

Materiality Assessment and Risk Management

1. Materiality Assessment

Kuaishou has integrated material ESG issue assessment into the Company's risk management process. We maintain regular communication with various stakeholders and conduct material ESG issue assessments through four steps — identification, engagement, prioritization, and validation — to review and report on our sustainability policies and disclosures. For the 2025 assessment results, please refer to the [Kuaishou 2025 ESG Report](#).

From the 2025 materiality analysis, we identified the top three issues critically important to the Company's development — **Content Ecosystem Governance**, **Compliance Operations**, and **AI Safety and Governance** — and have established corresponding objectives for each.

Issue	Content Ecosystem Governance	Compliance Operations	AI Safety and Governance
Associated Risks or Opportunities	• Reputational risk arising from insufficient penalties against violating users • Regulatory penalties and reputational risk arising from inadequate platform content oversight	• Risk of intensified government regulation of the industry • Copyright infringement risk	Business growth opportunity presented by new AI ventures
Impact	Revenue decline caused by user attrition	• Restriction of the Group's ability to grow its user base or traffic, leading to revenue decline • Increase in compliance costs	Revenue increase driven by new business expansion
Objective	Ensure the Company is equipped with the latest large-model-related	Implement a compliance culture and ensure 100% compliance training	Ensure the fulfillment of ethical compliance requirements, develop

	safety technologies to enhance the identification of non-compliant content	coverage for all employees, including Board members, management, and all staff (including part-time, intern, and dispatched non-full-time personnel)	industry-leading AI products and services, and enable sustainable development
2025 Progress and Key Initiatives	● Identified over 15 new fraud schemes; reporting and enforcement efficiency improved by 400% year over year ● Average daily interception of over 400 suspected cyberbullying videos	● 100% legal compliance training rate for new employees ● Conducted 2 anti-corruption training sessions for the Board	Select Kuaishou AI products received ISO 42001 Artificial Intelligence Management System certification in 2025 and completed regulatory filing in accordance with GB/T 45654-2025 <i>Cybersecurity Technology — Basic Requirements for Generative AI Service Safety</i> , signifying that AI safety governance has reached industry-leading levels both domestically and internationally
Business Case	As a leading content community and social platform in China and globally, Kuaishou's content ecosystem governance directly impacts user experience and platform reputation. Kuaishou is therefore committed to delivering	Compliance operations form the core baseline for Kuaishou's long-term sustainable development. On one hand, it directly concerns the platform's regulatory red lines; on the other, compliance capability has become a	Kuaishou's Kling AI has become a leading global video generation model. Kling AI is actively expanding its international reach and serving as a bridge for Chinese AIGC creators to connect with the world, fully

	high-quality, safe, and responsible services to mitigate operational risk.	core competitive differentiator, preventing governance gaps from eroding user trust and undermining business growth expectations.	demonstrating the outstanding contribution of Chinese AI tools in unlocking global creative potential.
--	--	---	--

Business Strategy	Content Ecosystem Governance	Compliance Operations	AI Safety and Governance
	Through a comprehensive content moderation and governance framework coupled with product features, Kuaishou continuously enhances ecosystem governance and content diversity. We place a high priority on the protection of minors and spare no effort in safeguarding a healthy, safe, and diverse platform environment, building a trustworthy and vibrant digital community for our users.	Kuaishou consistently upholds integrity in its operations and adopts a zero-tolerance approach toward any form of corruption, bribery, money laundering, or other unethical conduct. We continuously refine our business ethics management policies and governance structure to strictly regulate the Group's business practices. At the same time, we are committed to strengthening employees' ethical awareness, ensuring the effectiveness of our whistleblowing mechanism, and working together with our partners to foster a clean and upright business environment.	We have formulated and implemented a series of standards, including the <i>AI-Generated and Synthetic Content Labeling Management Policy</i> , the <i>Large Model and AIGC Application Security Specification</i> , and the <i>Large Model Security Specification</i> , which strictly prescribe security requirements across the model training, development and deployment, and application lifecycle, and establish mandatory security baselines for data provenance review, de-identification, and output quality control. We actively participate in industry standard-setting to raise the ethical standards of the entire sector.

In addition, from the 2025 materiality analysis, we identified the top two issues critically important to **external stakeholders** — **Information Security and Privacy Protection** and **Content Ecosystem Governance** — and assessed their impact.

Issue	Information Security and Privacy Protection	Content Ecosystem Governance
Relevance to Kuaishou's External Stakeholders and Impact Assessment	As a leading content community and social platform in China and globally, Kuaishou processes vast amounts of user personal information on a daily basis. The protection of sensitive information—including user account details and behavioral data—directly concerns users' privacy rights, property security, and even personal safety. User expectations regarding corporate information security and privacy protection capabilities continue to rise. The effectiveness of the Company's management in this area will directly translate into either user trust or user attrition, producing a material impact on external stakeholders. Positive: Robust information security and privacy protection mechanisms allow users to use the platform with confidence, enhance user trust, and solidify the user base. Negative: In the event of an information security incident, users may face risks including personal privacy breaches, account theft, financial loss, and minors' exposure to harmful	As a platform of national reach, the integrity of Kuaishou's content ecosystem directly bears on the core interests of multiple parties. The content creation, dissemination, and consumption activities carried on the platform each day are deeply embedded in users' daily lives, merchants' business operations, creators' livelihoods, and investors' value assessments. Positive: Robust content safety governance ensures that users—particularly adolescents—can safely use the platform within a clean online environment. Negative: When content safety defenses fail, users may be involuntarily exposed to harmful content, causing psychological harm.

	content, which in turn threatens Kuaishou's own business operations.	
Impact Type	Positive and Negative	Positive and Negative
Quantitative Indicator for Measuring External Impact	100% coverage of all-staff information security training	100% coverage of the "one-touch activation" feature for Minor Mode

2. Risk Management

Risk Management Process

As the complexity of Kuaishou's business operations increases and the external environment continues to evolve, the Company may face various risks, including ESG risks. Through risk management analysis and assessment of the severity and likelihood of various risks, management identified five principal risks for 2025: **Market Competition and Innovation Risk, Information Security and Privacy Risk, Compliance Risk, Fraud Risk, and Reputation Risk**. The Company conducts annual dynamic tracking of its risk management status and estimates potential outcomes for the next period and the full year to assess risk exposure. For detailed risk descriptions and mitigation measures, please refer to Kuaishou's [2025 Annual Report](#).

The Company has established a clearly defined risk appetite framework that sets forth the level and types of risk the Company is willing to accept in pursuit of its strategic objectives.

Risk Culture

We provide regular risk management education to our directors and deliver training on risk management principles to all employees through multiple channels—including online courses and in-person training sessions—covering the risk management system, key risk analysis, and internal controls, with the aim of enhancing employees' risk management awareness and capabilities and strengthening the Company's internal control environment. Concurrently, we incorporate risk management and internal control performance into employee performance evaluations to ensure accountability. Furthermore, we place significant emphasis on risk control throughout the full lifecycle of our products and services and employ a combination of risk forecasting and control measures to embed risk control standards into product development and service delivery processes, thereby effectively conducting risk assessment, identification, and prevention.

Emerging Risk Management

The Company actively identifies and assesses emerging risks that may have a material impact on its long-term strategy and business model. Below are two significant emerging risks identified by the Company in recent years:

Emerging Risk Event	Risk Description	Risk Response Measures
Generative AI Deepfake and Content Compliance Risk	With the proliferation of generative AI technology, the barriers to using AI to produce deepfake videos, disinformation, or non-compliant content have been substantially lowered. If the platform's moderation mechanisms fail to adapt promptly to the evolution of AI-generated content, a proliferation of non-compliant content may result, triggering regulatory penalties and undermining the platform's credibility and user trust.	Regulatory Compliance Alignment: Align with regulations such as the <i>Administrative Provisions on the Labeling of AI-Generated and Synthetic Content</i> by establishing AIGC content review and labeling rules, clearly defining governance principles and compliance baselines. Dynamic Risk Monitoring: Conduct periodic assessments of on-platform AI content risk levels through Violative View Rate (VVR) sampling, providing data to support strategy iteration and enabling early risk trend forecasting. Closed-Loop Disposition: Add a dedicated AI-content reporting entry to the reporting channel for rapid response to risks; build an AI risk case library for periodic analysis and review; dynamically update community rules to form a "detect–analyze–codify" governance closed loop. Tiered Differentiated Management: Display risk warnings during playback for high- and medium-risk content; label low-risk content as "(Suspected) AI-Generated," balancing platform responsibility with users' right to know.

New Types of Underground Industry Fraud Risk	Telecommunications and online fraud and underground industries currently exhibit characteristics of supply-chain integration, industrialization, and concealment. Fraud perpetrators leverage AI technology to precisely target users across short video, live streaming, e-commerce, and private messaging scenarios through rapidly changing conversation scripts and cross-platform traffic diversion. If the platform's risk control systems fail to promptly identify industrialized fraud chains, this may result in user financial losses, regulatory accountability, and erosion of platform trustworthiness.	Risk Control and Anti-Fraud Monitoring: The platform has deployed monitoring models to capture anomalous behavior and negative feedback signals, and refers content leads suspected of illegal activity to law enforcement authorities. Furthermore, we combine intelligent recognition with manual review to provide advance notifications to users at the client side for dramatized or staged content, reducing the risk that users may be misled, and comprehensively fulfill the platform's governance responsibilities.
--	--	---