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 pertaining 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.

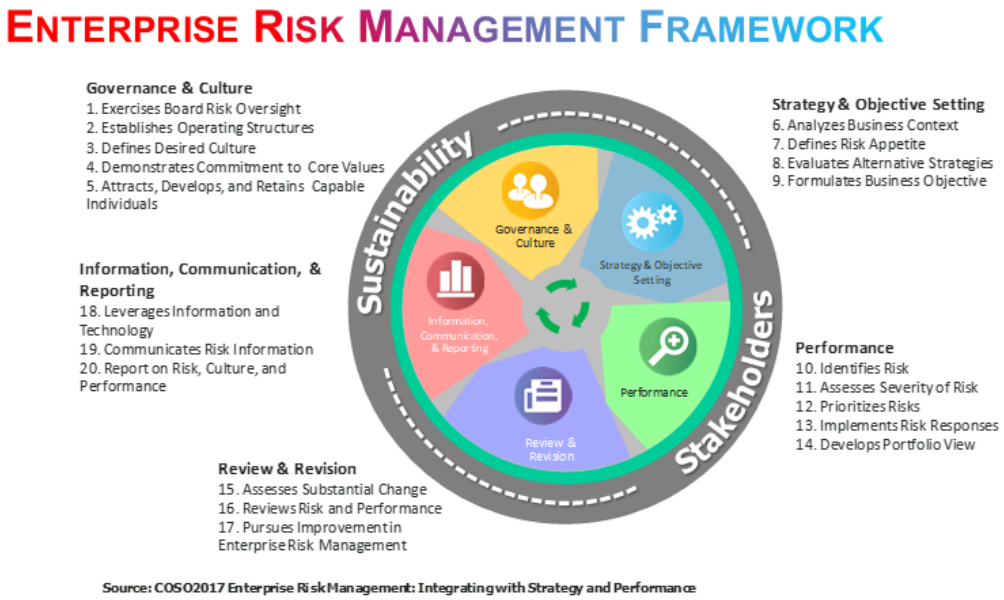
- **Review and Revision**

  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, analyse, and evaluate risk.

- **Risk Treatment**

  To select an implement option for addressing risk.

- **Recording & Reporting**

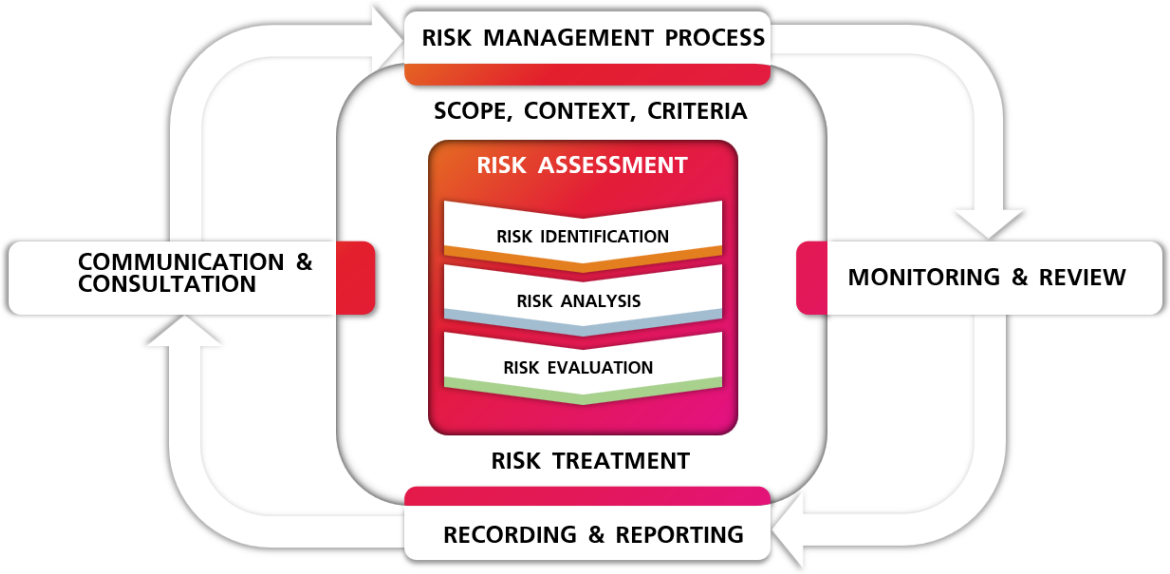
  To document and report the risk management process and its outcome.

- **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 in business operation

2.2.1 Risk factors in business operation

(1) Revenue Risk from Market Competition and Economic Conditions

In today's rapidly changing and uncertain business environment, True Corporation Public Company Limited continues to stand firm as a leading technology and telecommunications provider in Thailand. However, in 2025, the Company faces relentless challenges, particularly in terms of revenue risk, driven by intense market competition and fragile economic conditions.

Competition in the telecommunications industry has escalated continuously, with market players deploying aggressive pricing strategies, bundling diverse services, and developing digital platforms tailored to modern consumer needs. These dynamics compel True to adapt swiftly in order to maintain its customer base and revenue-generating capability. At the same time, the economic slowdown—stemming from external factors such as geopolitical tensions, global economic uncertainty, and the sluggish recovery of Thailand's tourism industry—has inevitably impacted consumer purchasing power.

To address these challenges, True Corporation has proactively implemented strategies across multiple dimensions, including:

- **Enhancing operational efficiency** through the adoption of AI technologies and automation in network management and customer service, aimed at improving agility and reducing costs.
- **Developing new products and services** that meet the demands of the digital era, such as TrueID, TrueVisions Now, and Smart Living solutions.

- **Elevating customer experience** via hyper-personalized services and omnichannel engagement to foster loyalty and maximize satisfaction.
- **Strengthening financial stability** through bond issuance and securing an A+ credit rating from TRIS Rating, reflecting the company's resilience and credibility.

Overall, True Corporation remains committed to continuous adaptation and innovation to preserve its competitive edge and ensure long-term business stability amid the ever-changing global landscape.

(2) Risk from operation associated with the regulatory agencies and change in the regulatory compliance

Risks from operation associated with the regulatory agencies.

Pursuant to the resolution of the NBTC Meeting (Special Meeting No. 5/2565 convened on 20 October 2022), specific measures were prescribed concerning the business merger between True and Dtac. 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 with such conditions or specific measures. The NBTC may also determine additional conditions or specific measures in the event of substantial changes in the telecommunications business.

Risks from changes in regulatory compliance

Presently, the business operations of the Company Group are under the rules and regulations of several government agencies and policies such as the NBTC, Ministry of Digital Economy and Society (DE) 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 associated with enforcement or with variations in statutory interpretation across 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. Group to increasingly obtain the costs of business operation and to encounter higher competition.

(3) Risk of Delay in synergy realization

Delays in efficiently integrating operations can result in adverse impacts to the Company and inability to benefit from subsequent synergies.

However, True Corporation successfully completed the consolidation of its network towers, marking a significant milestone in its post-amalgamation journey. The initiative, branded as "ONE Network," represents the largest network modernization in ASEAN, reiterating the Company's commitment

to delivering superior network experience for customers and unlocking long-term value for shareholders. This modernization reflects a collaborative effort between True's network experts and leading global technology partners. The consolidation is expected to further enhance network performance and customer experience, paving the way for further value creation for shareholders. With the successful completion of its network infrastructure consolidation, True Corporation is now approaching a steady-state operational phase post amalgamation. As key synergy initiatives reach their conclusion, the Company remains focused on its transformation journey, with a strong foundation of disciplined financial approach and performance-driven mindset.

(4) Risk of Cybersecurity Attacks

The exponential increase in customer data usage and online transactions has significantly heightened digital inter-dependencies. The Company is continuously enhancing and expanding services and digital platform to serve this growing demand. However, the rise in complex and frequent cyberattacks, utilizing advanced techniques including malware, ransomware, phishing and other means to obtaining unauthorized access to our telecom networks and systems has elevated cybersecurity risks. This necessitates the implementation of more advanced defense architectures to protect our telecom networks and systems.

Cybersecurity failures cause 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.
- Conduct the Responsible AI Framework in terms of ethics, transparency, and accountability to mitigate risks associated with AI and enhanced Trust and Transparency.

INFRASTRUCTURE AND TECHNOLOGIES

- Continually improve network security, data security system, and digital infrastructure according to ISO and CIS standard.
- Establish and continuously enhance the Security Operation Center (SOC) while upgrading to the certified ISO/IEC 27001:2022 standard
- 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 incidents of various 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 monthly and weekly on internal and external systems, respectively, while Penetration testing are performed on a regular basis to ensure all findings 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.
- Implement rigorous cyber hygiene processes to ensure comprehensive protection and resilience against evolving cybersecurity threats.

CAPACITY AND CULTURE

- Capacity building for IT workforce on evolving cybersecurity, including advanced technologies such as AI, NFT, and 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 Expert Journey projects to staff and managements.

(5) Risk of Personal Data Privacy

True is subject to obligations under the Personal Data Protection Act 2019 (PDPA). With over 46.9 million subscribers and a vast network of interconnected devices and platforms, the Company recognizes risks such as data breaches, unauthorized access, and non-compliance with the PDPA, and has emphasized it to ensure that all processing of personal data is lawful and transparent with data subjects (customers and employees).

This includes risk mitigation measures as follows:

- Designate a dedicated Data Protection Officer (DPO) for each subsidiary to oversee compliance, and provide affiliates with clear, actionable guidelines aligned with applicable laws and regulations.
- Collaborate across departments as well as governance agencies, including Legal, IT Security, Compliance, NBTC, and PDPC, to enforce comprehensive privacy measures in data collection, processing, 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.
- Create a strong data privacy culture through ongoing internal communication campaigns, online and on-site training, and targeted workshops. These initiatives address topics such as secure data handling, phishing awareness, and role-specific responsibilities, tailored to suit their roles and responsibilities, as well as provide intermediate and advanced training 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 433.7 billion at the end of 2025, decreasing from Baht 436.0 billion at the end of 2024 due to lower outstanding of debentures. The Company's 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, debenture and

B/E issuance, and loan from various financial institution – both domestic and international. 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 company's revenues and most operating and capital expenditures are generally denominated in Thai Baht, resulting in limited exposure to foreign exchange fluctuations.

Certain transactions and financial obligations may be denominated in foreign currencies. The company manages such risks through natural hedging, such as managing foreign currency income from international roaming services with expenditures and the use of appropriate hedging instruments.

Foreign currency denominated borrowings are generally hedged into Thai Baht at the time of utilization, with ongoing monitoring of mitigate potential volatility

(7) Emerging Risk

7.1 Emerging Risk from Agentic AI Adoption and Autonomous Execution in Critical Business Processes

Risk Category : Technological

Risk Factor : Lack of proper governance and user awareness

The adoption of agentic AI—capable of planning, making decisions, and executing actions across connected tools and enterprise systems—may increase the risk of excessive access, unintended data exposure, erroneous actions, or manipulation into operating beyond defined guardrails. Without robust governance and security controls, such incidents could adversely impact on service continuity, operating costs, regulatory compliance, and customer trust.

In 2026, industry adoption is shifting from AI that "assists" to AI that "acts." Agentic AI can chain tools and system calls across workflows (e.g., customer care, network operations, fraud detection, and employee productivity). While this enables efficiency and faster resolution, it also introduces a new attack surface and failure modes: compromised or misaligned agents can cause real-world changes in production systems, leading to cascading operational and security impacts.

Potential Impact:

- Cybersecurity & Privacy: Increased exposure to prompt manipulation and tool misuse that can lead to unauthorized access or sensitive data disclosure.
- Operations & Service Continuity: Agent errors or compromise may impact critical systems and availability of services.
- Reputation & Trust: Data exposure or service disruption may undermine stakeholder confidence.

Mitigation Actions:

To mitigate risks and promote the responsible use of artificial intelligence, the Company has implemented a number of key measures aligned with its publicly announced policies, including the principles of the GSMA Responsible AI Maturity Roadmap, which True has adopted for the governance of AI. True Corporation has established a Responsible AI (RAI) Framework based on five fundamental principles:

1. Vision, Values, and Strategic Objectives – Aligning AI initiatives with the organization's mission and long-term goals.
2. Operational Model and AI Governance – Ensuring AI governance is integrated into all business operations.
3. Technical Compliance and Regulatory Requirements – Implementing AI controls that adhere to legal and regulatory standards.
4. Collaboration with Third-Party Ecosystems – Engaging with external partners to ensure responsible AI adoption.
5. Change Management and Communication Strategies – Facilitating smooth AI integration while maintaining transparency.

In addition to these governance pillars, True Group incorporates key ethical factors into its AI strategy, including human oversight, fairness, privacy, security, accountability, and environmental impact assessments. All of the above are consistent with the Company's Ethical AI policy as well as its digital security requirements and the CyberSafe program, which the Company has announced and continues to operate to safeguard consumers on an ongoing basis.

7.2 Emerging Supply Chain Risk from Rare Earth Elements & Strategic Minerals

Risk Category : Operational - Supply chain

Risk Factor : Limited Natural Resources in Value Chain

In 2026, the global competition for rare earth elements and strategic minerals is expected to intensify and emerge as a structural risk to the telecommunications industry. These critical materials are essential inputs in the manufacturing of next generation network equipment, advanced electronic components, and digital infrastructure supporting technologies. Key components—such as radio access network equipment, transmission systems, optical modules, and core/edge network systems—may face procurement delays or price volatility. With rising demand across multiple sectors, supply chains are experiencing increasing constraints and heightened uncertainty. Increasing demand may result in a resource crisis, placing strain on supply chains, leading to geopolitical tensions, and potentially triggering conflicts and trade disputes.

Potential Impact

As the Company procures network equipment from international manufacturers, this risk may directly affect equipment delivery timelines and network investment costs. Such conditions may disrupt planned network expansion, capacity upgrades, and the ability to support high density usage areas. In addition, unpredictable equipment pricing and logistics costs may increase overall project expenditure. Competitively, operators with more flexible supplier portfolios or stronger supply chain resilience may gain advantages in accelerating network development and service rollout.

Mitigation Action

To mitigate these risks, True aims to strengthen supply chain resilience through proactive measures, including:

- Diversifying procurement sources and key suppliers for critical equipment to reduce single source dependency and to build a more adaptable supply chain capable of responding to resource related challenges
- Enhancing contractual frameworks and procurement processes to accommodate price and delivery volatility
- Improving end to end supply chain visibility through closer collaboration with manufacturers and strategic partners
- Establishing appropriate levels of critical equipment and spare parts to maintain service continuity
- Closely monitoring global market trends and external factors affecting supply availability.

These measures support more informed investment decisions and help safeguard the company's long term network expansion plans, cost efficiency, and competitive capability.

2.2.2 Investment risk imposed on the securities holders

Nature of Risk

Risk arising from the concentration of shareholding by major shareholders holding more than 50% of the Company's total issued and paid-up shares

According to the list of shareholders as of 18 November 2025, the major shareholders of the Company consist of:

(1) Charoen Pokphand Group Co., Ltd. and its related companies, which holds 29.72% of the Company's total issued and paid-up shares

(2) Telenor Thailand Investments Pte. Ltd., which holds 30.30% of the Company's total issued and paid-up shares.

Together, these major shareholders hold more than 50% of the Company's shares.

Impact of Risk

The concentration of shareholding by major shareholders, holding more than 50% of the Company's total issued and paid-up shares, may result in control over the Company's operations by such group of major shareholders. This may affect the rights of minority shareholders to participate in significant corporate decisions, particularly in resolutions that require a majority vote at the shareholders' meetings.

Risk Mitigation Measures

- Establish and implement corporate governance policies or guidelines to promote transparency and accountability.
- Appoint independent directors and an audit committee with authority to provide impartial oversight.
- Encourage minority shareholder participation in shareholders' meetings and ensure fair voting rights.
- Disclose material information accurately and in a timely manner to support informed decision-making by all shareholders.

2.2.3 Investment Risk in Foreign Securities

- None -