Child rights impact assessment: impact and legal analysis for the development of the CRIA

Hof, S. van der; Challis, L.; Wanroij, E. van; Schermer, B.W.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Children's Rights Impact Assessment

Manual

March 2024

Developed by Leiden University and Considerati,

Commissioned by the Ministry of the Interior and Kingdom Relations

Disclaimer: The translation of the CRIA is solely intended to provide information. The text of the translation is an unofficial translation. The Dutch text of the CRIA is the only authentic and formal text.

Table of contents

Introduction

Are you developing digital services aimed at children or actually accessible to them that allow them to use them? Or are you going to use these services? If so, you must take into account the risks they pose to children, their rights and wellbeing as set out in the UN Convention on the Rights of the Child 1989 (CRC). Keep in mind that even digital services and products that are not used by children themselves can still have an impact on their rights and well-being, for example because children's personal data are processed by the service.[1] In that case, too, it is necessary to carry out a CRIA. The Children's Rights Impact Assessment (CRIA) provides a structured framework to identify and evaluate the potential impact of your digital services on children's rights and well-being.[2]

The CRIA was commissioned by the Ministry of the Interior and Kingdom Relations as a guide for companies, governments and other organisations to take responsibility for safeguarding the rights and wellbeing of children in the digital age. By identifying risks and taking measures to prevent them, negative impacts on children's well-being and development in the digital world can be countered.

This CRIA takes a risk-based approach and provides an opportunity to interpret the risks of digital services to children's rights and well-being while recognising and promoting the benefits of these services.

What is the CRIA?

The CRIA is a tool for arriving at the best possible assessment of the digital service in relation to children's rights and wellbeing. You carry out the assessment during the design and development of the digital service and keep it up to date during the life cycle of the digital service. The main purpose of the assessment is to initiate a measured discussion around the impact of the digital service on children's rights with relevant stakeholders within (and outside) the organisation. The CRIA can also be used as an accountability tool: it shows what choices you have made in identifying and mitigating risks to children. But the emphasis is on the awareness aspect: the CRIA helps you ask the right questions during the development of the digital service and identify risks early on, which you can then mitigate through design changes. Disclosure of the results of the CRIA is encouraged in line with the UN Children's Rights Committee guideline.[3]

The CRIA looks at children's (potential) use of digital services by children through the lens of risks to children's rights and well-being. The classification of risks discussed in Chapter 3 of this assessment is based on scientific research and then linked to children's rights. Risk includes both the possibility of a violation of children's rights and, more specifically, the possibility of harm to children's development and well-being. Thus, the finding that a risk may occur means that children's rights under the UN Convention on the Rights of the Child 1989 (CRC) may be violated. For example, if your digital service entices children to make in-app purchases (a consumer risk), you may be violating the right to privacy and data protection (Article 16 UNCRC, Articles 7 and 8 EU Charter), the right to free, non-commercial play (Article 31 UNCRC) and the right to protection from economic exploitation (Article 32 UNCRC). Children's rights should also be taken into account when determining mitigation measures. For example, measures must be inclusive and must not

[1] Think of student monitoring systems in education, cameras in public places, databases in youth wellbeing or in the police and judiciary with information about children, and parental control tools.

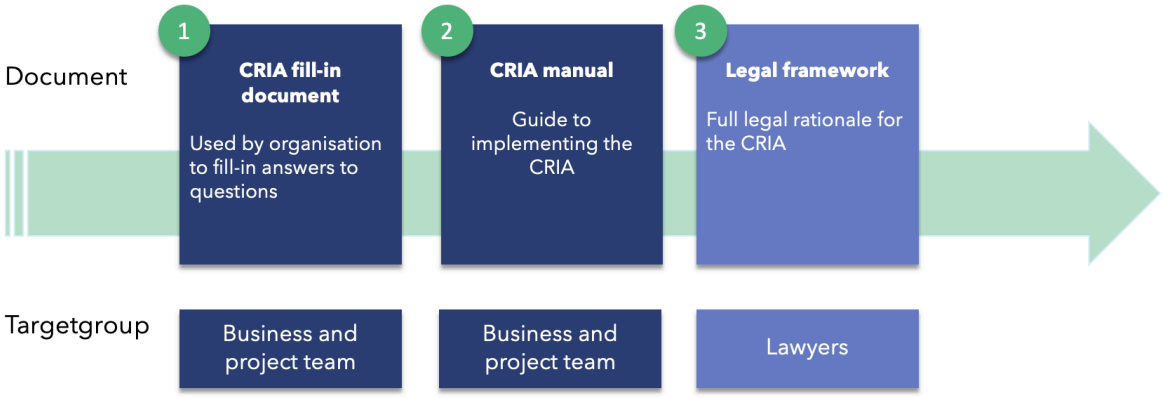
[2] For more background on the CRIA, see Mukherjee, S., Pothong, K., and Livingstone, S., 'Child Rights Impact Assessment - A Tool to Realise Children's Rights in the Digital Environment' (5Rights Foundation 2021) <https://digitalfuturescommission.org.uk/wp-content/uploads/2022/06/Child-Rights-Impact-Assessment.pdf> accessed 27 October 2023.

[3] Committee on the Rights of the Child, 'General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment' <https://digitallibrary.un.org/record/3906061> accessed 28 November 2022, No 38.

unnecessarily restrict children's autonomy and freedoms (consider, inter alia, the right to freedom of information (Article 17 CRC) and the right to freedom of expression (Article 13 CRC).

The CRIA focuses primarily on companies and organisations that design and develop digital services that are accessible to children, or have a potential impact on their rights and well-being. Other parties, such as licensees and clients, can use the CRIA when making an informed choice about purchasing or commissioning digital services. For example, a school purchasing a digital service from a provider can use the CRIA to assess the risks of this service to children's rights and wellbeing. The assessment allows them to ask relevant questions about the operation of and safeguards for children and their rights in a digital service. Digital services not used by children themselves should also conduct a CRIA if the service may nevertheless have an impact on their wellbeing and rights, for example because children's personal data is processed by the service.

The CRIA consists of three parts: a fill-in document, a manual and a legal background document. The fill-in document and the manual are prepared for those implementing the CRIA. You use the fill-in document to provide answers to questions about wellbeing, risks and mitigation measures. The manual (this document) explains each question. Finally, a background document is available with detailed legal information on relevant legislation for the protection of children and their rights when using digital services. This document is intended for legal experts and is not necessary to carry out the CRIA.



The three components of the Children's Rights Impact Assessment

The CRIA and other tools

Various laws and regulations apply to the marketing of digital services that are (potentially) used by children, or may have an impact on their rights and well-being. In addition to this CRIA, it may therefore be necessary to use other tools. We briefly discuss these below.

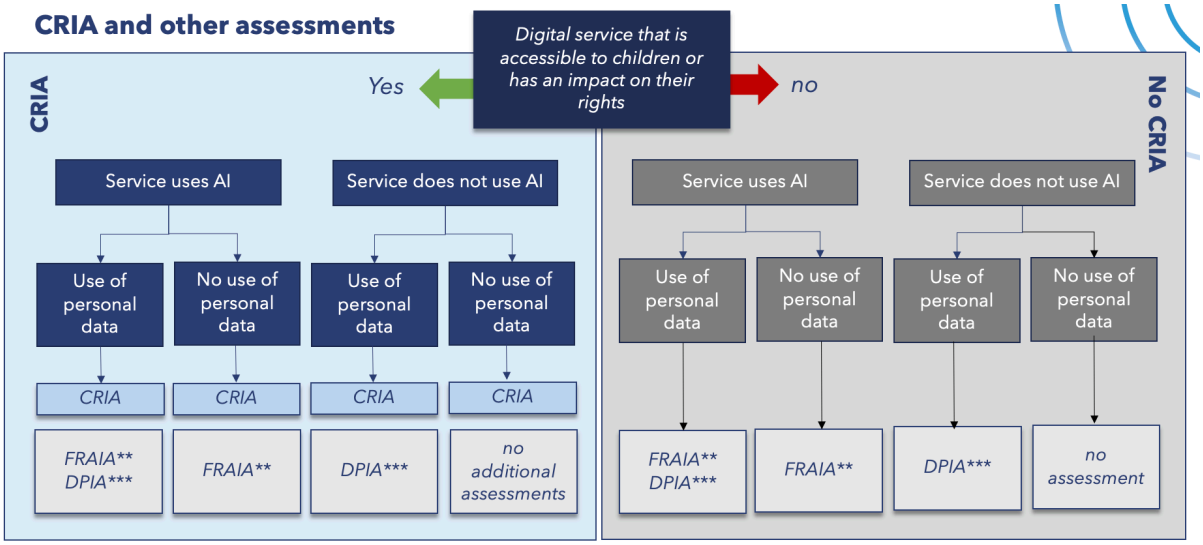
Code for Children's Rights
The Code for Children's Rights Online (CCRO) is a set of principles and guidelines established to protect and promote children's rights in the digital domain. It provides a framework for the responsible design of digital services that ensure children's well-being, development and safety. It is also recommended to consult other resources for age-appropriate design. [4]

[4] In particular, reference is made to: 'IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children' (IEEE) <https://5rightsfoundation.com/static/ieee-2089-2021.pdf> accessed 31 May 2023; CEN/CENELEC, 'Age Appropriate Digital Services Framework', CWA 18016, <https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf> accessed 12 October 2023; 5Rights Foundation and Digital Futures Commission, 'Child Rights by Design' <https://childrightsbydesign.digitalfuturescommission.org.uk/> accessed 27 October 2023.

Data protection impact assessment (DPIA)
A Data Protection Impact Assessment (DPIA) is an assessment conducted to evaluate the privacy risks of a data processing activity. It provides organisations with support in safeguarding the privacy of individuals, complying with the General Data Protection Regulation (GDPR) and identifying mitigating measures for (potential) privacy risks. In some respects, the CRIA overlaps with the DPIA in assessing privacy risks. While the DPIA looks in detail at the personal data being processed, the CRIA pays attention to all potential risks to children and safeguarding children's rights and wellbeing. The CRIA and DPIA can be carried out in an integrated manner. The CRIA clearly indicates which questions appear in both assessments or partially overlap, so that answers can be reused.

Fundamental Rights and Algorithm Impact Assessment (FRAIA)
An Fundamental Rights and Algorithm Impact Assessment (FRAIA) is an assessment conducted to evaluate the potential impact of algorithms on human rights. It aims to identify potential risks of algorithmic systems that may affect rights such as privacy, non-discrimination, freedom of expression and equal treatment. While the objectives of the FRAIA are similar to those of the CRIA, namely to identify the risk of violation of rights, the FRAIA focuses specifically on human rights and algorithms and the CRIA on children's rights and online risks, including algorithms.

Figure 2 shows when the different assessments, namely CRIA, DPIA and FRAIA, should be carried out or combined.



** Personal data of children need additional safeguards. These are partly captured in a DPIA*
*** IAMA only mandatory for governments for the time being. In case of High-risk AI systems possibly also conformity assessment*
**** Do a pre-scan first to see if a DPIA is necessary*

The CRIA in relation to the DPIA and FRAIA

When do you conduct a CRIA?

Now that we have discussed the broader context of a CRIA, it is equally important to know when such an assessment is most effective. This includes the best moment to conduct the CRIA, but also the delineation of the digital services to which the CRIA applies.

Within the scope of the CRIA are digital services that are specifically developed for children, that are accessible to children, and that are (potentially) used by children, even if they are not specifically targeted at children. Digital services also fall within the scope of the CRIA when they are not used by children but may nevertheless have an impact on their rights and well-being. These are generally so-called information society services.[5] This includes all commercial services

[5] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015L1535&qid=1686150727253

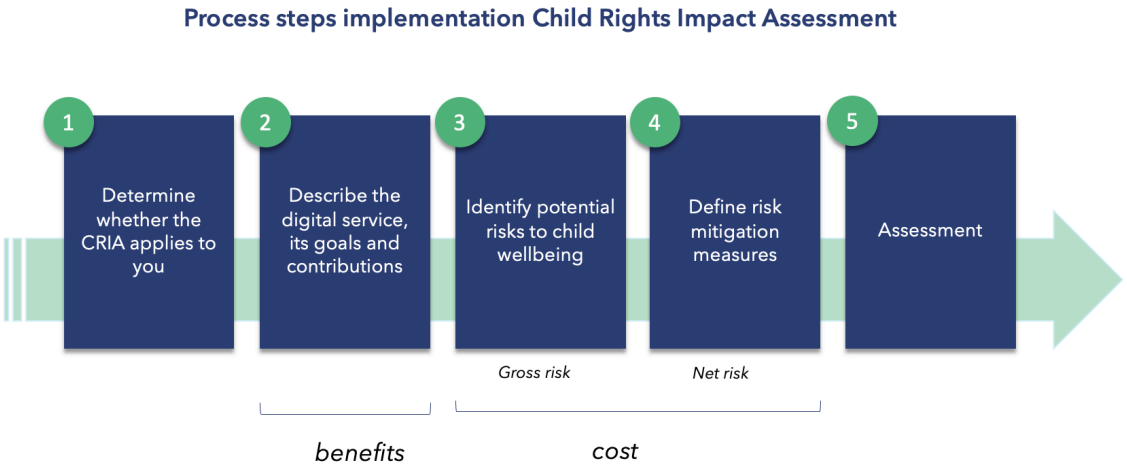
that use digital technology in any way, such as apps, games, websites and online platforms. In this assessment, we define children as persons under 18 years of age.[6] Specific age groups are taken into account when considering impact. Indeed, depending on children's development and age, the risks of the digital service may differ. If the digital service is not accessible to children *and* children do not use it, it is not necessary to conduct a CRIA.

Initially, it is advisable to conduct the CRIA during the design or development phase. That way, the CRIA can help guide decisions on service functionalities.
To extract valuable information from the implementation of a CRIA, it is important that the application and scope are already sufficiently clear. If the ideas are still very broad or general, and the application is not yet concrete, it can be difficult to determine what the impact on a child and their rights will be.

An example. Suppose you want to develop a child-friendly social media app, but don't yet know exactly what it will look like. You will develop this in a research and design phase. For effective implementation of a CRIA, it may then be too early. Indeed, to foresee impact on the child and their rights, it is necessary that you already have a more concrete picture of exactly what the app will look like. What is the goal? What is the intended target group? What type of content will it be about? Who will have access? What does the revenue model look like? What technology will be used? Et cetera. The trick is to carry out the CRIA at the moment when the application is already sufficiently concrete, but there is still room to adjust and fine-tune its design.[7]

In addition, it is essential to keep reviewing the service against the principles of the CRIA during its lifecycle. This is particularly necessary when there is a substantial change, such as adding or extending a key functionality. It is also advisable to carry out periodic reviews, for example once every two years, to check whether the risk assessment is still up to date.

Process for implementing the CRIA



Process steps for CRIA implementation

The CRIA consists of five parts. In part 1, you establish whether conducting a CRIA makes sense for you. In part 2, you describe the digital service on which the CRIA is focused and set the objectives. This gives you a concrete overview of the benefits or revenues of the digital service. In part 3, you identify the potential risks of the digital service. In part 4, you then identify the risk mitigation measures you will take. These 4 steps give you an overview of both benefits and

[6] See Article 1, CRC.
[7] However, in the early stages of digital service design, you can already use the Children's Rights Code that is specifically designed to give direction on the design of child-friendly apps.

potential costs. Finally, the last section is about balancing these costs and benefits. This is called the proportionality test.

The CRIA is a tool that can be used to facilitate discussion and decision-making. The discussion on the different questions should take place in a broad-based team in which people with different specialisations and backgrounds participate. For each digital service, it may differ which roles should logically provide input.

When discussing the questions in the CRIA, at least the following types of roles should be present:

- The client of the project. Someone who has a good understanding of why the digital service is being developed and its importance.
- Someone with a technical background. For example, a developer, data scientist or an engineer. This person understands how the digital service is put together and how any mitigating measures can be implemented.
- A lawyer, data protection officer and/or ethical advisor who can provide input on legal and social considerations and interests.

It is also advisable to have someone participate with domain knowledge in the area where the digital service will be deployed. For example, when designing a digital service aimed at education, it is important to involve a person who has domain knowledge and expertise in education.

Implementing the CRIA requires the use of an interdisciplinary team, within which there is knowledge of children's rights, and social and developmental psychology. It is also necessary to consult children, parents and relevant interest groups to identify risks to children's rights and well-being and to evaluate the effectiveness and user-friendliness of risk mitigation measures.

1. Preparations

The questions in this section aim to determine whether conducting a CRIA is necessary for your service.

1.1 *Do you offer or use a digital service*

'Digital services' refers to all services that use digital technology in any way, such as apps, games, websites and online platforms. The services covered by the CRIA are so-called information society services. This includes all digital services that children could potentially use, even if not explicitly targeted at children, or services that could otherwise impact children's rights and wellbeing.

- *If you answer 'yes' to the question, proceed to question 1.2.*
- *If the answer is 'no', then the CRIA does not apply to you.*

1.2 Is the digital service actually accessible to or deployed to persons under 18 years of age?

The CRIA applies to digital services that are actually accessible to persons under 18 or otherwise have a potential impact on their rights or well-being. Specific legal safeguards for children must be taken into account if a digital service is actually accessible to children or targeted at them. Even if children are not the target audience of your service, the legal safeguards for children apply if they can actually use it or it is targeted at children.

- *If you answer 'yes' to the question then it is advisable to carry out a CRIA.*
- *If the answer is 'no', the CRIA may not apply, but go to question 1.3 to be sure*

1.3 Can you demonstrate that the service will not be used by persons under 18 years of age or it will not be used with respect to persons under 18 years of age?

If the answer to the previous question is 'yes', and the digital service is only intended for or used with respect to persons aged 18 and over, then the specific safeguards do not apply and no CRIA needs to be carried out. However, it is then important that you can demonstrate with a demonstrably adequate age verification method that persons under 18 do not (and cannot) use the digital service. 'Demonstrably adequate' means that the method used is demonstrably capable of admitting only users based on the attribute '18 years and older'. Such a method is called age verification and includes techniques that can determine with a high degree of certainty whether a person has reached the required (legal) minimum age (e.g., 18 years and older) for a digital service. When determining the age verification method, it should be considered whether it is effective in view of the objective to be achieved (e.g. meeting a legal minimum age for a digital service or part thereof) (proportionality principle) and whether it is the method that least infringes users' rights (subsidiarity principle). The latter aspect takes into account certain (legal) requirements, including data protection, security, transparency, inclusiveness and user-friendliness.[8] Methods such as 'self-declaration' (users themselves provide their age or date of birth) and 'age estimation' (age is estimated on the basis of biometric characteristics and/or behavioural data) are not in themselves demonstrably adequate for this purpose. Keep in mind that if you conclude that a CRIA is not necessary, it may still be the case that a DPIA or an FRAIA is.

[8] For minimum requirements, see: CEN/CENELEC, 'Age Appropriate Digital Services Framework', CWA 18016, <https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf> accessed 12 October 2023.

2. Objective

This section focuses on the purpose of the digital service. When considering whether the development and deployment of the digital service are proportionate, it is important to get a clear picture of what the digital service will look like and what the specific goals and intended effects are. This seems very straightforward, but in many cases one finds out during the write-up that there are still ambiguities or that certain aspects have not yet been specifically considered. Questions 2.1 to 2.4 help you describe the digital service as concretely as possible. This helps to then properly assess the risks. Questions 2.5 to 2.14 can help to get the goals as sharp as possible.

In short, in this section you describe the digital service, the goals of the service and the benefits for the child and the organisation.

Description digital service

2.1 Give a description of the digital service.

Give a description of the digital service here. In order to assess possible risks, it is necessary to properly describe what the digital service entails. In the answer, also explain how the idea for the service came about and what the rationale is.

2.2 What technology will be used to realise the digital service?

Describe what technology is used and, if relevant, how the digital service interacts with other technologies or systems. Some risks arise from the use of (new) technologies, such as recommendation systems and biometrics. If the service uses artificial intelligence, it may be advisable to conduct the CRIA in conjunction with the Fundamental Rights and Algorithms Impact Assessment (FRAIA).[9] Also mention here technologies used or to be used in the digital service that are obtained from third parties.

2.3 What is the scope of the service?

What is the time and period in which the digital service will be provided? What is the region? How large is the group of people who will (potentially) use the service?

2.4 Who is the target audience?

Describe who the target audience is for the digital service. Try to make this as specific as possible. If children are (partly) the (direct or indirect) target group, indicate which age groups.

Description of the purpose of the digital service

2.5 What is the goal to be achieved by using the digital service? What is the main goal and what are sub-goals?
This question is related to question 1.1.2 from the FRAIA

These are the organisation's goals. It is important here to describe the purpose of using the digital service as concretely and specifically as possible. Moreover, any commercial goals should be made

[9] The FRAIA was developed primarily for governments. Obligation of this tool has not yet been formally regulated. However, a motion has been passed in the House of Representatives to make the tool mandatory for governments. In addition, the implementation of a Fundamental Rights Impact Assessment for high-risk applications of AI is also mentioned in the European Parliament's AI Regulation proposal. If adopted, such an obligation would also apply to private organisations.

transparent here. In addition, it makes sense to rank goals. In most cases, there are more goals. What are the most important goals and why?

2.6 Is the digital service to be provided an effective means of achieving the stated objectives? Explain.

In the final proportionality assessment, it is important to determine whether a service is effective (see also the FRAIA and DPIA). Indeed, if the service is not effective, it is probably not necessary. If a service is not effective *AND* there may be a violation of children's rights, provision of this digital service may be problematic.
If you are yet to develop the digital service, answering this question requires estimation.

2.7 When is the digital service a success? How and when do you measure this? (e.g. after 1 month or 2 years?)
This question is related to question 12, phase 1 from the Handbook on non-discrimination by-design

If you have yet to develop the digital service, answering the previous question requires foresight. That can be tricky. Therefore, it is also important to think about how you can measure the success of the service concretely. This question is about determining how the goals can be made measurable so that you can monitor whether your digital service is effective even at a later stage.

Description contribution to children's wellbeing

For the final proportionality assessment, it is important to properly identify how the digital service contributes to children's wellbeing and thus contributes more broadly to the realisation of their rights. UNICEF's Responsible Innovation in Technology for Children (RITEC) framework[10] provides guidance on this. To make the framework more accessible, we have explained the values. The original values can be found in the report.[11] Children can be involved in specifying the values or testing the digital service against these values.

- *Note: During the process of completing contributions, it is very likely that discussions on potential risks are already taking place. It is advisable to fill these in directly in section 3 Risks.*

2.8 In what ways does the digital service provide a sense of purpose, and does it contribute to their self-esteem?

This question was formulated using the value **self-actualisation**. In UNICEF's research, children indicated that a sense of meaning and self-worth is key to well-being, and this is supported by good online (play) experiences. A digital service can foster this kind of positive experience by offering useful content that inspires and activates children. What constitutes useful content may vary from person to person and cannot be determined in its generality. Certain types of content, such as 'DIY tutorials', are examples of inspiring and activating content. 'DIY-tutorials' are popular short videos with step-by-step instructions to make or craft something yourself. In addition, informative content, for example LGBTQIA+ content, can be important for self-acceptance, self-development or awareness-raising.[12] If risks come up during the discussion, pre-fill them in Chapter 3 on risks.

[10] https://www.unicef-irc.org/ritec
[11] Responsible Innovation in Technology for Children. UNICEF Office of Research - Innocenti, Florence, 2022.
[12] Berger, M.N., Taba, M., Marino, J.L., Lim, M.S.C., Skinner, S.R. (2022). Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review. J Med Internet Res. 2022 Sep 21;24(9):e38449. doi: 10.2196/38449. PMID: 36129741; PMCID: PMC9536523.

- *Most relevant children's rights: right to development (Article 6 CRC), right to access non-harmful information and the media (Article 17 CRC), right to health (Article 24 CRC), right to play and recreation (Article 31 CRC).*

2.9 *How does the digital service contribute to a sense of control and learning to make choices*?

This question is formulated using the value of **empowerment**. Children may lack control over their daily activities. Digital services provide opportunities for children to have that say, developing a sense of autonomy and control. For example, children can make choices about what content they share how, where and with whom and then receive positive feedback through *likes* and *comments*. In addition, children can gain control over the shaping of, and access by others to, their online identity. Empowerment is especially important also with digital services that children do not use themselves but have an impact on them and their rights (think of a student tracking system). Being able to influence what content they get to see is also an important form of empowerment. This includes being able to avoid content that is potentially harmful to their age group, such as pornographic, frightening or violent material. If these risks arise during the discussion, fill them in in advance in section 3 on risks.

- *Most relevant children's rights: right to development (Article 6 UNCRC), right to be heard (Article 12 UNCRC), right to freedom of expression (Article 13 UNCRC), right to freedom of thought (Article 14 UNCRC), right to privacy (Article 16 UNCRC), right to access to non-harmful information and the media (Article 17 UNCRC).*

2.10 How does the digital service encourage children's curiosity, openness to new experiences and creative skills?

This question is formulated using the value **creativity**. Creativity is an important quality that strongly overlaps with learning. Children have many examples of how digital experiences can enhance their creativity. Digital services offer them numerous opportunities for creative expression and act as inspiration for children. However, research shows that it is precisely from moments of boredom that creativity and creative activity often emerge,[13] which seems at odds with the nature of digital services that counter boredom through entertainment and distraction. Therefore, clearly differentiate how your service does and does not contribute to creativity. Are there any risks discussed with this question? If so, complete them in advance in section 3 on risks.

- *Most relevant children's rights: right to development (Article 6 CRC), right to freedom of expression (Article 13 CRC), right to freedom of thought (Article 14 CRC), right to access non-harmful information and the media (Article 17 CRC), right to play and recreation (Article 31 CRC).*

2.11 How does the digital service contribute to how children perceive their own skills?

This question is formulated using the value **competence**. A digital service influences how children perceive their own skills and competences. For example, a digital play experience can increase their ability to perform a task, gain new knowledge and solve problems. Of course, it can also work in the other direction, where a digital service makes the child feel incompetent, which has a negative effect on self-esteem. This can be caused, for example, by a child-unfriendly User Experience (UX) design (such as misleading or manipulative design) or the lack of different difficulty levels in a video game. This value also includes providing information relevant to children

[13] Gasper, K. & Middlewood, B. L. (2014). Approaching novel thoughts: Understanding why elation and boredom promote associative thought more than distress and relaxation, Journal of Experimental Social Psychology, Volume 52, 2014, pp. 50-57, ISSN 0022-1031, https://doi.org/10.1016/j.jesp.2013.12.007.

(such as privacy statements or ways to report harmful content) in a way that is recognisable, accessible and understandable to them.

- *Most relevant children's rights: right to development (Article 6 CRC), right to access non-harmful information and the media (Article 17 CRC), right to education (Articles 28 and 29 CRC), right to play and recreation (Article 31 CRC), right to protection from economic exploitation (Article 32 CRC).*

2.12 How does the digital service enable children to prevent or reduce feelings of stress by providing positive forms of peace, calm and escapism?

This question is formulated using the value **emotional regulation**. By providing positive forms of rest, calm and escapism, children can de-stress and then reconnect with peers and the world. Using a digital service can ensure that a child has a chance to escape reality for a while and enjoy the 'standstill of time' or *downtime*. However, some digital services are addictive in nature, preventing a child from detaching from the screen and allowing unhealthy use to take over. Consider carefully here whether your digital service offers healthy escapism. Are there any risks discussed with this question? If so, complete them in advance in section 3 on risks.

- *Most relevant children's rights: right to development (Article 6 CRC), right to access non-harmful information and the media (Article 17 CRC), right to play and recreation (Article 31 CRC), right to protection from economic exploitation (Article 32 CRC).*

2.13 In what ways does the digital service facilitate making safe connections with peers, family or other important people in their lives?

This question was formulated using the value **social connection**. Children in all consultations highlighted social connection as the key to their well-being. Analysis of the survey data showed that social connectedness is important for wellbeing constructs, such as a sense of belonging, stronger relationships and self-confidence. The aim of many digital services is to facilitate social connection. To make an actual contribution to the wellbeing factor of social connectedness, secure connections must be provided. These are connections aimed at promoting educational activities, creative interactions and positive social exchanges between children of similar ages. Therefore, carefully consider how your digital service contributes to **safe** social connections. Are there any risks discussed in this question? If so, complete them in advance in section 3 on risks.

- *Most relevant children's rights: right to development (Article 6 CRC), right to association (including social interaction (Article 15 CRC), right to privacy (Article 16 CRC), right to protection from (psychological) violence (including bullying) (Article 19 CRC), right to protection from sexual exploitation (Article 34 CRC).*

2.14 How does the digital service ensure an accessible, diverse and inclusive user experience?

This question was formulated using the values of **diversity, equity and inclusion**. Inclusive digital experiences enable children from different backgrounds and contexts to participate in a digital service while respecting human rights and ethical values. For example, providing translation options or subtitles makes a digital service more inclusive for children who do not speak the dominant language (often English) or are hearing impaired. In addition, representative content can create a respectful environment that contributes to these values. Here, it is also important that a digital service has a reporting system that is recognisable, accessible and understandable to children, so that users can effectively report discriminatory or hateful content. Are there any risks discussed with this question? If so, complete them in advance in section 3 on risks.

- *Most relevant children's rights: right to non-discrimination (Article 2 CRC), right to development (Article 6 CRC), right to be heard (Article 12 CRC), right to access non-harmful information and the media (Article 17 CRC), right to protection from (psychological) violence (including bullying) (Article 19 CRC).*

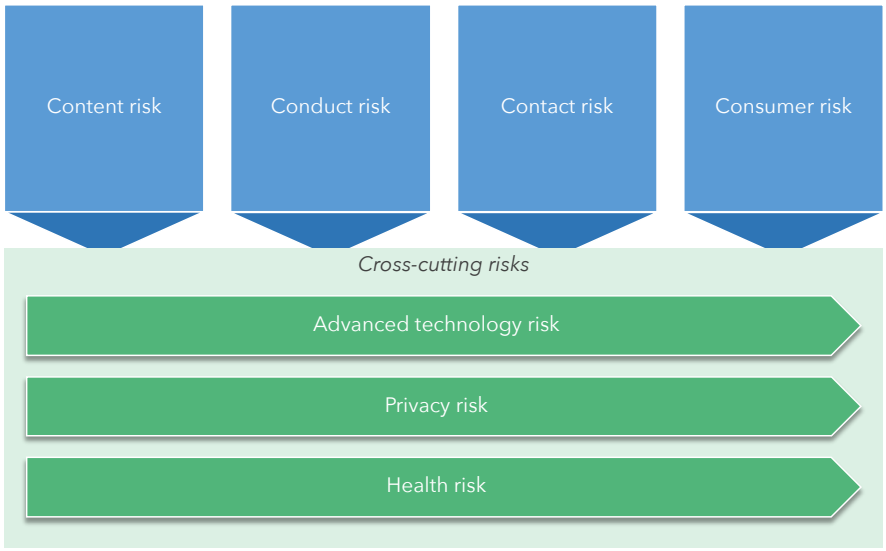
3. Risks

In section 2, the digital service where the CRIA is applied is defined and delineated as concretely as possible. In addition, the goals have been circumscribed. This gives a picture of the (possible) *benefits* of the digital service, both for the organisation and for the child. Besides the benefits, it is also important to look closely at the possible *costs*. In developing the CRIA, a risk-based approach was chosen. This means looking specifically at known types of risks when children use digital services.

General explanation of risks
Impact Assessments are useful tools because they help you identify the risks of your digital service. Recognising the risks is the first step in eliminating or reducing the risks through risk mitigation measures. In your CRIA report, you document this entire process. The report shows that you have been careful in developing your digital service. If you fail to identify risks and cannot justify why you made certain design choices, children are more likely to be harmed and have their rights infringed. Failing to do a proper impact assessment thus increases the likelihood of liability.

The negative impact of digital services may involve risks and impacts that actually harm children, but it is not necessary for the harm to actually occur. In children's law, the so-called *precautionary principle* applies. This means that companies (and others) must refrain from activities that may have harmful effects on (groups of) children. Indications of the existence of those consequences are sufficient (and definitive proof of harm is not necessary). The CRIA uses a risk classification developed in media studies. The risk classification includes content risks, conduct risks, contact risks, consumer risks (the so-called 4Cs) and cross-cutting risks, namely advanced technology risks, health risks, privacy risks.[14]

The categories (the Cs) are a tool for thinking about risks to children. Keep in mind that risks do not always fall exactly into one of the defined categories. Some risks fall outside the categories or into more than one category. Further, bear in mind that risks may change in nature and severity over time. Therefore, carefully monitor the use of your service and perform a CRIA again when your service changes substantially (e.g. by changing or adding a functionality).



[14] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/ docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E; Livingstone S and Stoilova M, 'The 4Cs: Classifying Online Risk to Children' (Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI) 2021) <https://www.ssoar.info/ssoar/handle/document/71817> accessed 28 November 2022.

Figure 1: Risk classification

Using the questions in Chapter 3, you will identify where potential risks may arise when children use your digital service or it is used with them.

- *Note: You may have identified risks early in the project. You may have already taken risk mitigation measures. When applying the CRIA, it is important to base the following questions on the situation* **before** *these measures were taken. This is called the gross risk. Mitigating measures are explicitly addressed in part 4 of the CRIA. Gross risk together with the mitigating measures taken then form the net risk (also often called the 'residual risk').*

All questions in this section have the same structure. First, you are asked to describe the risk. Next, you are asked to give a risk assessment. Here it is important to ask the question: what is the probability of the risk occurring and then what is the impact or severity of the risk *if* it occurs.

To estimate residual risk, it makes sense to follow the following matrix (see Figure 5). This means that you look, on the one hand, at the *probability* of a particular risk occurring and, on the other, at the *impact* on children if a risk actually occurs.

For example, you could say that the *chances* of a child using a digital service may be small, but the *impact* if it does happen is very high (e.g. the risk of exposure to harmful or illegal content).

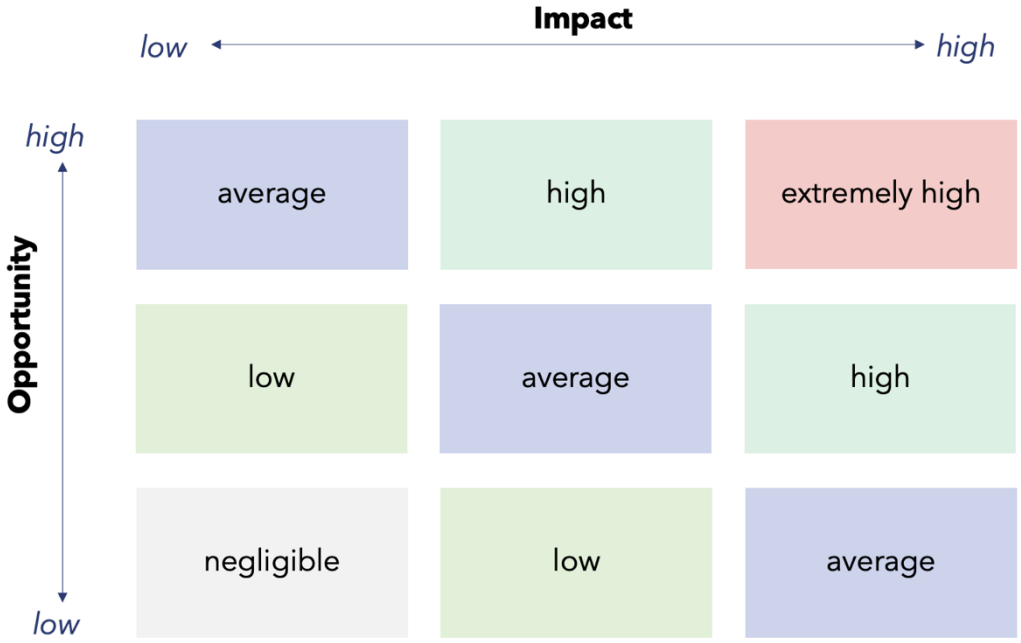


Figure 2 Risk matrix

The overall estimate for the risk is then based on the formula probability x impact. When in doubt about the exact risk estimate, for example because it lies exactly between two categories, always assume the highest risk.

For support in assessing risks, it may be useful to consult those affected or their representatives.

- *Note: In cases where a third party is responsible for developing your digital service, it remains essential to carefully consider the risks and provide a rationale for using this software.*

An example

Question: what risks can (underage) children create for third parties when using the digital service (conduct risk)?

Sample answer: *It is a public platform so there is a possibility of children uploading content that is harmful to other children. For example, consider a choking challenge. There is a chance of such a thing happening, but we see that the vast majority of users do not post this kind of content. However, the impact if it does happen can be significant, as the reach is potentially large, children are susceptible to this kind of challenge and it can lead to health risks or worse. This can be dangerous and is therefore undesirable.*

Opportunity	*Impact*	*Risk assessment*
Average	**High**	**High**

- *Note:The risk assessment in this section does not yet assume management measures. These are explicitly discussed in section 4.*

Notes to questions

3.1 ***Content risks:*** *What (potential) risks exist for children to be confronted (unexpectedly and unintentionally) with content potentially harmful to them when using the digital service?*

Content risks (or risks related to content) include situations where children are exposed to potentially harmful content.[15] This includes various scenarios where the child passively receives or is exposed to content that is available to all (internet) users. This content may be illegal, hateful and potentially harmful. It is important to emphasise that applications that facilitate the use of an online application, such as Youtube and chatbots, may also pose this type of risk. [16]

Young people point out that on online platforms, content warnings are not always given now. And if they do, the warning is only displayed very small, making it insufficiently visible. They wonder why there is no Kijkwijzer[17] for digital services. Children now see very violent images. Harsh examples cited by young people include people dying from challenges, severed limbs and a man shooting himself to death. Children become jaded from an early age as a result.[18]

[15] The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No.: . doi:10.1787/5kgcjf71pl28-en.
[16] Consider online teaching tools here, for example,
[17] The Dutch age classification system for audiovisual media.
[18] In collaboration with UNICEF Netherlands and the Foundation 'Discussiëren kun je leren', a youth consultation on children's rights in the digital environment was organised on 2 September 2023. Young people between 10 and 17 years old participated in the consultation. Insights from the discussions with them were incorporated as text boxes in the explanation of online risks.

Illegal content refers to material prohibited by law to protect all citizens, including children. Examples include distribution of child pornography, incitement to hatred, violence or terrorist activities. Such content poses a serious threat to the safety and well-being of children.

There is also hate content. This can take various forms, including text, visual or audio material, games and other media. Hate content can stem from prejudice based on a person's religion, race, gender, disability, sexual orientation or gender identity. [19]

Harmful content refers to content that is not illegal per se, but still poses a risk to children because of the potential negative impact on their health and well-being. This includes violent, frightening, pornographic and discriminatory content, as well as content that encourages an unhealthy lifestyle or behaviour, such as alcohol and drug use. It is important to note that the extent to which this content is harmful can vary depending on individual children and their age.

In the Netherlands, harmful and illegal content is regulated in part by the Media Act. Part of the Media Act is implemented by NICAM, which uses Kijkwijzer to inform children and parents about the harmfulness of certain age-based content.[20] With the introduction of Kijkwijzer Online, Dutch uploaders on video platforms must also share this information with their audience if their content contains harmful elements. [21]

For games, there are similar systems such as PEGI for game consoles in Europe[22] and IARC for (game) apps in app stores worldwide. [23] These systems help parents and children assess the harmfulness of games based on age categories and content ratings.

It is important to note that even if the content itself is not illegal, such as extreme scenes of violence or explicit pornography, granting children access to the most harmful content should be subject to strict measures. This may include, for example, age verification or parental controls to ensure that children do not access such content that may harm their well-being.

In addition, advertising for products that can lead to unhealthy lifestyles, such as unhealthy food and alcoholic beverages, is restricted in relation to children. Self-regulatory measures often apply to advertisements. Another category concerns advertising for gambling, where it is prohibited to target children and possibly young adults, as gambling for children and sometimes young adults is prohibited in many countries.

In addition, there is content that is potentially harmful to children, but against which the law offers no (clear) protection. This includes potentially harmful content that is not audiovisual in nature (and therefore not covered by the Media Act) or content with commercial purposes. These include disinformation, non-illegal hate content, misleading information or unhealthy information. The latter includes encouraging children to engage in extreme sports, unhealthy eating behaviour or other dangerous behaviour.

Fake news or disinformation is seen by young people as a major problem of digital services. Both online platforms and influencers play a role in spreading it. It is difficult for them to distinguish fake news from real news. They also see that disinformation has a negative impact on society. For example, it can lead to extremism.

[19] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/ docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E.
[20] NICAM. Kijkwijzer. [cited 22 March 2023]. Available: https://www.kijkwijzer.nl/.
[21] NICAM. YouTube viewing guide. [cited 22 March 2023]. Available: https://nicam.nl/news/kijkwijzer-online-start-dit-autumn-1.
[22] Pan European Game Information (PEGI). In: Pan European Game Information (PEGI) [Internet]. [cited 22 March 2023]. Available: https://pegi.info/.
[23] International Age Rating Coalition (IARC). In: International Age Rating Coalition (IARC) [Internet]. [cited 22 March 2023]. Available: https://www.globalratings.com/.

- *Most relevant children's rights: right to development (Article 6 CRC) right to access non-harmful information and the media, including protection from harmful content (Article 17 CRC), right to health (Article 24 CRC).*

3.2 ***Conduct risks:*** *what (potential) risks could arise for third parties from children's behaviour when using the digital service?*

Behavioural risks include situations where children engage in behaviour that poses risks to themselves or others, and which require attention when developing digital services to protect children.[24] Such behaviour may involve posting illegal, hateful or harmful content. Children may also be involved in other problematic behaviour, such as participation in online challenges. An example of such a dangerous challenge is the 'choking challenge', in which teenagers (and sometimes young children) squeeze their throats until they almost pass out, as this would give a feeling of euphoria.[25] This act is often filmed and shared online, giving other children the idea to try this too. However, participating in this 'game' can lead to serious brain damage or even death for children.[26]

Another behavioural risk for children is engaging in online activities that could be considered child labour, such as underage creators, influencers or e-sports enthusiasts.[27] This can lead to children spending a lot of time doing this work, which can be detrimental to their school performance, social activities and can lead to stress. Although making money by children does not necessarily mean economic exploitation, there is a legal ban on child labour in the Netherlands. However, laws regulating child labour may not apply to online child labour as there is usually no employment relationship.[28] Online platforms can teach parents and children how children can safely and responsibly engage in commercial activities online.[29]

Young people are very critical of vlog families. Small children do not understand what social media is. Therefore, they cannot decide if they want to join family vlogs. Teenagers may be better at that. But later you may regret vlogs. Besides, it takes kids a lot of time. Young people are also critical of parents who make family vlogs. They use their children to make money.

- *Most relevant children's rights: right to health (Article 24 CRC), right to play and recreation (Article 31 CRC), right to protection from economic exploitation (Article 32 CRC), right to protection from sexual exploitation (Article 34 CRC).*

[24] The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No.: . doi:10.1787/5kgcjf71pl28-en.
[25] Hof S van der, Lievens E, Milkaite I. The protection of children's personal data in a data-driven world: A closer look at the GDPR from a children's rights perspective. In: Liefaard T, Rap S, Rodrigues P, editors. Monitoring Children's Rights in the Netherlands: 30 Years of the UN Convention on the Rights of the Child. Leiden University Press; 2019.
[26] Youth and Media Agency. Information on the "choking game". Available: https:// www.bureaujeugdenmedia.nl/informatie-choking-game-wurgspel/.
[27] Verdoodt V, van der Hof S, Leiser M. Child labour and online protection in a world of influencers. The Regulation of Social Media Influencers. Edward Elgar Publishing; 2020. pp. 98-124.
[28] Verdoodt V, van der Hof S, Leiser M. Child labour and online protection in a world of influencers. The Regulation of Social Media Influencers. Edward Elgar Publishing; 2020. pp. 98-124.
[29] In France, this is regulated by law, see LOI n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne.

3.3 ***Contact risks:*** *what (potential) risks are there in the design and use of the digital service for children in their interaction with third parties?*

'Contact risks' include situations where children are at risk during their interaction with others.[30] This can include sexual abuse, such as online grooming, sextortion and sexual abuse via webcams. It may also include cyberbullying, hateful or otherwise harmful behaviour by others, such as trolling, doxing, sharing revenge porn, discrimination and extremism. In addition, online fraud practices also fall under 'contact risks', such as phishing, WhatsApp fraud, Marketplace fraud and identity fraud.

Cyberbullying is something young people find very unpleasant. Because it happens online, you take it home and even into your bedroom via your smartphone. Others call you, for example, and scold you. It invades your private sphere. It can make you feel very lonely.

Children engaging in commercial activities online (see behavioural risks in section 3.2) may also face 'contact risks' when streaming or publishing their activities online. An example is making money as a streamer on platforms such as Twitch, where viewers can make donations while the streaming gamer is playing. In these situations, children may face special requests as a streamer, such as engaging in seductive behaviour.[31]

In the latter case, economic exploitation (engaging or facing commercial activities that are harmful or abusive to the child) may coincide with sexual exploitation of the child. It is important to recognise these risks and take appropriate measures to protect children.

- *Most relevant children's rights: right to protection from violence (Article 19 CRC), right to protection from sexual abuse (Article 34 CRC), see also Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.*

3.4 ***Consumer risks:*** *what (potential) risks are there in the design and use of the digital service for children in their capacity as consumers?*

'Consumer risks' include situations where children are at risk as consumers.[32] In general, digital services that children can use are almost always offered commercially, which means that children are automatically considered consumers. Consumer risks can occur in the form of contract risks.[33] This occurs when children have the ability to enter into contracts with the digital service provider or third parties. Most legal systems require parental consent for in-app purchases or other types of agreements entered into by children. Consumer risks can also come in the form of unfair commercial practices, such as enticing or forcing children to make in-app purchases they do not

[30] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/ docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E.

[31] D'Anastasio C. Children Stream on Twitch-Where Potential Predators Find Them. Wired. 30 Jul 2020. Available: https:// www.wired.com/story/children-stream-twitch-potential-predators-exploitation/. Accessed 1 Sep 2021 & National Center on Sexual Exploitation. Amazon's Twitch Rife with Sexual Harassment, Predatory Grooming, Child Sexual Abuse. In: https:// endsexualexploitation.org [Internet]. Mar 2021 [cited 30 Mar 2023]. Available: https://endsexualexploitation.org/articles/ amazons-twitch-rife-with-sexual-harassment-predatory-grooming-child-sexual-abuse/.

[32] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E & The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Paris: OECD; 2011. Report No: . doi:10.1787/5kgcjf71pl28-en.

[33] Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children.* (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817.

actually want, or using virtual currency where the true value of virtual items is not always clear.[34] We call this misleading or manipulative design ('deceptive design' or 'dark patterns'). For example, when a consumer visits a price comparison site, they are asked to enter data during the ordering process. The consumer is given the choice to agree, but in these windows, one notices that the 'yes' button is coloured bright red, while the ''no' button is bright green. The manipulative button colours encourage an action that the consumer does not actually want.[35]

Young people wonder why companies pressure children in games and other apps. This happens, for example, in TikTok battles where children have to acquire TikTok 'coins' to buy 'gifts'. They donate these 'gifts' to TikTok players who compete against each other so that the one with the most 'gifts' wins. If you give a lot of 'gifts' as a viewer, you get a 'shout out' (a TikTokker calls your name) and some children feel pressure to participate. It can cost them a lot of money.

There may also be digital services similar to (online) gambling, such as loot boxes or games that contain casino elements, such as Coin Master.[36] Consumer risks may also arise in the form of unlawful processing of personal data or online profiling of children for commercial purposes. Data protection law offers children a higher level of protection when their personal data is processed, and digital service providers should take this into account when children use their services.[37] Moreover, information about children's personal data processing should be shared with them in an understandable way.[38]

Young people feel that online gambling or mechanisms similar to it (such as loot boxes, black jack or casino elements in games and apps) do not belong in digital services used by children. It is addictive and can cost children a lot of money. You lose more than you win. Winning a prize gives a positive feeling. But companies should not charge money for it.

In addition, marketing activities aimed at children can pose risks. Not only advertising[39] , but also online marketing[40] , such as native marketing, influencer marketing and advergames[41] , can have a negative impact on children's well-being.[42] Buying products online that are unhealthy or

---

[34] Consumer and Market Authority (2023). Protecting the Online Consumer: *Limits to online influence*. Available: https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf; van der Hof S, van Hilten S, Ouburg S, Birk MV, van Rooij AJ. "Don't Gamble With Children's Rights"-How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment. Frontiers in Digital Health. 2022;4.

[35] Consumer and Market Authority (2023). Protecting the Online Consumer: *Limits to online influence*. Available: https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf.

[36] See https://www.coinmastergame.com/.

[37] Hof S van der, Lievens E, Milkaite I. The protection of children's personal data in a data-driven world: A closer look at the GDPR from a children's rights perspective. In: Liefaard T, Rap S, Rodrigues P, editors. Monitoring Children's Rights in the Netherlands: 30 Years of the UN Convention on the Rights of the Child. Leiden University Press; 2019. - Lievens E, Verdoodt V. Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. Comput Law Secur Rep. 2018;34: 269-278. - Van der Hof S, Lievens E, Milkaite I. The GDPR and Children's Personal Data. Oxford Encyclopedia of EU Law (OEEUL). Oxford University Press; 2022. Available: https://opil.ouplaw.com/ home/OEEUL.

[38] Milkaite I, Lievens E. Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. J Child Media. 2020;14: 5-21.

[39] Valkenburg PM, Piotrowski JT. Plugged In: How Media Attract and Affect Youth. 1st ed. Plugged In. 1st ed. Yale University Press; 2017.

[40] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/ docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E.

[41] Verdoodt V, Clifford D, Lievens E. Toying with children's emotions, the new game in town? The legality of advergames in the EU. Comput Law Secur Rep. 2016;32: 599-614.

[42] Verdoodt V, Lievens E. Targeting children with personalised advertising: how to reconcile the (best) interests of children and advertisers. Data Protection and Privacy Under Pressure: Transatlantic tensions, EU surveillance, and big

dangerous for children, such as cigarettes, alcohol, drugs and weapons, also poses a consumer risk.

Young people are aware that companies keep children glued to the screen for as long as possible so they can show them as many ads as possible. However, the choice to see ads should lie with children themselves.

- *Most relevant children's rights: right to privacy and data protection (Article 16 CRC, Articles 7 and 8 EU Charter), right to free, non-commercial, play (Article 31 CRC), protection from economic exploitation (Article 32 CRC), right to protection from substance abuse (Article 33 CRC).*

Cross-cutting risks

'Cross-cutting risks' are risks that can co-occur with all other categories of risks and potentially - in combination - increase or multiply risks to children. The following risks (advanced technology, privacy and health) together constitute the cross-cutting risks. Chances are these have already been reflected in the previous questions. If so, there is no need to mention them again here.

3.5 ***Advanced technology risks:*** *Which advanced technologies as part of the design of the digital service may pose (potential) risks to children, also considering their age and evolving capacities?*

Risks from advanced technologies include situations where children are at risk as the technology becomes more sophisticated. These can include technologies such as smart toys or other smart products, digital services driven by algorithms, data-driven behavioural design of digital services and biometric applications.

Smart toys can pose both privacy risks (by collecting personal data to feed the AI system)[43] and content or consumer risks (such as the dissemination of harmful or commercial information during the interaction between the smart toy and the child).[44] A personalised timeline on social media or video platforms aimed at increasing engagement poses both consumer risks (such as excessive processing of personal data) and an increased risk of children being exposed to commercial content, disinformation or harmful content (such as extremist or radicalising content,[45] or information about eating disorders or extreme sports[46]).

Young people are very worried about the effects of algorithms on children. The younger you are, the more impressionable you are. As a result, you get to see more and more of the same content. Also harmful content, such as information about war, extremism, eating disorders, depressive topics. You can end up in a rabbit hole of disinformation (e.g. Holocaust denial), fake news and other negative content. Children may believe untrue information and stop thinking for themselves. Their freedom of thought is restricted. It is

data. Maklu; 2017. pp. 313-341. -Verdoodt V. The role of children's rights in regulating digital advertising. Int J Child Rights. 2019;27: 455-481. - Zarouali B, Verdoodt V, Walrave M, Poels K, Ponnet K, Lievens E. Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: implications for regulation. Young Consumers. 2020. Available: https://www.emerald.com/insight/content/doi/10.1108/YC-04-2020-1122/full/html.

[43] Milkaite I, Lievens E. The internet of toys: Playing games with children's data? The Internet of Toys. Cham: Springer International Publishing; 2019. pp. 285-305.

[44] Keymolen E, Van der Hof S. Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. J cyber policy. 2019;4: 143-159.

[45] Schlegel L. Into the Rabbit Hole: How Extremists are Seeking to Exploit Gaming. ITNOW. 2022;64: 14-15.

[46] Milmo D. TikTok 'acting too slow' to tackle self-harm and eating disorder content. The Guardian. 3 Mar 2023. Available: https://www.theguardian.com/technology/2023/mar/03/tiktok-too-slow-tackle-self-harm-eating-disorder-content. Accessed 30 Mar 2023.

difficult to escape such a trap again. An algorithm can also be discriminatory, for example, when LGBT+ 'comments' are blocked. Algorithms let children spend much more time scrolling than is healthy for them. This is how companies make a lot of money. Children should have the option to turn off algorithms. Parents should be educated about their dangers.

Data-driven behavioural design of digital services combines so-called 'dark patterns' with targeted targeting of children's vulnerabilities based on their personal data. Dark patterns are design choices that prompt users to do what the company wants, for example to maximise profits, rather than letting players follow their own preferences.[47] Examples of dark patterns in games include asking players to pay for progress in the game by reducing the player's skills or increasing the difficulty ('pay to skip'), or making success in the game dependent on additional investments ('pay to win').[48] But dark patterns also appear in other digital services, such as misleading privacy policies and irritating settings or constant notifications that lure users back to the application.[49] Children and young people can be more susceptible to the negative effects of dark patterns, and data-driven dark patterns can take targeted advantage of children's vulnerability.

Biometric applications, such as the use of biometrics for 'age determination', can lead to potential privacy risks for children (and for data security), but also to the exclusion of children through, for example, algorithm bias and reduced accuracy of its operation (depending on factors such as age, gender, validity and skin colour).[50] More generally, the deployment of AI systems to children (think adaptive learning) can raise risks.

- *Most relevant children's rights: right to development (Article 6 UNCRC), freedom of thought (Article 14 UNCRC), right of access to non-harmful information and the media, including protection from harmful content (Article 17 UNCRC), right to privacy and data protection (Article 16 UNCRC, Articles 7 and 8 EU Charter), right to health (Article 24 UNCRC), right to play freely (from commerce) and unconstrained (Article 31 UNCRC), protection from economic exploitation (Article 32 UNCRC).*

*3.6 **Privacy risks:** What breaches of children's privacy might the design or use of the digital service lead to?*

Infringements of children's privacy include arbitrary or unlawful interference with the child's private life and communications, unlawful processing of the child's personal data or (potential) damage to the child's integrity, honour or reputation.
'Privacy risks' include the processing of children's personal data. As indicated earlier under consumer risks, such processing enjoys a higher level of protection under data protection law. The data-driven nature of many digital services as part of their business model leads to extensive or even excessive processing of children's personal data. The examples mentioned earlier under the 'risks of advanced technology' (data-driven deceptive and manipulative design, algorithms) also pose privacy risks. More generally, automated and AI systems can pose privacy risks to children. Those risks may include those associated with the profiling of children for commercial and non-commercial purposes.

---

[47] Leiser MR, Caruana M. Dark Patterns: Light to be found in Europe's Consumer Protection Regime. Journal Of European Consumer And Market Law. 2021;10: 237-251. - Zagal JP, Björk S, Lewis C. Dark Patterns in the Design of games.

[48] Van der Hof S, van Hilten S, Ouburg S, Birk MV, van Rooij AJ. "Don't Gamble With Children's Rights"-How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment. Frontiers in Digital Health. 2022;4. doi:10.3389/fdgth.2022.822933.

[49] European Data Protection Board. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. 2022 Mar. Available: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/
guidelines-32022-dark-patterns-social-media_en.

[50] UNICEF. Faces, Fingerprints & Feet, Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes. UNICEF; 2019 Jul. Available: https://data.unicef.org/resources/biometrics/.

In addition, privacy risks for children can arise from themselves or others sharing personal information about them on social media or video platforms. A well-known example of this is 'sharenting' (a combination of 'sharing' and 'parenting'), where parents share photos and videos of their children.[51] In the case of so-called family vloggers, sharenting can even lead to a form of child labour,[52] which can also create 'behavioural risks' for children. In addition, contact risks can arise when malicious third parties, such as child abusers or cyber criminals, have easy access to children's photos and videos because their personal information is public by default.

Breaches of children's privacy are a concern for young people. They cite all kinds of breaches. Companies collect information about what children see, 'like', and what interactions they have with whom and about what to feed the algorithms that keep them glued to the screen. Others (including parents) share photos of children without their consent. There can also be deepfakes that are bad for children's reputation and can affect their future. Children should be able to play freely and not stress about their future reputation. Young people further think it is important for children to have control over their information. The internet does not forget once personal information is shared. Young people believe that digital services should take children's ages into account. However, age control should not lead to an invasion of their privacy.

- *Children's rights: right to privacy and data protection (Article 16 CRC, Articles 7 and 8 EU Charter), right to protection from violence (Article 19 CRC), right to protection from sexual abuse (Article 34 CRC), see also Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.*

3.7 ***Health risk:*** *To what potential harm to children's mental, emotional or physical health could the use of the digital service lead, also taking into account their developing abilities?*

'Health risks' include risks inherent in the choices in the specific design of digital services that may be detrimental to children's physical, emotional and mental health.[53]

Several previously discussed risks can negatively affect children's mental, emotional and physical well-being, causing them to experience stress, depression, sleep deprivation, lack of physical activity, social anxiety and other problems. Cyberbullying, for example, can lead to depression and social anxiety.[54]

It was previously highlighted that harmful content can be detrimental to children's well-being and health. For example, children may become anxious and stop sleeping at night. Moreover, content

[51] Ferrara P, Cammisa I, Corsello G, Giardino I, Vural M, Pop TL, et al. Online "Sharenting": The Dangers of Posting Sensitive Information About Children on Social Media. J Pediatr. 2023. doi:10.1016/j.jpeds.2023.01.002.
[52] Verdoodt V, van der Hof S, Leiser M. Child labour and online protection in a world of influencers. The Regulation of Social Media Influencers. Edward Elgar Publishing; 2020. pp. 98-124.
[53] Children in the Digital Environment: Revised Typology of Risks. OECD; 2021 Jan. Available: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1678964855&id=id&accname=guest&checksum=D7F9A773A74CAD9FBA981F43DA9B348E.
[54] Perren, Sonja & Dooley, Julian & Shaw, Thérèse & Cross, Donna (2010). Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. Child and adolescent psychiatry and mental health. 4. 28. 10.1186/1753-2000-4-28.

can encourage them to adopt unhealthy lifestyles, such as advertisements for unhealthy food[55] or information about eating disorders and excessive exercise.[56]

Algorithms on social media and video platforms can pull users into a 'filter bubble', in which they are mainly shown extreme, sensational or unhealthy information (see also advanced technology risks). In addition, the aforementioned dark patterns that are part of advanced technology risks' can be detrimental to children's well-being and health. Timed events ('timed events') in video games, for example, can lead to family conflict, while constant notifications or other 'sticky features' of digital services can lead to obsessive use, sleep deprivation and stress.[57]

Young people make a connection between the operation of algorithms and children's well-being. Children can fall into an information trap of eating disorders and depressive content. Their mental well-being may be negatively affected as a result. The younger you are, they say, the greater the impact.

Moreover, digital services can give children access to products or services that are unhealthy or dangerous for them, such as tobacco, alcohol, drugs, weapons and online gambling.

Finally, as was mentioned earlier, social media can entice children to participate in online challenges that can be unhealthy or even life-threatening for them.

- *Children's rights: right to optimal development (Article 6 CRC), right to health (Article 28 CRC).*

3.8 ***Other risks****: What other risks are there on your platform before measures have been taken?*

In addition to the risks discussed earlier, there may be other risks that may arise when using your digital service. Enter these here.

[55] Folkvord F, Anschütz DJ, Buijzen M, Valkenburg PM. The effect of playing advergames that promote energy-dense snacks or fruit on actual food intake among children. Am J Clin Nutr. 2013;97: 239-245.
[56] Milmo D. TikTok 'acting too slow' to tackle self-harm and eating disorder content. The Guardian. 3 Mar 2023. Available: https://www.theguardian.com/technology/2023/mar/03/tiktok-too-slow-tackle-self-harm-eating-disorder-content. Accessed 30 Mar 2023.
[57] Van der Hof S, van Hilten S, Ouburg S, Birk MV, van Rooij AJ. "Don't Gamble With Children's Rights"-How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment. Frontiers in Digital Health. 2022;4. doi:10.3389/fdgth.2022.822933 - van Rooij AJ, Birk MV, van der Hof S, Ouburg S, van Hilten S. Behavioral design in video games: A roadmap for ethical and responsible games that contribute to long-term consumer health and well-being. Trimbos institute, Eindhoven University of Technology & Leiden University; 2021.

4. Courses of Action

This section is about options for taking action to mitigate risks, also often called 'risk mitigation measures' or 'management measures'. Here you describe how you plan to eliminate, or drastically reduce ('mitigate'), the (potential) impact you described in the previous section. We use the word action options here because the emphasis is on *action* - what can you *do* concretely to counter the negative impact on children and their rights?

How will the (potential) impact of the digital service on children be mitigated? In this step, you focus on defining measures that can eliminate or reduce the previously formulated risks of negative impact on children's rights and well-being. Risk mitigation measures play a crucial role in safeguarding children's rights and wellbeing and minimising any harm or negative impact. However, it is important to stress that in some cases these risk mitigation measures are inadequate. In such situations, where the risk is of such magnitude, it requires reconsideration and redesign of the digital service to properly reduce or completely eliminate the risks.

4.1 What child-centred measures have been taken, or will you take, to prevent risks?

The answer box contains a schedule that can be used to walk through the risks identified in Chapter 3 in a structured way, identify measures and weigh the remaining risk. In the fill-in schedule, you can indicate for each risk what measures you plan to take to counter the risk of impact on children's rights.

Risk classification	**Risk description**	**Measures**	**Residual risk**	**Administrator**
Content risk				
Behavioural risk				
Contact risk				
Consumer risk				
Advanced technology risk				
Privacy risk				
Health risk				
Other risks				

Risk rating
The risk classification column represents the risk clusters from chapter 3. Of course, you can have more than one risk listed for a cluster. You then insert an extra row. You may also not have found any risks in a cluster. You can then leave it blank.

Risk description
In this column, you describe (briefly) what the risk is. You have already described it in more detail in Chapter 3. Use a separate line per risk, insert additional lines where necessary. Also add the risks for which you cannot (yet) take measures.

Measures
In this column, you indicate for each risk what measures you will take to eliminate or reduce the risk. When taking measures, technical solutions are often thought of. But it makes sense to look wider than that. In addition, 1 measure may reduce several risks. When setting up measures, think not only about technical measures, but also, for instance, about setting rules of conduct, informing users, etc. In addition, it is good to realise that measures can complement each other. Informing users on the (correct) use of the application is good, but never takes away the entire 'behavioural

risk', for instance. More measures will probably be needed. So it is not an exact science. The key here is to take all aspects into account.

- *Note: when considering proportionality, it is important to only write down the measures you will actually take.*

Residual risk
In the last column, describe what risk remains after taking the measures. In the column, write what the residual risk is. Again, use the method risk = probability x impact (see Figure 4). In addition, provide an explanation (see reporting example below).

Administrator of the measure
It is good to name who is responsible for implementing the measures. It is important that these are names of people or teams who can actually *act.* So in the case of technical measures, it makes more sense to name designers, technicians or technology buyers here. In the case of context measures, this could include managers, policymakers and insurers.

A reporting example

Risk rating	**Risk description**	**Measures**	**Residual risk**	**Administrator**
Conduct risk	Children may upload harmful content	- Educating users on proper usage - Automatic detection via algorithm to remove such content - Alerting users to potentially harmful content in an understandable way - Options to filter content based on content classification	Average: The probability of the risk occurring is reduced but not 0 with the measures, the impact per se has not changed. Children may ignore instructions or fail to consider the consequences. Automatic detection helps, but is never 100% foolproof. Clear warnings give users control over content that see or do not want to see. Filter options give them more control and convenience in avoiding potentially harmful content.	Department x, role x, person x

5. Assessment

In part 1, you have identified whether conducting a CRIA is necessary for you. In part 2, you have concretely defined and delineated the digital service targeted by the CRIA and set the objectives. This gives you a concrete overview of the benefits or revenues of the digital service. Then, in parts 3 and 4, you have identified the (potential) impact of using your digital service on children's rights and well-being. This gives you an overview of both benefits and costs.[58] The final section is about balancing these costs and benefits. This is called the proportionality test.

5.1 ***Effectiveness****: Look at your answer to question 2.7: Does this digital service indeed achieve the goal? Explain.*

In order to ultimately assess whether the benefits outweigh the potential costs, it is important to first establish whether the stated objectives are (in all likelihood) being achieved with the development and deployment of the digital service. This is called effectiveness. If your digital service turns out to be ineffective and children's rights are also violated, then rolling out the digital service is problematic. In other words, if your service is not effective, you are unlikely to realise the desired benefits. That leaves only costs on the balance sheet.

5.2 ***Subsidiarity****: Is the service the best way (taking into account the rights and wellbeing of the child) to achieve the goal? Are there no other ways available to do this? Explain.*

Subsidiarity is about whether the means you intend to use is the best means to achieve the objective. In doing so, it is important to consider whether there are no other (less intrusive) means to achieve the same goal. If there is an alternative available that does not affect children's rights or to a lesser extent, but still achieves the goal, this alternative should be used. If this is not possible, it should be explained why this less intrusive means was not chosen.

5.3 ***Proportionality/balancing of interests****: Is the identified (potential) violation of children's rights proportionate to the goals? Substantiate the balance of interests.*

This last question is what ultimately matters. Are the goals - all things considered - robust enough to justify the risk of a potential violation of children's rights after measures taken?

This is a comprehensive question. To give structure to your consideration, it helps to fill in the following chart. Here you basically summarise what you discussed in the assessment. In doing so, you list the pros and cons discussed earlier. For the advantages, look back to what you described in section 2 about the goals. The disadvantages are mainly about parts 3 and 4.

Benefits (see intended goals)	**Disadvantages (negative impact on children)**
Benefits for your organisation: Sum up here what benefits the digital service has for your organisation. Consider, for example, commercial or other organisational goals	List here the (potential) risks to children, their rights and wellbeing. It is important that here you describe the impact on the child, their rights and wellbeing.
Benefits for children's rights and wellbeing: Sum up here what benefits your digital service may have on child wellbeing and to which children's rights it contributes.	

[58] Costs and benefits in this context are not strictly meant in a material sense. Benefits can include, for example, positive effects on child wellbeing. Costs here refer to the potentially negative effects on child wellbeing.

Here, it is especially essential that you make a good case for how you have weighed the different interests against each other, and why you ultimately feel that one interest outweighs the other.

There are no hard and objective criteria for balancing the different rights, interests and goals. In general, however, it can be said that the more serious the expected impact on children's rights and wellbeing is, the heavier the objectives should weigh. A mere commercial purpose can never be sufficient in this respect.

5.4 ***Conclusion****: Given your answers to the above questions, what is your conclusion regarding the design and deployment of your (proposed) digital service?*

Describe here what your conclusion is following the answer to question 5.3. What does this mean for the (roll-out of) the digital service?

5.5 ***Follow-up actions****: What actions are needed to properly secure the findings from this assessment?*

List any follow-up actions here.

5.6 ***Monitoring****: How can you monitor that formulated management measures are effectively implemented? At what time and under what circumstances will you re-run the CRIA?*

Make explicit here how you will ensure that the control measures are implemented and how you will deal with future changes to the design and periodic implementation of the CRIA.