2023 Stress testing

According to the " Risk Management Regulations" which was approved by the Board of Directors in in December 2020, each risk management team should, based on its own operational function, identify operational process risks, evaluate risk factors, set up risk indicators and prevention mechanisms, and establish risk appetite and tolerance or perform stress tests for high-risk items, in order to control and manage risks effectively.

The results of sensitivity analysis or stress testing conducted by the Company on financial and non-financial risks in 2023 are as follows:

A. on changes in financial risks, such as Exchange rate risks stress test.

DRAM sales are mainly in US dollars. Assuming that the exchange rate of New Taiwan dollar against U.S. dollar in 2023 will rises to 29.50 from 30.71 at the end of 2022, it's estimated that the maximum of loss will be NT$350 million.

B. Non-financial risks: such as changes in water availability, Operational risks- Electricity supply), Market risks– ASP and Quantity; Strategic business risks- Operation Profit Forecast and Compliance risks- Violation of U.S. Antitrust regulations etc.

a. Water availability - Water availability stress test

- We inspect the company's internal and external water supply and storage systems, simulate the water restriction conditions at each stage. We use our own wells for 5,500 CMD, 43,000 tons of reservoirs, and dispatch Chang Gung Golf Course wells for 3,600 CMD to maintain production for 47 days under the condition of complete stop of raw water.
- Simulating the possible conditions of first and second-stage water restriction and third-stage water restriction, all will not affect production.

b. Operational risks - electricity supply

- Power outages will seriously affect the company's production and manufacturing. The company's important production systems and equipment are connected to the DUPS system and emergency generators in the factory to avoid the impact caused by sudden power voltage drops or Taipower's planned power cuts.
- After reviewing the company's internal and external power supply systems, when the simulated power supply is reduced by 5%, 10%, 15%, and 20% according to the contract capacity, the factory can still maintain production with the emergency generator and DUPS in the factory. However, the complete interruption of external power supply will cause the loss of production suspension. According to revenues in 2022, the impact is estimated to be about NT$4.7 billion per month.

c. Market risks – ASP and Shipment Quantity

Nanya regularly conduct two-factor sensitivity analysis to confirm the achievability of business objectives and formulate contingency strategies and plans.

- We expected that price decrease 33% compared with 2022 and calculated changes of EPS changes if the decrease is -38%~-29%.
- We expected that sales volume increase 13% compared with 2022 and calculated changes of EPS if the increase is +1%~+25%.

d. Business strategic risks – Operation Profit Forecast

We conduct profit and loss sensitivity analysis to formulate sales and production strategies. We can see the impact of profit and loss of each product combination from the analysis of target price under 90%, 110%, and 120% price change and formulate a favorable production strategy.

e. Compliance risks - Violations of US antitrust regulations

- The results of performing the risk assessment are as follows:

(1) Assuming the actual profit that sales of memory modules for servers shipped to the United States is US$6.25 million. And it is assumed that the victims determine the damage based on the company's actual profit.

(2) Since the total amount of benefits obtained from the acts did not exceed US$100 million, the maximum fine of the criminal penalty may not be increased to twice. Therefore, in terms of the criminal fines, the company can be fined up to US$100 million, and the punitive damages for civil compensation can be multiplied by 3 times, which is approximately US$18.75 million. Based on these calculations, the total amount would be about NT$3.56 billion.

(3) In addition, it may cause varying degrees of negative impact, such as corporate value index (CSR, DJSI), company reputation and stock price fluctuations, etc.

- Risk Management:

(1) The impact of investigation procedures, litigation costs, company reputation and finances:

To prudently evaluate all internal evidence to gain a more favorable position and conditions for settlement negotiations in seeking early termination of litigation or mitigation of liability to avoid punitive damages and effectively control the litigation costs to reduce risks.

(2) The impact of the compliance risks for employees & the management: We can offer an operational legal compliance plan with regularly internal audit process and conduct legal compliance training for general and the high-risk employees to prevent and mitigate the future risks and ensure the implementation of the legal compliance plan as well. In addition, we can

manage the liability insurance for the directors and officers to guarantee the expenses and the cost of compensation arising from the related litigations are covered.

f. Information Security Risk- Hacking incidents

- In response to the emergence of hacking incidents in recent years, enterprises face hacker threats everyday. In addition to prevention, the handling of hacking incidents requires regular drills to achieve the purpose of procedure verification, tool verification and improvement of proficiency.
- Once a hacking incident occurs in an enterprise, it must race against time from notification, response and recovery. Through drills, the processing timeliness of each stage can be actually evaluated or tested, and the operation can be standardized or automated to simplify and improve the overall timeliness and reduce the impact of hacker intrusions.
- According to the drill of hacking incidents, adjust the system detection and reporting methods, revise the emergency response procedures, and draw up the priority of restoration of personal computers by the principle of reducing disaster losses, to achieve the goals of incident prevention, detection and damage control at each stage.
- According to a professional information security survey, the hacker group can complete the invasion in 18 minutes and 49 seconds at the fastest; and according to the 2022 iThome CIO survey, it is found that the high-tech manufacturing industry is in the state of hacker attacks on average 74% of the time, and it takes an average of 9.1 days to discover the hacker attack.
- If the hackers can be stopped before the intrusion, the harm can be effectively prevented. This time, without warning, the hacking activity can be found within 15 minutes, and the system can be restored within 2 hours, confirming the current intrusion detection and the response time both meets the target.