity of these systems varies significantly between services. You may choose to operate a more sophisticated content moderation system which measures more complex types of exposure if you are seeking to improve your understanding of and response to illegal content. For example, measuring how long a piece of illegal content is present on your service, the type of content you are taking down, or the virality of pieces of content, rather than only the number of user reports and steps taken in response. Assessing the effectiveness of content moderation decisions and the systems themselves also helps you to understand the level of mitigation provided by this measure in your risk assessment. Including this in your risk assessment will help you understand the likelihood of illegal harm taking place on your service, the effectiveness of your mitigation measures, and the effect of different characteristics of your service on risk levels (e.g. if a product change increases/reduces the amount of illegal content you detect)

[27] When we use the word 'product' we are using it as an all-encompassing term that includes any functionality, feature, tool, or policy that you provide to users for them to interact with through your service. This includes but is not limited to terms and conditions (Ts&Cs), content feeds, react buttons or privacy settings. By 'testing' we mean services should be considering any potential risks of technical and design choices, and testing the components used as part of their products, before the final product is developed. We recognise that services, depending on their size, could have different employees responsible for different products and that these products are designed separately from one another.

[28] By 'on platform testing of recommender algorithms' we mean the process of testing two or more variants of recommender system before proceeding with the design change. This could include but it not limited to A/B/x Testing or Multi Arm Bandit (MAB) Testing.

Enhanced inputs	Explanation
Consultation with internal experts on risks and safety measures	To improve your understanding of a specific risk users may face, or a technical measure to mitigate such a risk, you should consult with experts. A thorough examination process for a technical safety measure should consist of regular thematic technical expert meetings supported with focused follow up work. This examination process should provide a clearer understanding of how technical measures, system and processes may help address risk. Consultation could happen regularly, and records of the engagement should feed into an annual risk assessment review, or experts can be brought into the four-step process while the risk assessment is underway to provide formal and targeted input.
Views of independent experts	This input is likely to be valuable when considering complex topics such as a specific kind of illegal harm, or the intersection of harm, mitigation measures and freedom of expression for example. Expert consultation call help you consider how a particular harm manifests online in general and/or on your service specifically, which would in turn help you develop mitigation and management techniques which are targeted and effective. You should take steps to ensure the quality and accuracy of any third-party advice. Other types of expert consultation may also be relevant for your service to consider. This could include view of experts on industry trends, regulatory standards and the views of certain trade bodies or technical experts in relevant fields.
Internal and external commissioned research	If you are seeking to access additional expert resource and expertise to incorporate into your risk assessment, you may commission internal and/or external research. For instance, some services often commission research into specific trends or harms which informs their approach to safety and moderation on the platform. The purpose of this input is that expert research would allow your service to improve its understanding of the factors which may drive the likelihood of illegal content appearing on your service, the impact of that harmful content, and how it may be mitigated effectively.

Enhanced inputs	Explanation
Outcomes of external audit or other risk assurance processes	To improve your confidence that your trust and safety processes or wider risk management systems are robust, you may commission a third party to audit aspects of your service or undergo another form of risk assurance process. Independent audits can provide insights and analysis which services are unable to produce or assure themselves. They offer services the chance to be robustly assessed and offer the opportunity for services to identify new ways of improving their trust and safety processes. Services and any third-party suppliers should take steps to ensure that any methodology applied is robust and that the assurance process provides an independent and objective assessment of performance and recommendations for improvement. Including the outcomes of these audits in the risk assessment process can provide greater independence and granularity of detail as to the accuracy and quality of the risk assessment. Services which lack in-house capacity to carry out these processes may benefit from seeking third party audits; some services may also choose to work with third parties to seek independent and objective scrutiny of their risk assessment processes.
Consultation with users and user research	To improve your understanding of user experience or the experience of a specific group of users on your service, you may engage in consultation with users or carry out other forms of user research. You can choose the method and frequency of consultation and how you wish to undertake this engagement with users – this could include a platform-wide initiative which gives users an opportunity to give feedback on aspects of the service, or more targeted consultation with a specific group on specific issues which the platform has reason to believe will impact them. Alternatively, you may wish to contract external agencies to deliver qualitative research, other studies and obtain objective user feedback. This input will help your service embed safety by design into your platform. The research should complement existing user design processes but maintain a focus on understanding how users might interact with a new product or service. Research could focus on what behavioural factors (e.g. behavioural biases) could be present at key points in the user journey that could impact on their decision-making and increase the risk of them being exposed to illegal content. This could be particularly important if a product or service is intended to operate as part of a broader ecosystem rather than on a stand-alone basis. A continued dialogue with users of your platform will help to ensure that safety features, mitigations and other key points of engagement (for instance, terms of service) are accessible and meets the needs of users. Engagement could be general or designed to target specific users, such as those with vulnerabilities or certain age groups.

Enhanced inputs	Explanation
Engaging with relevant representative groups	You may choose to engage with relevant representative groups to improve your understanding of the risk of illegal content appearing on your site. To do this, your service may reach out to organisations representing specific groups to help give these groups a channel through which they are able to directly feedback any concerns they have around the handling of illegal content on your platform. This is a helpful action to take if your service has evidence that certain vulnerable groups will be particularly impacted by an aspect of your service's design, and particularly beneficial for services reviewing their risk assessment in light of undertaking a specific significant change to an aspect of its service design.

When to review or carry out a new risk assessment

A5.119 After you have completed your first risk assessment, you must take appropriate steps to **keep your risk assessment up to date**, including by responding to key triggers.

A5.120 The Act includes the following key duties on reviewing or carrying out a new risk assessment:

- a duty to take appropriate steps to keep an illegal content risk assessment up to date;
- a duty to update your risk assessment if Ofcom makes any significant change to a Risk Profile that relates to the service of the kind in question; and
- a duty to carry out a further suitable and sufficient illegal content risk assessment relating to the impacts of that proposed change before making any significant change to any aspect of your service's design or operation.

Table 12. When to review or carry out a new risk assessment

Duty	A duty to take appropriate steps to keep an illegal content risk assessment up to date	A duty to review your risk assessment if Ofcom makes any significant change to Risk Profiles which relates to the service of the kind in question	A duty to carry out a further suitable and sufficient illegal content risk assessment relating to the impacts of a proposed change before making any significant change to any aspect of a service's design or operation
Action	**REVIEW and UPDATE**		**CARRY OUT A NEW ASSESSMENT**
When do you need to do this?	A responsible person should oversee the duty to review and update the risk assessment **at least every 12 months**.	You need to review and update your risk assessments **if Ofcom makes a significant change to Risk Profiles**. Services should update their risk assessments **if** the change Ofcom is relevant to your service.	You must carry out a new risk assessment **before implementing a significant change** to any aspect of your service's design or operation. For these purposes, we consider that a change is significant if it is reasonably likely on its own to affect the likelihood or impact of users encountering illegal harm.
Why do you need to do this?	This duty is about ensuring your existing assessment remains accurate. Among other things, services will need to account for internal changes since the previous assessment (e.g. updates to the service), any new evidence that has been collected during the operation of a service, and developments in the external environment for risks online.	This duty is about whether the existing assessment remains accurate based on changes which Ofcom has made to Risk Profiles since your previous assessment. For instance, Ofcom could update Risk Profiles to identify new or different risk factors, such as additional functionalities that may increase risk. You should update your assessment if this change is relevant to your service.	A new risk assessment is required to ensure the impact of any significant changes is understood, recorded and where necessary, managed and mitigated. You should undertake a new risk assessment relating to any change which could impact your existing assessment of the risks of illegal harm. More guidance on what amounts to a significant change is detailed below.
How do you do this?	• Using your existing risk assessment, consider which risks or harms may have changed on your service based on any new evidence, developments in the external environment or changes which Ofcom has made to Risk Profiles • Using your existing risk assessment, identify any evidence gaps • Using your existing risk assessment adjust or confirm your evaluation of each risks of illegal content and existing measures to mitigate or manage risk • Adjust or confirm your safety measures based on the outcome of this review • **Record any changes to your risk assessment**		• Using Ofcom's four step process, carry out a **new risk assessment** relating to the proposed significant change • The new risk assessment should consider core or enhanced evidence inputs **relating to the proposed change** to help you understand how it will impact risk of illegal harm • Adjust, confirm or implement new safety measures based on this new assessment • **Make a record of your new risk assessment**

Review and update at least every 12 months

A5.121 You have a duty to take steps to keep your assessment up to date. It is likely that your risk assessment will become out of date after a certain amount of time has passed, even if you have not made any significant changes to your service. Incremental changes to your service, trends in user behaviour and technological changes will alter the evidence base underpinning your assessment, which means you should review your assessment. You should review your risk assessment if the underlying evidence changes.

A5.122 This process can be done by considering your most recent risk assessment alongside any new evidence that you have collected during the operation of your service, or new developments in the external environment and the risks online which your assessment needs to account for. If you think the new evidence will impact your assessment of risk then you should review each step of the four-step process with the updated evidence.

A5.123 Reviewing and updating an existing assessment should not be as burdensome as carrying out a new risk assessment, it should take account of new evidence to update your most recent assessment.

A5.124 You should decide your own policy for reviewing the risk assessment and recording it. You should be able to explain your approach and what appropriate steps you are taking to meet this duty. A succinct written policy will be a valuable tool to help you to demonstrate compliance.

A5.125 Your written policy on keeping a risk assessment up to date should include:

- A timeframe for regular review. Ofcom recommends that risk assessments are reviewed at least every 12 months. This aligns with other common annual governance, reporting and compliance cycles, and with other international online safety regimes (including the Digital Services Act); and
- A responsible person overseeing risk assessment processes.

Review and update if Ofcom makes a change to Risk Profiles

A5.126 The Act requires Ofcom to review and revise its Register and Risk Profiles to keep them up to date.

A5.127 If Ofcom makes a significant change to a Risk Profile which is relevant to your service, you must review and update your risk assessment.

A5.128 This can be done by considering your most recent risk assessment alongside Ofcom's changes to the Risk Profiles, to understand if any aspect of your assessment needs to be updated. For example, new risk factors relevant to your service could have been added (e.g. new functionalities), or new links between risk factors and harms could have been identified (e.g. a functionality which increases the risk of grooming or fraud).

A5.129 If these changes are relevant to your service, you should consider if your assessment of the risk of each harm needs to change.

A5.130 If you think the changes to the Risk Profiles have impacted your risk assessment, then you should review each step of the four-step process in light of Ofcom's change and update your record.

A5.131 Reviewing and updating an existing assessment should not be as burdensome as carrying out a new risk assessment; it should take account of specific changes which Ofcom has made to Risk Profiles.

Carry out a new risk assessment before making a significant change to your service

A5.132 If you plan to make a significant change to your service, you must carry out a new risk assessment **before** making the change. This applies to a change to any aspect of the service design or operation which is reasonably likely to have a significant impact on the risk to users. **This is a specific legal duty, so you should carefully consider proposed changes to your service.**

A5.133 While the duty only requires you to carry out a new risk assessment as it relates to the impacts of the proposed change, this may in practice require you to carry out a new assessment of the whole service as it is unlikely that the significant change would not impact other aspects of the service. This new assessment can be done by carrying out each step of the four-step process.

A5.134 Below, we have provided guidance on what amounts to a significant change. We indicate the types of scenarios that are likely to amount to a significant change.

Table 13. Guidance on significant change

Type of change	Guidance	Outcome
One overarching question you should consider when evaluating whether a change is significant is the size of your service. For instance, a relatively minor change on a large service is likely to have a significant impact, while it could take a much larger change on a smaller service to trigger the need to review their risk assessment.		
Likely to amount to a significant change	Your proposed change is very likely to amount to a significant change on your service if any of the following apply: • The proposed change alters the risk factors which you identified in your last risk assessment. • The proposed change impacts a substantial proportion of your user base or changes the kind of users you expect to see on your service. • The proposed change impacts a vulnerable user group, such as children. • The proposed change impacts the efficacy of the measures you have put in place following your last assessment to reduce the risk of illegal content appearing on your service. • The proposed change impacts your revenue model, growth strategy and/ or ownership in a way that affects its service design. When considering these statements, you should consider if any of the following apply to the proposed change:	If yes, **you must carry out a new risk assessment relating to this change**

	• Would the change clearly impact users, user experience or user behaviour in a way that may affect risk? • Does the change affect the ability or incentives of bad actors to commit offences related to illegal content on your service? • Will the change affect user reporting abilities – particularly something to consider if the change impacts the user interface or alters reporting processes? • Does the change include new functionalities or enable users to interact differently? • Does it include changes that would affect content or network recommendations on your service? • Does the change involve a new or different content moderation process or approach? • Does it include changes to your business model in terms of how you generate revenue or your growth strategy?	
Unlikely to amount to a significant change but it may impact some aspect of the service design or operation	Your proposed change is unlikely to amount to a significant change on your service if any of the following apply: • The proposed change is unlikely to alter the risk factors which you identified in your last risk assessment • The proposed change is unlikely to impact a substantial proportion of your userbase or change the kind of users you expect to see on your service • The proposed change is unlikely to impact a vulnerable user group, such as children • The proposed change does not involve a change in business model or ownership of the service. The proposed change impacts the efficacy of the measures you have put in place following your last assessment to reduce the risk of illegal content appearing on your service	**You should review your assessment** to ensure that it remains up to date
A very minor or routine change which will not impact any aspect of the service's design or operation	Your proposed change is unlikely to amount to a significant change if the following statements apply: • The proposed change does not alter the risk factors which you identified in your last risk assessment • The proposed change will only impact a small portion of non-vulnerable users and will not change the kind of users you expect to see on your service • The proposed change will not impact the efficacy of the measures you have put in place following your	**No action needed**; the change can be accounted for in the next scheduled review cycle

	last assessment to reduce the risk of illegal content appearing on your service	

A5.135 Examples of the types of design and operational changes which are likely to amount to a significant change include – but are not limited to – the following:

Significant updates to the design of user-facing algorithms, systems and processes, for example changing the operation of the recommendation system, such as including a new input or changing the weighting of existing inputs. Key examples include:

- Introduction of a new recommender system: this may include a recommender to suggest friends and groups to follow, alongside the existing content feed recommender. It may also include a complete replacement of the existing content recommender.
- Introduction of a new machine learning model within the existing recommender system: a service could implement a new machine learning model to enhance the predictions that are made by a recommender system (e.g. regarding whether a user will click on a piece of content, or whether that piece of content is clickbait). These new or enhanced predictions would in turn alter the content users are recommended.
- Changing the "Goal Criteria" of Recommender Systems: changing the overall aims that the service has in mind for those systems, for instance, to maximise the number of views, the average viewing time, or the diversity of content presented to users.
- On platform testing indicates that a change to a recommender system may have a significant impact on the risk of illegal content

Adding or removing functionalities: the risk assessment must assess the impact of functionalities on the risk of illegal harm, so adding or removing functionalities – such as sharing content, direct messaging or live streaming – must be accounted for in the risk assessment

Changes to platform content rules or content prioritisation: these may alter the types of content that users encounter and subsequently alter the sites userbase. For instance, the decision to allow or prohibit adult content on a platform.

Updates to the design of user facing functionalities and features such as changing the location of the report button or changing the design of icons related to reporting or reacting to content which could impact how users engage with online safety measures

Any acquisition that may change the core product offered to users: for instance integrating functionality from another platform following a product acquisition

Changes in ownership or investment: these may influence how the platform operates (a new owner may have different views on how the platform should operate).

Changes in the revenue models: examples that may affect level of risk include new streams of revenue, a significant change in the factors or key performance indicators that the service maximises to achieve its revenue goals, or changes in sources of revenue that has a significant impact on the design choices of the service.

Changes in the services' growth strategy: for example, if changes in growth strategy that affects service design choices or the speed of growth of your user base.

Change in capacity (in terms of number of employees): that may affect the number and quality of technical resources to assess and mitigate risk of illegal harm on your service.

Appendix A: Risk Profiles

Supporting resources

Register of Risks Glossary
Volume 2: The causes and impacts of harm (draft Register of Risks)
Appendix B: Offences and kinds of illegal harm

A5.136 **The draft U2U and Search Risk Profiles** are resources to consult when conducting your risk assessment. All services must take account of the relevant Risk Profile when conducting their own risk assessment.

A5.137 Risk Profiles are made up of a list of different risk factors. After consulting the Risk Profiles (using our guidance), you should have a **list of your risk factors** and **key kinds of illegal harm associated with these risk factors** where relevant.[29] You should then assess these risk factors alongside your own evidence under Step 2.

A5.138 These risk factors represent a selection of service characteristics (such as user base, business models and functionalities) that our draft **Register of Risks (Register)** indicates are most strongly linked to a risk of one or more kinds of illegal harm outlined in Appendix B of this document.

A5.139 The Register provides a detailed analysis of the risks of harm to individuals we have identified across U2U and search services. It therefore contains our evidence in full and in some cases identifies risk factors in addition to those highlighted in Risk Profiles. The Risk Profiles will be updated as necessary when changes are made to the Register. Further information on the Register is available in Volume 2 (The causes and impacts of online harm).

A5.140 When consulting the list of risk factors, you should keep in mind:

a) We do not include all the characteristics that may lead to a risk of harm. We do not include risk factors from the Register where we have more limited evidence, or where we have drawn parallels based on the similarity between two kinds of illegal harm.

b) Additionally, the description of the risks provided is a high-level summary only. The effect of any risk factors will vary depending on the context, including the combinations of risk factor present, the governance, systems and processes a service has in place, and the motivations and dynamics that may be unique to the kind of illegal harm or the nature of a service itself.[30]

A5.141 Given this, you should see the Risk Profile as your starting point to understand which kinds of illegal harm are most likely to occur on a service like yours, and which risk factors may play a role.

[29] The **key kinds of illegal harm** associated with a risk factor are those where our evidence indicated the strongest link. There may be other kinds of illegal harm which may be relevant. For further information, see Volume 2, Chapter 6 (Introduction to the Register of Risks).

[30] For further information on how we see these dynamics play out in our evidence base, see Volume 2, Chapter 6B (Part 1: Introduction to User-to-User services) and Volume 2, Chapter 6T (Part 2: Search services).

U2U Risk Profile and risk factors

A5.142 The Ofcom U2U Risk Profile is presented in Table 14 below. Each row represents a unique risk factor that services should consider when conducting their risk assessment. The information provided on the risk factors in the table is based on the evidence in Volume 2, Part 1 of the Register (User-to-user services).

A5.143 When consulting the table, services should do the following:

First, answer the 'Yes' / 'No' questions in Figure 3 below about the characteristics of your service;[31]

Second, use your answers to select which **specific risk factors** from Table 14 apply to you. Each 'Yes' answer corresponds to a risk factor you will need to take account of in your risk assessment. For example, if you answered 'Yes' to questions 2a, 3b, and 5f then you should select those three risk factors from the risk factor table. A Glossary is available to help you interpret your risk factors accurately;[32]

Third, review the **three general risk factors** at the bottom of the risk factor table - user base, business model (revenue model and growth strategy) and commercial profile. These apply to all services, and you will need to take account of each in your risk assessment.

A5.144 After you have taken these three steps, you should have the **list of risk factors** you will need to take account of when conducting your own risk assessment. This list includes any specific risk factors you have selected, plus all three of the general risk factors.

A5.145 Step 2 of the RAG provides details on how to use this list of risk factors as part of your risk assessment. At Step 2, you will also consider how the risk factors you have selected affect your service (e.g. whether this is a risk that you are already managing, or one that you may need to pay extra attention to).

[31] If your service offers multiple versions – e.g. mobile and web – you should select 'Y' if *any* versions of the service has the relevant characteristic(s). However, this only applies where versions are similar enough to be treated as a single service. Service providers should refer to Volume 1, Chapter 3: Overview of Regulated Services to determine if versions of your service should be treated as distinct 'services' under the Act. In cases where a provider has control over multiple services, they are required to conduct a Risk Assessment for each service, and to consult the Risk Profiles which are relevant to each.

[32] If, after consulting the Register of Risks Glossary, you are still unsure if the risk factor applies to you, we would suggest you read the corresponding information provided about that risk factor in Table 13 and consider if this information is relevant to your service. You may also wish to consult the Volume 2, Part 1 of the Register (User-to-user services) for more detailed information on the corresponding risk factor or kind of illegal harm.

Figure 3. Questions for identifying your risk factors.

Select Yes (Y) or No (N) for the following questions about your U2U service.	
1. Is my service any of the following service types? Select all that apply:	
a. **Social media service** (services which connect users and enable them to build communities around common interests or connections)	Y / N
b. **Messaging service** (services that are typically centred around allowing users to send messages that can only be viewed or read by a specific recipient or group of people)	Y / N
c. **Gaming service** (services which allow users to interact within partially or fully simulated virtual environments)	Y / N
d. **Adult service** (services which are primarily used for the dissemination of user-generated adult content)	Y / N
e. **Discussion forum or chat room service** (services which allow users to send or post messages that can be read by the public or an open group of people)	Y / N
f. **Marketplace or listing service** (services which allow users to buy and sell their goods or services)	Y / N
g. **File-storage and file-sharing service** (services whose primary functionalities involve enabling users to store digital content and share access to that content through links)	Y / N
2. Does my service allow child users to access some or all of the service?[33]	Y / N
3. Does my service have any of the following functionalities related to how users identify themselves to one another? Select all that apply:	
a. Users can display identifying information through a user profile that can be viewed by others (e.g. images, usernames, age)	Y / N
b. Users can share content anonymously (e.g. anonymous profiles or access without an account)[34]	Y / N
4. Does my service have any of the following functionalities related to how users network with one another? Select all that apply:	
a. Users can connect with other users[35]	Y / N
b. Users can form closed groups or send group messages	Y / N
5. Does my service have any of the following functionalities that allow users to communicate with one another? Select all that apply:	
a. Livestreaming (either open or closed channels)	Y / N
b. Direct messaging (including ephemeral direct messaging)	Y / N
c. Encrypted messaging	Y / N
d. Commenting on content	Y / N
e. Posting or sending images or videos (either open or closed channels)	Y / N
f. Posting or sending location information	Y / N
g. Re-posting and forwarding content	Y / N
6. Does my service allow users to post goods and services for sale?[36]	Y / N

[33] Child users refers to under 18s. We recognise there are other ways to indicate presence of children on a service beyond whether a service 'allows' children, and will continue to monitor this approach to ensure alignment with our forthcoming work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

[34] The majority of our evidence base speaks of the risks posed by user-to-user anonymity. However, we have indicated where research indicates specifically service-to-user anonymity presents a risk.

[35] We describe 'user connections' as a user-to-user service functionality that allows users to follow or subscribe to other users. Users must sometimes be connected to view all or some of the content that each user shares. Further information on risk factors is available in the Register of Risks Glossary.

[36] We describe 'posting goods and services' as a user-to-user service functionality allowing users to post content dedicated to offering goods and services for sale. This does not include paid-for advertisements, but may serve the function of allowing users to promote goods or services. Further information on risk factors is available in the Register of Risks Glossary.

Select Yes (Y) or No (N) for the following questions about your U2U service.	
7. Does my service have any of the following functionalities that allow users to find or encounter content? Select all that apply:	
a. Searching for user-generated content	Y / N
b. Hyperlinking	Y / N
8. Does my service use content or network recommender systems?	Y / N

Source: Ofcom analysis

Table 14. U2U risk factors (U2U Risk Profile).

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
1. Service type factors		
☐	**1a** Social media services	• **Risk factor:** Social media services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of nearly all kinds of illegal harm. Many social media services are designed to maximise engagement between users. If your service is a social media service, you should consider how potential perpetrators may exploit this design for illegal purposes. For example, potential perpetrators may exploit the likelihood of virality to share illegal content with very large groups of people. Social media services can also be used by potential perpetrators of grooming to target young users by sending out many messages. These services are also used in large-scale foreign interference campaigns to spread disinformation. Research shows that social media services can increase the risk of nearly all kinds of illegal harm, except for firearms and other weapons offences where we do not currently have evidence. This may be due to more research on social media services, or greater probability of risk due to the wide range of functionalities and features on many social media services.
☐	**1b** Messaging services	• **Risk factor:** Messaging services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming and CSAM**), controlling or coercive behaviour, drugs and psychoactive substances, unlawful immigration/human trafficking, proceeds of crime, fraud and financial services, and foreign interference offences. Messaging services allow users to protect their privacy. If your service is a messaging service, you should consider how this design may also be used by potential perpetrators to communicate and share illegal content in a setting that is hidden from public view. This can result in more targeted behaviours and can make detection more difficult, particularly on messaging services with encryption (see 5c). Potential perpetrators often seek to move other users from services where they initially connected (see 4a) to messaging services.
☐	**1c** Gaming services	• **Risk factor:** Gaming services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (grooming), hate and harassment/stalking/threats/abuse offences. If your service is a gaming service, you should consider how it may bring potential perpetrators in contact with other users and may create a space where potentially illegal behaviour is normalised. Gaming services can allow hateful content to spread and become sites of 'normalised harassment', where name-calling or insults are part of user interactions. Gaming services can also be created and modified by terrorist organisations as recruitment tools and be used by potential perpetrators of online grooming to approach children.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**1d** Adult services	• **Risk factor:** Adult services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (image-based CSAM), extreme pornography, and intimate image abuse offences. If your service is an adult service, you should consider how your service may be used by potential perpetrators to share illegal content that is sexual in nature. This includes intimate images, child sexual abuse material, and extreme pornography.
☐	**1e** Discussion forums and chat rooms	• **Risk factor:** Discussion forums and chat rooms • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (CSAM**) and encouraging or assisting suicide or serious self-harm offences. If your service is a discussion forum or chat room, you should consider how your service may be used by potential perpetrators to discuss and share illegal content in a setting that is typically visible to the public. For example, our evidence shows that discussion forums and chat room services can act as spaces where suicide or serious self-harm is assisted or encouraged.
☐	**1f** Marketplace and listing services	• **Risk factor:** Marketplace and listing services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, sexual exploitation of adults, firearms and other weapons and fraud and financial services offences. If your service is a marketplace or listings service, you should consider how your service may be used by potential perpetrators to sell or buy illegal goods or services. They are often used in purchase scams in fraud offences and can also be used to raise funds that are used for potentially illegal purposes such as terrorist activities. The ability to make online payments on online marketplaces or listing services can increase the risk of harm.
☐	**1g** File-storage and file-sharing services	• **Risk factor:** File-storage or file-sharing services • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (image-based CSAM) and intimate image abuse offences. If your service is a file-storage or file-sharing service, you should consider how it may be used by potential perpetrators to store and share illegal content. File-sharing services, in particular those that allow users to upload and share images, are used to store CSAM that can be shared through URLs that perpetrators embed on other services. Potential perpetrators can also create folders of non-consensual intimate images on these services that can be downloaded by others.
2. User base factors		
☐	**2** Services which allow child users[37]	• **Risk factor:** Child users (under 18s) • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming and CSAM**) offences. If your service has a high proportion of child users or is aimed at children, your service may be used by potential perpetrators to identify and initiate contact with children for the purposes of grooming them. Child users may also upload, post or share self-generated indecent images.[38] These risks can increase for both CSAM and grooming if your service has direct messaging and/or encrypted messaging (see 5b and 5c). Children may also experience different or increased risks across other kinds of illegal harm. See User Base Demographics.

[37] Child users refers to under 18s. We recognise there are other ways to indicate presence of children on a service beyond whether a service 'allows' children, and will continue to monitor this approach to ensure alignment with our forthcoming work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

[37] We do not include features of revenue models covered in other risk factors, e.g. the role of recommender systems.

[38] Self-generated indecent images (SGII) refers to indecent images that are shared often consensually between children and can be non-consensually reshared. For further information, see Chapter 6C of the Register of Risks (Child Sexual Exploitation and Abuse).

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
3. User identification factors		
☐	**3a** Services with user profiles	If your service allows users to create a user profile that displays identifying information that can be viewed by others (e.g. images, usernames, age), we would expect you to take account of the risks that can arise from this. While there is some overlap, our evidence indicates there are broadly two main manifestations of risk arising from user profiles: • **Risk factor:** User profiles • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming), harassment/stalking/threats/abuse, drugs and psychoactive substances, unlawful immigration/human trafficking, and sexual exploitation of adults offences. In some cases, potential perpetrators may be able to use the information displayed on a profile to identify and target a specific user or group of users for illegal purposes. This is especially relevant for gendered illegal harms such as harassment/stalking, where the information can help potential perpetrators find specific individuals to target (see User Demographics). For CSEA (grooming), user profile information can enable potential perpetrators to identify children to target. • **Risk factor:** Fake user profiles • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming), harassment/stalking/threats/abuse, controlling or coercive behaviour, proceeds of crime, fraud and financial services and foreign interference offences. In a different context, users can create fake user profiles that do not accurately reflect the official identity of the account holder. While this can be an important tool for protecting the identity of some users who may be targeted for their views or online activity, particularly marginalised communities, whistle-blowers, and dissenting voices, it also comes with risks. For example, our evidence indicates potential perpetrators may create fake user profiles to impersonate another entity, often with fake images and usernames. This may allow them to impersonate others as part of illegal behaviours such as fraud (impersonation or misrepresentation offences), foreign interference or to monitor, harass or humiliate victims and survivors of controlling or coercive behaviour.
☐	**3b** Services where users can post or send content anonymously, including without an account	• **Risk factor:** Anonymous user profiles[39] or users without accounts • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (CSAM**), encouraging or assisting suicide or serious self-harm, hate and harassment/stalking/threats/ abuse offences. Anonymity is an important tool for users to protect themselves from being identified and targeted for their views, particularly for marginalised communities, whistle-blowers and dissenting voices. However, our evidence indicates that in certain contexts, if your service allows users to share content anonymously, risks can increase. The evidence suggests these risks arise from the disinhibition effect, where users are emboldened because they cannot be identified by other users. This increases the likelihood that users will share illegal material, for example CSAM. Anonymity can also increase the risk that users on your service conduct illegal behaviour such as harassment and stalking.

[39] We describe 'anonymous user profiles' as a user-to-user service functionality allowing users to create a user profile where their identity is unknown to an extent. This includes instances where a user's identity (an individual's formal or officially recognised identity) is unknown to other users, for example through the use of aliases ('pseudonymity'). It also includes where a user's identity may be unknown to a service, for example services that do not require users to register by creating an account. Further information on risk factors is available in the Register of Risks Glossary.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
4. User networking factors		
☐	**4a** Services with user connections	• **Risk factor:** User connections • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (grooming), harassment/stalking/threats/abuse, controlling or coercive behaviour, drugs and psychoactive substances, fraud and financial services and foreign interference offences. User connections may be used by potential perpetrators to build networks and establish contact with users to target (see 3a). For terrorism and drug offences, user connections can be used by potential perpetrators to connect with thousands of other users to widely share illegal content. Our evidence also suggests that terrorists may exploit these networks to raise funds, in particular if online payments can be made on the service. Potential perpetrators can also use connections to build online networks which can enable them to access other users indirectly; for example to gain visibility of a target's user profile in cyberstalking offences or to serve to add legitimacy to fraudsters and their content. These connections can also be used by online groomers to appear as if they are part of a child's social network (see 1) allowing them to establish contact with child users and begin communicating.
☐	**4b** Services where users can form user groups or send group messages	• **Risk factor:** User groups • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming), encouraging or assisting suicide or serious self-harm, drugs and psychoactive substances and unlawful immigration/human trafficking offences. Given the similarity with group messaging, we would also expect you to consider the key kinds of illegal harm associated with that functionality. User groups can enable potential perpetrators to create communities where illegal content can be shared and where illegal behaviour can be encouraged and normalised. In grooming offences for example, user groups allow potential perpetrators to build networks and share how to offend. User groups may also enable potential perpetrators to identify and target vulnerable users on your service, such as children or those experiencing mental health problems (see User Base Demographics). • **Risk factor:** Group messaging • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (CSAM**), intimate image abuse, and fraud and financial services offences. Given the similarity with user groups, we would also suggest you consider if any key illegal harms associated with that functionality are relevant to your service. Similarly to user groups, group messaging allows communities of users to post content in a closed setting. Group messaging can also allow potential perpetrators to share illegal content such as CSAM URLs with numerous users at once. The risk posed by group messaging, and the numerous users that group messages may reach, can be exacerbated when those messages are encrypted (see 5c).
5. User communication factors		
☐	**5a** Services with livestreaming	• **Risk factor:** Livestreaming • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (grooming and image-based CSAM), encouraging or assisting suicide or serious self-harm, and harassment/stalking /threats/abuse offences. If your service allows livestreaming, there is an increased risk of multiple offences, in part due to difficulty of moderating content that is shared in real-time. There is a substantial evidence base detailing the role that livestreaming plays in the commission of sexual abuse and exploitation of children. There is also evidence to suggest that comments on livestreams are used to facilitate grooming offences (see 5d). By using screen capturing and recording functionalities, the livestreaming of CSEA can be used to create CSAM. This functionality can also be used to broadcast terror attacks, often on open channels which can similarly be circulated to wider audiences if captured or recorded (see 5e and 5g).

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**5b** Services with direct messaging	• **Risk factor:** Direct messaging • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming and CSAM**), hate, harassment/stalking/threats/abuse, controlling or coercive behaviour, intimate image abuse and fraud and financial services offences. There is a strong link between direct messaging and various offences due to the closed nature of these messages. While direct messaging can enable users to protect their privacy, direct messaging can be used to facilitate offences or share illegal content in a way that is not immediately visible to the public. For example, our evidence indicates that the ability to communicate on a regular basis is key to potential perpetrators establishing a grooming relationship with children (see 2, 3a and 4a). The relatively private nature of direct messaging can also be used by potential perpetrators share CSAM or other illegal content such as articles for use in fraud. Others may use it to harass, stalk and threaten users in a targeted way. In addition, you should take account of any additional risks posed by ephemeral direct messages, which can reassure users that there is no permanent record of the content they are sending. This can, for example, increase the risk of users facilitating drug offences, or of children sharing self-generated intimate images. Ephemeral messaging also relates to grooming, as perpetrators may use it to contact children and hide records of the communication.
☐	**5c** Services with encrypted messaging	• **Risk factor:** Encrypted messaging • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (grooming and CSAM**), drugs and psychoactive substances, sexual exploitation of adults, foreign interference and fraud and financial services offences. End-to-end encryption guarantees a user's privacy and security of their messages, while at the same time making it more difficult for services to moderate for illegal content being sent on their service. If your service allows encrypted messaging, we would expect you to consider how this functionality can be used by potential perpetrators to avoid monitoring of communications while sharing illegal content such as CSAM or conducting illegal behaviour. For example, our evidence indicates that potential perpetrators of grooming may initially communicate on unencrypted channels and then move child users towards encrypted channels where it is harder to detect offenders' contact with children (see 1b and 2).
☐	**5d** Services with commenting on content	• **Risk factor:** Commenting on content • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (grooming), encouraging or assisting suicide or serious self-harm, hate, and harassment/stalking/threats/abuse offences. Commenting on content can enable potential perpetrators to target users who share content and to amplify or signpost to existing illegal content. For example, potential perpetrators may share comments containing hateful content on a user's post, sometimes with a coordinated group of users, as a means of targeting the user who posted the content. Comments can also be used by potential perpetrators to amplify illegal content. For example, potential perpetrators of terrorism may share comments containing or hyperlinking to terrorist content (see 7b). However, you should also be aware that comments can serve as a means for other users to counter illegal content, for example by providing advice such as warnings about fraud or discouraging suicide or serious self-harm.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**5e** Services with posting images or videos	• **Risk factor:** Posting images or videos • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (image-based CSAM), encouraging or assisting suicide or serious self-harm, controlling or coercive behaviour, drugs and psychoactive substances, extreme pornography and intimate image abuse offences. Posting images or videos can allow potential perpetrators to share illegal content with many users in open channels of communication. Posting images is a key functionality in the commission of image-based offences, including intimate image abuse, extreme pornography and CSAM. In addition, image-based content can also facilitate other kinds of harm; for example, users may be able to post 'memes' that include terrorist content. In addition, you should consider how potential perpetrators can post images or videos that were edited – potentially using functionalities on U2U services. For example, 'deepfakes,' can depict participants in legal pornography as children in image-based CSAM.
☐	**5f** Services where users can post or send location information	• **Risk factor:** Posting or sending location information • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to harassment/stalking/threats/abuse and controlling or coercive behaviour offences. Posting or sending location information may be used by potential perpetrators to track the whereabouts of survivors and victims. This information may enable potential perpetrators to stalk and harass targets. You should consider how the sharing of a user's location, sometimes inadvertently, can play an important role in controlling or coercive behaviour and stalking / harassment, as perpetrators can use geo-location tracking (for example, attached to status updates) as a means to monitor survivors and victims. While any user can experience these kinds of harm, you should also pay particular attention to User Demographics when considering this risk factor as our evidence indicates that women and girls are disproportionately impacted by the key kinds of illegal harm associated with this functionality.
☐	**5g** Services with re-posting or forwarding of content	• **Risk factor:** Re-posting or forwarding content • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to encouraging or assisting suicide or serious self-harm, harassment/stalking/threats/abuse, intimate image abuse and foreign interference offences. If your service allows the re-posting or forwarding of content, you should consider how this may allow illegal content to be disseminated to a much larger audience than it was originally shared with, often without the context and information that surrounded the content. For example, in intimate image abuse, the secondary distribution of images can cause non-consensual intimate images to 'go viral' (see 5e). It also becomes more difficult to get images removed when they are repeatedly re-posted on the original service, as well as on others.
6. Transaction and offers factors		
☐	**6** Services where users can post goods or services for sale	• **Risk factor:** Posting of goods or services for sale • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to drugs and psychoactive substances, firearms and other weapons, sexual exploitation of adults and fraud and financial services offences. Potential perpetrators may try to promote illegal goods or services by posting them for sale using this functionality. Often illegal items such as drugs and firearms are posted for sale using code names. In certain contexts, the ability to post goods or services for sale, such as through user-generated advertisements, also enables potential perpetrators to advertise and broadcast the sexual services of adults in exploitative environments. The risk of harm can be increased if your services also allows users to make online payments directly.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
7. Content exploring factors		
☐	**7a** Services where users can search for user-generated content	• **Risk factor:** User-generated content searching • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to drugs and psychoactive substances, firearms and other weapons, extreme pornography, and fraud and financial services offences. The ability to search for user-generated content within services may allow users to find illegal content and identify users to target on your service. For example, fraudsters may post content relating to the supply of stolen bank details alongside advice on how to use them to commit fraud which can be found by other users through content searching. Often, these posts include combinations of key terms or hashtags to make it easier for users to find this kind of content. Our evidence indicates that search results on U2U services can include illegal content such as scams or extreme pornography, even when users are not actively searching for it.
☐	**7b** Services with hyperlinks	• **Risk factor:** Hyperlinking • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, CSEA (CSAM URLs) and foreign interference offences. You should consider how hyperlinks can be used by potential perpetrators to direct users towards illegal material, including on third-party services. For example, perpetrators use hyperlinks and plain-text URLs linking to share illegal images among themselves on various types of services, giving opportunity to access and download CSAM.
8. Recommender systems		
☐	**8** Services with recommender systems	Recommender systems refers to algorithmic systems which, by means of a machine learning model, determine the relative ranking of suggestions made to users. These include systems that suggest either content or other users on the service. Although recommender systems deliver content to users on your service that they may find interesting, they can also lead to a risk of harm. • **Risk factor:** Content recommender systems • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to encouraging or assisting suicide or serious self-harm and hate offences. Content recommenders are used to curate the content that is suggested to users, and there is a risk they inadvertently amplify illegal content to a wide set of users who may otherwise not organically come across this content. Our evidence, for example, indicates that if not properly tested and deployed, content recommendation systems may amplify hateful content if they are optimised for user engagement. • **Risk factor:** Network recommender systems • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming) offences. Network recommender systems suggest users or groups of other users to connect with. These systems may connect users in ways that increase risks, for example recommending children connect with others, or recommending the children be connected with. This can inadvertently facilitate grooming if appropriate checks are not in place.

General risk factors All U2U services should take account in their risk assessment.		
☑	All U2U services	• **Risk factor:** User base demographics The demographics of your user base (including things like users' protected characteristics, media literacy levels, mental health) will influence the risk of harm related to all kinds of illegal harm. **Overall, we have found that vulnerable users, and particularly users with multiple protected characteristics, are more likely to experience harm from illegal content and are impacted differently by it.** For example, we would expect you to consider: - How the **gender** of users affects your assessment of risk – women and girls are disproportionately impacted by kinds of illegal harm related to CSEA (both grooming and CSAM), cyberstalking/harassment/threats/abuse, controlling or coercive behaviour and intimate image abuse. - How users with other protected characteristics (including **age**[40]**, race (including ethnicity)**, **sexuality**, **sexual identity**, **age, religion, disability**) affects your assessment of risk, including the risk of harm to users with **multiple protected characteristics**. These dynamics are highly complex and context-specific, and evidence is provided in the Register on user base demographics for each kind of illegal harm (see Volume 2, Part 1). This can help you assess this risk factor even if you do not have any service-specific information on the make-up of your user base.
☑	All U2U services	• **Risk factor:** Business model (revenue model and growth strategy) Your revenue model may inadvertently increase the risk of different kinds of illegal harm occurring. For example, we would expect you to consider: - How the **design of your service to optimise your revenue** may influence risk. For instance, to increase user engagement, service design may encourage engaging content that is illegal such as hate or may minimise 'friction' when sharing content in a way that increases the risk of illegal content on your service. - How aspects of your revenue model may be misused by potential perpetrators. For instance, potential perpetrators may misuse the opportunity to **'boost posts'** to promote and amplify fraudulent content. They may also **advertise and use ad targeting** to reach and lure in potential victims for sexual exploitation or foreign interference, and **attract niche or likeminded users through subscriptions**, which may create an environment that fosters harmful activity. Related to this, we also expect you to consider how your growth strategy[41] may influence service design in a way that may increase the risk of some kinds of illegal harm. For instance, minimising friction to grow your user base may result in less effective moderation for some kinds of illegal harm such as extreme pornography.

[40] We include 'child users' as a specific risk factor, however age can also be considered as part of user base demographics. This is because, unlike other demographic factors, there are services that allow child users, and services that do not, and we wanted to draw out the risks associated with this distinction. We recognise there are other ways to indicate presence of children on a service and will continue to monitor this approach to ensure alignment with our forthcoming work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

[41] We describe 'growth strategy' as how the service plans to expand its business. For example, through growing revenue and number of users. Further information on risk factors is available in the Register of Risks Glossary.

General risk factors All U2U services should take account in their risk assessment.		
☑	All U2U services	• **Risk factor:** Commercial profile Your commercial profile may increase the risk of different kinds of illegal harm occurring. For example, we would expect you to consider: - How **low capacity** or **early-stage services** may increase the likelihood of different illegal harms as they may have limited technical skills and financial resources to introduce effective risk management. - How a **fast-growing user base** may negatively affect effective risk management, given the increased scale and sophistication of the moderation technologies and processes required to keep track of a fast-growing user base (particularly since the sources of risk can change quickly as the user base develops). Our analysis suggests that potential perpetrators may opt to uses these services to post CSAM or terrorist content, for example, because the content is less likely to be identified and action taken.
* See Appendix B for further information on the individual offences for each kind of illegal harm. Given the complexity of many of these harms, we recognise that there may be other kinds of illegal harm which are associated with the risk factor not listed here. This is because our evidence on the link with a risk of harm is weaker or we may not have any evidence presently. For our detailed analysis of each kind of illegal harm see Volume 2 Chapter 6 (Register of Risks). For further information on our evidence base and methodology, see Volume 2 Chapter 5 (Evidence and methodology of our risk assessment). ** Unless otherwise stated, CSAM includes both image-based and URL-based CSAM.		

Source: Ofcom analysis

Search Risk Profile and risk factors

A5.146 The Ofcom Search Risk Profile is presented in Table 15. Each row represents a unique risk factor that services should consider when conducting their risk assessment. The information provided on the risk factors is based on the evidence in Volume 2, Part 2 of the Register (Search services).

A5.147 When consulting the table, services should do the following:

First, answer the 'Yes' / 'No' questions in Figure 4 below about the characteristics of your service[42];

Second, use your answers to select which **specific risk factors** from Table 15 apply to you. Each 'Yes' answer corresponds to a risk factor you will need to take account of in your risk assessment. For example, if you answered 'Yes' to questions 1a, 2, and 3b then you should select those three risk factors from the table. A Glossary is available to help you interpret your risk factors accurately;[43]

[42] If your service offers multiple versions – e.g. mobile and web – you should select 'Y' if *any* versions of the service has the relevant characteristic(s). However, this only applies where versions are similar enough to be treated as a single service. Service providers should refer to Volume 1, Chapter 3: Overview of Regulated Services to determine if versions of their service should be treated as distinct 'services' under the Act. In cases where a provider has control over multiple services, they are required to conduct a Risk Assessment for each service, and to consult the Risk Profiles which are relevant to each.

[43] If, after consulting the Glossary, you are still unsure if the risk factor applies to you, we would suggest you read the relevant information provided about that risk factor in Table 14 and consider if this information is relevant to your service. You may also wish to consult the Volume 2, Part 2 of the Register (Search services) for more detailed information on the corresponding risk factor or kind of illegal harm.

Third, review the **three general risk factors** (user base, revenue model and commercial profile) at the bottom of the table. These apply to all services, and you will need to take account of each in your risk assessment.

A5.148 After you have taken these three steps, you should have the **list of risk factors** you will need to take account of when conducting your own risk assessment. This list includes any specific risk factors you have selected, plus all three of the general risk factors.

A5.149 Step 2 of the RAG provides details on how to use this list of risk factors as part of your risk assessment. At Step 2, you will also consider how the risk factors you have selected affect your service (e.g. you have considered if this is a risk that you are already managing, or one that you may need to pay extra attention to).

Figure 4. Questions for identifying your risk factors.

Select Yes (Y) or No (N) for the following questions about your Search service.	
1. Is my service any of the following service types Select all that apply:	
a. General or downstream search service	Y / N
b. Vertical search service	Y / N
2. Does my service allow child users?[44]	Y / N
3. Does my service have any of the following functionalities? Select all that apply:	
a. Provide users with search predictions or suggestions	Y / N
b. Allow users to search for photographs, videos or visual images	Y / N

Source: Ofcom analysis

Table 15. Search risk factors (Search Risk Profile).

Specific risk factors Search services with relevant characteristics should take account in their risk assessment.		
1. Service type factors		
☐	**1a** General and downstream search services	• **Risk factor:** General and downstream search services General search services are the starting point of many users' online journeys and play a crucial role in making content accessible. General search services present users with access to webpages from across the entire clear web. We would expect you to consider how this may provide a means for users to locate and access illegal content; a user who knows what to look for can access a wide range of illegal content from among the potentially billions of indexed web pages that are made accessible. For example, search engines have been identified as one of the most common methods of finding CSAM online, alongside U2U services. There is also evidence showing the ways in which search engines can enable users to access websites hosting illegal items such as prohibited drugs and firearms or sites offering to supply articles for use in fraud. Additionally, general search services use proprietary algorithms ('ranking') which are designed to prioritise the most accurate and reliable results based on the user's search query. However, you should assess how this ranking may be manipulated by users to increase the likelihood of illegal content being displayed to other users.

[44] Child users refers to under 18s. We recognise there are other ways to indicate presence of children on a service beyond whether a service 'allows' children, and will continue to monitor this approach to ensure alignment with our forthcoming work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

Specific risk factors Search services with relevant characteristics should take account in their risk assessment.		
		If your service is a downstream search service, you should similarly assess how your service may lead to risk of harm by providing a means for users to locate and access illegal content once it has been indexed and is ranked within search results. However, because downstream search services obtain or supplement their search results by contracting from general search providers, they may have limited control over how search results are displayed.
☐	**1b** Vertical search services	• **Risk factor:** Vertical search services Vertical search services, sometimes known as specialty search engines, serve narrower results compared to general (and downstream) search services. For example, they draw results from pre-determined websites that contain professional or curated content, rather than indexing sites from across the clear web. If your service is a vertical search service, you should be aware that there may still be risks, but your service may be less likely to present illegal content to users compared to general (and downstream) search services.
2. User base factors		
☐	**2** Services allowing child users[45]	• **Risk factor:** Child users (under 18s) If your services allow child users to access it, we would expect you to consider how children are more likely to encounter and experience harm from some kinds of illegal content which may be present on online services. While there is evidence to suggest that younger users are far less likely than older users to use search services in the first place, as they conduct more searching on U2U services such as social media services, many children still use search services and can experience harm through viewing illegal content in the search results.
3. Functionality factors		
☐	**3a** Services with search predictions or suggestions	• **Risk factor:** Predictive or suggestive search If your service has tools that predict and personalise user searches, we expect you to consider how these tools may also increase the risk of users accessing illegal content. While these tools can allow searches to be more targeted and accurate, our evidence indicates that search bar predictions can suggest potential methods or instructions on how to end one's life, can recommend hateful or racist search queries, and point users to prohibited fraud-related content.
☐	**3b** Services where users can search for or with images or videos	• **Risk factors:** Image/video search and reverse image search If your service allows image/video searches, we expect you to consider the increased risk of harm to individuals by providing a means for users to find and access illegal image-based content such as CSAM. Additionally, if your service allows users to use images as a query to find other images or relevant results ('reverse image search'), you should consider the evidence that indicates that this functionality has been demonstrated as an effective way to find services selling drugs via search. Reverse image search also presents opportunities to access content relating to other prohibited items.

[45] Child users refers to under 18s. We recognise there are other ways to indicate presence of children on a service beyond whether a service 'allows' children, and will continue to monitor this approach to ensure alignment with our forthcoming work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

General risk factors All Search services should take account in their risk assessment.		
☑	All search services	• **Risk factor:** User base demographics Search services are used by a wide range of users, and the demographics of your user base (including users' protected characteristics, media literacy levels, mental health) may influence the risk of harm related to all kinds of illegal harm. **Vulnerable users (and particularly users with multiple protected characteristics) are more likely to experience harm from illegal content and are impacted differently by it.** We would expect you to consider these dynamics when you assess the risk of each type of illegal harm. These dynamics are highly complex and context-specific, and evidence is provided in the Register on user base demographics for each kind of illegal harm (see Volume 2, Chapter 6T). This can help you assess this risk factor even if you do not have any service-specific information on the make-up of your user base.
☑	All search services	• **Risk factor:** Business model (revenue model and growth strategy) Your revenue model may inadvertently increase the risk of different kinds of illegal harm occurring. For example, general search services, including downstream ones, may allow advertising to be seen by users while they use the service. The evidence suggests that these advertisements may suggest products and information to users that which could enable them to engage in illegal behaviours. We would also expect you to consider how the **design of your service** to optimise your revenue, (e.g. how you prioritise developing and growing your index) may influence risk.
☑	All search services	• **Risk factor:** Commercial profile You should assess how your commercial profile may increase the likelihood of different harms or their impact on users. For example, if your service is **low capacity** (in terms of number of employees or revenues), **early-stage** (i.e. start-ups or at growth stage), or developing its index rapidly, this may increase the likelihood of different kinds of harms appearing on your service. Our analysis suggests that potential perpetrators may target these services if they perceive them to have weak risk management processes in place.[46]

Source: Ofcom analysis

[46] Low-capacity and early-stage services may have limited financial or technical resources. For services with fast growing index database, the sources of risks and types of illegal harms on the service can change quickly and the service may not have timely technical or financial resources to quickly update their risk management sufficiently promptly to catch up with the rapid change.

Appendix B: Offences and kinds of illegal harm

A5.150 You need to assess the risk of each kind of illegal harm set out in the Act. This includes many individual offences. Ofcom has grouped these into 15 kinds of illegal harm, as set out in the Table below.

A5.151 In relation to each priority offence listed in the table below, the offence also includes the priority offences of encouraging, assisting, conspiring to commit, aiding, abetting, counselling, procuring, attempting, or, (in Scotland), inciting or being involved art and part in the commission of that offence. The offences are priority offences unless otherwise specified.

Table 16. Kinds of illegal harm

	Column 1: Kind of illegal harm	Column 2: Offences
1.	Terrorism	An offence specified in Schedule 5 of the Act.
2.	Child sexual exploitation and abuse (CSEA)	An offence specified in Schedule 6 of the Act.
2A	Grooming	An offence specified in any of paragraphs 5, 6, 11 or 12 of Schedule 6 to the Act.
2B	CSAM	An offence specified in any of paragraphs 1 to 4, 7, 8 or 10 of Schedule 6 to the Act.
2B(i)	Image-based CSAM – U2U services only	An offence specified in any of paragraphs 1 to 4, 7, 8 or 10 of Schedule 6 to the **Act**, so far as the risk in relation to those offences relates to **CSAM** in the form of photographs, videos or visual images.
2B(ii)	CSAM URLs – U2U services only	An offence specified in any of paragraphs 1 to 4, 7, 8 or 10 of Schedule 6 to the **Act**, so far as the risk in relation to those offences relates to users encountering **CSAM** by means of or facilitated by **CSAM URLs** present on the service.
3.	Encouraging or assisting suicide (or attempted suicide) or serious self-harm[47]	An offence under: section 2 of the Suicide Act 1961 (assisting suicide etc); section 13 of the Criminal Justice Act (Northern Ireland) 1966 (c. 20 (N.I.)) (assisting suicide etc); section 184 of the Online Safety Act 2023 (a relevant non-priority offence).

[47] The new self-harm offence is not yet in force and is not a priority offence. However, we have included suicide and self-harm in the same kind of illegal harm. Most of our evidence base relates to both suicide and self-harm, so we have considered them together in our risk assessment. The evidence we analysed does not often distinguish between content that focuses solely on suicide, compared to content which focuses on self-harm that is potentially life-threatening. We also think that services may find it easier to consider these offences together, so have provisionally included it here and throughout this guidance, for consistency. For the avoidance of doubt however, services are not required to treat self-harm as a priority offence. We will keep our approach to self-harm under review when we finalise the guidance.

	Column 1: Kind of illegal harm	Column 2: Offences
4.	Hate	An offence under any of the following provisions of the Public Order Act 1986— (a) section 18 (use of words or behaviour or display of written material); (b) section 19 (publishing or distributing written material); (c) section 21 (distributing, showing or playing a recording); (d) section 29B (use of words or behaviour or display of written material); (e) section 29C (publishing or distributing written material); (f) section 29E (distributing, showing or playing a recording). An offence under any of the following provisions of the Crime and Disorder Act 1998— (a) section 31 (racially or religiously aggravated public order offences); (b) section 32 (racially or religiously aggravated harassment etc). An offence under section 50A of the Criminal Law (Consolidation) (Scotland) Act 1995 (racially-aggravated harassment).

	Column 1: Kind of illegal harm	Column 2: Offences
5.	Harassment, stalking threats and abuse	An offence under section 16 of the Offences against the Person Act 1861 (threats to kill). An offence under any of the following provisions of the Public Order Act 1986— (a) section 4 (fear or provocation of violence); (b) section 4A (intentional harassment, alarm or distress); (c) section 5 (harassment, alarm or distress). An offence under any of the following provisions of the Protection from Harassment Act 1997— (a) section 2 (harassment); (b) section 2A (stalking); (c) section 4 (putting people in fear of violence); (d) section 4A (stalking involving fear of violence or serious alarm or distress). An offence under any of the following provisions of the Protection from Harassment (Northern Ireland) Order 1997 (S.I. 1997/1180 (N.I. 9))— (a) Article 4 (harassment); (b) Article 6 (putting people in fear of violence) An offence under any of the following provisions of the Criminal Justice and Licensing (Scotland) Act 2010 (asp 13)— (a) section 38 (threatening or abusive behaviour); (b) section 39 (stalking).
6.	Controlling or coercive behaviour	An offence under section 76 of the Serious Crime Act 2015 (controlling or coercive behaviour in an intimate or family relationship).
7.	Drugs and psychoactive substances	An offence under any of the following provisions of the Misuse of Drugs Act 1971— (a) section 4(3) (unlawful supply, or offer to supply, of controlled drugs); (b) section 9A (prohibition of supply etc of articles for administering or preparing controlled drugs); (c) section 19 (inciting any other offence under that Act). An offence under section 5 of the Psychoactive Substances Act 2016 (supplying, or offering to supply, a psychoactive substance).

8.	Firearms and other weapons	An offence under section 1(1) or (2) of the Restriction of Offensive Weapons Act 1959 (sale etc of flick knife etc). An offence under any of the following provisions of the Firearms Act 1968— (a) section 1(1) (purchase etc of firearms or ammunition without certificate); (b) section 2(1) (purchase etc of shot gun without certificate); (c) section 3(1) (dealing etc in firearms or ammunition by way of trade or business without being registered); (d) section 3(2) (sale etc of firearms or ammunition to person other than registered dealer); (e) section 5(1), (1A) or (2A) (purchase, sale etc of prohibited weapons); (f) section 21(5) (sale etc of firearms or ammunition to persons previously convicted of crime); (g) section 22(1) (purchase etc of firearms or ammunition by person under 18); (h) section 24 (supplying firearms to minors); (i) section 24A (supplying imitation firearms to minors). An offence under any of the following provisions of the Crossbows Act 1987— (a) section 1 (sale and letting on hire of crossbow); (b) section 2 (purchase and hiring of crossbow). An offence under any of the following provisions of the Criminal Justice Act 1988— (a) section 141(1) or (4) (sale etc of offensive weapons); (b) section 141A (sale of knives etc to persons under 18). An offence under any of the following provisions of the Criminal Justice (Northern Ireland) Order 1996 (S.I. 1996/3160 (N.I. 24))— (a) Article 53 (sale etc of knives); (b) Article 54 (sale of knives etc to minors). An offence under any of the following provisions of the Knives Act 1997— (a) section 1 (unlawful marketing of knives);

	Column 1: Kind of illegal harm	Column 2: Offences
		(b) section 2 (publication of material in connection with marketing of knives). An offence under any of the following provisions of the Firearms (Northern Ireland) Order 2004 (S.I. 2004/702 (N.I. 3))— (a) Article 24 (sale etc of firearms or ammunition without certificate); (b) Article 37(1) (sale etc of firearms or ammunition to person without certificate etc); (c) Article 45(1) or (2) (purchase, sale etc of prohibited weapons); (d) Article 63(8) (sale etc of firearms or ammunition to people who have been in prison etc); (e) Article 66A (supplying imitation firearms to minors). An offence under section 36(1)(c) or (d) of the Violent Crime Reduction Act 2006 (sale etc of realistic imitation firearms). An offence under any of the following provisions of the Air Weapons and Licensing (Scotland) Act 2015 (asp 10)— (a) section 2 (requirement for air weapon certificate); (b) section 24 (restrictions on sale etc of air weapons).
9.	Unlawful immigration and human trafficking	An offence under any of the following provisions of the Immigration Act 1971— (a) section 24(A1), (B1), (C1) or (D1) (illegal entry and similar offences); (b) section 25 (assisting unlawful immigration). An offence under section 2 of the Modern Slavery Act 2015 (human trafficking). An offence under section 1 of the Human Trafficking and Exploitation (Scotland) Act 2015 (asp 12) (human trafficking). An offence under section 2 of the Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015 (c. 2 (N.I.)) (human trafficking).
10.	Sexual exploitation of adults	An offence under any of the following provisions of the Sexual Offences Act 2003— (a) section 52 (causing or inciting prostitution for gain); (b) section 53 (controlling prostitution for gain). An offence under any of the following provisions of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2))— (a) Article 62 (causing or inciting prostitution for gain); (b) Article 63 (controlling prostitution for gain).

	Column 1: Kind of illegal harm	Column 2: Offences
11.	Extreme pornography	An offence under section 63 of the Criminal Justice and Immigration Act 2008 (possession of extreme pornographic images).
12.	Intimate image abuse	An offence under section 33 of the Criminal Justice and Courts Act 2015 (disclosing, or threatening to disclose, private sexual photographs and films with intent to cause distress) *[OR, if section 188 of the Online Safety Act is brought into force and Schedule 7 to the Act is amended accordingly before we issue our final document, section 66B of the Sexual Offences Act 2003]*. An offence under section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 (asp 22) (disclosing, or threatening to disclose, an intimate photograph or film).
13.	Proceeds of crime	An offence under any of the following provisions of the Proceeds of Crime Act 2002— (a) section 327 (concealing etc criminal property); (b) section 328 (arrangements facilitating acquisition etc of criminal property); (c) section 329 (acquisition, use and possession of criminal property).
14.	Fraud and financial services	An offence under any of the following provisions of the Fraud Act 2006— (a) section 2 (fraud by false representation); (b) section 4 (fraud by abuse of position); (c) section 7 (making or supplying articles for use in frauds); (d) section 9 (participating in fraudulent business carried on by sole trader etc). An offence under section 49(3) of the Criminal Justice and Licensing (Scotland) Act 2010 (articles for use in fraud). An offence under any of the following provisions of the Financial Services and Markets Act 2000— (a) section 23 (contravention of prohibition on carrying on regulated activity unless authorised or exempt); (b) section 24 (false claims to be authorised or exempt); (c) section 25 (contravention of restrictions on financial promotion). An offence under any of the following provisions of the Financial Services Act 2012— (a) section 89 (misleading statements); (b) section 90 (misleading impressions).

	Column 1: Kind of illegal harm	Column 2: Offences
15.	Foreign interference offence	An offence under section 13 of the National Security Act 2023 (foreign interference).

Source: Ofcom