ENTERPRISE RISK MANAGEMENT AT TRUE

MANAGEMENT APPROACH

True Corporation is committed to implementing effective risk management practices, encompassing the promotion of a culture, processes, and structures that enable the identification, assessment, and management of both opportunities and potential impacts.

The Company has adopted the **COSO 2017 Enterprise Risk Management - Integrating with Strategy and Performance and the ISO 31000 – Risk Management** as a corporate framework of risk management.

This approach ensures that all risk factors are duly identified, assessed, and addressed, providing the necessary information to support the company's business decisions and facilitate the achievement of its goals.

Risk Management Policy has been developed and approved by board of directors.

The risk management is governed by the board of directors and The Risk Management Committee is independent and responsible for overall risk management.

ENTERPRISE RISK MANAGEMENT STRUCTURE & INTERNAL AUDIT

TOPICS

- Management Structure
- Enterprise Risk Framework
- Internal Audit Management
- Enterprise Risk Management Process
- Risk Management Audit
- Risk Culture
- Financial Incentives Incorporating Management Metrics

ENTERPRISE RISK MANAGEMENT STRUCTURE & INTERNAL AUDIT

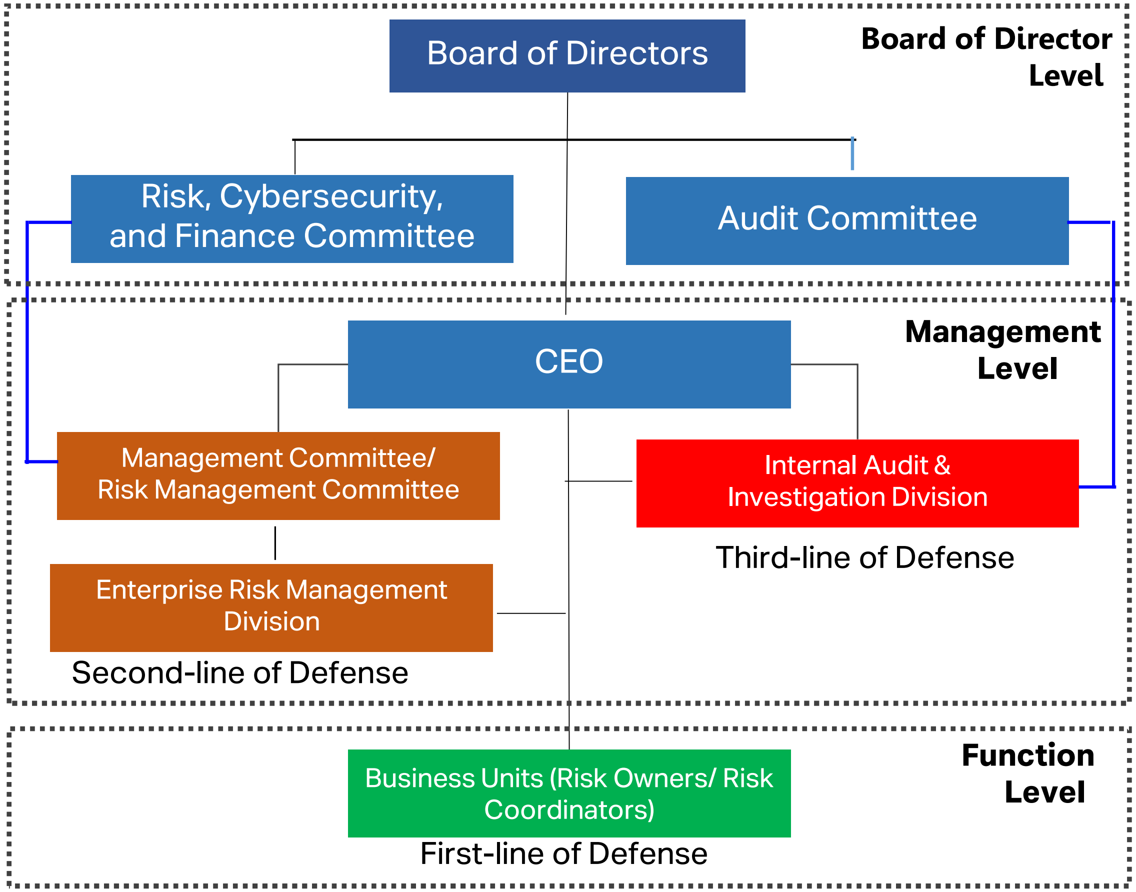
BOARD OVERSIGHT
Board of Directors: Oversee the Company's risk management frameworks and policies and ensures that management maintains a sound system of risk management.

Risk, Cyber Security and Finance Committee: Supports the Board with overseeing the risk management framework and process, including all strategies, policies, rules and operational procedures adopted by the Company.

Audit Committee: Supports the Board with overseeing the internal audit & investigation process, according to corporate objectives and stakeholder confidences.

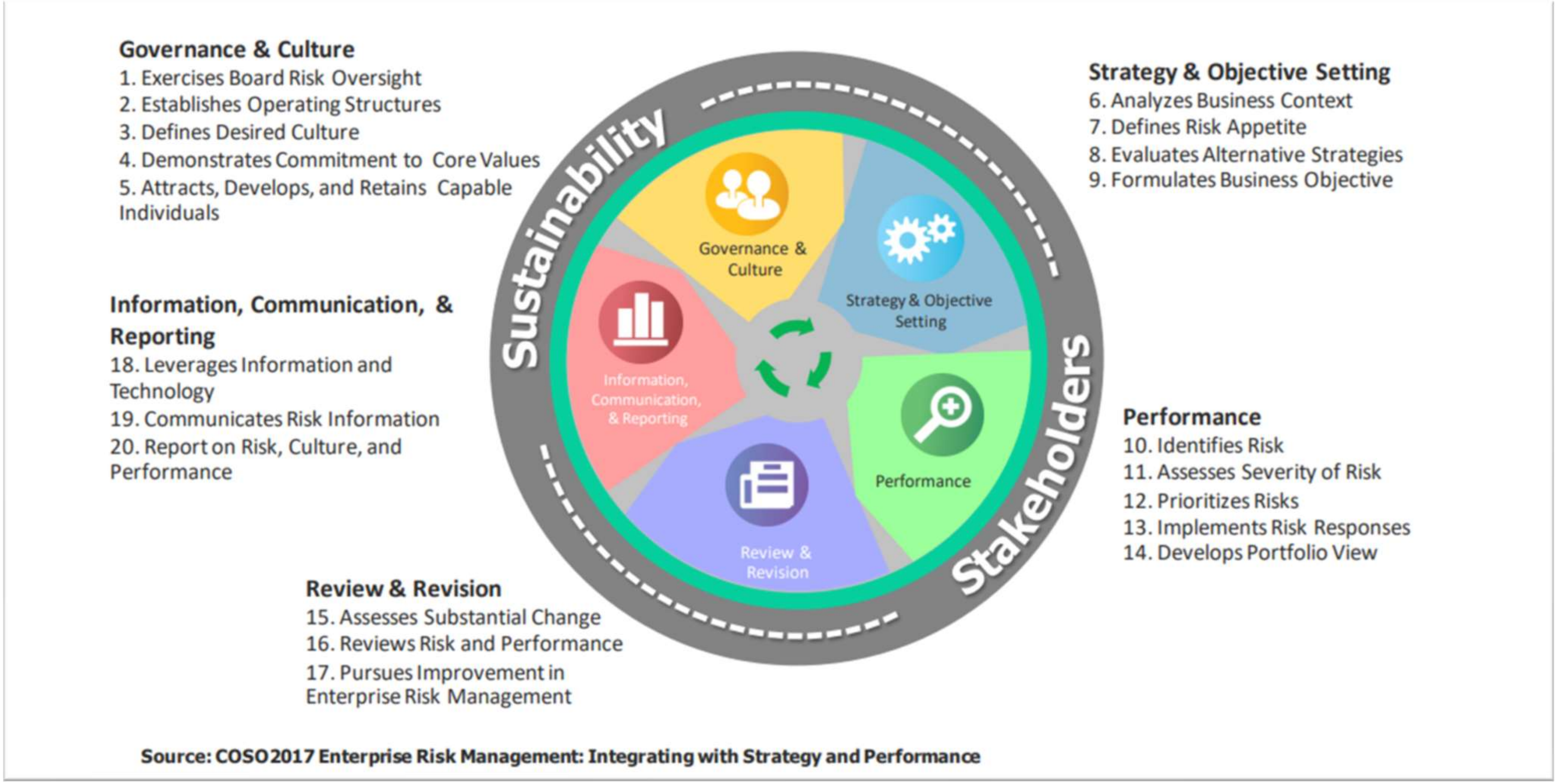
MANAGEMENT & FUNCTION LEVEL
True has applies the **IIA's Three Lines of Defense Model** to manage risk governance.

- **Business units, risk owners and risk coordinators** (first-line) are responsible to manage their own risks.
- **Enterprise Risk Management** (second-line) support the management, including monitoring and reporting to ensure effective risk management.
- **The Internal Audit & Investigation Division** (third-line) conduct internal audits in line with the integrity risk-based approach while upholding independence and objectivity.


Board of Director Level
Board of Directors
Risk, Cybersecurity, and Finance Committee
Audit Committee
Management Level
CEO
Management Committee/ Risk Management Committee
Internal Audit & Investigation Division
Third-line of Defense
Enterprise Risk Management Division
Second-line of Defense
Function Level
Business Units (Risk Owners/ Risk Coordinators)
First-line of Defense

ENTERPRISE RISK MANAGEMENT FRAMEWORK

true



Governance & Culture
1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective Setting
6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objective

Performance
10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting
18. Leverages Information and Technology
19. Communicates Risk Information
20. Report on Risk, Culture, and Performance

Source: COSO 2017 Enterprise Risk Management: Integrating with Strategy and Performance

INTERNAL AUDIT MANAGEMENT

The COSO 2013 Internal Control Framework

The internal control framework is a conceptual framework designed to assist in evaluating the effectiveness of internal control systems to achieve organizational goals that the Company embraces the COSO 2013 integrated internal control framework to ensure efficiency and effectiveness of the internal control across the organization.

The IIA's Three Lines of Defense Model

The Company aligns with the Institute of Internal Auditors (IIA) Three Lines of Defense Model. Additionally, True fosters synergy across different lines of defense, promoting a culture of accountability and continuous improvement.

Automation in Internal Audit

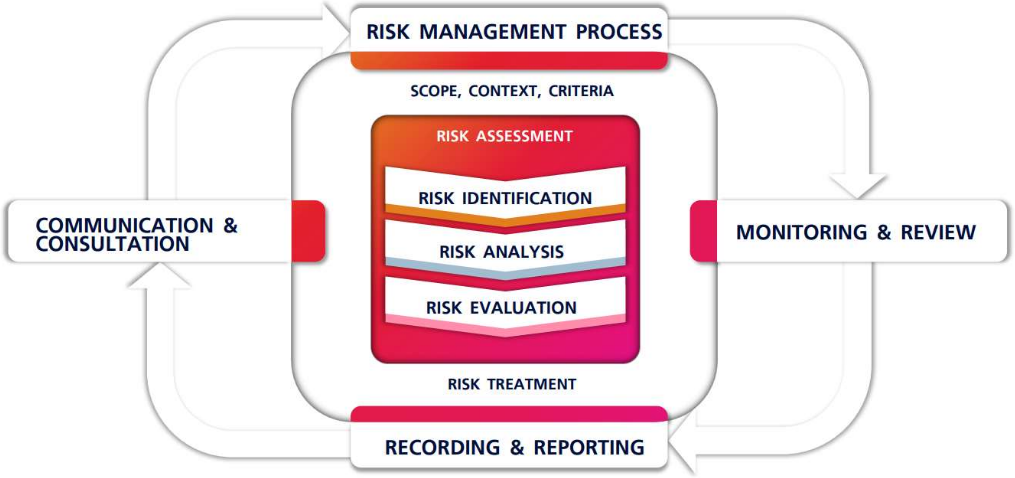
True is also at the forefront of embracing the latest trend in internal audit by leveraging automation, aiming to unlock value beyond mere assurance provision. Through automation, True streamlines audit processes, enhance efficiency, and harness data analytics to derive actionable insights. By incorporating automation into the Internal Audit Processes, True not only optimizes resource allocation but also elevates its ability to proactively identify risks and opportunities. This strategic integration empowers True to deliver deeper, more meaningful contributions to organizational objectives and stakeholder confidence.

ENTERPRISE 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.

6-STEP OF RISK MANAGEMENT PROCESS

1. Scope, Context, Criteria – To define the scope of the process and understand the external and internal context.
2. Risk Assessment – To identify, analysis, and evaluate risk
3. Risk Treatment – To select an implement option for addressing risk.
4. Recording & Reporting – To document and report the risk management process and its outcome.
5. Monitoring & Review – To assure and improve the quality and effectiveness of process design, implementation, and outcome.
6. 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.



ENTERPRISE RISK CATEGORIES

- REGULATORY
- LEGAL
- TECHNOLOGY
- DATA PRIVACY
- OPERATIONS
- MARKETING/SUPPLIER /CUSTOMER/PARTNER
- PEOPLE
- FINANCE
- SUSTAINABILITY

RISK ASSESMENT: IDENTIFICATION & PRIORITIZATION

True regularly conducts corporate enterprise risk assessment on a quarterly basis.

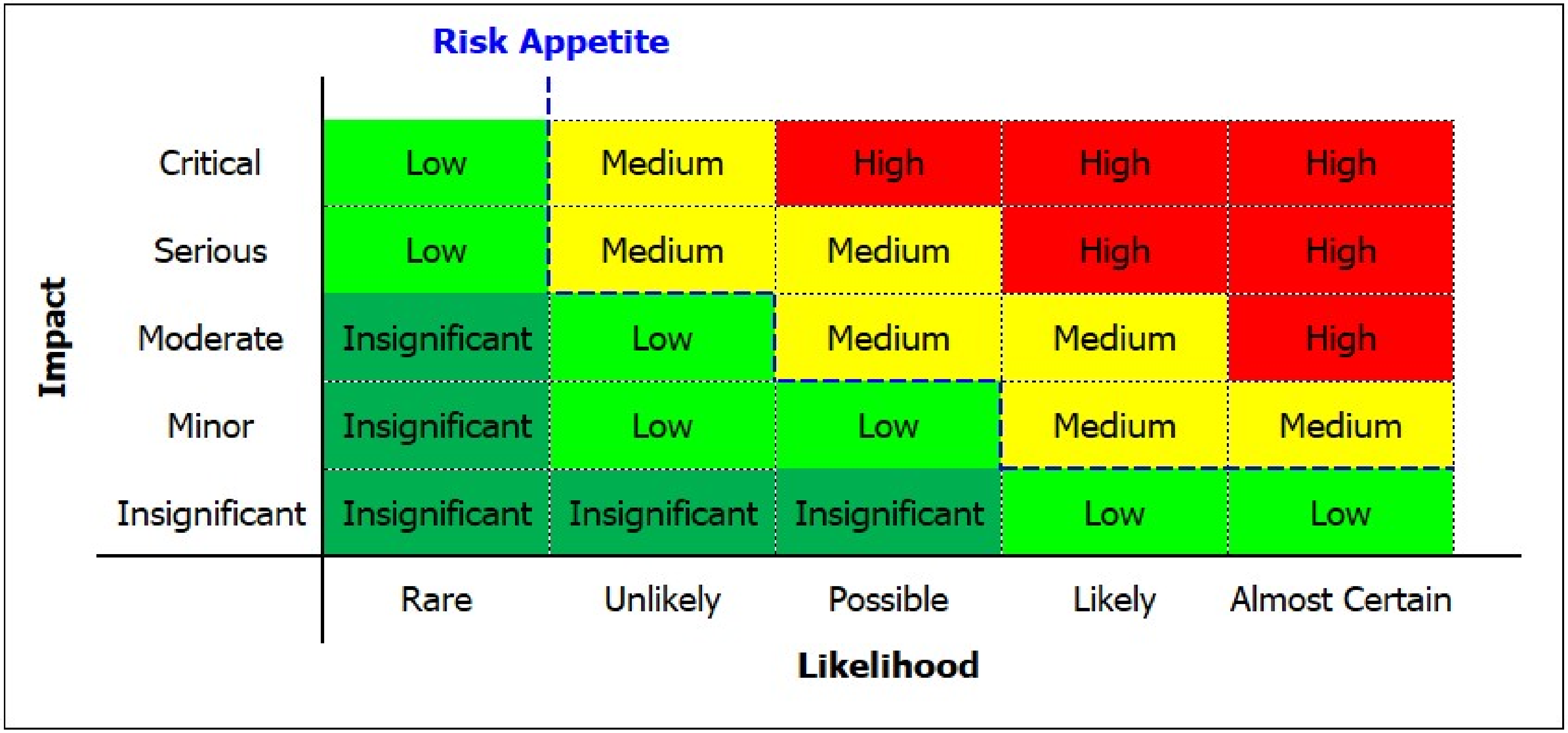
The main points for risk assessment are:

- Identify risks that may impact your objectives
- Assess impact and likelihood for each risk
- Name one Risk Owner per risk

The main points for decide actions are:

- Evaluate risk level against risk appetite – decide whether or not action(s) shall be initiated
- Identify and prioritize action(s) that may affect the risk level
- Estimate a due date for each action
- Name one Action Owner per action

ENTERPRISE RISK METRICS



Risk Appetite

Impact	Rare	Unlikely	Possible	Likely	Almost Certain
Critical	Low	Medium	High	High	High
Serious	Low	Medium	Medium	High	High
Moderate	Insignificant	Low	Medium	Medium	High
Minor	Insignificant	Low	Low	Medium	Medium
Insignificant	Insignificant	Insignificant	Insignificant	Low	Low

Likelihood

LIKELIHOOD AND IMPACT CRITERIA

Likelihood Criteria

The Company has defined the likelihood rating from 1 (rare) to 5 (almost certain) with specific description, frequency and probability details.

Impact Criteria

The Company has defined the impact rating from 1 (insignificant) – 5 (critical) with specific description of impact areas covering:

- Financial;
- Operational (impact to customers);
- Health, safety & people (impact to employees, third party and customers);
- Environment;
- Compliance;
- Legal/regulatory; and
- Brand/ reputation.

RISK RATING DEFINITION

LEVEL	DESCRIPTION	MANAGEMENT'S ACTION	RISK MANAGEMENT ACTIVITY
High	The loss, injury, damage, disadvantage, or anything that has a severe effect on organizational objectives, operations, reputation, assets or individuals.	Requires management's high-priority attention and remedy and need Board's approval.	Require mitigation actions to manage the risk
Medium	The loss, injury, damage, disadvantage, or anything that has a moderate effect on organizational objectives, operations, reputation, assets or individuals.	Requires management's attention and keep Board informed.	
Low	The loss, injury, damage, disadvantage, or anything that has a minimal effect on organizational objectives, operations, reputation, assets or individuals.	Requires management's attention and continuous monitoring.	There should be a cost-benefit assessment to decide the need of actions
Insignificant	The loss, injury, damage, disadvantage, or anything that has no important effect on organizational objectives, operations, reputation, assets or individuals.	Requires management's continuous monitoring.	

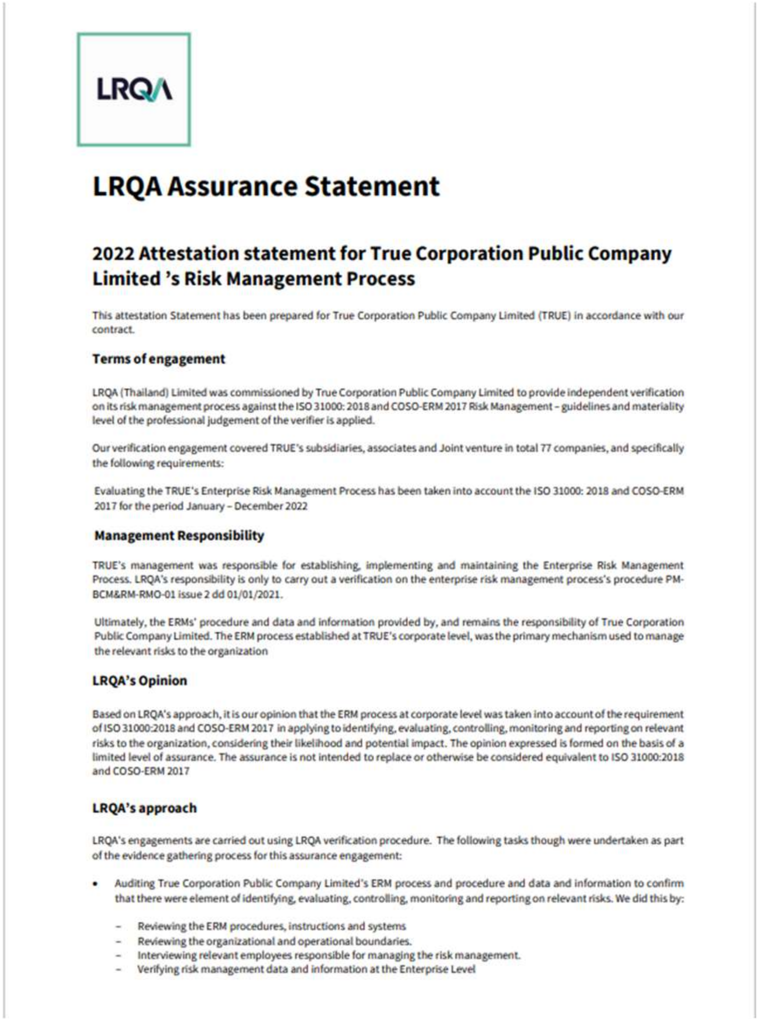
RISK MANAGEMENT PROCESS AUDITS

The company regularly conducts internal audit of its risk management process on a yearly basis, and external audit utilizing third-party auditors every two years. These audits are carried out to ensure that the company's risk management practices align with internationally recognized Enterprise Risk Management (ERM) standards, such as COSO-ERM 2017 and ISO 31001.

The audits of the risk management process evaluated the measures, tools, and procedures employed in identifying, evaluating, controlling, monitoring, and reporting on pertinent risks to the organization. These assessments take into account the probability/ likelihood and potential impact of these risks.

In 2023, LRQA which is an independent verifier evaluated True's enterprise risk management process against the ISO 31000: 2018 and COSO ERM 2017 for the period of 1 January to 31 Dec 2022 and the assurance statement was issued, accordingly. Please click to see the Assurance Statement.

ENTERPRISE RISK MANAGEMENT PROCESS EXTERNAL AUDIT



LRQA Assurance Statement

2022 Attestation statement for True Corporation Public Company Limited 's Risk Management Process

This attestation Statement has been prepared for True Corporation Public Company Limited (TRUE) in accordance with our contract.

Terms of engagement

LRQA (Thailand) Limited was commissioned by True Corporation Public Company Limited to provide independent verification on its risk management process against the ISO 31000: 2018 and COSO-ERM 2017 Risk Management – guidelines and materiality level of the professional judgement of the verifier is applied.

Our verification engagement covered TRUE's subsidiaries, associates and Joint venture in total 77 companies, and specifically the following requirements:

Evaluating the TRUE's Enterprise Risk Management Process has been taken into account the ISO 31000: 2018 and COSO-ERM 2017 for the period January – December 2022

Management Responsibility

TRUE's management was responsible for establishing, implementing and maintaining the Enterprise Risk Management Process. LRQA's responsibility is only to carry out a verification on the enterprise risk management process's procedure PM-BCM&RM-RMO-01 issue 2 dd 01/01/2021.

Ultimately, the ERMs' procedure and data and information provided by, and remains the responsibility of True Corporation Public Company Limited. The ERM process established at TRUE's corporate level, was the primary mechanism used to manage the relevant risks to the organization

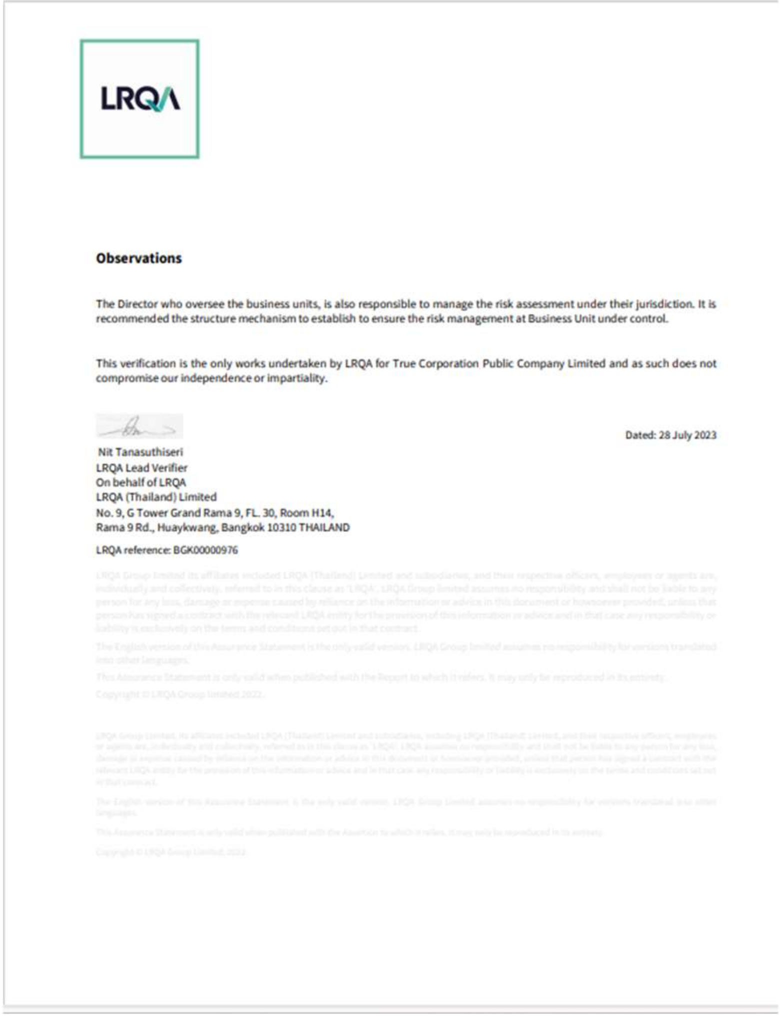
LRQA's Opinion

Based on LRQA's approach, it is our opinion that the ERM process at corporate level was taken into account of the requirement of ISO 31000:2018 and COSO-ERM 2017 in applying to identifying, evaluating, controlling, monitoring and reporting on relevant risks to the organization, considering their likelihood and potential impact. The opinion expressed is formed on the basis of a limited level of assurance. The assurance is not intended to replace or otherwise be considered equivalent to ISO 31000:2018 and COSO-ERM 2017

LRQA's approach

LRQA's engagements are carried out using LRQA verification procedure. The following tasks though were undertaken as part of the evidence gathering process for this assurance engagement:

- Auditing True Corporation Public Company Limited's ERM process and procedure and data and information to confirm that there were element of identifying, evaluating, controlling, monitoring and reporting on relevant risks. We did this by:
  - Reviewing the ERM procedures, instructions and systems
  - Reviewing the organizational and operational boundaries.
  - Interviewing relevant employees responsible for managing the risk management.
  - Verifying risk management data and information at the Enterprise Level



Observations

The Director who oversee the business units, is also responsible to manage the risk assessment under their jurisdiction. It is recommended the structure mechanism to establish to ensure the risk management at Business Unit under control.

This verification is the only works undertaken by LRQA for True Corporation Public Company Limited and as such does not compromise our independence or impartiality.

Dated: 28 July 2023

Nit Tanasuthiseri
LRQA Lead Verifier
On behalf of LRQA
LRQA (Thailand) Limited
No. 9, G Tower Grand Rama 9, FL. 30, Room H14,
Rama 9 Rd., Huaykwang, Bangkok 10310 THAILAND

LRQA reference: BGK00000976

LRQA Group limited its affiliates included LRQA (Thailand) Limited and subsidiaries, and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA Group limited assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

The English version of this Assurance Statement is the only valid version. LRQA Group limited assumes no responsibility for versions translated into other languages.

This Assurance Statement is only valid when published with the Report to which it refers. It may only be reproduced in its entirety.

LRQA Group Limited, its affiliates included LRQA (Thailand) Limited and subsidiaries, including LRQA (Thailand) Limited, and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

The English version of this Assurance Statement is the only valid version. LRQA Group Limited assumes no responsibility for versions translated into other languages.

This Assurance Statement is only valid when published with the Assertion to which it refers. It may only be reproduced in its entirety.

RISK CULTURE AT TRUE

EMPLOYEE	PROCESS
Board of Directors: True fosters a culture of risk management within the organization. The Board of Directors regularly attend comprehensive risk management courses such as **Information Security Workshop including Annual Information Security Policy Risk, How to Develop a Risk Management Plan (HRP) and the Geopolitical Risk and Opportunity training course.** There are also Enterprise Risk Management online training course for all staff, management as well as board members. **Executives and all employee** are required to attend the mandatory Enterprise Risk Management e-learning. All are educated and communicated of best practices in risk monitoring, risk assessment and risk protection as well as mitigation measures. **Risk Coordinators** have been appointed within the organization from various units to serve as representatives communicating and understanding risk management within their respective teams effectively and at the fullest.	**Product and Service Launch:** Prior to launching products and services, the business units are required to ensure **the pre-launch checklist criteria** are properly assessed as a part of due diligence/ risk assessment prior to the product/ service launch approval. The checklist contains the key aspects to be considered for approval on the development of products and services and all investment projects. The risk criteria includes financial feasibility (payback, ROI), legal terms and conditions (fraud protection, applicant consent), testing (billing, payment, security check), SLA, operation & maintenance readiness (escalation handover process, rollout plan). Innovation: In addition, **True uses the Innovation Sprint to accelerate the development of product and processes**. Emphasis is places on cost reduction, revenue generation, controlling potential risks, and intellectual property rights. In 2023, all True's products and services must comply with this pre-launch checklist and the innovation sprint before launching.

FINANCIAL INCENTIVES INCORPORATING RISK MANAGEMENT METRICS

At True, employees' key performance indicators (KPIs) are tied to performance evaluations and merit-based incentive structures. These KPIs operate on **three tiers: corporate, divisional, and individual/team levels.** The corporate KPIs encompass vital categories such as financial and non-financial performance, while also integrating key risk indicators such as market and customer dynamics, operational risks, human resources, and innovation/sustainability initiatives.

Each function has its specific KPIs aimed at achieving targets in areas of specific risks identified as key concerns for the company. In 2023, the primary risk associated with KPIs are as follows:

Function	The primary risk associated with KPIs
Cybersecurity	Achieve 80% of resolved case within 72 hours, and 100% data breach protection
Network Strategy	Reduce 12.6% GHG emission (Scope 1 & 2), compared to base year
Health, Safety & Security	Achieve zero employee fatalities in the workplace

For senior management, their performance is fully (100%) evaluated based on their contributions towards achieving corporate KPIs. **For other staff members**, the allocation of KPIs is tailored to their respective positions, with a designated percentage allotted to corporate, divisional, and individual KPIs.

The assessment of KPI performance adheres closely to corporate protocols and is directly linked to **annual bonus payouts and merit-based salary increments.**