Protecting people from illegal harms online

Risk Assessment Guidance and Risk Profiles

V2.0 Guidance

Published 25 June 2026

Contents

Part 1: Duties and carrying out an illegal content risk assessment

1. Introduction

1.1 This guidance aims to help service providers 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 different kinds of illegal harm could arise on your service, and what safety measures you need to put in place to protect users. It is compulsory that you complete an illegal content risk assessment to meet your duties under the Act.

Box 1: Illegal harm

To meet the requirements of the illegal content risk assessment set out in the Act, you should assess the risk of harm arising from each of the 18 kinds of priority illegal content and other illegal content (including non-priority content).[1]

When we use the term 'illegal harm' we refer to the psychological or physical harm which can occur from a user encountering any illegal content (the 18 kinds of priority illegal content or other illegal content), or from your U2U service being used for the commission or facilitation of an offence.

1.2 This guidance recommends a four-step methodology to carry out risk assessments, and following this process will help you to comply with the illegal content risk assessment duties, and the linked safety duties and record-keeping and review duties.

1.3 The guidance consists of three parts and two appendices:

a) **Part 1** includes a summary of the risk assessment duties, and an overview of the four-step risk assessment methodology.
b) **Part 2** includes more detailed information to help you conduct your risk assessment, and explains:
    i) The four-step methodology: We recommend that all service providers follow these steps to carry out risk assessments. Following this can also help you meet other duties under the Act.
    ii) What evidence to use: Risk assessments require evidence to ensure accuracy. We expect all in-scope service providers to consult 'core' evidence, and some providers to use additional 'enhanced' evidence where this is available or appropriate.
    iii) 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.
c) **Part 3** includes detailed information to support and complete each step in the four-step methodology.
d) **Appendix A** lists the priority offences covered by the Act.
e) **Appendix B** provides examples of how to use the Risk Level Tables for U2U Services.

1.4 We will also publish supporting resources and tools on the Ofcom website to help you understand how to meet your obligations.

[1] These are set out in Table 15 in Appendix A.

2. Risk Assessment Duties

2.1 This section of the guidance explains the illegal content risk assessment duties.

What are the illegal content risk assessment duties?

2.2 If you provide a user-to-user ('U2U') or search service, you must carry out an illegal content risk assessment. Broadly speaking, **this legal obligation requires you to assess the risks on your service associated with priority offences and other illegal content.**[2]

2.3 The Act sets out the specific elements that an illegal content risk assessment needs to include.[3] When doing your risk assessment, you should give particular consideration to your service's characteristics – such as its user base and functionalities. [4] To help you do your risk assessment we have produced a series of tables, called Risk Profiles, which you must take account of. They identify which features or functionalities could lead to a risk of kinds of harm on your service if you have them.[5]

2.4 Your risk assessment must be **suitable and sufficient**,[6] which we explain in more detail in the section 'What is a 'suitable and sufficient' risk assessment?'.

2.5 Once you have completed your first risk assessment, there are several duties in the Act related to reviewing, updating, or completing new risk assessments:

- You must take appropriate steps to keep your risk assessment **up to date**, including when Ofcom makes a **significant change to a Risk Profile** that relates to your service;
- You must carry out a further risk assessment before making any significant change to any aspect of your service's design or operation, relating to that proposed change;[7] and
- You need to **keep a record** of each risk assessment you carry out.[8] We have published separate Record-Keeping and Review Guidance to help you with this.

2.6 To help service providers meet these duties, 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 duties and record-keeping duties. We recommend that you also consult the detailed research and analysis of the harms in our Register of Risks.[9]

---

[2] Section 59(2) of the Act.
[3] Risk Assessment Duties are set out in Section 9 of the Act (for user-to-user service providers), and Section 26 of the Act (for search service providers).
[4] Section 9(5) and 26(5) of the Act.
[5] Section 9(5) and 26(5) of the Act.
[6] Section 9(2) and 26(2) of the Act.
[7] Section 9(3) and (4) and 26(3) and (4) of the Act. We explain what a significant change may involve in Part 3, Section 4.
[8] Section 23(2) of the Act.
[9] The Illegal Harms **Register of Risks** ('Register of Risks') is our assessment of the causes and impacts of illegal online harms based on the evidence that we have gathered over the past four years.

What is a 'suitable and sufficient' risk assessment?

2.7 Risk assessments must meet the requirements of the legal risk assessment duties, including the 'suitable and sufficient' standard.

2.8 To be suitable and sufficient, your risk assessment must include all the elements of an illegal content risk assessment specified in the Act (section 9(5) for U2U service providers and section 26(5) for search service providers). This means it should be **specific** to your service and **reflect the risks accurately.** This will lead you to an adequate understanding of risks on your service to **implement appropriate safety measures.**

2.9 Your assessment **must**:

a) Assess the risk of users encountering each of the 18 kinds of priority illegal content and other illegal content, and the risk of a U2U service being used for the commission or facilitation of a priority offence;[10]
b) Take into account Ofcom's Risk Profiles;[11]
c) Consider the **characteristics** of your service: its **user base** (for example, user numbers, age, languages, groups at risk, and groups increasing risk), **functionalities, algorithmic systems** (and how easily, quickly and widely they disseminate content), and the **business model**;
d) Consider any other relevant aspects of your service's **design and operation**, including any existing controls to mitigate harm such as governance, use of proactive technology, measures to promote users' media literacy and safe use of your service, and other systems and processes which could affect the level of risk; and
e) Consider **how your service is used** – both the intended and unintended ways that people may use your service.

2.10 You should make a judgement about the risk level of **each** of the different kinds of illegal harm covered by the Act. Our detailed guidance helps you do this by assessing the **likelihood** of each kind of illegal harm taking place, and the **impact** of that harm on users.

2.11 Your assessment should be based on **relevant information and evidence** to accurately reflect the risks of harm so that you can keep a record of your analysis and conclusions. Services which have complex risk factors, characteristics, design features, or different user types, may require more types of evidence to inform their judgements of risk.

2.12 Our guidance on evidence sets out:

a) The **core evidence** that all service providers 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 service providers, and failing to consider it may mean that the risk assessment is not suitable and sufficient.
b) Service providers should consider additional **enhanced evidence** where the core evidence is insufficient to make accurate assessments. Examples of enhanced evidence include: results of product testing; outputs from content moderation systems;

[10] See the section on 'What illegal content do you need to assess' for more information on illegal content.
[11] These are set out in Part 3, Section 1 and include a list of risk factors (such as features and functionalities) with an explanation of how they could increase the risk of particular harms covered by the Act (such as terrorism offences).

consultation with technical or independent experts, or with users and representative groups; research into users' behaviours and needs; or external audit and risk assurance processes. See Part 3, Section 2 for guidance on the kinds of evidence that should be collected and assessed.

Record-Keeping duties

2.13 You need to keep a record of each illegal content risk assessment you carry out, including details of how the assessment was carried out and its findings.

2.14 We have published separate Guidance on Record-Keeping and Review to help providers understand what is expected of them and what to record, and we provide further information at Part 2, Step 3 of this document.

Additional duties for categorised service providers

2.15 Ofcom will publish a register of categorised services. These services have additional duties relating to their illegal content risk assessments. Category 1 and Category 2A service providers **must**:[12]

a) Publish a summary of their most recent illegal content risk assessment in their terms of service (Category 1) or in a publicly available statement (Category 2A). The summary must include the findings of the most recent illegal content risk assessment of a service (including as to levels of risk and as to nature, and severity, of potential harm to individuals);[13] and
b) Provide Ofcom with a copy of their risk assessment record as soon as reasonably practicable.[14]

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

2.16 If we suspect that you have failed to carry out a suitable and sufficient risk assessment, then we are able to take enforcement action.[15] Any decision we take regarding enforcement action would be made in line with our **Online Safety Enforcement Guidance**.[16]

2.17 If we decide to open an investigation and find that your service has failed to comply with its duties, we may 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.[17]

[12] Section 95(10) of the Act.
[13] Section 10(9) of the Act (U2U service providers) and Section 17(9) of the Act (search service providers).
[14] Section 23(10) of the Act (U2U service providers) and Section 34(9) of the Act (search service providers).
[15] Section 131 of the Act.
[16] See the Online Safety Enforcement Guidance.
[17] Section 143 of the Act and Schedule 13 to the Act.

When do you need to complete the first illegal content risk assessment?

2.18 If your service is in operation on or before the publication of this guidance, you need to complete your first risk assessment **within three months** of the date on which this guidance is published.

2.19 If you start a new service or change an existing service so that it falls within scope of the Act, you must complete your risk assessment within three months of doing so.

2.20 If you have more than one service in scope of the Act, you need to complete a risk assessment for each service separately. It is the service provider's responsibility to determine the distinct services it has which are in scope of the Act and the boundaries between these services.

2.21 There are also duties about reviewing, updating, or carrying out a new illegal content risk assessment. In summary:

- You must take **appropriate steps** to keep your risk assessment up to date, including 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 a significant change** to any aspect of your service's design or operation.

2.22 See Part 3, Section 4 for further details on what constitutes a significant change.

What illegal content do you need to assess?

2.23 You will need a working understanding of what 'illegal content' is, and what offences you must consider. The Act defines 'illegal content' as content that "amounts to an offence" and explains what this means. The Act distinguishes between 'priority' and other (non-priority) illegal content.[18] An example of priority illegal content includes content sharing a terrorist publication or which invites users to support a proscribed organisation (for example, a terrorist group).

2.24 Carrying out an illegal content risk assessment requires you to assess the risks on your service associated with **priority offences** and **other illegal content.**[19]

2.25 The Act lists over 130 **priority offences**, which Ofcom has grouped into 18 kinds of priority illegal content.[20] [21] (See Table 15 and Appendix A.)[22]

2.26 The Act also requires you to undertake an assessment of the risk arising from **other illegal content**. This includes but is not limited to non-priority illegal content; see the Register of Risks chapters for 'non-priority offences'.

[18] Priority offences are defined in Section 59 of the Act. Section 59 of the Act also explains the circumstances in which content may "amount to an offence".
[19] Section 59(2) of the Act.
[20] These offences are set out in section 59 and Schedules 5, 6 and 7 of the Act.
[21] These 18 kinds of illegal harm cover the priority offences, as explained further below. Other kinds of illegal harm referred to in Ofcom's risk assessment relate to other relevant non-priority offences.
[22] Service providers can find more information on each kind of harm in Ofcom's Register of Risks, and guidance on 'illegal content' in Ofcom's illegal content judgements guidance.

2.27 You should assign an overall risk level to each of the **18 kinds of priority illegal content**, and for **other illegal content**.

Table 1: List of illegal content to assess (this includes 18 kinds of priority illegal content and other illegal content)

18 kinds of priority illegal content

1. Terrorism
2. Child Sexual Exploitation and Abuse (CSEA)
  a. Grooming
  b. Child Sexual Abuse Material (CSAM) – imagery
  c. Child Sexual Abuse Material (CSAM) - URLs
3. Hate
4. Harassment, stalking, threats and abuse
5. Controlling or coercive behaviour
6. Intimate image abuse
7. Extreme pornography
8. Sexual exploitation of adults
9. Human trafficking
10. Unlawful immigration
11. Fraud and financial offences
12. Proceeds of crime
13. Drugs and psychoactive substances
14. Firearms, knives and other weapons
15. Encouraging or assisting suicide and serious self-harm
16. Foreign interference
17. Animal cruelty
18. Cyberflashing

Other illegal content (including non-priority offences)
All service providers must consider whether there is a risk of harm from other illegal content appearing on the service and, if so, what the magnitude of this risk is. Some of this illegal content is described in the Register of Risks as 'non-priority illegal content', but it may also be appropriate to consider other offences depending on the circumstances of your service and the evidence you hold.[23] In addition to considering each of the 18 kinds of priority illegal content, you should consider whether 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. If you do have evidence that a particular kind of non-priority illegal content is likely to occur then you should include it in your risk assessment.

2.28 You can consult our Register of Risks for research and analysis on each kind of illegal harm to support your assessment. The Illegal Content Judgements Guidance ('ICJG') can also help service providers identify illegal content.

[23] By 'non-priority offence' we mean an offence within Section 59(5) of the Act.

What to assess about each kind of priority illegal content, and other illegal content

2.29 To meet the requirements of the illegal content risk assessment set out in the Act, you should assess the risk of harm arising from each of the 18 kinds of priority illegal content, and other illegal content.

2.30 In the assessment, you must consider all the requirements in section 9 (for U2U service providers) or section 26 (for search service providers) of the Act and should use evidence about your service to make your assessment.

2.31 You should then assign a risk level for each kind of priority illegal content: negligible, low, medium or high. Determining a risk level requires evaluating the **likelihood** and the **impact** (such as the nature and severity) of the harm which could arise from each kind of priority illegal content; this is explained in Step 2 of the four-step methodology in this guidance.

2.32 The assessment criteria for illegal harms is summarised in Table 2:

Table 2: Assessment of illegal harms

Illegal harms	Assessment criteria
18 kinds of priority illegal content	Separately assess the risk of users **encountering each kind** of priority illegal content. Separately assess the risk of your service being used for the **facilitation** or **commission** of each kind of priority illegal content (U2U services only).
Other illegal content	Assess the risk of encountering other kinds of illegal content, some of these are set out in the Act and included in the Register of Risks and ICJG as 'non-priority illegal content'.

2.33 Encountering (in relation to content) is defined as reading, viewing, hearing or otherwise experiencing content.[24]

2.34 **Providers of search services** must consider the risk of individuals encountering 'search content' that is illegal content.[25] Search content is content that may be encountered in or via search results of a search service, for example, content presented to a user of the service by operation of the search engine in response to a search request made by an individual.

2.35 **Providers of U2U services** are required to consider the risk of the service being used for the commission or facilitation of a priority offence.

Using risk profiles and risk level tables in your risk assessment

2.36 To help you carry out your risk assessment, you must take account of the **Risk Profile** relevant to your service. There are two sets of Risk Profiles – one for U2U services and one

[24] Section 236 of the Act.
[25] Search content is defined in Section 57 of the Act.

for search services. Ofcom has a duty to prepare Risk Profiles, setting out the risk factors (features and functionalities) that are most strongly linked to one or more kinds of illegal harm. Risk Profiles will help you to identify and record the relevant risk factors for your service. These are set out in Part 3, Section 1.

2.37 Service providers can use their own risk assessment methodology. However, please note that the Risk Assessment Guidance includes four tables to help service providers identify levels of risk, and to guide you to specific measures in Ofcom's Codes of Practice. The four tables are: a General Risk Level Table, a risk level table for CSAM URL, a risk level table for CSAM Images, and a risk level table for Grooming. The Risk Level Tables can be found in Part 3, Section 3.

2.38 The General Risk Level Table provides guidance about the circumstances in which it is likely to be appropriate to conclude a service is high, medium or low risk for a particular harm. The CSAM URL risk table, CSAM Image risk table and the Grooming risk table provide more detailed information on how providers of U2U services should determine whether their service is high, medium or low risk of grooming.

2.39 The guidance intends to help service providers to assess whether your service is negligible, low, medium or high risk for each kind of priority illegal content. To determine the level of risk for each of the 18 kinds of priority illegal content, you must consider the Risk Profiles, and make a judgement of the level of risk based on relevant evidence inputs, taking account of the impact of any existing controls on your service.

2.40 If service providers use their own risk assessment methodology, they are still expected to justify separate conclusions of high, medium, low or negligible risk for each kind of priority illegal content, and any other illegal content you assess. This is to ensure that you keep a record of all judgements of risk that relate to any measures in the Codes of Practice.

Keeping your illegal content risk assessment up to date

2.41 Depending on circumstances, service providers may fully review their risk assessment (for example, as a matter of course every year), or target the review to specific aspects of the service (for example, due to the introduction of a new feature or functionality outside a regular annual review cycle).

2.42 We recognise that some service providers may want to consider the timing of their risk assessments in the context of their obligations under other legal regimes (such as the EU Digital Services Act, or privacy and data protection impact assessments). This is a matter for individual service providers, provided that the approach they take meets their obligations under the Act.

2.43 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.

2.44 The Act includes the following duties about reviewing or carrying out a new risk assessment, to be considered as key triggers:

a) a duty to take appropriate steps to keep an illegal content risk assessment up to date;
b) a duty to update your risk assessment if Ofcom makes any significant change to a Risk Profile that relates to your service; and

c) before making any significant change to any aspect of your service's design or operation, a duty to carry out a further suitable and sufficient illegal content risk assessment relating to the impacts of that proposed change.

Review and update at least every 12 months

2.45 You have a duty to take steps to keep your assessment up to date. Ofcom recommends that risk assessments are reviewed at least every 12 months.

2.46 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 would require you to review your assessment.

2.47 Reviewing your assessment 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 may impact your assessment of risk, then you should review each step of the four-step process with the updated evidence.

2.48 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 written policy will be a valuable tool to help you to demonstrate compliance.**

2.49 Your written policy on keeping a risk assessment up to date should include:

- A timeframe for regular review (at least 12 months). 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

2.50 The Act requires Ofcom to review and revise its Register of Risks and Risk Profiles to keep them up to date.

2.51 If Ofcom makes a significant change to a Risk Profile which is relevant to your service, you must review and update your risk assessment. You can sign up for updates from Ofcom to be made aware of changes to Risk Profiles by signing up here: Subscribe to email updates.

2.52 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 (such as new functionalities), or new links between risk factors and harms could have been identified (such as a new functionality which increases the risk of grooming or fraud).

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

Relevance of the children's risk assessment duty

2.54 The Act sets out that services that are likely to be accessed by children also need to conduct a 'children's risk assessment'. They must assess the risk of harm they pose to children by the kinds of content harmful to children set out in the Act, and how the design of the service affects the level of risk of harm to children.[26] You may have to complete a children's risk assessment as well as an illegal content risk assessment if you are in scope of both the illegal content and child protection duties. If you decide to conduct the separate risk assessments concurrently because it suits your organisation, you should be mindful of the following:

- Service providers must carry out risk assessments for both duties, and hold separate records for each risk assessment.
- Service providers will identify different Codes measures to reduce the risk of each kind of illegal content or content harmful to children, as a result of the respective risk assessments.

2.55 When considering evidence and making assessments, service providers should note that some categories of content harmful to children may be related to or overlap with some categories of illegal content. For example, content that promotes, encourages or provides instructions for suicide or serious self-harm may, in addition to being priority illegal content, also amount to primary priority content (encouraging, promoting or providing instructions for suicide, an act of deliberate self-injury or an eating disorder or behaviour associated with an eating disorder) for the purposes of the children's risk assessment.

2.56 Similarly, some characteristics of the service that affect the level of risk of illegal harm (such as user base, functionalities, and the ways in which a service is used) may also be relevant for your children's risk assessment.

2.57 Should you conduct risk assessments concurrently, you still need to ensure that the illegal content risk assessment and the children's risk assessment are distinct and clearly identifiable.

2.58 Finally, the findings of your children's risk assessment may inform your illegal content risk assessment – for example, to help you consider the risk of illegal harm to children as a specific vulnerable group.

[26] All Part 3 services must complete a children's access assessment. Your children's access assessment will help you work out if your service, or part of your service, is likely to be accessed by children.

Part 2: How to carry out an Illegal Content Risk Assessment

1. Overview of the four-step risk assessment process

Step 1: Understand the kinds of illegal content that need to be assessed

Step 1 will help you to know which kinds of illegal content to assess, and to make accurate judgements about your risks.

Sequence of activities and outcomes:

- Identify the 18 kinds of priority illegal content that need to be separately assessed.
- Identify whether there is a risk of other illegal content taking place on your service, including relevant non-priority illegal content.
- Consult Ofcom's Risk Profiles and identify the key risk factors which are relevant to your service for each of the 18 kinds of priority illegal content.
- If you are a U2U service, understand how the service may be used to commit or facilitate a priority offence.

Essential records:

- Confirmation that the service provider has consulted Ofcom's Risk Profiles and recorded any risk factors relevant to the service.

Step 2: Assess the risk of harm

Step 2 will help you use evidence to assess and assign a risk level to: the risk of harm to users encountering each of the 18 kinds of priority illegal content and other illegal content; and also the risk of harm of your U2U service being used for the commission or facilitation of a priority offence.

Sequence of activities and outcomes:

- Separately assess the likelihood and impact of each of the 18 kinds of priority illegal content, and of any other illegal content which you have identified as being likely to occur on your service (including non-priority illegal content), using all relevant evidence.
- Then assess the different ways in which the service is used, including ways which are unintended. Further, identify whether there are any specific characteristics or functionalities of the service's design or operation, not covered in Ofcom's Risk Profiles, which could increase the risk of harm.
- Consider the effectiveness of any existing control measures which could impact the level of risk of harm to service users.
- Consult the four Risk Level Tables to assign a risk level for each of the 18 kinds of priority illegal content, and any other illegal content. This risk level should reflect risk as

it exists on the service at the time of assessment, having had regard to the efficacy of any existing control measures you have in place.

- Conclude the assessment of all the risks relating to each kind of illegal content, and the design and operation of the service, to mitigate in Step 3.

Essential records:

- A list of evidence that has informed the assessment of likelihood and impact of each of the 18 kinds of priority illegal content and any other illegal content, and how this has informed the risk level assigned to each.
- Where applicable, a record of how any evidence relating to existing control measures has affected the risk levels.
- Where applicable, a list of any additional characteristics (including user base, business models, functionalities, governance, and systems and processes) considered alongside the risk factors identified in Ofcom's Risk Profiles.
- Risk level (of high, medium, low or negligible) for each of the 18 kinds of priority illegal content (and, for U2U services this should also include the level of risk assigned to sub-categories of harm (including image-based CSAM, CSAM URLs, and Grooming)) and any relevant other illegal content, and an evidence-based explanation of the decision. This level should reflect risk as it exists on the service at the time of assessment.

Step 3: Decide measures, implement, and record

Step 3 will help you identify any relevant measures to implement to address risk, record any measures you have taken, and make a record of your assessment.

Sequence of activities and outcomes:

- Consult Ofcom's Codes of Practice, check which measures are recommended for your service, and decide whether to implement applicable measures to reduce risk of harm to individuals/users, or use alternative measures.
- Identify any additional measures that may be appropriate for your service.
- Implement all relevant measures.
- Record the outcomes of the risk assessment.

Essential records:

- A complete record of the risk assessment.
- All measures from Ofcom's Codes of Practice that have been, or are planned to be, implemented, and any applicable measures that are not planned to be implemented.
- Measures that are alternatives to those set out in Ofcom's Codes of Practice, with evidence that demonstrates how these alternative measures meet the relevant duties.

Step 4: Report, review, and update

Step 4 will help you understand how to keep your risk assessment up to date, and put in place appropriate steps to review your assessment.

Sequence of activities and outcomes:

- Report on the illegal content risk assessment and measures through appropriate Governance and Accountability channels.
- Monitor the effectiveness of safety measures at reducing the risk of harm to users.
- Monitor developing risks and the level of risk exposure after appropriate measures are implemented (also known as residual risk).
- Review and/or update the risk assessment when appropriate, including before making any significant change to any aspect of the service's design or operation.

Essential records:

- A written record of the annual review cycle for the illegal content risk assessment, and a named person responsible who has been appointed for this process.
- Confirmation that the findings of the risk assessment have been reported through appropriate Governance and Accountability channels.
- Category 1 and 2A services to supply Ofcom with a copy of their risk assessment record.
- Category 1 services to summarise the findings of their most recent risk assessment in their terms of service; category 2A in a publicly available statement.

2. What to consider in the four steps

2.1 This section explains in detail the activities and outcomes for each step of your risk assessment.

Step 1: Understand the kinds of illegal content that need to be assessed

2.2 The objectives of this step are for service providers to identify and develop an understanding of the kinds of illegal content that they need to assess; consult Ofcom's Risk Profiles; and separately assess the presence of priority illegal content and other illegal content (including non-priority illegal content).

Sequence of activities and outcomes for Step 1

Identify types of illegal content you need to assess

2.3 The Act distinguishes between priority and other (i.e. non-priority) illegal content.[27] An example of priority illegal content could be content sharing a terrorist publication or which invites users to support a proscribed organisation (for example a terrorist group).

2.4 All service providers are required to assess each of the 18 kinds of priority illegal content separately in their assessments, and to separately make an assessment considering the risk of "other illegal content".

2.5 Table 3 summarises differences in the assessment of the different types of illegal content.

Table 3: Summary of assessments for illegal harms

Illegal harms	Assessment criteria
18 kinds of priority illegal content	Separately assess the risk of users **encountering each kind** of priority illegal content. Separately assess the risk of your service being used for the **facilitation** or **commission** of each kind of priority illegal content (U2U services only).
Other illegal content	Assess the risk of **encountering** other kinds of illegal content, some of these are set out in the Act and included in the Register of Risks and ICJG as 'relevant non-priority illegal content' or 'Communication offence'.

[27] Priority offences are set out in section 59 of the Online Safety Act (2023). Section 59 of the Act also explains the circumstances in which content may "amount to an offence" and this is other illegal content.

2.6 The Act lists over 130 priority offences.[28] For ease, Ofcom has grouped these into **18 kinds of priority content**. See Table 4 below and Table 15 in Appendix A for the full list of offences. As part of the first step of your risk assessment, we recommend that you familiarise yourself with the list in Table 4.

Table 4: List of illegal content to assess (this includes 18 kinds of priority illegal content and other illegal content)

Kinds of priority illegal content[29]

1. **Terrorism**
2. **Child Sexual Exploitation and Abuse (CSEA)**
    a. **Grooming**
    b. **Child Sexual Abuse Material (CSAM) – imagery**
    c. **Child Sexual Abuse Material (CSAM) - URLs**
3. **Hate**
4. **Harassment, stalking, threats and abuse**
5. **Controlling or coercive behaviour**
6. **Intimate image abuse**
7. **Extreme pornography**
8. **Sexual exploitation of adults**
9. **Human trafficking**
10. **Unlawful immigration**
11. **Fraud and financial offences**
12. **Proceeds of crime**
13. **Drugs and psychoactive substances**
14. **Firearms, knives and other weapons**
15. **Encouraging or assisting suicide and serious self-harm**
16. **Foreign interference**
17. **Animal cruelty**
18. **Cyberflashing**

Other illegal content (including non-priority offences)

All service providers must consider whether there is a risk of harm from other illegal content appearing on the service and, if so, what the magnitude of this risk is. Some of this illegal content is described in the Register of Risks as 'non-priority illegal harm, but it may also be appropriate to consider other offences depending on the circumstances of your service and the evidence you hold.[30] In addition to considering each of the 18 kinds of priority illegal content, you should consider whether 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. If you do have evidence that a particular kind of non-priority illegal content is likely to occur then you should include it in your risk assessment.

[28] See Ofcom's illegal content judgements guidance (ICJG) for information about each offence.
[29] All services have a duty to assess each 18 kinds of priority illegal content separately in their risk assessment. Some services may find it appropriate to further separate the kind of illegal content 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.
[30] By 'non-priority offence' we mean an offence within Section 59(5) of the Act.

Source: Ofcom

U2U service providers must understand additional kinds of CSEA

2.7 If you provide a U2U service, we expect you to understand how specific kinds of CSEA could manifest on your service. This is because different types of offences are associated with specific risk factors, and we have measures in Codes where the application of the measure depends on whether the service has a specific kind of CSEA risk. When you get to Step 2, as well as making an assessment of an overall risk of harm from CSEA, our guidance also sets out three further assessments for you to make:

a) the risk of image-based CSAM;
b) the risk of CSAM URLs; and
c) the risk of Grooming.

2.8 If you provide a search service, you do not need to make these three further assessments for that service.

2.9 You should consult the relevant Risk Level Tables in Section 6 to make assessments on risk levels for these types of illegal content.

What to assess about each kind of priority illegal content

2.10 Your risk assessment must consider the risk of users encountering each of the 18 kinds of priority illegal content; and

2.11 If you are a U2U service, you also need to consider the risk that your service could be used for:[31]

- **The commission of a priority offence**: consider the risk of the service being used to commit a priority offence.[32]
- **The facilitation of a priority offence:** consider the risk of the service being used for the facilitation of a priority offence.[33] In very general terms, facilitating a criminal offence means doing something to help with or make the performance of the offence easier.

2.12 In practice, the difference between content that amounts to illegal content and the service being used for commission and/or facilitation of priority offences may often be blurred. Given this, you can choose to make a single holistic assessment of each kind of illegal harm that encompasses these three elements.[34]

2.13 The primary objective is for you to consider how your service may be used in a way that leads to harm and risk of harm. Therefore, your risk assessment should not be limited to considering individual pieces of content, but rather should consider how your service is used overall.

[31] Section 9(5)(b) and (c) of the Act for U2U services and Section 26(5)(a) of the Act for search services.
[32] Section 9(5)(c) of the Act.
[33] Section 9(5)(c) of the Act.
[34] See Ofcom's Register of Risks for information on how services may be used for in the commission or facilitation of priority offences how facilitation of an offence can happen.

Other illegal content

2.14 Service providers need to consider whether there is a risk of users encountering "other illegal content" on their service.[35] [36] Encountering (in relation to content) is defined in the Act as reading, viewing, hearing or otherwise experiencing content. The Act defines "illegal content" as content that "amounts to a relevant offence".[37]

2.15 To carry out your risk assessment, you will need a working understanding of what "other illegal content" is, and what offences you must consider. These offences are not included in the 18 kinds of priority illegal content set out above.[38] Our Register of Risks discusses certain other offences (referred to as non-priority offences), such as false and threatening communications offences, but it does not cover every possible relevant offence.

2.16 When assessing the risk of other illegal content, you should take a reasonable and proportionate approach based on your understanding of your service and any information you hold.

2.17 We do not expect that services will consider every non-priority offence individually, but if you have any knowledge, experience, or evidence that non-priority illegal content may be present on your service (or at risk of appearing), then you should assess this. Unlike the 18 kinds of priority illegal content, you do not need to assess harm arising from each kind of non-priority illegal content separately.

Consult Ofcom's Risk Profiles

2.18 Service providers **must take account** of the relevant Risk Profiles when conducting their risk assessment.[39] There are separate Risk Profiles for U2U services and for Search services. Each Risk Profile identifies risk factors associated with each kind of priority offence. These risk factors are a good starting point when thinking about which harms could manifest on your service, and are important to understand before carrying out the assessment at Step 2.

2.19 However, the risk factors are not comprehensive. Service providers will find it helpful to consult the Register of Risks to gain a better understanding of each kind of illegal harm, how it could manifest on your service, and the risk factors associated with it.

2.20 You should use the risk factors identified when assessing the kinds of priority illegal harm in Step 2.

2.21 See Part 3, Section 1 for the Risk Profiles and instructions on how to use them.

Essential records for Step 1

2.22 You should keep written records confirming that you have consulted Ofcom's Risk Profiles.

2.23 You should keep written records of all of your service's relevant risk factors by using the check boxes provided in the Risk Profiles. Note that each risk factor will be relevant to one or multiple kinds of illegal harm as explained in the Risk Profiles.

---

[35] Section 9(5)(b) of the Act.
[36] Section 26(5)(a) of the Act.
[37] Section 59 of the Act.
[38] See Ofcom's Register of Risks for information about certain other offences.
[39] Note that the separate Children's Risk Assessment Guidance for Service Providers includes different Ofcom Children's Risk Profiles to help meet your children's risk assessment duty.

Step 2: Assess the risk of illegal harm

2.24 In Step 1, you will have understood the 18 kinds of priority illegal content, and any other relevant illegal content that you need to assess on your service. You will also have used the Risk Profiles to identify the risk factors that relate to each of them. The objective of this next step will be to use evidence to assess and assign a risk level for each kind of illegal content.

Sequence of activities and outcomes for Step 2

2.25 You now need to assess the level of risk of harm presented by your service for each of the 18 kinds of priority illegal content, and other illegal content you identified in Step 1. As part of this, you should consider the **likelihood** and **impact** of the illegal harms in question occurring on your service.

2.26 Practically, this means that you should:

a) Consider if there are any **additional characteristics** of your service which might increase risk of harm, but which may not be present in Ofcom's Risk Profiles.
b) Consider if there are any **existing controls** on your service which affect the level of risk of each kind of illegal harm on your service. If so, you should consider how and to what extent these controls affect the risk of harm.
c) Identify and **consult evidence** relating to your service to complete your risk assessment. The level of risk of each kind of illegal harm can 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.

2.27 The risk assessment should not be a theoretical exercise. Service providers should consider evidence they have about the ways the service in question is, or could be, actually used.

2.28 To complete a suitable and sufficient assessment, services must assess everything set out in the Act (sections 9(5) and 26(5)) and assign a risk level to each of the 18 kinds of priority illegal content based on evidence about the likelihood and impact of that harm occurring on their service. They must also repeat this exercise for any other types of illegal content which they have reason to believe is likely to be present on their service.

2.29 To assist you with this, we have provided a General Risk Level Table detailing the circumstances in which you are likely to be a high, medium, low, or negligible risk level for each of the 18 kinds of priority illegal content or other illegal content. We have provided more specific guidance on how to assess the risk of CSAM URLs, CSAM Images and Grooming occurring on your service. This guidance can be found in Part 3, Section 3. These four risk level tables are not in themselves a full risk assessment, but will guide you to decide which Codes of Practice measures may be relevant to your service.

Identifying relevant evidence

2.30 The use of appropriate evidence is fundamental to allow you to make accurate judgements of the level of risk for each kind of priority illegal content and other illegal content.

2.31 Table 5, below, lists the two types of evidence service providers should consider: **core inputs** and **enhanced inputs**. All services should consider core inputs. Only some services should also consider **enhanced inputs**. Large services, and service providers who identify several specific risk factors for a harm using the Risk Profile, should refer to enhanced

inputs. Other services that have enhanced inputs available should also consider using them. The section in Part 3 on 'Evidence' provides more detailed information on these inputs.

Table 5: Summary of relevant types of evidence

Type	Overview of inputs
Core inputs ***All service providers should consider***	• Risk factors identified through relevant Risk Profile (Step 1) • User complaints and reports • User data (for example age, language, groups at risk) • Retrospective analysis of incidents of harm • Relevant sections of Ofcom's Register of Risks, to understand the context of the risk factors in Risk Profiles[40] • Evidence drawn from existing controls • Other relevant information (including other characteristics of your service that may increase or decrease risk of harm, such as existing controls)
Enhanced inputs ***Should be considered by large service providers and those who have identified multiple specific risk factors for a kind of illegal content.***	• Results of product testing • Results of content moderation systems • Consultation with internal experts on risks and technical mitigations • 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
NB. These are not exhaustive examples - may vary by service or business model. See also Part 3, Section 2: 'Evidence inputs'.	

Source: Ofcom analysis

2.32 When considering user data, you must also consider privacy rights and your duties under the UK General Data Protection Regulation ('GDPR'). We encourage you to consult guidance from the Information Commissioner's Office's ('ICO') guidance on UK GDPR requirements and the Age-Appropriate Design Code.[41]

Evaluate likelihood and impact by assigning a risk level to each of the 18 kinds of priority illegal content and other illegal content

2.33 Considering relevant evidence, you should use your judgement to assign a risk level of high, medium, low, or negligible to each of the 18 kinds of illegal content. You should also assign a shared/collective risk level for other illegal content, including non-priority offences you have chosen to assess (noting that you are not required to assess non-priority offences individually).

2.34 The risk level that you assign to each kind of illegal content will be important when considering which safety measures you should implement as part of Step 3. Note that certain measures listed in our Codes of Practice address specific kinds of illegal content. The Risk Level Tables for illegal content in Part 3, Section 3 provide further guidance for addressing risks from image-based CSAM, CSAM URLs and Grooming.

[40] A service provider can consult the Register of Risks to better understand different kinds of priority harm, for instance those which they identify risk factors for when consulting Risk Profiles.
[41] ICO UK GDPR guidance and resources; ICO Age appropriate design: a code of practice for online services.

Assessing the likelihood of illegal content

2.35 When evaluating the likelihood of a kind of illegal content occurring on your service and the chance of your service being used to commit or facilitate an offence, you should ask yourself the questions set out in Table 6:

Table 6: What to consider when assessing likelihood of illegal content

Guiding questions 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 to occur on your service?**[42] If so, how many risk factors do you have that are associated with this 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 of Risks chapter on search indicate evidence that this type of harm is likely to occur on your service? • Are there any **other identified characteristics** of your service (including functionalities, user-base, business model and governance, systems and processes) that may make the kind of illegal harm more likely? • Is there any evidence from your **core inputs** that illegal harm is likely to occur on your service? You should consider: > 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 > 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, consider any additional evidence from **enhanced inputs.** For example, you may consider: > Evidence from independent experts or externally commissioned research that highlights the potential for harm to occur; > Evidence based on results of product testing of the potential for harm to occur; and > Evidence based on results of content moderation of harm occurring. • Are there measures 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

2.36 When evaluating the impact of each of the 18 kinds of illegal content and other illegal content occurring on your service, and the chance of your service being used to commit or facilitate an offence, you should ask yourself the questions set out in Table 7:

Table 7: What to consider when assessing the impact of illegal content

Guiding questions when assessing impact

[42] See Box 1 for what is meant by 'illegal harm'.

- **To make judgements on nature and severity of harm, you need to consider:**
  - If individuals on your service have had a materially harmful experience. For example, due to the **nature** of content and how **users** may **encounter it on the service.**
  - If harm is suffered indirectly, by individuals who are not users of the service. For example, victims of crimes such as CSEA or fraud. If so, how severe of an impact is the harm likely to have on them?
  - What the potential reach of each kind of illegal content on your service could be, and the number of individuals that could be impacted.

- **To make judgements on impact on the individuals affected, you need to consider:**
  - Who are the users of your service? How many of your users are disproportionately likely to be affected by the online harm in question due to their characteristics, such as age or belonging to vulnerable groups? 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.
  - What does user data tell you about your user base demographics (including age, gender, and any vulnerable groups)?
  - How user base demographics affect the way in which users experience harm on your service?
  - How are different users on your service, or third-party individuals, affected?

- **To make judgements about the design and operation of your service, you need to consider:**
  - How does your service's revenue model and commercial profile influence the way the 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? For example, how functionalities may amplify harmful content.
  - 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 over a period.

- **Evaluating the impact will depend on your understanding of the evidence about your own service.**

- 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.
  - The potential reach of illegal content measured by the number of users who could be affected.

- 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**. For example, you may consider:
  - What user research and consultation with users (including vulnerable users and children) tells you about impact on users and other individuals;

- What independent experts or research tells you about the impact of harm on a service of your type;
- Identifying metrics regarding the virality of illegal content (including its potential reach and speed of spread); and
- Evidence about how illegal content may affect third parties beyond your service (this is particularly relevant for certain kinds of illegal harm, such as fraud or CSEA).

- For the avoidance of doubt, where evidence shows potential for severe harm in relation to a kind of content, we expect that this may lead to an assessment of medium or high impact, even if the number of users potentially impacted is relatively small or smaller than the indicative values provided in the **General Risk Level Table included in Part 3, Section 3 of this guidance.**

Source: Ofcom analysis

Essential records for Step 2

2.37 You should keep a written record of the evidence that has informed the assessment of likelihood and impact of each of the 18 kinds of priority illegal content and other illegal content and how this has informed the risk level assigned to each. This should include, where applicable, written records of how any evidence relating to existing control measures has affected the assigned risk levels.

2.38 Where applicable, you should also keep a list of any additional characteristics (including user base, business models, functionalities, governance, and systems and processes) considered alongside the risk factors identified in Ofcom's Risk Profiles.

2.39 You should keep written records of the risk level (of high, medium, low, or negligible) for each of the 18 kinds of priority illegal content, (and, for U2U services this should also include the level of risk assigned to sub-categories of harm (including image-based CSAM, CSAM URLs, and Grooming)), and other illegal content and a summary of the reasoning which has informed the assessment. This level should reflect risk as it exists on the service at the time of assessment.

Step 3: Decide measures, implement, and record

2.40 In Step 2, you will have assigned a risk level to each of the 18 kinds of illegal content and any other illegal content. You now need to decide how you will meet the Illegal Content Safety Duties. The objective of this step is to make a record of your assessment, identify any relevant measures to implement to address risk, and record any measures you have taken.

Sequence of activities and outcomes for Step 3

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

2.41 You should now refer to Ofcom's Illegal Content Codes of Practice. The measures recommended for your service will be based on your service's size, functionalities, or risk levels:

a) Some measures in the Codes of Practice are applicable to all services.
b) Other measures in the Codes of Practice will be informed by your assignment of risk levels in Step 2. Some of the measures only apply to services which are medium or high risk for one particular type of harm. Some measures in the Codes of Practice only apply to services which are medium or high risk for two or more types of harm.

c) The size of your service or specific functionalities of your service will also determine which measures in the Codes of Practice are recommended for your service.

2.42 We provide a more detailed explanation of our package of measures in 'Our approach to developing Codes measures'.

2.43 You can choose to implement the recommended safety measures from our Codes of Practice based on the findings of your risk assessment. The Act says the Codes are like a 'safe harbour', meaning that service providers who choose to implement all applicable measures in the Codes will be treated as complying with their relevant duties under the Act.

Alternative measures to consider

2.44 You do not need to follow our Codes and you may seek to alternative measures to comply with your duties. If you do take alternative measures, you must keep a record of what you have done and explain how the relevant safety duties have been met. In doing so, you must consider the importance of protecting users' rights to freedom of expression and of protecting users from breaches of relevant privacy laws.

2.45 You will only be considered compliant if we are satisfied that the measures are suitably robust to meet the underlying duties set out in the Act.

Additional measures to consider

2.46 For some services, the measures recommended by Ofcom's Codes of Practice may not eliminate all of the risks you have identified. In such cases, we encourage services to consider additional measures to manage or mitigate your risks. For example, some service providers may put in place bespoke controls needed for their unique risk context.

Implement all measures to mitigate and manage risk

2.47 Once you have decided which Codes of Practice measures to take, you should implement them.

Changes to measures and controls

2.48 If you make any changes to existing systems, processes, or other measures in place on your service, this could affect your risk levels for each kind of priority harm, and you may need to re-evaluate if your approach is still adequate. If your existing measures contribute to reducing your risk level, we consider that it will be appropriate to continue implementing these, even if they are additional or alternative to those recommended in our Codes of Practice.

2.49 If you stop implementing existing measures, **this may constitute a significant change** and may impact your risk levels. Further guidance on what constitutes a significant change is set out Part 3, Section 4.

Essential records for Step 3

Record the outcomes of the risk assessment

2.50 At this stage, you should ensure you have a written record of all aspects of your risk assessment, including details about how it has been carried out and its findings. Records should be durable, accessible, easy to understand, and up-to-date, as set out in our Record-Keeping and Review Guidance.

2.51 You should keep a record of all measures from Ofcom's Codes of Practice that have been, or are planned to be, implemented, and any applicable measures that are not planned to be implemented.

2.52 If you have chosen to take alternative measures, you must record what measures you have taken and how these measures achieve the safety duties. Further information is provided in paragraphs 5.3 to 5.5 of the guidance on Record-Keeping and Review.

2.53 Well-maintained and accurate records and regular, timely reviews of compliance will help you to keep track of how you are complying with the illegal harms duties and ensure that the measures that you have taken are fit for purpose. The records will also provide a useful resource for Ofcom in monitoring how the relevant duties are being fulfilled.

2.54 When making a record of your risk assessment, you should capture all information shown in Table 8 below. This will help you to ensure that your risk assessment is suitable and sufficient, that you have considered all the elements of section 9 or section 26 of the Act (as applicable), and included the evidence you have relied on to assess the risks relevant to your service:

Table 8: Information to include in the record of your risk assessment

- The service to which the risk assessment relates;
- The date the risk assessment was completed;
- If applicable, the date the risk assessment was reviewed or updated;
- Who completed the risk assessment, and the named person responsible for 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, see Part 3, Section 1;
- 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;
- If you have considered the role of any existing controls already in operation on your service at the time of this risk assessment, you should record what these controls are, what risks they are intended to mitigate and how they do this, and how the consideration of the existing controls has impacted the risk level you have assigned a kind of illegal content;
- The level of risk (high, medium, low, negligible) assigned to each of the 18 kinds of priority illegal content (and if you are a U2U service, a risk level for each kind of CSAM) and any relevant other illegal content, and an evidence-based explanation of the decision. Where appropriate, this should also include the level of risk assigned to sub-categories of harm (including image-based CSAM, CSAM URLs, and Grooming);
- A list of the evidence and summary of the reasoning that has informed the assessment of likelihood and impact of each of the 18 kinds of priority illegal content and any relevant other illegal content;
- Confirmation that the findings of this risk assessment have been reported, and recorded, 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).

Record all relevant measures and how the safety duties have been met

2.55 You have identified, implemented, and made a written record of all measures from Ofcom's Codes of Practice that have been, or are planned to be, implemented and any measures that are recommended but not planned to be implemented.

2.56 You have made written records of the measures that are alternatives to those set out in Ofcom's Codes of Practice, with evidence that demonstrates how these alternative measures meet the relevant duties.

Step 4: Report, review and update

2.57 The objective of this step is to understand how to keep your risk assessment up to date, and reported appropriately both internally and externally.

2.58 In Step 3, you will have made a complete record of your assessment, identified the relevant measures to implement to address your identified risk, and recorded any measures you have taken and explained how they meet the relevant safety duties.

2.59 In this final step, you will understand and implement the systems and processes by which your risk assessment should be reviewed and updated, as well as implementing arrangements to monitor the effectiveness of your implemented safety measures from Step 3.

Sequence of activities and outcomes for Step 4

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

2.60 All services must keep a written record of their illegal content risk assessment, including details of how the risk assessment was done and its findings.

2.61 Reporting on risk is a primary 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.

2.62 Our Illegal Content Codes of Practice include specific Governance and Accountability measures to help service providers meet their separate safety duty to mitigate and manage risk.[43] Having in place adequate governance is key to how a service identifies, assesses, manages, reports and reviews online safety risks to its users to meet the risk assessment duty. This also helps to consider the range of risks identified in your latest risk assessment.

2.63 If you are a Category 1 or 2A service you must also supply Ofcom with a copy of your illegal content risk assessment as soon as reasonably practicable after completing or revising your illegal content risk assessment. Category 1 service providers must also include a summary of the findings of their risk assessment in their Terms of Service, and Category 2A service providers must include a summary of the findings of their illegal content risk assessment in a publicly available statement.[44]

[43] Measures ICU A1, ICU A2, ICU A3, ICU A4, ICU A5, ICU A6, ICU A7, ICS A1, ICS A2, ICS A3, ICS A4, ICS A5, ICS A6, ICS A7 in the Illegal Content Codes of Practice.

[44] This summary should include the findings of the most recent illegal content risk assessment of a service (including as to levels of risk and as to nature, and severity, of potential harm to individuals).

Monitor the effectiveness of your safety measures

2.64 Monitoring the effectiveness of the measures you implement, alongside your levels of residual risk, is important for ongoing risk management. This will also help you keep your risk assessment up to date, as we explain in Part 1 in the section 'Keeping your illegal content risk assessment up to date'.

Review your risk assessment

2.65 You will need to keep your risk assessments up to date by **reviewing your illegal content risk assessment annually.** We explain this in Part 1 of this guidance, under 'Keeping your illegal content risk assessment up to date'. A review involves checking that your latest risk assessment still accurately reflects the risks on your service. If there have been very few or minor changes to the design, operation and user base of your service since your last risk assessment, you may consider a limited review to be adequate.

2.66 Outside of annual reviews, the Act includes triggers for services to:

a) Review your assessment if Ofcom makes a **significant change to a Risk Profile** relevant to your service;

b) Before making a significant change to the design or operation of your service, **a duty to carry out a new risk assessment in relation to this change.**[45]

2.67 Further guidance on what constitutes a significant change is in Part 3 of this guidance under 'Making a significant change to your service'.

Essential records for Step 4

2.68 You will have made a written record that establishes an annual review cycle for your illegal content risk assessment, and identifies a named person responsible for this process.

2.69 You will, if representing a Category 1 or 2A service, have supplied Ofcom with a copy of your risk assessment record made in Step 3.

2.70 You will, if representing a Category 1 service, have summarised the findings of your most recent risk assessment in your Terms of Service.

2.71 You will, if representing a Category 2A service, have summarised the findings of your most recent risk assessment in a publicly available statement.

[45] This could include deciding to change any existing measures, or measures which are additional to those set out in our Illegal Content Codes of Practice.

Part 3: Supporting information

1. Risk Profiles

1.1 The **U2U and Search Risk Profiles** are resources to consult when conducting your risk assessment. All service providers must take account of the relevant Risk Profile when conducting their own risk assessment.

1.2 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.[46] You should then assess these risk factors alongside your own evidence under Step 2.

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

1.4 The Register of Risks 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 additional risk factors to those highlighted in Risk Profiles. The Risk Profiles will be updated as necessary when changes are made to the Register of Risks.

1.5 When consulting the list of risk factors in the Risk Profiles, you should keep in mind:

- We do not include all the characteristics that may lead to a risk of harm. We do not include risk factors from the Register of Risks where we have more limited evidence, or where we have drawn parallels based on the similarity between two kinds of illegal harm.
- 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 factors 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.[47]

1.6 Given this, you should see the Risk Profiles as the starting point of a multi-step risk assessment process. They will help you 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.

U2U Risk Profile and risk factors

1.7 Risk Profile and risk factors

1.8 The Ofcom U2U Risk Profile is presented in Table 9 below. Each row represents an individual 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 Part 1 (User-to-user services) of the Register of Risks.

[46] 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 the introduction to the Register of Risks.

[47] For further information on how we see these dynamics play out in our evidence base, see Part 1 (User-to-user services) and Part 2 (Search services) of the Register of Risks.

1.9 When consulting the table, you should do the following:

a) **First**, answer the 'Yes' / 'No' questions in Figure 1 below about the characteristics of your service;[48]

b) **Second**, use your answers to select which **specific risk factors** from Table 9 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 in the Register of Risks to help you identify your risk factors accurately;[49]

c) **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.

1.10 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.

1.11 Step 2 of the Risk Assessment Guidance 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 (for example, whether this is a risk that you are already managing, or one that you may need to pay extra attention to).

1.12 When carrying out the risk assessment, service providers should consider the number of specific risk factors they have identified in the U2U Risk Profile associated with each kind of harm. Service providers who identify a large proportion of risk factors associated with a kind of illegal harm may find they are higher risk of that kind of illegal harm. To help them work out the proportion of risk factors they identified, we produced Table 9.1 for service providers to consult when they are using the risk level tables provided in the Risk Assessment Guidance.[50]

Figure 1. 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

[48] If your service offers multiple versions – e.g. mobile and web – you should select 'Y' if *any* versions of the service have 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 the 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.

[49] 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 9 and consider if this information is relevant to your service. You may also wish to consult Part 1 (User-to-user services) of the Register of Risks for more detailed information on the corresponding risk factor or kind of illegal harm.

[50] See the 'Risk Level Tables for illegal content' section in the Risk Assessment Guidance.

Select Yes (Y) or No (N) for the following questions about your U2U service.	
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. Do child users access some or all of my service?[51]	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)[52]	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[53]	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?[54]	Y / N
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

[51] Child users refers to under 18s. This question is to help services include as part of their illegal content risk assessment the risk of illegal harm to children. This is separate from the children's access assessments, which are a new assessment that all regulated U2U and Search services must carry out to establish whether a service – or part of it – is likely to be accessed by children. Services likely to be accessed by children will have additional duties to protect children online and they will need to also undertake a children's risk assessment and implement safety measures to protect children online. We will continue to monitor this approach to ensure alignment with our work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

[52] 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.

[53] 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.

[54] 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.

Source: Ofcom analysis

Table 9. 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 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 all kinds of illegal harm. 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 nearly all kinds of illegal harm (except intimate image abuse and extreme pornography 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.
☐	**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. Furthermore, children could be harmed from exposure to this material if they are not effectively restricted from accessing these services.
☐	**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 terrorism, foreign interference, CSEA (grooming and CSAM**), intimate image abuse and encouraging or assisting suicide and 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 is assisted or encouraged.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**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, drugs and psychoactive substances, sexual exploitation of adults, firearms, knives and other weapons, human trafficking 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, firearms, knives and other weapons, 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 and instructions used to 3D-print firearms on these services – which can be downloaded by others.
2. User base factors		
☐	**2** Services which are accessed by child users[55]	• **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.[56] 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.
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 fraud and financial services, proceeds of crime, foreign interference, CSEA (grooming), harassment/stalking/threats/abuse, drugs and psychoactive substances, hate, unlawful immigration, human trafficking, and sexual exploitation of adults and cyberflashing 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.

[55] Child users refers to under 18s.

[56] Self-generated indecent images refer to indecent images that are shared often consensually between children and can be non-consensually reshared. For further information, see 2.Child Sexual Exploitation and Abuse (CSEA) in the Register of Risks.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
		• **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[57] or users without accounts • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, foreign interference, drugs and psychoactive substances, CSEA (CSAM**), firearms, knives and other weapons, encouraging or assisting suicide and serious self-harm, hate and harassment/stalking/threats/ abuse and cyberflashing 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 and terrorist content, or engage in the buying and selling of illegal goods, such as drugs and weapons. Anonymity can also increase the risk that users on your service conduct illegal behaviour such as harassment and stalking.
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 and cyberflashing 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	• **Risk factor:** User groups • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to CSEA (grooming and CSAM**), encouraging or assisting suicide and serious self-harm, drugs and psychoactive substances, hate, fraud and financial services, controlling or coercive behaviour, foreign interference, intimate image abuse and unlawful immigration and human

[57] 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.		
	send group messages	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 (grooming and CSAM**), animal cruelty, 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. It can also allow perpetrators to form a community around a shared idea, such as discuss ideas for, and commissioning acts of animal cruelty. 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), animal cruelty and, encouraging or assisting suicide and serious self-harm, hate 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).
☐	**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 terrorism, drugs and psychoactive substances, CSEA (grooming and CSAM**), hate, harassment/stalking/threats/abuse, controlling or coercive behaviour, intimate image abuse, unlawful immigration, human trafficking, proceeds of crime and fraud and financial services, encouraging or assisting suicide and serious self-harm, and cyberflashing 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 or contact vulnerable users for the purposes of committing unlawful immigration and/or human trafficking offences. 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.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**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, unlawful immigration, firearms, knives and other weapons, human trafficking, 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, conducting illegal behaviour or facilitate the buying or selling of illegal goods and services. 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, animal cruelty, CSEA (grooming), encouraging or assisting suicide and serious self-harm, fraud and financial services, 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.
☐	**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, hate, foreign interference, harassment/stalking/threats/abuse, CSEA (image-based CSAM), animal cruelty, encouraging or assisting suicide and serious self-harm, controlling or coercive behaviour, drugs and psychoactive substances, extreme pornography unlawful immigration, human trafficking and intimate image abuse and cyberflashing 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 or hateful 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 CSEA (grooming), harassment/stalking/threats/abuse, human trafficking 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, grooming 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.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
☐	**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 and 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, knives and other weapons, sexual exploitation of adults, human trafficking 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 service also allows users to make online payments directly.
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 terrorism, drugs and psychoactive substances, firearms, knives and other weapons, extreme pornography, proceeds of crime 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 or money alongside advice on how to use them to commit fraud or launder the money 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), fraud and financial services, drugs and psychoactive substances, encouraging or assisting suicide and serious self-harm 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 URL linking to share illegal images among themselves on various types of services, providing the opportunity to access and download CSAM, or direct users to marketplaces where they are able to buy and sell illegal goods such as drugs.
8. Recommender systems		
☐	**8** Services with content and/or network 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. We highlight two types of relevant recommender systems below: • **Risk factor:** Content recommender systems • **Key kinds of illegal harm*:** Your service is likely to have an increased risk of harm related to terrorism, foreign interference, encouraging or assisting suicide and serious self-harm and hate offences.

Specific risk factors U2U services with relevant characteristics should take account in their risk assessment.		
		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 terrorism, CSEA (grooming) and drugs and psychoactive substances 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 that the children be connected with others. This can inadvertently facilitate grooming if appropriate checks are not in place. It may also connect users with other users that have similar terrorist ideologies or are willing to buy or sell illegal goods.

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, cyberflashing and intimate image abuse. - How users belonging to minorities and those with other protected characteristics (including **age**[58]**, 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 of Risks on user base demographics for each kind of illegal harm. 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**

[58] 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 work regarding age assurance, children's safety duties, children's access assessments and children's risk assessment.

General risk factors All U2U services should take account in their risk assessment.		
		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[59] 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.
☑	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).[60] 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 A 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 and further information on our evidence base and methodology see the Register of Risks. ** Unless otherwise stated, CSAM includes both image-based and URL-based CSAM.		

Source: Ofcom analysis

Table 9.1. Summary of specific risk factors in the U2U Risk Profile associated with each kind of illegal harm

	Kind of illegal harm	Where it is listed as a key kind of illegal harm ~~for~~ in the U2U Risk Profile
1.	Terrorism	1a. Social media services, 1b. Messaging services, 1c. Gaming services, 1e. Discussion forums and chat rooms, 1f. Marketplace and listing services, 1g. File-storage and file-sharing services, 3b. Anonymous user profiles or users without accounts, 4a. User connections, 4b. Group messaging, 5a. Livestreaming, 5b. Direct messaging, 5c. Encrypted messaging, 5d. commenting on content, 5e. Posting images or videos, 7a. User-generated content searching, 7b. Hyperlinks and 8. Content and network recommender systems.
2.	Child sexual exploitation and abuse (CSEA)	**See 2A, 2B, 2B(i) and 2B(ii) below**

[59] 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.

[60] 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 update their risk management quickly enough to catch up with the rapid change.

	Kind of illegal harm	Where it is listed as a key kind of illegal harm ~~for~~ in the U2U Risk Profile
2A.	Grooming	1a. Social media services, 1b. Messaging services, 1c. Gaming services, 1e. Discussion forums and chat rooms, 2. Child users (under 18s), 3a. User profiles, 3a. Fake user profiles, 4a. User connections, 4b. User groups, 4b. Group messaging, 5a. Livestreaming, 5b. Direct messaging, 5c. encrypted messaging, 5d. commenting on content, 5f. Posting or sending location information and 8. Network recommender systems.
2B.	CSAM (including both image-based CSAM and CSAM URLs)	1a. Social media services, 1b. Messaging services, 1e. Discussion forums and chat rooms, 2. Child users (under 18s), 3b. Anonymous user profiles or users without accounts, 4b. User groups, 4b. Group messaging, 5b. Direct messaging and 5c. Encrypted messaging.
2B(i).	Image-based CSAM	1d. Adult services, 1g. File-storage and file-sharing services, 5a. Livestreaming and 5e. Posting images or videos.
2B(ii).	CSAM URLs	7b. Hyperlinks.
3.	Encouraging or assisting suicide (or attempted suicide) and serious self-harm	1a. Social media services, 1b. Messaging services, 1e. Discussion forums and chat rooms, 3b. Anonymous user profiles or users without accounts, 4a. User groups, 4b. Group messaging, 5a. Livestreaming, 5b. Direct messaging, 5d. Commenting on content, 5e. Posting images or videos, 5g. Re-posting or forwarding content, 7b. Hyperlinking and 8. Content recommender systems.
4.	Hate	1a. Social media services, 1b. Messaging services, 1c. Gaming services, 3a. User profiles, 3b. Anonymous user profiles or users without accounts, 4b. User groups, 5a. Livestreaming, 5b. Direct messaging, 5d. commenting on content, 5e. Posting images or videos and 8. Content recommender systems.
5.	Harassment, stalking threats and abuse	1a. Social media services, 1b. Messaging services, 1c. Gaming services, 3a. User profiles, 3a. Fake user profiles, 3b. Anonymous user profiles or users without accounts, 4a. User connections, 5a. Livestreaming, 5b. Direct messaging, 5d. Commenting on content, 5e. Posting images or videos, 5f. Posting or sending location information and 5g. Re-posting or forwarding content.
6.	Controlling or coercive behaviour	1a. Social media services, 1b. Messaging services, 3a. Fake user profiles, 4a. User connections, 4b. User groups, 5b. Direct messaging, 5e. Posting images or videos and 5f. Posting or sending location information.
7.	Drugs and psychoactive substances	1a. Social media services, 1b. Messaging services, 1f. Marketplace and listing services, 3a. User profiles, 3b. Anonymous user profiles or users without accounts, 4a. User connections, 4b. User groups, 5b. Direct messaging, 5c. Encrypted messaging, 5e. Posting images or videos, 6. Posting goods or services for sale, 7a. User-generated content searching, 7b. Hyperlinks and 8. Network recommender systems.

	Kind of illegal harm	Where it is listed as a key kind of illegal harm ~~for~~ in the U2U Risk Profile
8.	Firearms, knives and other weapons	1a. Social media services, 1b. Messaging services, 1f. Marketplace and listing services, 1g. File-storage and file-sharing services, 3b. Anonymous user profiles or users without accounts, 5c. Encrypted messaging, 6. Posting goods or services for sale and 7a. User-generated content searching.
9.	Human trafficking	1a. Social media services, 1b. Messaging services, 1f. Marketplace and listing services, 3a. User profiles, 4b. User groups, 5b. Direct messaging, 5c. Encrypted messaging, 5e. Posting images or videos, 5f. Posting or sending location information and 6. Posting goods or services for sale.
10.	Unlawful immigration	1a. Social media services, 1b. Messaging services, 3a. User profiles, 4b. User groups, 5b. Direct messaging, 5c. Encrypted messaging and 5e. Posting images or videos.
11.	Sexual exploitation of adults	1a. Social media services, 1b. Messaging services, 1f. Marketplace and listing services, 3a. User profiles, 5c. Encrypted messaging and 6. Posting goods or services for sale.
12.	Extreme pornography	1a. Social media services, 1d. Adult services, 5e. Posting images or videos and 7a. User-generated content searching.
13.	Intimate image abuse	1a. Social media services, 1d. Adult services, 1e. Discussion forums and chat rooms, 1g. File-storage and file-sharing services, 4b. User groups, 4b. Group messaging, 5b. Direct messaging, 5e. Posting images or videos and 5g. Re-posting or forwarding content.
14.	Proceeds of crime	1a. Social media services, 1b. Messaging services, 3a. User profiles, 3a. Fake user profiles, 5b. Direct messaging and 7a. User-generated content searching.
15.	Fraud and financial services	1a. Social media services, 1b. Messaging services, 1f. Marketplace and listing services, 3a. User profiles, 3a. Fake user profiles, 4a. User connections, 4b. User groups, 4b. Group messaging, 5b. Direct messaging, 5c. Encrypted messaging, 5d. Commenting on content, 6. Posting goods or services for sale, 7a. User-generated content searching and 7b. Hyperlinking.
16.	Foreign interference offence	1a. Social media services, 1b. Messaging services, 1e. Discussion forums and chat rooms, 3a. User profiles, 3a. Fake user profile, 3b. Anonymous user profiles or users without accounts, 4a. User connections, 4b. User groups, 5c. Encrypted messaging, 5e. Posting images or videos, 5g. Re-posting or forwarding content, 7b. Hyperlinking and 8. Content recommender systems.
17.	Animal cruelty	1a. Social media services, 1b. Messaging services, 4b. Group messaging, 5a. Livestreaming, 5d. Commenting on content and 5e. Posting images or videos.

	Kind of illegal harm	Where it is listed as a key kind of illegal harm ~~for~~ in the U2U Risk Profile
18.	Cyberflashing	1a. Social media services, 1b. Messaging services, 3a. User profiles, 3b. Anonymous user profiles or users without accounts, 4a. User connections, 5b. Direct messaging and 5e. Posting images or videos.

Source: Ofcom analysis

Search Risk Profile and risk factors

1.13 The Ofcom Search Risk Profile is presented in Table 9.2. Each row represents an individual risk factor that service providers should consider when conducting their risk assessment. The information provided on the risk factors is based on the evidence in Part 2 (Search services) of the Register of Risks.

1.14 When consulting the table, you should do the following:

a) **First,** answer the 'Yes' / 'No' questions in Figure 2 below about the characteristics of your service;[61]
b) **Second**, use your answers to select which **specific risk factors** from Table 9.2 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 in the Register of Risks to help you identify your risk factors accurately;[62]
c) **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.

1.15 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.

1.16 Step 2 of the Risk Assessment Guidance 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 (for example, 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 2. 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?	Y / N

[61] 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 our 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.

[62] 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 9.2 and consider if this information is relevant to your service. You may also wish to consult Part 2 (Search services) of the Register of Risks for more detailed information on the corresponding risk factor or kind of illegal harm.

a. General search service (including downstream general search service[63]) b. Vertical search service	Y / N
2. Do child users access my service?[64]	Y / N
3. Does my service have any of the following functionalities? Select all that apply: a. Provide users with search predictions or suggestions b. Allow users to search for photographs, videos or visual images	 Y / N Y / N

Source: Ofcom analysis

Table 9.2. Search Risk Profile

Specific risk factors Search services with relevant characteristics should take account in their risk assessment.		
1. Service type factors		
☐	**1a** General search services (including downstream general search services)	• **Risk factor:** General search services (including downstream general 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 that content amounting to terrorism offences, drugs, weapons and fraud offences can be accessed via search services. Search services have also been shown to enable relatively easy access to content such as extreme pornography or non-consensual intimate images, particularly 'deepfake pornography'. General search services use proprietary algorithms ('ranking system') to prioritise the most accurate and reliable results based on the user's search query. You should also assess how the ranking system may be manipulated by users to increase the likelihood of illegal content being displayed to other users.
☐	**1b** Vertical search services	• **Risk factor:** Vertical search services Vertical search services, sometimes known as specialty search engines, serve narrower results compared to general search services. They enable users to search for specific topics, products or services and use an API or equivalent technical means to draw results from pre-determined websites or databases with which the provider has a relevant arrangement, rather than indexing sites from across the web.

[63] For the purposes of the Search Risk Profile and our recommended measures, a downstream general search service is still a 'general search service'. The unique business models of downstream general search services do not change the type of search service that is offered to users. That being said, it will be relevant when determining who the 'provider' of the downstream general search service is. We set out our expectations about how entities involved in a downstream general search service arrangement should decide on the provider of the downstream general search service and ensure compliance with the Act in 'Our approach to developing Codes measures' chapter.

[64] Child users refers to under 18s. This question is to help services include as part of their illegal content risk assessment the risk of illegal harm to children. This is separate from the children's access assessments, which are a new assessment that all regulated U2U and Search services must carry out to establish whether a service – or part of it – is likely to be accessed by children. Services likely to be accessed by children will have additional duties to protect children online and they will need to also undertake a children's risk assessment and implement safety measures to protect children online. We will continue to monitor this approach to ensure coherence with our 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 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 search services.
2. User base factors		
☐	**2** Services which are accessed by child users[65]	• **Risk factor:** Child users (under 18s) If child users access your service, 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 not as frequent users of search services compared to adults, as they conduct more searching on U2U services such as social media services, most children still use search services in some capacity and can experience harm through exposure to 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 search queries, we expect you to consider how these tools may also increase the risk of users accessing illegal content. While these tools can allow search queries to be more targeted and accurate, our evidence indicates that search bar predictions and 'suggested searches' features can direct users to potentially illegal content. For example, potential methods or instructions on how to end one's life or self-harm, hateful or racist search queries, and 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 this functionality has been demonstrated as another way for users to find illegal content online, such as services offering to supply illegal drugs. There are also concerns about reverse image search being used to locate content based on someone's likeness, such as illegal nonconsensual intimate images (including deepfake content).

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 Part 2 (Search services) of the Register of Risks on user base demographics for

[65] Child users refers to under 18s.

		each kind of illegal harm. 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 may allow advertising to be seen by users while they use the service. The evidence indicates 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 (for example, 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.[66]

Source: Ofcom analysis

[66] 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 update their risk management quickly enough to catch up with the rapid change.

2. Evidence inputs

2.1 This section of the guidance focuses on the different types of evidence that you should consider when assessing risks.

Why is evidence important?

2.2 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. The guiding principle when deciding what evidence to collect should be what will enable you to make an **accurate risk assessment that meets the suitable and sufficient standard.**

2.3 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.

2.4 It is important that you understand the risks posed by each kind of priority illegal content and other illegal content to **implement appropriate safety measures**. This means that your judgements on risk should be based on relevant information and evidence.

How should you decide what evidence to collect?

2.5 We understand that the appropriate level of evidence will vary based on the size and nature of the service.

2.6 We expect all service providers to use core inputs as part of their assessment. 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.

2.7 You should use **enhanced types of evidence** if your service is large, if you have identified several specific risk factors, or if you are not confident that the core inputs have enabled you to make an accurate assessment of the risk of illegal harm to users on your service.

2.8 When considering any type of evidence, you should consider privacy rights and your duties under the UK GDPR and the ICO's Age-Appropriate Design Code.

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

2.10 In this step, you should consider for each of the 18 kinds of priority illegal content, and other illegal content, **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.

2.11 Each kind of input is explained in the next sections. While we expect the core and enhanced inputs to provide service providers with a good understanding of risk, **the suggestions are not exhaustive**. Service providers should consider whether they need to consider any further evidence.

What is a core input?

2.12 We expect you to use core inputs to complete your risk assessment.

2.13 Some service providers may be able to rely on core inputs alone to confidently assess risk of illegal harm to users.[67] This could be the case where:

- 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 with confidence the likelihood and impact of a harm on your service and to use the Risk Level Tables to assign a risk level to this kind of illegal harm.

2.14 You should also consider any information you already hold, including past risk assessments, that may be relevant to your risk assessment. Table 10 includes examples of core inputs.

2.15 Failing to consider all core inputs 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 in your risk assessment. **We encourage services to consult the relevant section of the Register of Risks, to understand the context of the risk factors in Risk Profiles.** You can prioritise the most relevant parts of the Register of Risks after 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 of Risks. The Register of Risks looks at risks by kind of priority illegal harm. Each chapter presents a summary box and full analysis of risk factors associated to each kind of priority illegal harm.
User complaints, including user reports	Under the Act, you are required to provide complaints procedures which are easy-to-access and use. These should 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. Evidence gathered from this input 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**.

[67] See Box 1 for the meaning of illegal harms.

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 because 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 your service. In particular, you should consider reports or findings relevant to children's experiences online or on your service. This is relevant because, as set out in the Risk Profiles and Register of Risks, certain harms are disproportionately likely to affect certain demographic groups (for example, 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[68] and The Age-Appropriate Design Code.[69]
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 kinds 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.
Evidence drawn from existing controls	If you already have existing controls to mitigate risk as part of the design or operation of your service, then you may want to consider how these controls impact the level of risk posed to users on your service. You should use evidence drawn from these processes which demonstrates their effectiveness in mitigating a kind of illegal content.

[68] See the ICO's guidance and resources on the UK GDPR.
[69] See the ICO's Children's code guidance and resources.

Core inputs	Explanation
Other relevant information	**Consider if you already have the enhanced inputs in Table 12 (for example, the results of content moderation, the results of testing, any research commissioned) to support 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. You may also find relevant to consider other risk-based or impact assessments you have already conducted to meet other regulatory obligations such as the Digital Services Act (DSA) or to comply with privacy and data protection laws in the UK. In addition, service providers may have evidence or data about specific features or functionalities. For example, from product testing them, optimising the design of the service, or running A/B tests to understand their adoption. We would expect the availability of this information to be considered when risk assessing service features and functionalities. **Any other information you hold that can support your risk assessment. You may want to also consider additional enhanced inputs**.

What is an enhanced input?

2.16 We expect that service providers should also use **enhanced inputs** if your service is large, you have identified several specific risk factors, or 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 each of the 18 kinds of priority illegal content, and other illegal content using the Risk Level Table;[70]
- You identify several risk factors for a certain harm which means you are more likely to need to consider enhanced inputs relating to 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 than 7 million UK users) to use more than the core inputs.**

2.17 **Large service providers or service providers that have identified several specific risk factors on their service** for a harm using the Risk Profiles, will typically need to include some or many enhanced inputs to ensure their risk assessments are suitable and sufficient. This is illustrated in the box below:

[70] 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.

Table 11: Illustrative examples of how to decide on evidence inputs

Illustration: Using core and enhanced inputs for services
Using the Risk Profiles, **service provider A** has identified several risk factors suggesting its service may be high risk for a certain kind of illegal harm. **Service provider A gathers evidence from all the core inputs, but it finds very little to no evidence of this harm occurring**, despite the Risk Profile indicating otherwise. There is therefore some ambiguity about the risk of that harm, 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 provider B** has identified several risk factors suggesting its service is high risk for a certain kind of illegal harm. **Service provider 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 can assign itself a risk level for this harm using the Risk Level Table, and without including additional evidence from the enhanced inputs. Using the Risk Profiles, **service provider C** has identified no specific risk factors which suggests it is not high risk for a certain kind of illegal harm. To assess whether this is correct, **Service provider 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 can determine the likelihood and impact of this harm occurring on its service and assign itself a risk level for this harm using the Risk Level Table, and without including additional evidence from the enhanced inputs.

2.18 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**. In general, you should use as many of the enhanced evidence inputs as you need to provide you with a clear and detailed understanding of the risks your service poses.** We provide descriptions of the different types of enhanced evidence in Table 12 below to help you decide if an input is relevant to your assessment of risk.

Table 12: Enhanced evidence inputs

Enhanced inputs	Explanation
Results of product testing[71]	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 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 may improve your risk assessment, because testing can indicate the potential effect of any product changes and help determine whether the effect may increase or decrease the likelihood of illegal content appearing on or being disseminated by your service. For example, services running on-platform tests[72] of their recommender systems should include any additional safety metrics (such as prevalence) they gather as part of this routine testing to provide insights as to how frequent design adjustments 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. This kind of input is particularly relevant for services carrying out a new risk assessment relating to a proposed **significant change**. Product testing is particularly likely to be appropriate where you are launching new features that have not been widely deployed before.

[71] 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.

[72] 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 is not limited to A/B/x Testing or Multi Arm Bandit ('MAB') Testing.

Enhanced inputs	Explanation
Results of content moderation systems	Many services are likely to have a content moderation system in place, though the nature, scope and maturity of these systems may vary significantly. You may operate a sophisticated content moderation system which measures more complex types of exposure to improve your understanding of, and response to, illegal content. For example, measuring how long illegal content is present on your service, the type of content you are taking down, or the virality of specific 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 such evidence in your risk assessment will support your analysis of the likelihood of a kind of priority illegal harm taking place on your service, the effectiveness of your mitigation measures, and the role of the characteristics of your service on risk levels (for example, if a product change increases or reduces the amount of illegal content you detect).
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 clear understanding of how technical measures, systems and processes may help address risk. Consultation should 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	Expert consultation can 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 a view of experts on industry trends, regulatory standards and the views of certain trade bodies or technical experts in relevant fields.

Enhanced inputs	Explanation
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, on specific trends or harms which informs their approach to safety and moderation on the service. 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.
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 comprehensive, 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 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 well thought out 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 that 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.

Enhanced inputs	Explanation
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. 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 (such as behavioural biases) could be present at primary points in the user journey that might 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 service will help to ensure that safety features, mitigations, and other primary points of engagement (for instance, terms of service) are accessible and meet the needs of users. Engagement could be general or designed to target specific users, such as those with vulnerabilities or certain age groups.
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 can feedback any concerns 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.

3. Risk Level Tables for illegal content

3.1 This section presents a General Risk Level Table to use as part of Step 2 in the risk assessment process. Using this table should help you to classify the risk level into high risk, medium risk, low risk and negligible or no risk. Calibrating risk levels should be based on all the evidence you have gathered to conduct your risk assessment. This needs to be done separately for each kind of priority illegal content.

3.2 The table captures considerations relevant to impact and likelihood separately. If you are a U2U service, you should consider the number of risk factors you have identified in the Risk Profiles that are likely to apply to your service. If you are a Search service, instead of the number of risk factors, you should rely on information in the Register of Risks, and your own evidence to make an assessment of likelihood.

3.3 Likelihood and impact may often be correlated. If your assessment of these diverges (for example, relatively low likelihood and relatively high impact, or vice versa), you will need to reach a view on the risk level overall, taking account of the guidance in the Table. Where the evidence of risk is not conclusive of the appropriate level of risk, **we expect providers to err on the side of caution and select the higher risk level**, being mindful of the harm that may result from underestimating the level of risk.

3.4 For U2U services, in addition to assessing an overall CSEA risk, you should separately use the three additional tables (Tables 13.1, 13.2 and 13.3) to assess the risk of image-based Child Sexual Abuse Material (CSAM), CSAM URLs, and Grooming. Search services do not need to do this, and it is sufficient for them to only consider an overall CSEA risk.

3.5 In addition to these tables, we also provide illustrative examples in Appendix B of different risk levels for hypothetical services, to help you calibrate your risk level appropriately.

3.6 You should not apply the General Risk Level Table or the CSEA specific tables mechanically. They are intended to help inform your judgement on a risk level, rather than to determine risk levels. However, if you have evidence of a substantial amount of illegal content on your service, then we would generally expect you to assess as high risk.

Table 13: General Risk Level Table

Risk level	Description	Your service may decide on this risk level if some of the following conditions are met
High risk	You assess that there is a **high likelihood** that a user could encounter this kind of illegal content	• There is **significant evidence of this kind of illegal content**[73] **being encountered** on your services (for example from complaints) or it being **very likely to be encountered** on your service (for example, evidence from external experts). • You have identified **many**[74] **specific risk factors** in the relevant Risk Profiles* (used in Step 1) which increase the likelihood of this kind of illegal content occurring **and** there are **no effective systems** and processes in place to address this harm nor other factors which reduce risks to users and affected individuals.

[73] Illegal content here refers to each of the 18 kinds of priority illegal content, and other illegal content.
[74] We consider 'many' to be a large number of risk factors in proportion to the total number of specific risk factors for a particular kind of illegal harm in the Risk Profiles. The number of risk factors we have identified for different kinds of illegal harms in the Risk Profiles varies in line with the evidence available and the way harm manifests. A kind of illegal harm which involves many different offences, pathways and behaviours may have more evidence available, and in turn more risk factors associated with it than one which has fewer. Therefore, for a kind of illegal harm with a small total number of risk factors, even a few may be considered 'many'. Similar considerations apply to 'several' and 'few' for the risk levels below.

Risk level	Description	Your service may decide on this risk level if some of the following conditions are met
	You assess that there is **high impact** to users of your service or other individuals from this illegal content	• Even if you have controls/existing measures in place for this kind of illegal content, **there is evidence of (1) a substantial amount of illegal content being present on your service or of it being used to commit or facilitate priority offences; or (2) actual illegal harm[75] to many individuals overall. Evidence of either (1) or (2) is a strong indicator of being high risk and we would normally expect all services with such evidence to be high risk for that kind of illegal content.** Such evidence could be from core or enhanced evidence inputs, for example from external experts or from complaints. • Based on your analysis of core and enhanced evidence, you identify that this kind of illegal content would have a **severe impact** for your users or other affected individuals, **even if the number of individuals affected is low**. For example, this could be because of the nature of the content encountered by users or of the harm indirectly suffered outside the service, or the way in which users encounter it. • There is **broad scope for this kind of illegal content to impact many individuals**, who may be users of your service or other affected individuals (for example, individuals who are affected by harms such as illegal hateful content and are not users of your service). This is particularly if the users or affected individuals impacted belong to vulnerable groups (based on your understanding of user base demographics on your service). This is more likely if one or more of the following applies: o Your service has over 7 million monthly active United Kingdom users ('monthly UK users'),[76] and especially if it is a category 1 or 2A service. o Content can be shared and disseminated on your service in a way that has the potential to affect a significant number of users. Having the potential to impact a large number of users is not necessarily – by itself – a strong indicator of being high risk, especially compared to evidence of substantial illegal content being present or having a severe impact on users or affected individuals.

[75] When we use the term 'illegal harm' we refer to the psychological or physical harm which can occur from a user encountering any illegal content, or from your U2U service being used for the commission or facilitation of an offence.

[76] As calculated in accordance with the methodology set out in the Codes of Practice.

Risk level	Description	Your service may decide on this risk level if some of the following conditions are met
Medium risk	You assess that there is a **moderate likelihood** that a user could encounter this illegal content	• There is **evidence of this kind of illegal content being (or likely to be) encountered** on your service. • You have identified **several**[77]**specific risk factors** in the relevant Risk Profiles* (Step 1) which increases the likelihood of this kind of illegal content occurring **and**, while you may have some systems and processes in place to address this harm, you cannot demonstrate they are effective at reducing risks to users and other affected individuals, nor are there any existing controls and/or aspects of your services design or operation that sufficiently reduces risks.

	You assess that there is **moderate impact** to users of your service or other individuals from this illegal content	• Even if you have controls/existing measures in place for this kind of illegal content, **there is evidence of (1) a moderate amount of illegal content being present on your service or of it being used to commit or facilitate priority offences; or (2) actual illegal harm to a moderate number of individuals, who may be users of your service or other affected individuals. Evidence of either (1) or (2) is a strong indicator that your service is at least medium risk, and we would normally expect all services with such evidence to be medium or high risk for that kind of illegal content.** Such evidence could be from the core or enhanced evidence.
		• Based on your analysis of evidence, you identify that this kind of illegal content would have a **moderate impact** for your users or other affected individuals.
		• There is **some scope for this kind of illegal content to impact many individuals**, who may be users of your service or other affected individuals. This is more likely if one or more of the following applies:
		  ○ Your service has between 700,000 and 7 million monthly UK users.
		  ○ Content can be shared and disseminated on your service in a way that has the potential to affect many users or other individuals.
		Having the potential to impact many users is not necessarily – by itself – a strong indicator of being medium risk, especially compared to evidence of a moderate amount of illegal content.

[77] This is intended as an overall guide, but rather than focusing purely on the number of risk factors, you should consider the combined effect of the risk factors to make an overall judgement about the level of risk on your service.

Risk level	Description	Your service may decide on this risk level if some of the following conditions are met
Low risk	You assess that there is a **low likelihood** that a user would encounter illegal harm on your service	• You have used evidence to assess whether the harm is taking place on your service and have **concluded that there is no evidence** of this, **and** you have identified **no or few specific risk factors** associated with the kind of harm in the relevant Risk Profiles.* • There are **comprehensive systems and processes in place**, or other factors which sufficiently reduce risks of this kind of illegal harm to users, and your evidence shows they are very effective. Even if taking all relevant measures in Ofcom's Codes of Practice, this may not always be sufficient to mean your service is low risk.
	You assess that there is **limited impact** to users or other individuals of your service from this illegal harm	• Even if there are occasional examples of the kind of illegal content occurring on your service, there is **limited potential for harm** to impact users or other affected individuals. For example, this could be because the harm impacts very few users or other individuals **and** the **severity of that harm is low**. If the severity of the harm were high, then even a small number of instances would mean your service was not low risk.
Negligible or no risk	If your evidence shows it is **not possible or extremely unlikely** that this kind of illegal harm takes place by means of your service, you may assess the risk of that harm as 'negligible or no risk', irrespective of whether you meet one or more of the conditions for low/medium/high risk as defined in the rows above. If you have some of the relevant risk factors and the kind of illegal harm is possible on your service, then to assess as 'negligible or no risk' for that kind of illegal harm, you will normally need comprehensive evidence to demonstrate that your service does not pose low, medium or high risk.	
* For the avoidance of doubt, a service with few risk factors for the kind of illegal harm in question may still have a high or medium risk for that kind of content, depending on the assessment of relevant evidence and factors as set out in this guidance.		

Source: Ofcom

Guidance on assessing risks for certain types of CSEA for U2U services

3.7 As set out in the Register of Risk, CSEA manifests in a number of forms. Our Codes of Practice have specific measures to deal with different types of CSEA risks. To help establish which of these measures you should put in place, you should separately assess your risk level for the following types of CSEA when you do your risk assessment:

- Image-based CSAM
- CSAM URLs[78]
- Grooming

[78] 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).

3.8 This guidance includes additional information to help you assess the risk of CSEA occurring on your service. The following tables will help you make an assessment of the risks of these harms and help inform your judgement of the risk level. These explain the circumstances in which we would ordinarily expect a service to pose a high, medium or low risk of these types of CSEA. You may need to identify a medium or high risk for one of these types of CSEA because of your service's functionalities, even if the harm has not yet materialised.[79] However, we recognise that risk is context specific and that there may be circumstances in which other evidence-based factors mean a service concludes that it is higher or lower risk than the tables would appear to suggest.

Child Sexual Abuse Material (CSAM)

3.9 CSAM is a category of CSEA content, including in particular indecent or prohibited images of children. This includes still and animated images, and videos, 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.[80]

3.10 It is important to understand that being low risk for image-based CSAM or CSAM URLs does not preclude your service from being high risk for the other.

[79] Perpetrators have demonstrated the ability to exploit a variety of services with the necessary features for CSEA, making it difficult to predict which services might be targeted. Your service may therefore assess as medium risk even though it has not faced any CSEA offences and such an occurrence may appear unlikely.
[80] For more information see the Register of Risks chapter 'Child sexual abuse material (CSAM)', particularly the section 'How child sexual abuse material offences manifest online'.

Table 13.1: Image-based CSAM Risk Level Table

Risk level	*Guidance*
High risk	There is evidence[81] that image-based CSAM has been present to a significant extent [82] on the service. Such evidence is the strongest indicator of being high risk and we would normally expect all services with such evidence to be assessed as high risk. OR Your service enables images or videos to be generated, uploaded or shared, and the service is: • a file-storage and file-sharing service, or • an online adult (pornography) service, or • you have identified a lot of the following specific risk factors: (a) child users; (b) social media services; (c) messaging services; (d) discussion forums and chat rooms; (e) group messaging; (f) livestreaming; (g) direct messaging; (h) encrypted messaging; (i) users can share images or videos without creating a user account. We would normally expect such services to be assessed as high risk, unless there are strong reasons to assess at a lower risk level.
Medium risk	There is evidence[83] that image-based CSAM has been present on the service, but not to a significant extent. Such evidence is a strong indicator of being medium risk and we would normally expect all services with such evidence to be assessed as medium risk. OR Your service enables images or videos to be generated, uploaded or shared, and you have identified several[84] of the following specific risk factors: (a) child users; (b) social media services; (c) messaging services; (d) discussion forums and chat rooms; (e) group messaging; (f) livestreaming; (g) direct messaging; (h) encrypted messaging; (i) users can share images or videos without creating a user account. We would normally expect such services to be assessed as at least medium risk, unless there are strong reasons to assess at a lower risk level.

[81] This evidence could come from core or enhanced evidence and could include user complaints and reports; the results of content moderation; takedown notices issued by organisations such as the IWF, C3P, NCMEC or other INHOPE member hotlines; or information received from law enforcement agencies or Ofcom.
[82] For these purposes, image-based CSAM has been present to a significant extent both where a significant amount of image-based CSAM is generated, uploaded or shared on the service in a short period of time, and where smaller amounts of image-based CSAM are generated, uploaded or shared on the service over a significant period of time.
[83] See footnote 60.
[84] This is intended as an overall guide, but rather than focusing purely on the number of risk factors, you should consider the combined effect of the risk factors to make an overall judgement about the level of risk on your service.

Risk level	Guidance
Low risk	Your service enables images or videos to be generated, uploaded or shared, but either of the following conditions apply: • You have comprehensive systems and processes in place that ensure that image-based CSAM is very unlikely to be present. We would generally expect such systems and processes to include effective human or automated systems or processes (such as a combination of hash matching and automated content classifiers) which are used to review all images and videos generated on a service. In certain circumstances, if there has never been any evidence of CSAM, other systems and processes may be sufficient provided they are demonstrably effective at preventing or deterring the sharing of CSAM. OR • Your service meets all of these three conditions: • There is no evidence[85] that image-based CSAM has been present on the service; and • The service is not a file-storage and file-sharing service, nor an online adult (pornography) service; and • You have identified none or few of the following specific risk factors for image-based CSAM on your service: (a) child users; (b) social media services; (c) messaging services; (d) discussion forums and chat rooms; (e) group messaging; (f) livestreaming; (g) direct messaging; (h) encrypted messaging; (i) users can share images or videos without creating a user account.
Negligible or no risk	Where the service's functionalities do not enable images or videos to be generated, uploaded or shared on the service and image-based CSAM is therefore impossible or extremely unlikely to be encountered on the service.

Table 13.1: CSAM URLs Risk Level Table

Risk level	Guidance
High risk	There is evidence[86] that CSAM URLs have been shared to a significant extent on the service. Such evidence is the strongest indicator of being high risk and we would normally expect all services with such evidence to be assessed as high risk. OR Your service allows users to share text or hyperlinks without creating a user account. We would normally expect such services to be assessed as high risk, unless there are strong reasons to assess at a lower risk level.

[85] See footnote 60.
[86] This evidence could come from core or enhanced evidence and could include user complaints and reports; the results of content moderation; takedown notices issued by organisations such as the IWF, C3P, NCMEC or other INHOPE member hotlines; or information received from law enforcement agencies or Ofcom.

Risk level	*Guidance*
Medium risk	There is evidence[87] that CSAM URLs have been shared on the service, but not to a significant extent. Such evidence is a strong indicator of being medium risk and we would normally expect all services with such evidence to be assessed as medium risk. OR Your service enables users to share text or hyperlinks, and you have identified several [88] of the following specific risk factors: (a) child users; (b) social media services; (c) messaging services; (d) discussion forums and chat rooms; (e) user groups; (f) direct messaging; (g) encrypted messaging. We would normally expect such services to be assessed as at least medium risk, unless there are strong reasons to assess at a lower risk level.
Low risk	Your service enables users to share text or hyperlinks, but either of the following conditions apply: • There are comprehensive systems and processes in place that ensure that CSAM URLs are very unlikely to be shared on the service. For example, automated (e.g. URL detection) or manual (e.g. human reviews) systems and processes that can be used to check all text or hyperlinks shared. OR • There is no evidence[89] that CSAM URLs have been shared on the service, and you have identified no or few of the following specific risk factors: (a) child users; (b) social media services; (c) messaging services; (d) discussion forums and chat rooms; (e) user groups; (f) direct messaging; (g) encrypted messaging.
Negligible or no risk	Where the service's functionalities do not enable users to share text or hyperlinks and CSAM URLs in those forms are therefore impossible or extremely unlikely to be encountered on the service.

[87] See footnote 65.
[88] This is intended as an overall guide, but rather than focusing purely on the number of risk factors, you should consider the combined effect of the risk factors to make an overall judgement about the level of risk on your service.
[89] See footnote 65.

Grooming

Table 13.3: Grooming Risk Level Table

Risk level	Guidance
High risk	There is evidence[90] that grooming has occurred to a significant extent on the service. Such evidence is a strong indicator of being high risk and we would normally expect all services with such evidence to be assessed as high risk. OR It is possible for children to access the service or a part of the service[91], **and** the service's functionalities enable users to communicate one-to-one with child users (e.g. direct messaging), **and** any of the following conditions apply: • The service includes child users when users are prompted to expand their networks, including through network recommender systems (e.g. network expansion prompts); **or** • The service allows users to view child users in the lists of other users' connections; **or** • The service has user profiles or user groups which may allow other users to determine whether an individual user is likely to be a child; **or** • You have identified a lot of the following specific risk factors: (a) social media services; (b) messaging services; (c) gaming services; (d) livestreaming; (e) encrypted messaging; (f) commenting on content.[92] We would normally expect such services to be assessed as high risk, unless there are strong reasons to assess at a lower risk level.
Medium risk	There is evidence[93] that grooming has occurred on the service, but not to a significant extent. Such evidence is a strong indicator of being medium risk and we would normally expect all services with such evidence to be assessed as medium risk. OR It is possible for children to access the service, or a part of the service, **and** the service's functionalities enable users to communicate one-to-one with child users (e.g. direct messaging), **and** you have identified several[94] of the following specific risk factors: (a) social media services; (b) messaging services; (c) gaming services; (d) livestreaming; (e) encrypted messaging; (f) commenting on content. We would normally expect such services to be assessed as at least medium risk, unless there are strong reasons to assess at a lower risk level.

[90] Evidence of actual harm could be from core or enhanced evidence, including user complaints and reports; the results of content moderation; or information received from NGOs, law enforcement agencies or Ofcom.
[91] For the purpose of assessing the risk of grooming, when deciding whether it is possible for children to access a service, or a part of a service, service providers should consider both UK and non-UK child users. This is because, under UK law, grooming offences can be committed where the victim is a non-UK child user.
[92] This list reflects the risk factors for grooming in the U2U Risk Profile, other than those already built into the guidance. See Part 3, Section 1 for further information.
[93] See footnote 69.
[94] This is intended as an overall guide, but rather than focusing purely on the number of risk factors, you should consider the combined effect of the risk factors to make an overall judgement about the level of risk on your service.

Risk level	Guidance
Low risk	It is possible for children to access your service or a part of the service, but either of the following conditions applies: • You have comprehensive systems and processes in place that ensure grooming is very unlikely to occur on the service. OR • There is no evidence[95] that grooming has occurred on your service **and** you have identified no or few risk factors associated with grooming.
Negligible or no risk	Where it is not possible for children to access the service, and grooming is therefore extremely unlikely to take place on the service.

[95] See footnote 69.

4. Making a significant change to your service

4.1 This section of the Guidance explains the circumstances which could amount to a significant change to your service where you may need to carry out a new risk assessment relating to that proposed change.

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

4.2 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 in advance of putting them into operation.**

4.3 The legal duty requires you to carry out a new risk assessment as it relates to the impacts of the proposed change. In practice, this may require you to carry out a new assessment of the whole service. To ensure that your risk assessment is suitable and sufficient, you should consider whether the impact of the change may affect other parts of the service and undertake a risk assessment accordingly. This new assessment can be done by carrying out each step of the four-step process.

4.4 This duty is intended to capture changes which could impact the risk of harm from illegal content. A very minor or routine change should not require you to carry out a new risk assessment.

4.5 In Table 14 we have provided guidance on what could amount to a significant change by listing a few indicative scenarios that are likely to amount to a significant change.

Table 14: 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 materially impacts a substantial proportion of your user base or	If yes, **you must carry out a new risk assessment relating to this change**

	changes the kind of users you expect to see on your service. • The proposed change materially impacts a vulnerable user group, such as children. • The proposed change materially 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 materially 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: • Would the change materially impact users, user experience or user behaviour in a way that may affect risk of illegal harm? • 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?	

4.6 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(s). 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 (for example, 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 types of content that 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 harm arising from 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, end-to-end encryption or live streaming – must be accounted for in the risk assessment. The addition of these functionalities would require a provider to revise its risk assessment as it relates to the impacts of the proposed change.
- **Changes to platform content rules or content prioritisation:** these may alter the types of content that users encounter and subsequently alter the site's user base. 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 or prominence of the reporting function or changing the design of icons related to reporting or reacting to content which could impact how users engage with online safety measures.
- **Introducing the use of prompts** to alert or remind users about options to change content control settings: the timing and language used in these prompts could impact the choices users make and go on to impact the risk of encountering certain types of content.
- **Any acquisition that may change the core product offered to users**: for instance, integrating functionality from another service following a product acquisition.
- **Changes in ownership or investment:** these may influence how the service operates (a new owner may have different views on how the service 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 service's 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.

A1. Appendix A: Offences and kinds of illegal content

A1.1 You need to assess the risk of each kind of priority illegal content set out in the Act. This includes many individual offences. Ofcom has grouped these into 18 kinds of priority illegal content, as set out in Table 15 below.

A1.2 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 and part in the commission of that offence. The offences are priority offences unless otherwise specified.

Table 15: Kinds of illegal content

	Column 1: Kind of illegal content	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[96]	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[97]	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.

[96] Image-based CSAM may also be a risk present on Search services and is covered by 2B (CSAM). See paragraph 2.63 of the Risk Assessment Guidance for more information.

[97] CSAM URLs may also be a risk present on Search services and is covered by 2B (CSAM). See paragraph [2.63] of the Risk Assessment Guidance for more information.

	Column 1: Kind of illegal content	Column 2: Offences
3.	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 content	Column 2: Offences
4.	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).
5.	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).
6.	Intimate image abuse	An offence under section 66B of the Sexual Offences Act 2003 (sharing or threatening to share an intimate photograph or film). 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).
7.	Extreme pornography	An offence under section 63 of the Criminal Justice and Immigration Act 2008 (possession of extreme pornographic images).

	Column 1: Kind of illegal content	Column 2: Offences
8.	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).
9.	Human trafficking	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.	Unlawful immigration	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).

	Column 1: Kind of illegal content	Column 2: Offences
11.	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).
12.	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).
13.	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).

14.	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 content	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).
15.	Encouraging or assisting suicide (or attempted suicide) and serious self-harm	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). An offence under section 184 of the Online Safety Act 2023 (encouraging or assisting serious self-harm)
16.	Foreign interference offence	An offence under section 13 of the National Security Act 2023 (foreign interference).
17.	Animal welfare offence	An offence under section 4(1) of the Animal Welfare Act 2006 (unnecessary suffering of an animal).
18.	Cyberflashing	An offence under section 66A of the Sexual Offences Act 2003 (sending etc photograph or film of genitals).

Source: Ofcom

A2. Appendix B: Examples of how to use the Risk Level Tables (for U2U services)

A2.1 This section includes hypothetical examples to help U2U services understand how to use the Risk Level Tables to make accurate judgements about risk levels, as part of their risk assessment about each of the 18 kinds of priority illegal content, and other illegal content.

A2.2 These examples are not intended to be conclusive risk assessment evaluations for the specific content identified – they are not based on real, evidence-based judgements. For example, they do not explain the accuracy of information; the volume of reporting; the rating for likelihood and impact of the harm; whether the risk is about encountering, facilitation or commission of an offence; nor do they explain the degree of confidence in the effectiveness of any measures. Services should not seek parity or comparison with these illustrations to justify their own risk assessments.

Table 16: Risk Level Tables theoretical examples

Fraud – high risk
An online marketplace has over 5 million monthly UK users. Users have profiles and the service has a recommender system that suggests goods that are similar to those a user previously searched for or purchased. When the service receives a user report about a suspect counterfeit good, it conducts an in-depth check of the user who posted the good and/or of goods posted. Even without a user report, the service also conducts some proactive checks. Following in-depth checks, if appropriate, the service takes action. This can include taking down the posts of illegal goods and removing accounts of fraudsters. The service receives a large number of user reports about suspect goods being sold, while others report having purchased goods via bank transfer, which were subsequently never delivered. This is consistent with third-party expert research which found evidence of significant fraud on the service. Given the evidence of a substantial amount of fraud, the provider concludes the service is high risk for fraud.

Fraud – medium risk
An online event ticketing service enables users to buy tickets to various events in the UK. It has about 200,000 monthly UK users, who can create, promote, or buy tickets to events via the service. Its design and safety measures include multi-factor authentication of user's account upon creation, via email. The service also has a report function for listings that appear to be fake or suspicious, which are then reviewed by either AI or human moderators.

Despite these precautions, there is evidence from user complaints and external sources of a small number of users being tricked into purchasing fake tickets on the service each month. Partly because of the relatively low value of tickets and its size, the provider concludes it is medium risk for fraud.

Fraud – low risk

A small gaming service has around 15,000 monthly UK users. Users have profiles to play the game and when playing the game can interact with all other users who are playing at that time through a chat function.

The service has a user reporting system, but few other safety processes relevant for fraud.

User complaints have never indicated fraud is an issue. The service does not have most of the risk factors identified in Ofcom's Risk Profiles that are typically associated with increased risk of fraud (such as user connections, user groups, space for users to comment and/or post). One risk factor the service has is user chat, but there has never been any indications of this being used for fraud. The provider concludes the service is low risk for fraud.

Controlling or coercive behaviour – high risk

A large social media service has around 10 million monthly UK users. Users can update their profiles and connect to other users. They can post images and videos as well as text, and can comment on other users' posts. Users can direct message one another and can post location information (e.g. adding location information to images/videos posted).

The service has various safety systems and processes in place. This includes automatically scanning images/videos posted for various types of content that violate its terms of service, a user reporting system, and user controls that allow users to block or mute other users. It also uses automatic tools to pick up mentions in complaints of keywords associated with controlling or coercive behaviour (such as "ex-boyfriend" or "stalking"), and of reports of fake profiles or monitoring through shared accounts. It prioritises investigating reports of illegal content.

The service has identified some complaints relating to controlling or coercive behaviour offences, and it has many of the risk factors in Ofcom's Risk Profiles that are typically associated with increased risk of such offences. The provider cannot be sure that controlling or coercive behaviour offences are not take place on the service much more often than user reports indicate. It concludes it is high risk for controlling or coercive behaviour.

Hate – high risk

A large video-sharing platform has around 10 million monthly UK users. Users can post videos with anonymous user profiles. Users can comment on the posts of others. It has recommender systems that suggest content and new user connections.

The service has extensive and sophisticated safety measures in place. These include automatic content moderation systems and blocking or restricting users found to post violative content. It has a user-friendly content reporting system and works with various trusted flaggers.

The service has a sophisticated process for estimating the 'violative view rate' (or 'prevalence' rate), which is the percentage of views on the service that are of content violating its terms of service. Because of its investment in safety measures, the service has been able to reduce its violative view rate for hateful content to a very low rate of 0.01%. While its violative view rate is very low, given the high number of monthly users and views, the number of users experiencing hateful content is still significant. This is consistent with user reports indicating many incidents of hateful content on the service. Based on the evidence on the volume of hateful content and the likely harm, the provider concludes the service is high risk for hate.

Hate – medium risk

An online game involves teams competing. Users can communicate with their teammates through voice chat while playing and it has over 500,000 monthly UK users. Teams can be formed from within user groups or with non-connected users.

The service allows a user to report another user if they say something hateful. Users are warned or banned for using hateful language. The service encourages users to use the reporting system, including reassuring them that if they report someone, that person will not know who reported them. However, it does employ product nudges such as a pop-up prompt when it detects a potentially hateful message being written (before posting).

From user reports, the service has evidence of illegal hate speech within the chat and each year bans some users. While there may be unreported hate speech, the provider believes this to be rare. This is because teams typically include randomly selected non-connected users and when incidents are reported, they are typically reported by more than one person playing at the time. While the number of users directly affected by each incident is small, there are tens of such instances each month and the impact on those affected may be high. The provider concludes the service is medium risk for hate.

Hate – low risk

A publishing house runs a book club which allows users to share articles about its books and allows other users to comment on these. All articles and comments are public. The service has around 5,000 monthly UK users.

All articles are reviewed by the staff of the publishing house before they can be read by others to ensure they have no offensive material. The service does not do this for comments, but does review some of these after they have been posted. It has a user reporting system.

Despite the service operating for many years, hateful content was reported only in a couple of instances and was swiftly taken down by the service. There could be undetected hateful content, but the likelihood of this is reduced because all content is public, the service has a diverse user base, and because of the service's own proactive monitoring. Despite the service having some of the risk factors in Ofcom's Risk Profiles that are typically associated with increased risk of hate offences, the provider concludes the service is low risk because of the evidence of limited occurrences and harm, especially given its small size.

Image-based CSAM – high risk

A file sharing service enables users to share large numbers of files and has around 60,000 monthly UK users. It allows users to share files anonymously and allows users to create closed user groups to share files.

The service has a complaints handling process and violative content is promptly taken down. It does a limited amount of proactive checking of content on larger user groups. However, it does not have any processes in place to check all content and does not use CSAM hash matching technology.

The provider is aware of a small number of instances in which CSAM was shared via some user groups, based on user complaints and the limited proactive reviews it does. Despite these being a small number of instances, the provider acknowledges the severity of the harm caused. The provider also does not know how widespread the problem is. As a file sharing service, it is likely to be at increased risk of being targeted by perpetrators to store and share CSAM, and it has other functionalities identified as risk factors typically associated with an increased risk of CSAM. It would not know if CSAM offences occur in closed user groups, the content of which are not reviewed by the service. The provider concludes the service is high risk for image-based CSAM.

CSAM URLs – medium risk

A service markets holidays and has around 8 million monthly UK users. It provides users with destination-focused discussion forums and chat rooms, via which users can comment and therefore share text and hyperlinks.

If notified of illegal content, the service quickly removes it. However, the service does not currently have any systems and processes in place to proactively check all text and hyperlinks shared via its discussion forums and chat rooms for CSAM URLs.

In the past, the service has been notified by organisations such as the IWF, NCMEC and C3P of a few instances where its discussion forums and chat rooms were used to share CSAM URLs. Moreover, it has several risk factors for URL-based CSAM. Given the evidence of a few instances of CSAM URLs being shared, the seriousness of the harm and the risk of it happening again undetected, the provider concludes the service is medium risk for CSAM URLs.

CSAM URLs and Image-based CSAM - low risk

A health charity has a website which shares information about a particular illness. Part of the website is a forum where users can describe their experiences and offer support to one another. It has 10,000 monthly UK users. Users can share images, text and hyperlinks, and respond to each other's comments.

People at the charity review all content and comment boxes, after it is uploaded by users. This includes checking any links that have been included. It also has a complaint system and looks at any complaints promptly.

The service has a few of the risk factors for CSAM URLs and image-based CSAM. However, as the service reviews all content shared by users, it would be likely to know if there had ever been CSAM images or URLs on the service, and there has never been any. The provider therefore concludes the service is low risk for CSAM URLs and image-based CSAM.

Grooming – high risk

A social media site has over 10 million monthly UK users. It allows direct messaging and has network expansion prompts. The terms of service say the service is only for people aged 16 and over.

As well as a content reporting system, the service allows users to report and block other users.

While in theory only those aged 16 and over are allowed to use the service, it does not use highly effective age assurance and it is known to be used by younger children. While the service has received few reports from users of grooming, external expert organisations have highlighted that it is known to be used for grooming. It has been named in various police cases and in a prominent newspaper investigation about grooming. The provider concludes the service is high risk for grooming.

Grooming – low risk

On a voluntary basis, an individual runs a site with information on sporting activities in and around a particular town. It has around 5,000 monthly UK users. Users can post information about events, including both text and images. Users can also add comments. All content is public. While aimed at sporting activities likely to be of interest to adults, it does not have any age restrictions.

The individual who runs the service periodically checks all content to ensure it is suitable and there is a basic reporting system.

There is no evidence of grooming ever having happened on the service. The service does not have many of the risk factors associated with increased risk of grooming. In particular, it does not allow direct messaging. It is likely that only a relatively small number, and proportion, of users are children. The individual who provides the service concludes it is low risk for grooming.

Suicide and self-harm – high risk

A discussion forum is intended to provide support for individuals experiencing suicidal thoughts. It has 50,000 monthly UK users. Users can post content anonymously, including text, images and videos. Users can also comment on other users' content.

The service has a user reporting system, and all reported content is reviewed by human moderators. However, the service has limited resources and it can take some time before content that goes against the forum's terms of service is removed. Very occasionally, the service also reviews content on the service even when it has not been reported.

User reports indicate a substantial number of incidents of content encouraging or assisting suicide being shared. The occasional reviews of content the service undertakes have revealed other instances of illegal suicide content being shared which has not been reported. The provider cannot exclude there are more instances, especially as it has some of the risk factors associated with the encouraging or assisting suicide offence. Despite being a relatively small service, the provider concludes it is high risk for suicide and self-harm, especially considering the content could have a severe impact.

Suicide and self-harm – negligible or no risk

A large vertical search service specialised in travel searches, including for flights and hotels. It has around 10 million monthly UK users. It uses recommender systems, including for suggesting destinations.

It has a basic user reporting system.

There has never been any evidence or suggestion of illegal suicide or self-harm content appearing in search results, and the provider can see no way in which this could ever happen. Even though it is a large service, the provider concludes it has negligible or no risk for suicide and self-harm.