WebGroup Czech Republic a.s. (xvideos.com)

RISK ASSESSMENT & RISK MANAGEMENT REPORT

Created on:	April 18, 2024
Prepared by:	David Hradecký, Compliance Officer
Approved on:	April 19, 2024
Approved by:	Robert William Seifert, Board Member
	Stéphane Michaël Pacaud, Board Member

Contents

1. Introduction

1.1. Purpose and scope of the report

This report presents a risk assessment conducted by WebGroup Czech Republic a.s. (also referred to as “we” or “WGCZ”), operator of the xvideos.com platform which has been designated as Very Large Online Platform (VLOP)in accordance with Article 33(4) of Regulation (EU) 2022/2065 (Digital Services Act or DSA). The primary purpose of the risk assessment is to:

- identify and evaluate risks associated with all aspects of our operations that could negatively impact users, society, or our ability to comply with all relevant regulations,

- specifically address risks related to the DSA, including data transparency, reporting obligations, risk of dissemination of illegal content, negative effects for the exercise of fundamental rights, effects in relation to gender-based violence, risks for public health and minors, consequences to the person’s physical and mental well-being and advertiser and commercial content integrity.

The scope of this report encompasses all processes, systems, and controls relevant to our online platform's functionality and compliance with regulations. This includes, but is not limited to, content moderation, user safety, data privacy, advertising practices, and reporting procedures. Identified risks are assessed based on their likelihood of occurrence and potential impact on various aspects, such as user trust, public safety and health, protection of minors, regulatory compliance, material and immaterial damages and our overall business objectives.

The conducted risk assessment considered the diverse regional and linguistic landscape of our user base. Despite the complexity due to such a vast landscape, we fully recognize the importance of tailoring our approach to mitigate risks specific to different regions and languages. Our approach to the challenges the linguistic landscape poses in front of us is driven by principles as recited by DSA – those of risk-based approach and proportionality. These principles are reflected not only in our risk management system but are adopted across all related activities.

The report comprises three parts to be read in conjunction with each other:

(i) the present risk assessment and risk management report;
(ii) the risk management dashboard; and
(iii) the risk register.

1.2. Risk management framework

The risk assessment was conducted following the principles and guidelines established in the international standard ISO 31000: Risk Management. This standard provides a comprehensive framework for organizations to effectively identify, assess, treat, monitor, and communicate risks. During this assessment, we particularly focused on the standard's emphasis on continuous improvement and the importance of involving top management and other relevant stakeholders throughout the risk assessment process.

Building upon the principles of ISO 31000, we recognize the crucial role of leadership in fostering a strong risk management culture. Our governing body demonstrates a clear commitment to risk management by actively engaging in discussions and providing the necessary resources. This commitment translates into tangible actions, as evidenced by our top management devoting sufficient time and resources to consider measures related to risk management and actively participating in decisions regarding risk mitigation strategies.

The ISO 31000 framework aligns well with the requirements of the Digital Services Act (DSA) for Very Large Online Platforms (VLOPs). The standard's focus on systematic risk identification, assessment,

and treatment ensures we proactively address potential issues related to data transparency, reporting obligations, and content integrity, as mandated by the DSA.

We chose ISO 31000 as the foundation for our risk assessment process and risk management system due to several factors:

- ISO 31000 offers a well-established, internationally recognized framework for risk management. It provides a structured approach that encompasses all stages of the risk management process, from identifying risks to evaluating, treating, monitoring, and communicating them;

- while the DSA itself doesn't explicitly mandate the use of ISO 31000, the standard's core principles align well with the objectives outlined in the DSA. These principles emphasize proactive risk identification, risk mitigation strategies, and continuous improvement – all crucial aspects of a robust risk management program under the DSA;

- the flexibility of ISO 31000 allows us to tailor the approach to the specific needs of our platform and the evolving regulatory landscape. We can integrate additional considerations specific to the DSA while leveraging the core principles of the standard.

Hence, utilizing ISO 31000 for our risk assessment and risk management process leverages several advantages:

- provides a well-established and systematic approach to managing risks across the organization,

- encourages a proactive and continuous improvement cycle for identifying, assessing, and mitigating risks,

- facilitates clear communication and collaboration among stakeholders regarding risk identification, evaluation, and treatment strategies.

1.3. Methodology used for risk assessment

Risk Assessment Steps

1. Defining the scope and objectives of the assessment

2. Employing a variety of techniques to systematically identify potential risks relevant to our operations and DSA compliance

3. Assessing the likelihood and potential impact of each identified risk using a pre-defined scoring system

4. Prioritizing risks based on their likelihood and impact scores to determine which require further mitigation efforts

5. Developing and implementing appropriate risk mitigation strategies to address identified risks

6. Continuously monitoring the effectiveness of risk controls and reviewing the risk management process at regular intervals

Data collection

A combination of data collection techniques was used to gather information for this assessment, including:

- internal workshops with relevant stakeholders from various departments (e.g., legal, compliance, IT, content moderation),

- interviews with key personnel to gain in-depth insights into specific processes and potential risks,
- review of internal documents and policies related to data management, content moderation, and regulatory compliance, including the Terms of Service, with specific focus on our content moderation system as a whole and design of our recommender system and algorithms,
- benchmarking against industry best practices and other VLOPs.

Risk identification

In order to comprehensively identify potential risks, we carried out the following activities:

- brainstorming sessions with cross-functional teams to generate a broad range of risk scenarios,
- scenario planning exercises to consider potential future events and their impact on our operations,
- review of existing risk registers and industry threat intelligence to identify relevant risks specific to VLOPs.

Risk assessment criteria

A scoring system was used to assess the likelihood and impact of each identified risk. The scoring criteria were defined based on pre-determined scales considering factors such as frequency of occurrence, severity of consequences, and potential for business continuity disruption.

Risks and regional linguistic aspects

We acknowledge the importance of regional and linguistic variations in user behavior and content moderation. Our risk assessment process incorporates our multilingual content moderation team. We employ a team of content moderators proficient in various languages, including, but not limited to, German, French, Italian, English, Spanish, Polish, Russian, Slovak and Czech allowing for a nuanced understanding of content across different regions and effective content moderation.

We understand the importance of effective content moderation across a variety of languages spoken within the European Union. To achieve this, we leverage a two-pronged approach that combines the expertise of our multilingual moderation team with the assistance of a reliable translation software.

Our moderation team is comprised of individuals with understanding of the cultural nuances and sensitivities present within the EU. This allows them to effectively assess content in their native languages, ensuring a high degree of accuracy and comprehension.

Risk documentation

The identified risks and their assessments are documented in a form of a Risk Register. This register includes details such as risk category, risk description, likelihood and impact scores, inherent and residual final risk scores (values), and recommended risk management treatment based on selected Risk management strategies. The risk register is a live document and serves as a central repository for ongoing monitoring and review of risks.

2. Risk identification

A comprehensive approach to risk identification was undertaken, involving participation from a wide range of stakeholders across WGCZ. This included representatives from departments such as:

- Legal and Compliance
- Content Moderation
- IT Security and operations

Through workshops, brainstorming sessions, and individual interviews, stakeholders contributed their unique perspectives and expertise to identify potential risks related to our operations and compliance with the DSA. During the risk identification process, particular emphasis was placed on potential risks associated with various aspects of the DSA that VLOPs need to comply with (see Chapter 2.1 for more detail). This included:

- data transparency obligations,
- reporting requirements to regulator,
- content moderation practices, where we focused primarily on definition of risk scenarios related to detecting and removing illegal content, preventing manipulation of users, and protecting minors online were identified,
- advertiser and commercial content integrity, where we aimed at exploring potential risks associated with misleading advertising practices and ensuring the integrity of commercial content displayed on our platform.

By employing a multi-pronged approach that incorporates industry best practices, we aimed to create a comprehensive picture of potential risks that could threaten the objects of protection outlined in the regulation. This includes risks that could negatively impact:

- users, their health and safety, fundamental rights (such as privacy and freedom of expression), and overall well-being. This could involve risks associated with exposure to harmful content, manipulation, or privacy breaches;
- society, such as the spread of misinformation or threats to external security; and
- our organization, despite the primary focus, we acknowledge that risks to user safety and society can ultimately impact our organization through reputational damage, regulatory actions, or user loss.

Our risk assessment focuses on the most significant risks relevant to the xvideos.com platform. While the DSA identifies a broad range of potential risks, some are not directly applicable to our service. For instance, the risk of negative effects on civic discourse and electoral processes (as per Art. 34(c) DSA) is considered minimal for our platform, which primarily focuses on adult entertainment content.

2.1. Risk Categories

This chapter outlines the various categories of risks identified during the assessment. Each category aligns with potential areas of concern regarding our operations and compliance with the DSA. By comprehensively understanding these risks, we developed effective mitigation strategies in order to maintain xvideos.com a responsible online platform.

Illegal content distribution

- Risks associated with distribution of illegal content on the platform, such as hate speech, violent content, terrorism-related material, or child sexual abuse content.
- Challenges in effectively detecting and removing illegal content due to factors like volume, automation limitations, or evolving tactics used by malicious actors.

- Risk of regulatory sanctions or reputational damage due to failures in preventing the spread of illegal content.

Adverse effects on fundamental rights

- Risks associated with platform functionalities or content moderation practices that could negatively impact user rights, such as freedom of expression, privacy, non-discrimination, or the basic right to human dignity.

- Potential for biased algorithms or content moderation decisions to disproportionately affect certain user groups.

- Risk of legal challenges or public backlash due to perceived infringements on fundamental rights.

Manipulation of the platform

- Risks associated with malicious actors manipulating the platform to spread misinformation, disrupt user experience, or exploit vulnerabilities.

- Potential for techniques like bots, fake accounts, or coordinated inauthentic behavior to manipulate platform algorithms (which are part of our recommender system) or trends.

- Risk of reputational damage or loss of user trust due to successful platform manipulation attempts.

Protection of minors

- Risks associated with exposure of minors to harmful content, such as age-inappropriate material, cyberbullying, or self-harm content.

- Challenges in effectively verifying user age.

- Risk of legal repercussions or public criticism for failing to adequately protect minors to visit the platform.

Data privacy and protection

- Potential for data breaches, unauthorized access, or misuse of user data.

- Risk of regulatory fines or user churn due to inadequate data privacy protection measures.

Systemic risks

- Potential for algorithmic bias, echo chambers, or filter bubbles to negatively impact user behavior or societal discourse.

- Risk of platform addiction or manipulation of user behavior.

Transparency and reporting obligations

- Risks associated with inaccurate or incomplete data collection that hinders transparency reporting to regulator.

- Challenges in meeting complex reporting requirements outlined by the DSA regarding user activity or content moderation practices etc.

- Risk of regulatory penalties or reputational damage due to non-compliance with transparency and reporting obligations.

Advertiser and commercial content integrity

- Risks associated with misleading advertising practices or deceptive commercial content displayed on the platform.
- Difficulty in effectively detecting and preventing fraudulent advertising or sponsored content that deceives users.
- Risk of user trust erosion and potential regulatory action due to compromised advertiser and commercial content integrity.

3. Risk Assessment

A two-step qualitative risk assessment approach was adopted for this assessment. This approach first evaluates the inherent risk, which considers the potential impact and likelihood of a risk occurring before any controls are implemented. Subsequently, the effectiveness of existing controls is assessed to determine the residual risk, which reflects the remaining risk after existing measures and controls are taken into account.

3.1. Inherent Risk Assessment

Likelihood assessment criteria: The inherent likelihood of a risk occurring was assessed based on the following criteria:

- **Very unlikely (Score 1):** Very low probability of occurring within the next year (e.g., no historical incidents, strong mitigating controls in place elsewhere)
- **Unlikely (Score 2):** Low probability of occurring within the next year (e.g., rare historical occurrences, some potential vulnerabilities)
- **Possible (Score 3):** Moderate probability of occurring within the next year (e.g., occasional historical occurrences, some vulnerabilities identified)
- **Likely (Score 4):** High probability of occurring within the next year (e.g., frequent historical occurrences, significant vulnerabilities identified)
- **Very likely (Score 5):** Almost certain to occur within the next year (e.g., ongoing incidents, critical vulnerabilities identified)

Impact Assessment criteria: The inherent impact of a risk on the organization was assessed based on the following criteria:

- **Insignificant (Score 1):** Minimal to no potential harm to users, society, or the organization. Regulatory intervention is unlikely, and any reputational impact would be isolated.
- **Minor (Score 2):** Potential for some harm to users (e.g., exposure to inappropriate content) or society (e.g., spread of misinformation). The organization could face minor reputational damage or regulatory warnings.

- **Moderate (Score 3):** Increased potential for harm to users (e.g., safety risks, privacy breaches) or society (e.g., manipulation, erosion of trust). The organization could experience moderate reputational damage or regulatory investigations.

- **Major (Score 4):** Significant potential for harm to users (e.g., widespread exposure to harmful content) or society (e.g., manipulation of elections). The organization could face substantial reputational damage, potential suspension of operations, or significant fines.

- **Critical (Score 5):** Severe potential for harm to users (e.g., exploitation, psychological harm) or society (e.g., major disruption of democratic processes). The organization could face severe reputational damage, license revocation, or complete platform shutdown.

It's important to emphasize that even in instances where the current risk assessment might not predict significant inherent impact to WGCZ e.g. regulatory fines, lawsuits etc., the potential harm to users and society (objects of protection) still exists. Our control environment is designed with this dual purpose in mind. By strengthening our internal controls, we not only safeguard the organization but also protect users and society from the potential consequences of these risks. This approach ensures a comprehensive risk management strategy that prioritizes user safety and societal well-being, while acknowledging the interconnectedness between organizational resilience and the protection of the objects outlined in the DSA.

An inherent risk score was then calculated by multiplying the inherent likelihood and impact scores (Score = Likelihood x Impact).

Risk Value Matrix (x-axis: impact, y-axis: probability)

		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Critical
5	Very Likely	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
4	Likely	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
3	Possible	Low Risk	Medium Risk	Medium Risk	Medium Risk	Medium Risk
2	Unlikely	Low Risk	Low Risk	Medium Risk	Medium Risk	Medium Risk
1	Very Unlikely	Low Risk	Low Risk	Low Risk	Low Risk	Low Risk

Figure: Risk Value Matrix defined for the purpose of conducting Risk Assessment

3.2. Residual Risk Assessment

Following the inherent risk assessment, existing controls and measures relevant to each risk scenario were identified and evaluated. The effectiveness and robustness of these controls were considered in determining the residual risk.

- **Control Effectiveness Assessment:** The effectiveness of each control was assessed based on factors such as:

    - strength of the control in mitigating the risk,

    - frequency of control monitoring and updates,

  - historical performance of the control.

- **Residual Risk Determination:** Based on the inherent risk score and the effectiveness of existing controls, a residual risk score was assigned to each risk. The residual risk score reflects the remaining level of risk after controls are implemented.

Risk prioritization

Risks were then prioritized based on their inherent and residual risk scores. Risk scenarios with scores higher than Low (with a few exceptions where the residual risk score was determined as Low) was further analyzed, and mitigation strategies are developed to address them effectively.

4. Risk assessment results & Risk management plan

4.1. Risk Assessment results

In accordance with the methodology outlined in Chapter 3, the risk assessment comprehensively evaluated thirty-eight realistic risk scenarios categorized across the eight risk categories defined in Chapter 2.1.

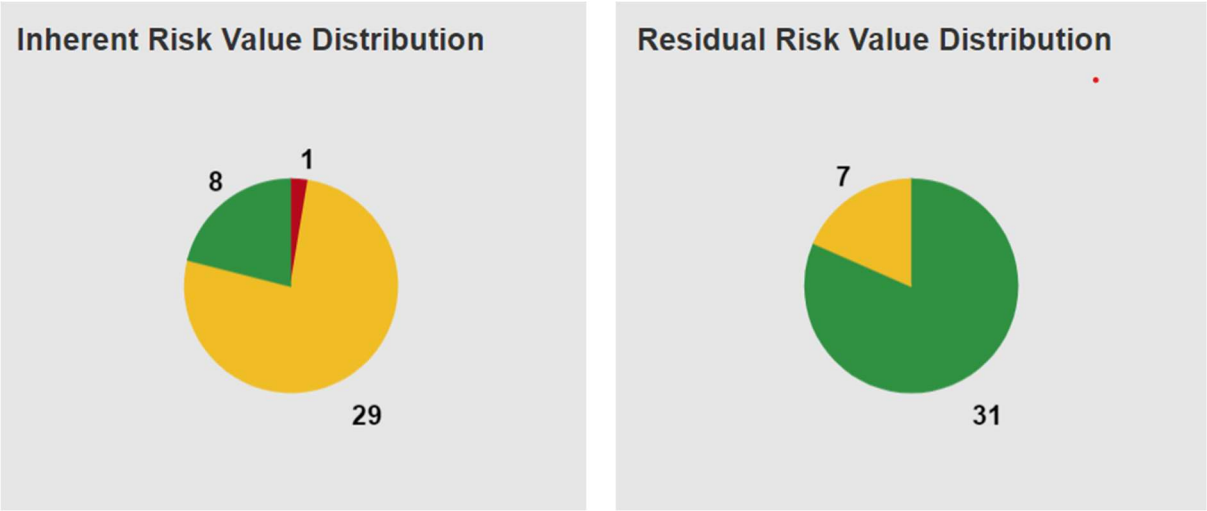

Figure: Comparison of Risk Assessment results in the inherent and residual phase of assessment

The inherent risk assessment identified that WGCZ faces higher than inherently low exposure to 30 risk scenarios. The majority (29 instances) fall within the medium risk category, with only one classified as high risk. This initial assessment is based on the inherent likelihood and impact of each risk scenario before considering existing controls.

As documented in the Risk Register, all identified risk scenarios have been mapped to corresponding measures and controls. The effectiveness of these controls in mitigating risks is evident, as they demonstrably prevent the materialization of the majority of the risk scenarios.

While the initial risk assessment indicates a well-controlled environment, a high-level overview of risk by category further indicates the primary areas where WGCZ will focus its risk management efforts:

Risk Category Comparison (click on Risk Category to see detail)

Risk Category	Number of Risks	Inherent Risk Score (AVG)
Transparency and Reporting Obligations	4	12.0
Data Privacy and Protection	4	10.3
Illegal Content Distribution	9	9.4
Protection of Minors	6	8.2
Systemic Risks	5	6.2
Advertiser and Commercial Content Integrity	4	6.0
Adverse Effects on Fundamental Rights	3	4.7
Manipulation of the Platform	3	4.0

Figure: Overview of Risk Category results in the inherent phase of assessment

4.2. Residual Risk Assessment

The residual risk assessment, which considers the effectiveness of existing controls, identified four risk scenarios with a score above "Low." These consist of three categorized as "Medium" risk and one classified as "High" risk.

			Risk Assessor		Final Risk Score (inherent)	Final Risk Value (inherent)	Measures in place (list)	Final Risk Value (residual)
Risk ID	Risk Category	Risk Scenario	Probability	Impact				
PM_1	Protection of Minors	Inadequate access verification systems allowing minors access to adult content	Likely	Major	16	High Risk	- warnings about adult content - age confirmation - guidance for guardians for protection of minors - security measures and parental controls setup - Terms of Service - Point 2 - Access (https://info.xvideos.net/legal/tos/)	Medium Risk
TR_1	Transparency and Reporting Obligations	Failure to accurately report on content moderation actions	Possible	Major	12	Medium Risk	- Compliance Officer nomination - resources allocated to secure compliance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - moderation team training - moderation database maintenance and regular reporting to Authorities	Medium Risk
TR_2	Transparency and Reporting Obligations	Inadequate disclosure of algorithmic decision-making processes	Possible	Major	12	Medium Risk	- Compliance Officer nomination - resources allocated to secure compliance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - algorithmic definitions and application subject to regular Compliance audits - close internal cooperation in case of any changes with algorithms should they become more complex (currently basic - see above)	Medium Risk
TR_3	Transparency and Reporting Obligations	Non-compliance with regulatory requests for platform data	Possible	Major	12	Medium Risk	- Compliance Officer nomination - resources allocated to secure compiance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - maintenance of required databases - regular reporting to Authorities in the required form and structure	Medium Risk

Figure: Overview of risks requiring additional measures to be implemented

Given the priorities and focus of various stakeholders, we provide detail on especially two areas of our risk assessment and risk management efforts:

1) Age verification system
2) Gender-based violence and non-consensual sexual acts

Age verification system

WGCZ, alongside many responsible actors across various industries (e.g., motion picture companies, alcohol and tobacco producers, video game developers, and online gambling platforms), shares a strong commitment to safeguarding minors from accessing age-restricted content.

We actively participate in industry discussions and experiments related to age verification solutions.

However, current site-based age-gating methods, have not only proven to be easily bypassed, but have also been fully rejected by users, resulting in an almost complete loss of userbase where they were applied (close to 90%).

Additionally, the various identity verification methods used pose major security risks in the event of a data breach, as well as cost issues.

On the other hand, already available parental control tools cannot be bypassed and do not pose any security or privacy risk, and are free. However their existence and availability may not be sufficiently known.WGCZ prioritizes user privacy and data protection. We believe a responsible age verification approach should not come at the expense of these fundamental rights. We are actively exploring alternative solutions that balance user privacy with effective age verification:

- we collaborate with leading cybersecurity and privacy experts to stay informed about emerging age verification technologies that prioritize user privacy;

- we closely monitor industry advancements in age verification and adapt our approach as more robust and secure technologies become available.

Despite the limitations, we employ a multi-layered approach to age verification that includes:

- the platform warns all visitors prior to them viewing any content that it is designed for an adult audience only;
- users are required to confirm their age during account creation, agreeing to our terms of service that prohibit underage access;
- age verification prompts appear before accessing age-restricted content;
- we provide educational resources to inform users about the importance of responsible online behavior and provide detailed guidance on the setup of parental controls for parents and guardians.

We acknowledge that the current age verification landscape presents a residual risk. However, we are monitoring developments across the globe for better age gate keeping measures and are committed to continuous improvement and responsible management of this risk.

Residual risk assessment: Gender-based violence and non-consensual sexual acts

WGCZ stresses that it does not tolerate the display and dissemination of illegal content on any of its platforms, including content featuring Non-Consensual Intimate Imagery (“NCII”) or Child Sexual Abuse Material (“CSAM”), and takes all forms of online abuse very seriously. WGCZ has always endeavored to make its sites safe for all individuals, users and non-users alike, and to support online safety.

As evident from the risk register, the risk assessment identified gender-based violence and non-consensual sexual acts as key risk scenarios. We acknowledge the potential for these scenarios to materialize on our platform, and we take a comprehensive approach to identifying, assessing, and mitigating them. Hence, we dedicated significant resources to thoroughly evaluate this risk:

- we analyzed the potential for content depicting or promoting gender-based violence to be uploaded to the platform;
- we assessed the possibility of users engaging in abusive or harassing behavior towards others;
- we evaluated the effectiveness of our systems in identifying and removing content related to gender-based violence, as well as the efficiency of our user reporting tools.

Based on this comprehensive analysis, it needs to be stated that the control environment effectively mitigates the risk of gender-based violence:

- we perform algorithmic review through digital fingerprinting software; we scan the XVideos platform for content that has been previously identified as NCII and CSAM. This fingerprint database is based on Vercury software and is managed by WGCZ;
- we also leverage machine learning algorithms within our "Hive" classification system. This system proactively identifies and flags content depicting or promoting violence, hate speech, and other harmful behavior;
- we also use additional software tools for content moderation such as Thorn Safer, a hashing technology, to identify CSAM content by means of a comparison with records contained in both the database of the National Center for Exploited and Missing Children (“NCMEC’s”) and the internal database of the technology supplier, Safer, as well as Google Safe API to detect possible CSAM content;
- our "Hive" system mentioned above also works hand-in-hand with a dedicated team of trained moderators. These moderators possess knowledge of online safety best practices, linguistic and cultural nuances, ensuring accurate review of flagged content. The team of reviewers browses the XVideos’ site just like regular users, reviewing reported videos and removing any illegal content and/or content that infringes XVideos’ Terms of Service, whether it be spam, possible illegal/doubtful content, or some other infringing content, always erring on the side of caution, i.e., by excluding doubtful material. These content moderators are responsible for reviewing all potentially illegal content and confirming that the content is NCII or CSAM.

- we encourage users to report any suspicious activity or content through a user-friendly, multilingual reporting system (“abuse reporting form”). Every report is promptly reviewed by our moderation team, and we maintain a zero-tolerance policy for violations. The abuse reporting form is a tool that allows anyone (be it an individual or a legal entity) to notify WGCZ of the presence on their service of specific items of information that is considered to be illegal content; it is easily accessible by electronic means and it is user-friendly.

- we have also recently introduced a trusted flaggers program, in compliance with DSA, which enables registered trusted flaggers to submit notices via a special account/portal accessible only by such trusted flaggers. Trusted flaggers are granted exclusive access to a dashboard to ensure that notices submitted by them are reviewed as a matter of priority and processed and decided upon without delay. The dashboard also allows the status of such notices to be tracked.

While our current controls have effectively reduced the residual risk of gender-based violence to a low level, we understand that online threats are constantly evolving. That is why:

- our operations actively research emerging technologies that could be misused to circumvent existing safeguards. This allows us to proactively adapt our controls and stay ahead of potential threats;
- we are committed to transparency. We openly communicate our efforts to combat gender-based violence and educate users on how to identify and report harmful content. We also empower users with tools to control their online experience and curate their content feed.

4.3. Risk Management Strategy

In accordance with the defined Risk Assessment Methodology, WGCZ decided to apply the following risk management strategies based on the residual risk scores:

- **Low** - for risk scenarios with a residual score of "Low," the applied strategy is **Accept**; this signifies that, after considering the mapped controls and mitigation measures, the remaining level of risk exposure is considered acceptable. It's important to clarify that "Accept" does not equate to inaction. Instead, it reflects a well-informed decision based on a robust control environment. This environment is designed to continuously monitor and evaluate the effectiveness of these controls. Should any weaknesses or changes in the risk landscape be identified, the control environment would trigger a prompt response. This could involve implementing additional controls, enhancing existing controls, or even reassessing the risk strategy if necessary. In essence, by accepting low residual risk, we acknowledge that the current controls are sufficient, but we remain vigilant and prepared to adapt should circumstances change. This ongoing monitoring and management process ensures the continued effectiveness of our controls and the continued acceptability of our residual risk exposure.

- **Medium or High -** for risks with a residual score of "Medium" or "High," the applied strategy is **Reduce (Mitigate)**; this requires design, development, implementation, and management of additional measures and controls to effectively address these higher-risk scenarios

4.4. Action plan for each medium – high risk

Following the identification and assessment of risks, this chapter outlines the action plan for mitigating those risks. The action plan details the specific controls and measures currently in place, as well as additional mitigation strategies planned for implementation. The focus is on addressing risks with a residual score of "Medium" or "High" as identified in the residual risk assessment (Chapter 4.3).

NOTE: Table detailing action plan follows on next page.

Risk Category	Risk Scenario	Controls & Measures in place	Additional (mitigation) Measures to implement
Protection of Minors	Inadequate access verification systems allowing minors access to adult content	- warnings about adult content - age confirmation - guidance for guardians for protection of minors - security measures and parental controls setup - Terms of Service - Point 2 - Access (https://info.xvideos.net/legal/tos/)	- consider liaising with UNICEF and other globally operating NGOs with similar impacts to fund programs focused on raising awareness of on-line safety and security of minors - consider expanding and improving the wording of the disclaimer about the inappropriateness of content for minors on entry and page - closely monitor the latest developments in age verification tools with a view to finding an instrument that strikes a sufficient balance between effective protection of minors and the fundamental right to do business - support the development and raising awareness of effective age verification tools, such as those integrated into the operating system of individual devices - consider liaising with experts and NGOs dealing with the protection of minors and age verification tools
Transparency and Reporting Obligations	Failure to accurately report on content moderation actions	- Compliance Officer nomination - resources allocated to secure compliance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - moderation team training - moderation database maintenance and regular reporting to Authorities	- continued implementation of Compliance Management System focusing on DSA and other regulations - external audit of CMS in 2024 - moderation processes and procedures deep dive by 08/2024
Transparency and Reporting Obligations	Inadequate disclosure of algorithmic decision-making processes	- Compliance Officer nomination - resources allocated to secure compliance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - algorithmic definitions and application subject to regular Compliance audits - close internal cooperation in case of any changes with algorithms should they become more complex (currently basic - see above)	- continued implementation of Compliance Management System focusing on DSA and other regulations - external audit of CMS in 2024 - performance of compliance audits 2H 2024
Transparency and Reporting Obligations	Non-compliance with regulatory requests for platform data	- Compliance Officer nomination - resources allocated to secure compliance with DSA requirements - process/procedural changes and updates to reflect DSA requirements - maintenance of required databases - regular reporting to Authorities in the required form and structure	- continued implementation of Compliance Management System focusing on DSA and other regulations - external audit of CMS in 2024 - performance of compliance audits 2H 2024 - preparation of standardized reporting procedures as required by the DSA and Authorities

The action plan outlined in this chapter provides a comprehensive roadmap for mitigating the identified risks with a residual score of "Medium" or "High." By implementing the additional mitigation measures alongside existing controls, WGCZ aims to significantly reduce the likelihood and impact of these risks.

The timeline for implementing the suggested additional measures is targeted for the second and third quarters of 2024 (Q2 & Q3 2024). Currently, the specific roles and responsibilities for each mitigation measure are being defined. Overall oversight will be attributed to the Compliance Officer, who will be responsible for liaising with relevant teams and ensuring progress on implementation. Management will be actively involved in the sound management of the systemic risks identified above and will convene to review the status of the action plan no later than June 30, 2024, to assess progress and address any potential roadblocks.

The ongoing monitoring and effectiveness of these mitigation measures will be crucial in ensuring WGCZ's continued compliance with regulations and its commitment to a safe and responsible online platform.

4.5. Risk monitoring and reporting procedures

Effective risk management requires a continuous process of monitoring and reporting. This chapter outlines the procedures in place to ensure timely identification and escalation of emerging risks, as well as regular communication of risk management activities.

The risk monitoring process will be conducted through a combination of ongoing activities and periodic reviews. Ongoing activities include:

- staying informed of industry trends and developments that may introduce new or exacerbate existing risks,
- regularly reviewing internal data and reports to identify potential risk indicators,
- monitoring regulatory changes and updates that might impact the risk landscape for WGCZ,
- encouraging a culture of risk awareness within the organization, where employees are empowered to report any concerns or potential risks they encounter.

Periodic reviews will be conducted as mentioned above – current periodicity is set to quarterly management reviews given the urgency and regulatory framework development. These reviews will involve a comprehensive assessment of the risk register, considering any changes in the risk landscape, the effectiveness of existing and newly implemented measures and controls, and the need for potential updates to the risk management strategy.

5. Conclusion

This report has comprehensively described the risk landscape for WGCZ in accordance with the Digital Services Act (DSA) and best practices in risk management.

5.1. Highlights

Identified Risks

A total of 38 risk scenarios were identified across eight risk categories. The inherent risk assessment indicated that the majority of these scenarios fall within the medium risk category, with only one classified as high risk.

Effectiveness of Controls

The existing control environment demonstrates effectiveness in mitigating the majority of identified risks. The residual risk assessment revealed only four scenarios with a score above "Low," highlighting the overall robustness of current controls.

Focus Areas

While the initial assessment indicates a well-controlled environment, further focus should be directed towards specific areas within each risk category. These areas are detailed in the action plan (see above).

5.2. Overall risk profile and control effectiveness

WGCZ exhibits a well-managed risk environment. The inherent risk assessment provided valuable insights into potential threats, and the effectiveness of existing controls significantly reduces the likelihood and impact of those risks. However, a proactive approach to risk management necessitates continuous monitoring and improvement.

5.3. Improvement insights

This report recommends ongoing efforts to strengthen the risk management framework and further enhance the internal control environment:

Staying ahead of the regulatory curve

The newly established Compliance Office should actively monitor developments in online safety regulations, particularly those related to the DSA and its potential revisions. Implementing a system for timely updates to the risk management framework based on these regulatory changes will ensure ongoing compliance.

Further enhancing online safety awareness

WGCZ will further its commitment to online safety by joining initiatives that raise awareness among users, especially minors and their guardians. This could involve collaborating with NGOs specializing in online safety to develop educational materials and campaigns. Additionally, consider expanding the existing resources for parents and guardians, offering clear and comprehensive guidance on how to safeguard their children in the online environment.