2. RISK MANAGEMENT

2.1 Risk management policy and plan

True group is committed to effective risk management which includes the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects. The purpose of risk management policy is to ensure that risks in the Company are identified, assessed, and treated in a way that supports the Company in achieving its goals and to ensure that the Company has risk-based information to support business decision-making.

The Company has adopted the frameworks developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), namely the COSO 2017 Enterprise Risk Management–Integrating with Strategy and Performance. In addition, the Company follows the standards as set out in the International Organization for Standardization (ISO) 31000 – Risk Management.

2.1.1 Risk Management Framework

The Company's risk management framework is adopted from COSO 2017 Enterprise Risk Management framework which consists of 5 main components:

- **Governance and Culture**

  Governance sets the Company's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise-wide risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk.

- **Strategy and Objective Setting**

  Enterprise-wide risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

- **Performance**

  Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The Company then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

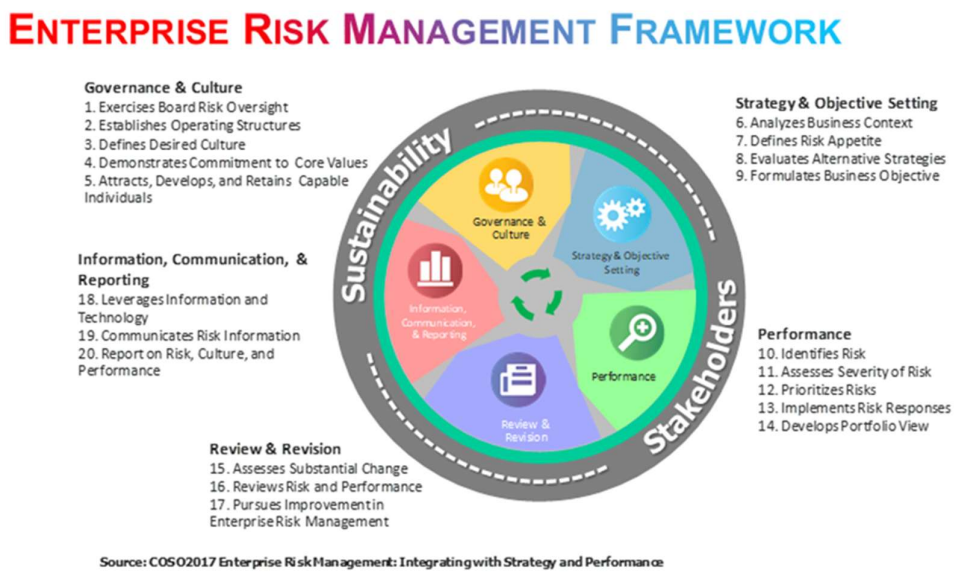
- **Review and Revision**

  By reviewing performance, the Company can consider how well the risk management components are functioning over time and any revisions needed are identified.

- **Information, Communication and Reporting**

  Risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

These 5 components are supported by a set of 20 principles as shown in Figure 1 Risk Management Framework below. These principles cover everything from governance to monitoring.



Source: COSO2017 Enterprise Risk Management: Integrating with Strategy and Performance

2.1.2 Risk Management Process

The Company's Risk Management process is adopted from ISO 31000 - Risk Management which sets out 6 steps to managing risks systematically where this process must be performed continuously. Further guidance provided in the Risk Management Procedure, state below.

- **Scope, Context, Criteria**

  To define the scope of the process and understand the external and internal context.

- **Risk Assessment** –

  To identify, analysis, and evaluate risk.

- **Risk Treatment**

  To select an implement option for addressing risk.

- **Recording & Reporting**

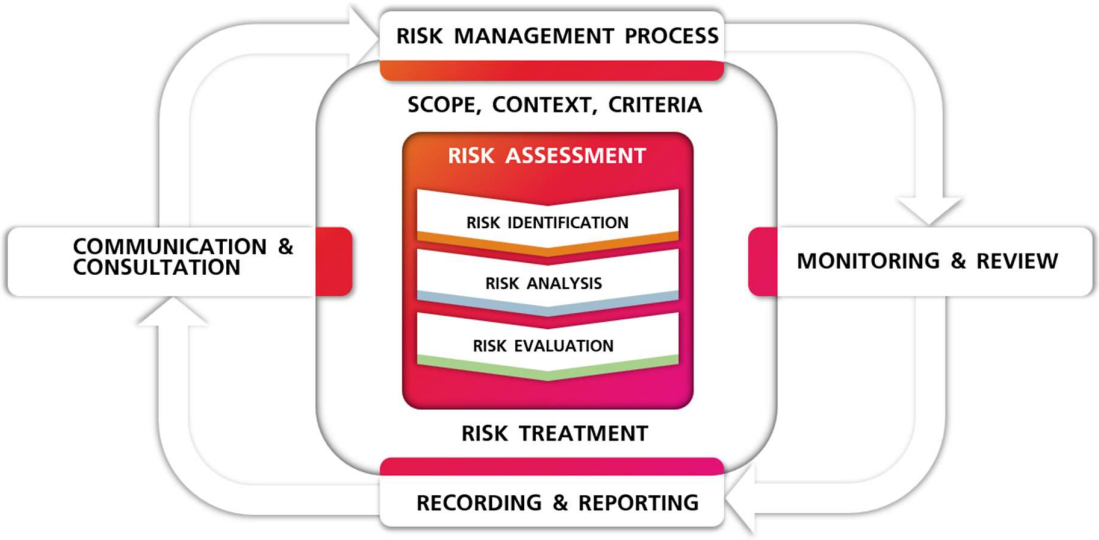
  To document and report the risk management process and its outcome.

- **Monitoring & Review**

  To assure and improve the quality and effectiveness of process design, implementation, and outcome.

- **Communication & Consultation**

  To assist relevant stakeholders in understanding risk, the basis of decision making, and the reason of action required. To promote awareness and understanding of risk.



2.2 Risk factors on business operation

2.2.1 Risk factors on business operation

(1) Risk of revenue erosion due to market, socio - economic situation and noncompliance with (NBTC) remedy requirement

Risk of economic situation

Thailand's economic situation affected by global economic conditions. Since the COVID-19 crisis hit in 2019, the country's economy has been affected by several global crises, including aggressive market competition, inflation rate, decreasing number of tourists, and instability of supply chain. As a result, the company must alter to maintain effective operations and provide essential telecommunication infrastructure and services as well as promoting the company competitiveness in the national level.

True Group has never stop looking for opportunities to elevate service efficiency. The merger between True and dtac provides many beneficials, for instance managing costs, development of products and services, transforming into a Technology Company, emphasizing on value-added services, integrating AI technology in analyzing process, improving customer services to enhance customer satisfaction, creating ecosystem to enrich customers experience on the company products and services.

Risk of noncompliance with NBTC remedy requirement

Thailand's National Broadcasting and Telecommunications Commission (NBTC) has given conditional clearance for the proposed merger of True and Dtac, which the company has given priority and *strictly adhere* to the NBTC's requirements.

(2) Risk from amalgamation

Risks from changes in the regulatory compliance

Presently, the business operations of the Company Group are under the rules and regulations of several government agencies such as the NBTC and the Electronic Transactions Development Agency (ETDA), etc. These government agencies have promulgated and revised many rules and regulations which may affect the business operation of the Company Group and put the Company Group in a regulatory risk from enforcement or different interpretations between the Company and its subsidiaries and different government agencies. In addition, as the regulatory policies of the NBTC directly impact on the structure and competition in telecommunications market, the changes of which might result the Company Group to increasingly obtain the costs of business operation and to encounter higher competition.

Risks from operation associated with the regulatory agencies

True (before the amalgamation) and DTAC notified the amalgamation to the NBTC pursuant to the Notification of the NBTC on the Regulatory Measures for Merger in Telecommunications Business. On 20 October 2022, the NBTC resolved to acknowledge the amalgamation between True (before the amalgamation) and DTAC, and has determined the conditions or specific measures for the amalgamation. Such conditions or specific measures may bring certain limitations to the business operation by the Company Group which include the increased responsibilities and business expenses arising out of the Company Group complying such conditions or specific measures. The NBTC may also determine additional conditions or specific measures in the event substantial change in telecommunications business.

(3) Risk of Delay in Integration (Post-Amalgamation)

Delays in efficiently integrating operations can result in adverse impacts to the Company such as lower employee engagement, raised talent attrition, failure to become a more efficient organization, loss of business value, additional costs, and inability to benefit from subsequent synergies.

In efforts to shape the Company, we actively monitor and pursue opportunities to optimize our portfolio, delivering value for our shareholders and improving returns. To enable this, we have robust policies and

governance structures in place, such as the Transformation Forum, dedicated to steering our transformation efforts and ensuring we execute at scale. We also have robust communication plans and employee engagement activities throughout periods of change to encourage talent retention and engagement. Moreover, the transition to a single grid as a multiband modernized network will maximize customer benefits and contribute to synergies.

(4) Risk of Cybersecurity Attacks

Customer behaviors in data usage and online transactions have increased digital inter-dependencies exponentially. The company continues to strengthen and expand services and digital platform to serve this growing demand. Whereas more complicated and frequent cyberattacks targeting on networks and data, including the use of malware, ransomware, phishing, and other means to obtaining unauthorized access to our telecom networks and systems elevates the vulnerabilities of cybersecurity risks and requires more advance defense architecture.

Cybersecurity failure causing data loss, sensitive personal data leakage as well as equipment failures and network interruption, could result in business disruption, financial loss, reputation damage and legal liability.

To cope with Cybersecurity threats, True has mitigation actions in terms of:

GOVERNANCE

- Appoint Business Security Officer and team to detect cybersecurity risks and to ensure the operation of Information System Security.
- Implement personal data protection system and procedure following NIST Cybersecurity Framework and other international standard like ISO/IEC 27000, and GSMA
- Cooperate with National Cyber Security Agency (NCSA) and relevant international agencies, namely GSMA, and T-ISAC.
- Develop a robust incident response plan that outlines the steps to be taken in the event of a cybersecurity incident to include procedure for detecting, containing, and mitigating the impact of an incident, as well as for communicating with stakeholders and reporting the incident to relevant authorities.

INFRASTRUCTURE AND TECHNOLOGIES

- Continual improvement of network security, data security system, and digital infrastructure according to ISO and CIS standard.
- Set up and continually improve the Security Operation Center (SOC), and certified ISO/IEC 27001:2013

- Implement Security Orchestration Automation Response and apply advanced Security Operation Center (SOC) threat modelling to improve identification of cybersecurity threats, prioritize, and perform risk mitigation as well as to develop Incident Response (IR) procedures for handling incident types such as malware, business email compromise, phishing, and Advanced Persistent Threat (APT), etc.
- Continuous Monitoring and Improvement to detect and respond to cybersecurity threats in real-time and adopt of Machine Learning for incident detection and Threat Intelligence Service as a threat hunting to detect emerging threats in the wild. Regularly review and update security measures to adapt to evolving threats and technologies.
- Automated security checks: Vulnerability Assessment scan is performed on internal (monthly) and external systems (weekly), all findings to be tracked and mitigated in a timeframe according to its risk level.
- Secure data protection for sensitive/personal data at both in-transit and at-rest data by having access control, authentication mechanism and encryption of data.

CAPACITY AND CULTURE

- Capacity building for IT workforce about evolving cybersecurity, including advanced technologies such as AI, NFT, crypto currency payment.
- Cybersecurity architecture forum and Cybersecurity Ambassador were set up to make sure all employees adhere to the policies and practices and comply with the Personal Data Protection Act and other related laws. Employees can consult Data & Security Governance and Data Privacy Center team.
- Continue building a culture for cybersecurity through internal communication media, cybersecurity hub, online and onsite training in both intermediate and advance journey projects to staff and managements.

(5) Risk of Data Privacy

True is subject to obligations under the Personal Data Protection Act 2019 (PDPA) with the full effectiveness on June 1, 2022. With over 51 million subscribers and tremendous scale of interconnected devices and platforms, the company and its subsidiaries are well aware of data privacy risk and has emphasized to ensure that all processing of personal data is lawful and transparent with data subjects (customers).

This includes risk mitigation measures as follows:

- Designate a Data Protection Officer (DPO) for every subsidiary and provide affiliates with guidelines to offer recommendations in accordance with relevant laws and regulations.
- Collaborate with all governance departments to collectively enforce privacy measures throughout the organization, encompassing data collection, utilization, and disclosure.
- Prioritize privacy as a fundamental requirement for any personal data usage and implement technical solutions and controls to ensure transparency in all personal data utilization.
- Ensure compliance with third-party service providers and have all parties sign Data Processing Agreements.
- Maintain and nurture a data privacy culture by utilizing internal communication channels, online and on-site training in both intermediate and advanced projects for both staff and management.

(6) Financial risk

Risks Relating to Leveraged Position

According to the consolidated financial statements, the Company had interest-bearing debt (including lease liabilities) totaling Baht 477.5 billion at the end of 2023, decreasing from Baht 478.6 billion at the end of 2022 due to lower outstanding of debentures. The Company's future funding sources may include additional borrowing and/or debenture issuance. As such, it may be at risk of not being able to obtain reasonable funding for principal repayments and interest payments or its future business expansion plan could be affected. Nevertheless, the Company should be able to raise new borrowings to repay existing debts and adjust their principal repayments to be in line with their cash flows. In addition, the Company has various funding sources including cash flows from operations, vendor financing, and asset divestment. The Company is committed to maintain its financial discipline and will select an optimal mix of capital structure to support future expansion.

In this regard, the Company Group has never defaulted on debt payments with financial institutions and any other creditors. Also, the Company Group has complied with the conditions to maintain relevant financial ratios (if any).

Risks of the Debenture

Credit risk: Credit risk refers to the risk that the issuer may be unable to pay interest (if any), or principal for no matter of any reason. Cessation by the issuer of paying interest or principal constitutes default under the debentures. If the issuer is declared bankrupt or in default of debt payment under the debentures, the debenture holders' right to apply for debt payment will rank *pari-passu* with that of other unsubordinated and unsecured creditors of the issuer. Investors can consider the credit ratings prepared by credit rating agencies to assess the issuer's credit risk, to support their investment decisions. The risk of the debentures reflects on their credit rating, the higher level of the risk, the lower level of the credit rating, and the greater probability of the higher return.

In addition to the issue's credit rating or issuer's credit rating, investors should study the issuer's performance before making an investment. Investors should also follow up on the updated information about the issuer, and the revisions to credit ratings published on the websites of the Office of the Securities and Exchange Commission, the Credit-rating agencies, and the Thai Bond Market Association.

Price risk: The investors who sell the debentures before the maturity date may face with the lower yield earning during times of rising market interest rates, and vice versa. The change on the market interest rate will have more effect on the debentures which have the longer time to maturity.

Liquidity risk: Liquidity risk refers to the risk that occurs when debenture holders wish to sell the debentures in the secondary market prior to the maturity date. Debenture holders may be unable to sell the debentures immediately at their preferred price due to low liquidity of the debt instrument in the secondary market. The issuer will not trade the debentures on any exchanges. Debenture holders may trade the debentures at commercial banks, securities companies, or any other juristic entities having debt instruments dealing license.

Risks from Foreign Exchange Rate Fluctuation

The principal revenues of the Company are denominated in Thai Baht currency. Capital expenditure constitutes most of the Company's expenditure. For capital expenditures, the Company has established an agreement with most of the suppliers to pay in Thai Baht.

For the remaining foreign currency exposure, the Company utilizes foreign currency revenue from International Roaming to partially match foreign currency expenses (Natural Hedge) and enters FX hedging transactions as it deems appropriate.

(7) Emerging Risk

(a.) Risks arising from increasingly severe environmental crisis due to the failure of measures to mitigate global warming

RISK CATEGORY : Environmental

RISK FACTOR : Natural Disaster

Environmental issues are the main cause of the world's biggest problem, the climate crisis. Many environmental situations are getting worse like severe drought, uncontrollable wildfire in many regions, melting ice caps and sea level rise. These are some of the consequences of human-made that damage environment. To name a few of major issues in Thailand contributed to climate rising, failure waste management, releasing wastewater to the environment without proper treatment, and crop residue burning. Environmental crises are becoming more frequent and severe, resulting from failure to slow global warming. This is a major concern for businesses and individuals alike, including the Telecommunication sector.

Potential Impact:

- These climate change-related risks can cause impact to True's network equipment and facilities located throughout the country to suffer failures.
- Increased risk of natural disaster may cause higher insurance premiums and other unforeseen impacts due to climate change are also possible.

Mitigation Actions:

- Developing climate change adaptation plan to identify climate change-related risk vulnerabilities across all relevant assets and operations. Mitigation measures can be planned ideally so that context-specific factors are considered.
- Implementing Business Continuity Plan (BCP) to the critical functions. For Example, the BCP includes the Network Engineering Operations team to monitor impacts of temperature variations on equipment reliability and lifespan and assess the need for specific management measures and selecting more resilient equipment to improve cooling systems.
- Identifying and preparing critical resources for crisis management, considering related aspects as in a) people; b) information and data; c) physical infrastructure such as buildings, workplaces or other facilities and associated utilities; d) equipment and consumables; e) information

and communication technology systems; f) transportation and logistics; g) finance; h) partners and suppliers.

- Coordinating and creating alliance with the government agencies as well as other network operators to monitor natural disaster, exchange information and develop natural disaster early warning system, to minimal the damage and ensure the continuity of the country major communication infrastructure.

(b.) Risks arising from resource rivalries (critical resources for telecommunication infrastructure)

RISK CATEGORY : TECHNOLOGICAL

RISK FACTOR : SCARCITY of NATURAL RESOURCES

The exponential increase in resource demand has proved difficult to meet through a rapid expansion of supply. This escalating demand can be attributed to the increased need for resources driven by the growth in technology infrastructure, especially in the areas of semiconductors.

The important relationship between semiconductors and telecommunications service providers is that semiconductors are crucial components in technological advancements and are vital in supporting the telecommunications industry's evolution. Semiconductors play a key role in enabling architectural shifts in these systems, including technologies like Ethernet switches, smart NICs, communication processors, artificial intelligence, network functions virtualization, and Customer Premises Equipment (CPE).

Potential Impact:

Constraints in resources can disrupt the supply chain, potentially causing scarcity for Telecom equipment. Moreover, certain natural resources are scarce and regionally concentrated.

The transition from globalization to regionalization is influencing resource crises, straining global supply chains, sparking geopolitical tensions, and resulting in conflicts and trade disputes, all exacerbating resource shortages.

Mitigation Actions:

Diversify Resource Sourcing: Reduce reliance on a single region or supplier to counter resource constraints and geopolitical tensions.

Supply Chain Resilience: Build adaptable supply chains to navigate resource challenges and geopolitical disruptions.

2.2.2 Investment risk imposed on the securities holders

Risks from having majority shareholders collectively holding more than a 50% of the total shares in the Company

As of 31 December 2023, the major shareholder group of the Company consists of: (1) Charoen Pokphand Group Co., Ltd. and its affiliated companies holding a combined percentage of 20.95 of the total issued and paid-up shares of the Company (2) Telenor Asia Pte. Ltd. and its affiliated company holding a combined percentage of 20.95 of the total issued and paid-up shares of the Company and (3) Citrine Group, which is a Joint Venture Company between CPH Telco Co., Ltd. (which held 99.99% interest by Charoen Pokphand Holding Co., Ltd.) and Telenor Asia Pte. Ltd., holding a combined percentage of 18.70 of the total issued and paid-up shares of the Company. Considering that the collective shareholdings exceed the 50% threshold, this could potentially have an impact on decisions that require a majority vote during shareholder meetings.

2.2.3 Foreign Investment Risk

- None-