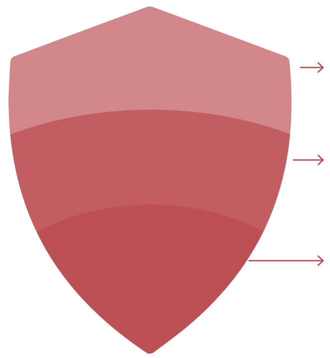
Risk Management

In accordance with the COSO framework, the Company adopted three defense lines for risk management and internal control.



- Internal infrastructure network failure
- Partial or complete server failure
- External operator network outage
- Critical data missing

- Unscheduled external power outages
- i p ete server fW

Business Continuity

Öűœ >ηɣƩĪIǫ űĪp ŎœGœ∃ηƩœŎ Ī ňηɣƩ2œűœIpΰGœ <njpΰIœpp >ηIΰInjΰǫ ¥ĪIĪũœɣœIΰ <>¥ pǫpΰœɣ Ŏœpΰũ IœŎ Ώη œIpnj2œ ηƩœ2ĪΰηIĪ∃ pΰĪņΰ∃ΰǫ This system integrates the Incident Management Plan (IMP) and the Business Continuity Plan (BCP), serving as a key component of the second defense line. To guide the effective planning, implementation, and ongoing enhancement of the BCM system, the Company has created a *: IĐŁŠĠĐĐ ;ŨŠFŁŠ IɟƵ xùŠùĶĠŞĠŠF xùŠIù* in accordance with the ISO 22301 Business Continuity Management Systems.

BCM System

Internal Audit

The Internal Audit Department, as the Company's internal independent audit institution, serving as the core of the third defense line. This department continuously oversees key risk domains, including social responsibility, financial transactions, procurement operations, asset management, sales activities, and information security, through regular inspections, audits, internal control evaluations, and specialized reviews. In 2024, we undertook targeted improvements to dozens of policies and systems, ensuring the robustness of the organization's internal control framework.

Completed of internal audit tasks

25 Ώΰɣœp

Audit frequency and coverage: Each BG/BU is required to undergo at least 1 comprehensive audit every 2 years

[10] BG/BU: Business Group/Business Unit