Yum China Holdings, Inc.

Risk Management Policy

Purpose

This Risk Management Policy sets out the key elements of Yum China's risk management, outlining the main principles behind our risk management framework and process for identifying, reporting, assessing, mitigating, and monitoring risks.

Risk Governance

The Board maintains overall responsibility for overseeing the Company's risk management framework. The Board regularly reviews risks that may be material to the Company. In furtherance of its responsibility, the Board has delegated specific risk-related responsibilities to the Audit Committee, the Compensation Committee and the Food Safety and Sustainability Committee. The Board and its committees consult with external advisors and internal experts regarding anticipated future threats, trends and risks that may be applicable to our Company, our industry and our operations. We regularly provide risk management training to our directors and we believe all our directors possess expertise in risk management.

At the management level, the Company maintains the Compliance Oversight Committee, a management-level committee, which is co-chaired by the Chief Legal Officer and the Chief Financial Officer of the Company and comprised of leaders from multiple functions. The Compliance Oversight Committee meets regularly to monitor and review the implementation of the Company's compliance programs. The Chief Legal Officer reports regularly to the Audit Committee on the Company's key risk areas and compliance programs.

At the operational level, generally, each restaurant that we operate is overseen by a management team led by a front-line store manager, or RGM, together with one or more assistant managers. The front-line restaurant management team is responsible for the day-to-day operation of our restaurants and for ensuring compliance with operating standards. Each RGM is also responsible for handling guest complaints and emergency situations.

The Head of Corporate Audit, who is a member of the Compliance Oversight Committee, directly reports to both the Audit Committee and the Chief Financial Officer of the Company. In addition, the corporate audit function, led by the Head of Corporate Audit, conducts independent risk assessments regularly, including but not limited to the review of management's risk assessment process, and develops audit plans accordingly. Our Head of Corporate Audit periodically reports the results of risk assessments and audit observations, including significant issues that have been discovered and recommendations for improvements, to the Audit Committee.

Risk Culture

All office employees are required to complete annual training on various risk management topics, including the code of conduct, food safety, information security, and human rights, with a target to reach 100% completion rate.

Risk Management Process

- Risk Identification

  The Company underscores the significance of risk identification and management from the Board of Directors to operations teams. We identified internal and external risks, along with business impacts. We categorize identified risks under five categories: Risks related to our business and industry / Risks related to doing business in China / Risks related to the Company's separation from Yum! Brands Inc. and related transactions / Risks related to our common stock / General risk factors. We identify both financial risk and non-financial risk (e.g. ESG risk).

- Risk Assessment

  Identified risks are prioritized and categorized based on various factors, including but not limited to their potential impact, likelihood of occurrence and urgency. Such factors are also used to determine our risk appetite and tolerance levels. The Company monitors the exposure to market risks and operational risks using several objective measurement systems, including a sensitivity analysis to measure our exposure to fluctuations in foreign currency exchange rates, interest rates and commodity prices.

- Risk Management Process

  Various risk management and compliance programs are in place to help build controls and mitigate potential risks and help reduce high level risks. Various measures have also been put in place to monitor if any deviation from our compliance programs. For example, in terms of the development of products and services, we assess risks related to regulatory compliance, food safety, and business continuity throughout the product development and approval process. This comprehensive approach includes:

  - Evaluating the sensory flavor of new products;
  - Reviewing the regulatory compliance applicable to new products, including but not limited to the use of food additives;
  - Conducting food safety and quality audits on the raw materials and suppliers of the new ingredients;
  - Collaborating with third-party agencies to conduct onsite Business Continuity Management (BCM) audits. These audits identify risks faced by suppliers in terms of assets and operations and recommend preventive measures accordingly.

- Risk Reporting, Compliance Programs and Audit

  The Company reviews and reports its risk disclosure on a quarterly basis in compliance with applicable stock exchange rules. Our corporate audit function designs various audit projects each year to assess the measures, tools and process applied to identifying and managing relevant risks in each specific area, considering the likelihood and the impact.

Appendix: Emerging Risk

The Company acknowledges the significant potential impact that emerging risks may have on operations. As part of our risk management process, the Company actively monitors, assesses, and addresses these risks, aiming to identify challenges and develop mitigation plans to minimize adverse impacts.

The example of Yum China emerging risks are as below:

Risk Name	**Our use of GenAI technologies presents new risks and challenges to our business**	**The use and handling of certain information is regulated by evolving and increasingly demanding laws and regulations.**
Risk Type	Technological	Technological
Risk Description	We use Generative AI technologies ("GenAI") to innovate new business scenarios and solutions, such as media creatives generation, digital avatars, customer feedback analysis and customer service. The use of GenAI may be affected by global trends and applicable laws. We may become subject to new or heightened legal, ethical or other challenges arising out of the perceived or actual impact of AI on intellectual property, privacy, and employment, among other issues, and we may experience brand or reputational harm, be subject to legal liabilities or increased costs associated with those issues.	The Chinese government has focused increasingly on regulation in the areas of information security and protection. For example, the PRC Personal Information Protection Law, which took effect on November 1, 2021, sets out the regulatory framework for handling and protection of personal information and transmission of personal information, and many specific requirements of the law remain to be clarified by the CAC and other regulatory authorities. The Measures for Security Assessment for Outbound Data Transfer, which took effect on September 1, 2022, mandate mandatory government security review by the CAC in advance of certain cross-border data transfer activities. We expect that cybersecurity, data privacy and security will continue to be a focus of regulators, as well as attract continued or greater public scrutiny and attention going forward, which could increase our compliance costs and subject us to heightened risks and challenges associated with information security and protection.

Potential Impact	Yum China perceives technological changes not only as significant business opportunities, but also recognized its potential risks. For example, if we fail to leverage GenAI technologies as effectively or rapidly as our peers, our competitiveness could be materially and adversely impacted.	If we are unable to manage these risks, we could become subject to penalties, including fines, suspension of business, shutdown of websites and revocation of required licenses, and our reputation and results of operations could be materially and adversely affected.
Mitigating Actions	**Enhance digital capabilities to seize the opportunities:** We plan to increase our investment in end-to-end digitalization, automation and artificial intelligence ("AI"), to more effectively connect online traffic with our offline assets. We also intend to use GenAI to innovate new business scenarios and solutions, such as media creatives generation, digital avatars, customer feedback analysis and customer service. To improve our operational efficiency, we plan to focus on connecting our front-end, guest facing systems to backend systems such as operations and supply chain. **Enhance AI Data Governance to mitigate the risks :** We will control the AI data training process to help ensure the use of clean data sources that fit AI application scenarios, thereby reducing the risk of malicious manipulation at the data input level. To maintain content integrity and authenticity, we will implement a flexible content review strategy tailored to different business scenarios and conduct data and content security tests on AI-generated content (AIGC) at both input and output stages. Internally, we will provide technology-related training sessions to	Our information technology systems are protected through technological safeguards and management measures. We detect, identify, assess and mitigate cybersecurity risks by adopting standard risk management methodologies, which are developed based on the international cybersecurity management system standard ISO 27001 as well as the asset-oriented risk assessment framework. To minimize potential impact on business operations in the event of a cybersecurity incident, we have formulated, and regularly tested, our incident response plan. We also established a framework for data security and personal information protection, including measures to prevent data loss and detect and block abnormal accounts and activities, as well as systems and processes to prevent, detect and mitigate vulnerabilities. Our employees participate in regular cybersecurity training to enhance their awareness of cybersecurity risks. We engage in the periodic assessment of these processes and practices that are designed to address cybersecurity threats and incidents. We regularly engage external consultants to assess and independently verify our cybersecurity risk management, striving

	enhance employees' proficiency with AI tools and increase their awareness of AI-related risk prevention. Additionally, we will establish a security and compliance review process for AIGC-related projects during the demand design phase, actively identifying risks in application security, data security, business security, content security and legal compliance. This process will include generating security review reports with identified risks, assessments, and remediation suggestions.	for continuous optimization of our cybersecurity policies, cybersecurity risk management processes, and technical measures. These engagements assist us in ensuring our cybersecurity management practices and technical measures comply with applicable laws, regulations, industry standards and the Company’s policies. The Company has maintained ISO/IEC 27001:2013 certification since 2018 for certain online business. We have established processes designed to manage cybersecurity threats associated with the use of third-party service providers. These processes include security evaluations before third-parties' admission, ongoing oversight and assessment of their security status, and adopting necessary security measures at termination of services.