AIS Enterprise Risk Management Framework & Processes

The AIS Enterprise Risk Management framework and process are aligned with the integrated framework of the COSO ERM 2017: Enterprise Risk Management Integrating with Strategy and Performance and is applied to business risk management and fraud risk management. The 7 steps in the risk management process are:

1. **Set objectives** at both corporate and functional levels, with alignment to the AIS corporate strategy and are within its risk appetite as approved by the Board of Directors and reviewed annually. In establishing its risk appetite and tolerances, AIS defined the types of risk that are acceptable and unacceptable in pursuit of value.

2. **Identify the events** that could have a negative impact (risks) on AIS's ability to achieve its goals and targets considering internal factors such as operational processes and human resources, and external factors such as customers, the economy, politics, and regulations.

3. **Assess** the identified risks by considering the likelihood of the risk occurring and the potential impact if the risk were to occur. Added to this is the correlation between the impact of any risk and how it could affect another risk.

4. **Prioritize risks** with consideration to the degree of importance of each risk and the potential damage to the Company.

5. Plan **risk response** measures with consideration to the level of risk involved and the corresponding cost and benefit.

6. Establish **control activities** to help ensure that the desired risk responses are implemented as intended and are carried out effectively.

7. **Monitor and report** the status of risks and the effectiveness of the risk management process. Reports are to be forwarded to the Audit and Risk Committee, the Executive Committee and the Board of Directors regularly.

Risk assessment

Risk assessment approaches may be qualitative, quantitative, or a combination of both.

- Qualitative assessment approaches, such as interviews, workshops, surveys, and benchmarking.

- Quantitative assessment approaches, such as Monte Carlo simulations, sensitivity analysis and scenario analysis.

Financial risk: Sensitivity and scenario analysis allow management to understand the uncertainty that might occur from liquidity risk, credit risk, interest rate, and exchange rates risk, as well as the resilience and tolerance level of our financial positions towards these risks. The potential impacts from sensitivity and scenario analysis are used in supporting decision-making and preparing proper mitigation such as in investment evaluation, managing cash flow and capital structure, and defining operating models.

Non-financial risk: AIS conducts sensitivity, scenario analysis, and stress testing to gauge strategic risk, technological risk, regulatory & legal risk, and operational risk. The analysis allows management to understand the company's exposures and worst-case scenarios that would impact our business, as well as to evaluate the financial impacts and our company's resiliency in various scenarios related to particular risks.

Effectiveness of Risk Management Process

To ensure appropriateness and effectiveness of the Risk Management Process, AIS conducts both internal audit and external audit.

Internal Audit:

- Audit and Risk Committee, appointed by the Board of Directors, is responsible for performing risk oversight to ensure compliance with the Company's risk management framework and guidelines. The Audit and Risk Committee conducts quarterly meetings to review and assess the adequacy and effectiveness of risk management.

External Audit:

- External parties including independent third-party auditors, assess the effectiveness of risk management process annually, as a part of other management standards i.e., ISO/IEC 27001 (Information Security Management Systems), ISO 22301:2019 (Business Continuity Management System), ISO 50001:2018 Energy management systems and ISO/IEC 20000-1:2018 Information technology — Service management.
- Regulators such as National Cyber Security Agency (NCSA) and Bank of Thailand (BOT) specifically review IT risks annually.

Significant risk factors

In 2022, AIS considering risk factors based on Sustainability (Environmental, Social, Governance: ESG) by considering risk factors that are ongoing risks and emerging risks that might occur under the changing environment. It can be classified as follows:

Risk category / ESG	Strategic Risks	Operational Risks	Financial Risks	Compliance Risks	Emerging Risks
Environmental (E)					Climate Change Risk

Risk category / ESG	Strategic Risks	Operational Risks	Financial Risks	Compliance Risks	Emerging Risks
Social (S)		• Risk of Data Privacy • Risk from inability to acquire and retain interdisciplinary talents			Emerging Regulatory Risks for Artificial Intelligence (AI) Technology
Governance and Economic (G)		• Risk from Intensive Competition in the Market • Risk from Technological Advancements and substitution of products and services • Supply Chain Risk • Risk from Major network Failure or Interruption to Important Systems • Risk to Information Security and Threats from Cyber-Attack	• Risk from Exchange Rate Fluctuation • Risks from the absence of a debt covenant ratio	• Risk from changes in government policies, rules, regulations and orders of regulators • Risks Arising from Disputes with Government Agencies	• Risk from the Potential Consolidation of Main Competitors • Geopolitical and Geoeconomics Risk

Emerging Risks

AIS has assessed the emerging risks, evaluated their impacts, as well as defined mitigation actions to manage those risks effectively as follows:

#1

Name **Emerging Regulatory Risks for Artificial Intelligence (AI) Technology**

Description Recent development and use cases of AI have been materializing in several areas. For example, machine-learning chatbot technology can be used to optimize customer experience and employee capabilities for our Call Center operations. AI and data analytics in customer behaviors can be used to create marketing campaigns and product/service offerings that meet the needs of the target groups. AI is also

playing a central role in smart business solutions that we offer to our Enterprise customers. While AI technology holds tremendous potential for the telecommunication industry, emerging regulatory risks must be addressed to ensure its responsible and ethical use. Data privacy, algorithm transparency, bias mitigation, and liability attribution are key areas which may be subject to regulatory frameworks. By proactively addressing these challenges, the telecommunication industry can harness the transformative power of AI while safeguarding consumer rights and fostering innovation.

Impact

- Data privacy: With the collection and processing of vast amounts of personal data in the telecommunication networks. We need to ensure that this data is handled securely, with explicit consent from users, and in compliance with privacy laws. Incidents of data leak are not only costly in terms of potential liabilities, but also a significant cause of reputational damage.
- Transparency: As AI and its algorithms make complex decisions that impact network management, service provisioning, and customer experience, it becomes essential for AIS to understand the reasoning behind these decisions. Telecom operators may be required to provide clear explanations for AI-driven actions, enabling transparency and building trust with customers and regulators. Inadequate transparency could be a subject of negative social sentiment and regulatory issues for AIS.
- Potential bias: Biased algorithms can lead to discriminatory outcomes, such as unequal access to services or biased pricing models packages like prepaid, postpaid, fixed broadband packages, etc. Such bias could create a broader impact on ethical and human rights implications. These issues relate to the social dimension of the ESG pillars; therefore, could cause reputational damage. Addressing and mitigating bias in AI systems is crucial to avoid reputational damage and ensure fair and equitable treatment of customers.
- Liability attribution: As AI system makes autonomous decisions, determining accountability for any harm or errors could become complex. Regulatory frameworks may provide guidelines to attribute liability and responsibility, ensuring that telecom companies are held accountable for any adverse impacts caused by their AI systems. Clear rules and guidelines regarding liability attribution can help protect customers and incentivize responsible AI implementation. Additionally, non-compliance with regulatory requirements can result in significant financial loss for telecommunication companies. This may include fines, penalties, legal expenses, and potential loss of business opportunities due to reputational damage. Compliance efforts, such as implementing necessary safeguards and conducting audits, also require significant resources.

Mitigation

- Implement strict guidelines to safeguard sensitive information and prevent unauthorized access or misuse. Refer to our Cybersecurity and Customer Privacy Protection. Cybersecurity and Customer Privacy Protection | Advanced Info Service Public Company Limited (ais.co.th)

- Ensure diverse and representative training data to mitigate biased results and perform testing to identify and rectify biases in AI systems before they go live.
- For algorithm transparency and liability attribution, as the regulatory frameworks in Thailand are still lagging, we need to monitor the regulatory landscape closely, and ensure that our work processes are designed to have adequate clarity so that we can provide the expected transparency to customers and regulators.
- AIS needs to closely monitor regulatory developments, actively engage with policymakers, and contribute to the development of appropriate policies that balance innovation with societal and consumer protection. Stay updated with relevant privacy regulations and ensure compliance with data protection requirements, such as the General Data Protection Regulation (GDPR) or other applicable laws that may be applied in Thailand.
- Proactively study AI-related standards and guidelines and their implications on our businesses, for example, the OECD principles on AI and Thailand National AI Strategy and Action Plan. These principles could be the foundation of AI-related regulations in the future.

#2

Name	**Geopolitical and Geoeconomic Risks**
Description	Major geopolitical events such as Russia-Ukraine conflict and U.S.-China tension are creating shocks on global markets as well as domestic economic conditions. The recovery of businesses post-pandemic is ongoing, but with different speed and scale for each sector. The pressure is mostly felt by smaller businesses and the low and middle-income households. These factors result in rising cost-of-living, uncertainty in the macroeconomic environment, consumer and business demand and supply, purchasing power, employment, and tourism. These shocks are prominent in many industries including technology and telecommunication.
Impact	• The rising cost-of-living forces customers to re-assess their spending priorities, especially in prepaid which holds a majority portion of the subscribers. This could lower the ability to generate revenue growth. • An uncertainty in economic conditions and an increase in operating cost of other businesses may result in the delay of their investments in CCIID (Cloud, Cyber Security, IoT, ICT, and Data Center) solutions; therefore, it could impact the ability to generate revenue growth from our enterprise business. • Geoeconomic risks, such as trade wars or restrictions on technology exports, can disrupt the global supply chains of telco companies. Dependencies on specific vendors or regions for critical equipment, components, or technologies may lead to delays, increased costs, or shortages, impacting operations and network deployment plans. • An increase in operating cost from higher energy price, inflation, and potential disruption in supply and demand could impact the ability to generate profit of the

company and may also delay investments in new businesses. These factors may reduce competitiveness in the long term.

Mitigation

- Provide products and services in a variety of price levels and packages for consumers to choose according to their purchasing power, including products and services that are targeted to specific customer groups to meet their needs. Moreover, implement targeted marketing campaigns to highlight the value and relevant features.
- Provide various distribution channels for customers to easily access including shops, online channel and agents.
- Conduct a comprehensive analysis of the supply chain to identify potential vulnerabilities and develop contingency plans. Additionally, maintain strategic inventories of critical equipment or components to mitigate potential delays or shortages during periods of supply chain disruptions.
- Enhance the features of myAIS application to include other services that meet consumer's lifestyle and several use cases.
- Implement energy-efficient technologies and practices to reduce energy costs and minimize the impact of higher energy prices.
- Regularly review the allocation of capital and cost structure among various businesses. Encourage business units to revisit operating model and do transformation programs to improve cost structure.

#3

Name **Climate Change Risk**

Description Climate change is an issue that has increasingly gained attention from the global community. As one of the top 10 countries that were most affected by extreme weather events, Thailand has joined forces with the international community to tackle the problem, announcing a plan to pursue a net-zero carbon emissions target by 2065. The development has made climate change an emerging risk, prompting the Thai government to adjust policies. It is now in the process of drafting climate change-related laws and revising the national energy plan to prepare for operations in line with the target. In addition, the failure of climate-change adaptation has been discussed in the global community, resulting in the need for adjusting the plans to tackle increased risks from climate change.

Impact AIS business operations are likely to be affected by physical risks and transition risks in 3 areas as follows:

1. Natural disasters which may damage the network infrastructure and devices can increase operating costs from leveling up preventive measures against damage and maintenance. Also, transportation and production may be impacted by supply chain disruption.
2. The changing regulations and government policy that tend to control greenhouse gas emissions and can put upward pressure on the operating and management

costs may prompt AIS to adjust its way of thinking and create innovations that enhance energy efficiency and reduce greenhouse gas emissions in compliance with future legislature.

3. The changing behaviors of consumers to become more eco-conscious bring both challenges and opportunities for AIS, demanding the Company to adjust business strategies and corporate image to align with such development. This can generate new sources of revenue from low carbon products and services for enterprise clients looking for digital services that help reduce greenhouse gas emissions and for general customers opting for companies with concern for the environment.

Mitigation

- Changing the targets to be aligned with the global and national trends. Aiming to be a part of global community to tackle with climate change, AIS has thus adjusted the Company's environmental targets to be more challenging by adopting the Science-based Target Initiative (SBTi) which stimulates the business value chain to streamline its operations to be more environmentally friendly.
- Promoting Energy Efficiency by studying customers' usage behavior and using power saving features to properly manage network channels to help reduce energy consumption and GHG emissions.
- Alternative Energy Use by installing solar panels at base stations, data centers and switching centers. Moreover, AIS has teamed with business partners with expertise in alternative energy to plan and accelerate the proportion of alternative energy use for lower operating and management costs.
- Preparation for climate adaptation. We assess climate-related risks through scenario analysis and formulate plans for new site construction such as elevating the Mobile Base Station (BTS) and build flood wall in flood-prone areas.
- Developing smart solution services to enable corporate clients to enhance energy efficiency as a means to reduce GHG emissions such as Smart factory and Smart property & building. Furthermore, AIS encourages customers to switch from mailing bills to E-billing and promotes my AIS application. This effort helps reduce paper usage and the need for travel.