Enterprise Risk Management Framework

Approved by the Board of Directors' Meeting No. 6, held on 14 November 2025 (B.E. 2568)

(Reviewed and updated in 2025 (B.E. 2568))

Table of Contents

Risk Management

This Risk Management Framework has been prepared as a tool for communication and to build understanding of the Enterprise Risk Management (ERM) process for the executives, employees, and stakeholders of Origin Property Public Company Limited and its subsidiaries (the "Company"), so that the Company's risk management operations comply with the policy established by the Board of Directors. The risk management process has been integrated with internal management processes to drive risk management as part of business operations in line with sustainability principles.

Definitions

The Company: means Origin Property Public Company Limited and its subsidiaries.

Risks: means opportunities/events involving uncertainty, or matters that cause current plans or operations to fail to achieve their stated objectives/goals, resulting in impact or damage to the organization.

Risk Management: means the process carried out by the Board of Directors, management, and all personnel within the organization to help determine strategy and conduct operations. The risk management process is designed to identify events that may occur and affect the organization, enabling the organization to manage risk to an acceptable level, in order to provide reasonable assurance regarding the achievement of the organization's stated objectives.

Risk Appetite: means the maximum level of risk acceptable at the organizational level, as approved by the Board of Directors, used for assessing and managing risk. Where any risk, after analysis and assessment, is found to potentially impact the Company or its subsidiaries beyond the acceptable risk level, the responsible risk-owning unit shall prepare a risk management action plan and report it to the Risk Management Committee for consideration, before presenting it to the Audit Committee and the Board of Directors.

Objectives of Risk Management

1. To enable the identification of risks or unexpected crises, and to respond appropriately and promptly to reduce loss or damage to the organization, with measures and guidelines established to manage residual risk to a level acceptable to the organization — by considering measures to effectively reduce the likelihood

and/or impact of potential risks — in order to drive the achievement of the organization's stated objectives.

2. To enable the Risk Management Committee, the Audit Committee, and the Board of Directors to acknowledge and effectively oversee the Company's material risk management, with systematic and continuous risk management covering environmental, social, and governance aspects of operations in line with sustainable business practices.

3. To communicate and build knowledge and understanding of risk management, including fostering awareness of risk ownership and collaborative risk management within areas of responsibility, and to develop this into an organizational culture.

Risk Management Policy

The Company and its subsidiaries recognize the importance and necessity of adopting an internationally standardized risk management system, with the aim that the Company and its subsidiaries give priority to risk management in order to reduce potential impacts on business operations, maintain a positive image, and develop the operations of the Company and its subsidiaries in a consistent direction throughout the organization. The Company therefore establishes the following risk management policy:

1. Risk management is designated as the responsibility of employees at every level, who must be aware of the risks present in the operations of their own unit and the organization, giving importance to risk management and internal controls across various areas to ensure they remain at an adequate and appropriate level.

2. There shall be an enterprise risk management process that follows good international standard practices, in order to effectively manage risks that may impact the operations of the Company and its subsidiaries, and to promote the development and practice of risk management throughout the organization in a consistent direction — by incorporating the risk management system as part of decision-making in strategic planning, work plans, and operations of the Company and its subsidiaries, including focusing on achieving the objectives, goals, vision, mission, and strategies established, in order to create operational excellence and build the confidence of stakeholders.

3. Guidelines shall be established to prevent and mitigate risks arising from the operations of the Company and its subsidiaries, in order to avoid potential damage

or loss, including regular monitoring and evaluation of risk management performance.

4. Promote and develop the adoption of modern information technology systems in the Company's and its subsidiaries' risk management processes, and support personnel at all levels in accessing risk management information thoroughly, as well as organizing an effective risk management reporting system.

Operating Framework

- The Company's risk management is under the oversight of the Board of Directors through the Risk Management Committee, which oversees systematic and continuous risk management and provides policy-level support to ensure effective risk management and awareness of risk in any of the Company's activities — covering business operations in line with sustainable development guidelines in the economic, social, and environmental dimensions.
- The Risk Management Committee comprises independent directors of the Company, the President/Executive Directors, and senior management. For maximum effectiveness in risk management, the Company integrates risk management with its business plan, emphasizing value creation for the Company and its stakeholders, by analyzing the relationship of each risk issue to cover both positive and negative aspects. The Company's risk management process begins with setting objectives according to the business plan, which are then cascaded down to business units, divisions, departments, and units by identifying risks and designating Risk Owners who are directly responsible for managing them.
- The Risk Management Committee continuously monitors risk management results by meeting with management and reporting to the Board of Directors on a regular basis, at least quarterly, and whenever significant changes occur that may affect the Company's business operations — including supporting the dissemination of risk management knowledge to build understanding among employees at all levels, so that it takes effect in practice throughout the organization.

Roles and Responsibilities in Risk Management

Board of Directors: Responsible for setting the policy and strategic direction of the Company, and overseeing the Company to ensure it has an effective and efficient risk management system, in order to ensure that management prioritizes risk management and instills it as part of the organizational culture.

Risk Management Committee: Responsible for overseeing and establishing guidelines for risk management to be systematic and continuous, covering risks from current business operations and investment in new businesses, as well as risks in sustainability operations (ESG Risks) in the economic, social, environmental, and governance dimensions. Reviews and approves the risk management framework for use as the Company's operating guideline, monitors risk management results, supports the dissemination of information to build understanding of risk management among employees at all levels so that it takes effect in practice throughout the organization, and provides opinions/recommendations/advice to management, reporting to the Board of Directors.

Audit Committee: Responsible for reviewing the financial and accounting reporting system, good corporate governance, the internal control system, the internal audit system, and the risk management system, including anti-corruption policies and measures, to ensure appropriate and adequate compliance with international standards, regulations, and relevant laws, and reports to the Board of Directors.

Corporate Governance and Sustainability Committee: Responsible for overseeing corporate governance and sustainability operations, setting policies for corporate governance and sustainability operations, business ethics, and policies related to the performance of duties by directors, executives, and employees, in compliance with laws and regulations of government agencies and regulators such as the Stock Exchange of Thailand and the Securities and Exchange Commission, in accordance with good corporate governance principles. Develops the Company's corporate governance system, provides guidance on the performance of the Board of Directors and management in accordance with the corporate governance and sustainability policy, and reports to the Board of Directors.

Sustainability Committee: Comprises senior executives (C-Level) of the Company and its subsidiaries. Responsible for driving policy, strategy, and sustainability operations throughout the organization in line with the direction set by the Board of Directors and/or the Corporate Governance and Sustainability Committee, ensuring systematic implementation integrated with business activities. Sets appropriate operating plans consistent with the strategic plan, allocates the sustainability operating budget for the

responsible group of companies as set by the Company, monitors sustainability operations, and develops understanding and awareness of ethics, environmental preservation, and social responsibility in line with sustainability principles, reporting to the Corporate Governance and Sustainability Committee.

Chief Executive Officer, President, and Executives: Responsible for establishing a risk management system in accordance with the policy and guidelines set by the Board of Directors, determining strategy and ensuring the preparation and monitoring of enterprise-wide risk management plans covering material risks in both business operations and sustainability risks (ESG Risks), designating and assigning Risk Owners, considering and setting the acceptable risk level for submission to the Board of Directors for approval, communicating and developing an organizational culture of risk awareness, and reviewing the appropriateness of systems and measures such as anti-corruption measures to keep them appropriate to changes in the business, regulations, and relevant legal requirements.

Sustainability Working Group: A working group appointed by each business group, comprising heads of units involved in ESG operations, to support sustainability operations within their responsible unit/company in accordance with established plans. Prepares and presents work plans and guidelines by linking the plans of responsible units with the Company's sustainability policy, strategy, and operating plans, communicates and builds understanding of ESG operations, monitors unit performance, coordinates and compiles ESG activities with relevant units, and reports to the CEO of each business group and the Sustainability Committee.

Risk Management Working Group: Responsible for developing an effective and efficient risk management system, providing advice, consultation, and training to build knowledge and understanding of risk management, monitoring and communicating future trends that may impact business operations and ESG risk issues that may affect business operations in the short, medium, and long term, as well as coordinating and monitoring risk management results from Risk Owners and the Sustainability Working Group, in order to prepare risk reports for presentation to management and the Risk Management Committee, the Audit Committee, the Sustainability Committee, and/or the Board of Directors as assigned, and supporting the effective operation of the Risk Management Committee.

Risk Owners: Responsible for evaluating and analyzing risk, determining measures/activities used to manage risk, analyzing the cost-benefit of each alternative, monitoring risk assessment results, and presenting them to the CEO and/or the Risk Management Committee.

Internal Audit Unit: Responsible for auditing and reviewing operational processes to ensure compliance with the policies and operating procedures set by the Company/good practice guidelines and relevant government rules and regulations, in order to ensure that the Company has adequate and appropriate internal control/risk management systems, and reports to the Audit Committee for presentation to the Board of Directors.

Risk Categories

- Business Risks
- Sustainability Risks (impacts on the Environment, Society and Governance: ESG Risks)

Business Risks:

Business risks can be divided as follows:

1) **Strategic Risk:** Risk arising from the formulation of strategy and operating plans that are inappropriate or impractical to implement, or a shortage of critical resources needed to successfully drive the strategic plan, among other factors.

2) **Operational Risk:** Risk arising from operational processes that affect the efficiency and effectiveness of business operations, resulting in failure to achieve the goals set.

3) **Financial Risk:** Risk related to finance, such as interest rate volatility, exchange rate volatility, and counterparty risk, among others.

4) **Compliance Risk:** Risk arising from an inability to comply with relevant laws, regulations, or rules, or where such rules are inappropriate or an obstacle to operations — which may lead to impacts such as fines, litigation, or damage to the organization's reputation. This also includes risk arising from changes in government policy.

    - Financial Regulations: Changes in banking law, securities regulations, or tax law may affect how the Company manages its finances, reports income, and conducts transactions.
    - Environmental Regulations: New or stricter environmental laws may require the Company to invest in cleaner technology or change operating processes to reduce pollution and waste, affecting the Company's costs and operations.

- Health and Safety Regulations: Improvements to safety standards requiring new compliance measures, which may lead to increased operating costs, for example in construction and healthcare.
- Data Protection and Privacy Laws: Due to growing concerns over data security, the Company must comply with regulations such as the General Data Protection Regulation (GDPR) and the Personal Data Protection Act, as well as similar laws governing how consumer data is managed and protected.
- Employment Law: Changes in labor law, including minimum wage, working hours, and benefits, may affect personnel costs and operations.

5) **Technology Risks:** Risk related to changes in information technology and social media, including digital transformation, which affects the Company's operations. Technology risk also encompasses information technology systems used by the organization for critical business activities that fail to meet business needs.

Technology Risks are further divided as follows:

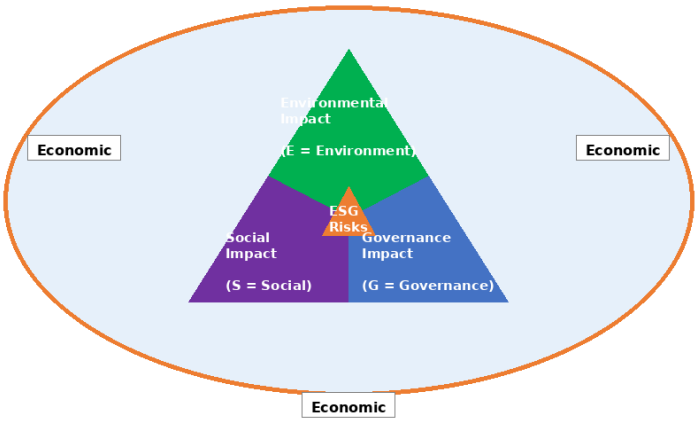
5.1) Risk related to changes in information technology/digital transformation that affects the Company's operations, also including information technology systems used by the organization for critical business activities that fail to meet business needs.

5.2) Social Media Risk: Risk arising from the use of internet-based channels that connect users, whereby users can produce, publish, and share content or information via rapid word-of-mouth as desired, creating widespread interaction between users and network members. Where information on social media reflects the poster's personal viewpoint, contains bias, lacks screening, or is negative toward the Company, the Company may suffer damage to its reputation, image, and customer confidence, which in turn affects the Company's business operations.

6) **Corruption Risk:** Risk arising from any act to seek unlawful benefit through the giving or receiving of bribes — whether in the form of money, goods, financial assistance, charitable donations, hospitality expenses, or other expenses — by offering, promising, pledging, demanding, giving, or receiving money or other improper benefits to government officials, government agencies, private parties, or duty holders, whether directly or indirectly, in order to induce such agency or person to perform or omit to perform their duties improperly.

Sustainability Risks (ESG Risks):

Risks related to Environment, Social, and Governance.



	Key ESG Issues
Environment	• Climate change from carbon dioxide emissions, greenhouse gas emissions, and global warming • Efficient use of natural resources and biodiversity • Waste management (emissions of toxic substances, waste, packaging materials, and rubbish) • Efficient energy use • Clean technology / green building
Social	• Responsibility for product and service quality and safety • Human rights, labor management, labor standards in the supply chain, and child labor • Occupational health and safety conditions • Integration with the well-being of local communities • Stakeholder opposition and conflict resolution
Governance	• Corporate governance and corporate behavior • Business ethics • Anti-competitive practices • Tax transparency

Enterprise Risk Management Process

To ensure the risk management process is systematic, the Company has adopted the international COSO-ERM standard (The Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management) and the guidelines of the Stock Exchange of Thailand as a framework for developing the Company's risk management process, which consists of 5 components:

1. Governance and Culture for ESG-related risks
2. Strategy and Objective-Setting for ESG-related risks
3. Performance for ESG-related risks: through the enterprise risk management process (identification, assessment, prioritization, and risk response), with a focus on performance
4. Review and Revision for ESG-related risks
5. Information, Communication, and Reporting for ESG-related risks

Risk Management Steps: 6 Steps

1. Setting Objectives
2. Establishing Risk Assessment Criteria and Acceptable Risk Level
3. Risk Identification and Preparation of the Risk Register

4. Risk Assessment
5. Determining Risk Treatment Measures
6. Monitoring and Reporting Risk Management Results

Details of each step are as follows:

1) Setting Objectives:

This involves setting objectives at the organizational/business-line level that are consistent with and aligned in the same direction as the organization's vision, mission, key policies, and goals — including ensuring that the risk management plan is consistent with and supports the objectives established.

2) Establishing Risk Assessment Criteria and Acceptable Risk Level:

This involves establishing criteria for assessing the Likelihood of a risk occurring and the Impact of a risk event, in order to prioritize risks using a Risk Map, as well as determining the acceptable risk level and Key Risk Indicators / Trigger Points (KRIs).

Risk Map - Risk Assessment

Impact					
Very High (5)	5 (C)	10 (B)	15 (B)	20 (A)	25 (A)
High (4)	4 (C)	8 (C)	12 (B)	16 (A)	20 (A)
Medium (3)	3 (D)	6 (C)	9 (C)	12 (B)	15 (B)
Low (2)	2 (D)	4 (C)	6 (C)	8 (C)	10 (B)
Very Low (1)	1 (D)	2 (D)	3 (D)	4 (C)	5 (C)
	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)

Likelihood

Score Range	Significance (Severity) of Risk	Symbol
16-20	Very high severity/significance level — requires immediate management	**A**
10-15	Relatively high severity/significance level — requires urgent management	**B**
4-9	Moderate severity/significance level — requires regular monitoring	**C**

Below 3	Low severity/significance level — risk is at a level the Company can accept	**D**

Prioritization (severity level) of risk and risk management approach

3) Risk Identification:

This involves searching for and identifying the causes or factors of risk, taking into account various internal and external factors, megatrends, and global trends — such as changes in the natural environment, demographic change, globalization, and rapid technological advancement — considering the economic, social, environmental, and good governance dimensions that affect the organization's goals. This is undertaken in order to record identified risks in the risk register.

4) Risk Assessment:

This step follows on from risk identification and consists of 2 main processes:

4.1) Risk Analysis and Assessment

This involves analyzing and assessing the risks identified in the Risk Identification step, considering the Likelihood and Impact — both positive and negative — of each risk, according to criteria set by the Company. Note that a single event or situation may affect multiple objectives/goals. In addition, the analysis should take into account current risk management measures already in place, including their effectiveness.

Risk Assessment Criteria

In assessing risk, consideration is given to the Likelihood and the Impact:

- Likelihood: Consideration of the probability that a risk event will occur within a given period — also referred to as the frequency or chance of the risk event occurring.
- Impact: The severity of the damage arising from a risk that affects the organization, which may be either positive or negative, and can be divided into financial impact and non-financial impact.

The Company has established criteria for assessing the level of likelihood and the level of impact, each divided into 5 levels, as follows:

Likelihood Assessment Criteria

1) General Criteria – considered based on the likelihood that a risk event will occur

Rank	1	2	3	4	5
Likelihood	Rare	Unlikely	Possible	Likely	Almost Certain

2) Specific Likelihood Assessment Criteria (by area)

No.	Indicator	1	2	3	4	5
1	Financial Management Area - Ability to pay interest, measured by Interest-Bearing Debt to Equity ratio (IBD/E)	IBD/E less than 1.00x	IBD/E ≥ 1.00x but < 1.25x	IBD/E ≥ 1.25x but < 1.50x	IBD/E ≥ 1.50x but < 1.80x	IBD/E ≥ 1.80x
2	Human Resources Area - Employee Turnover Rate	Turnover Rate < 4%	Turnover Rate ≥ 4% but < 5%	Turnover Rate ≥ 5% but < 6%	Turnover Rate ≥ 6% but < 7%	Turnover Rate ≥ 7%
	- Staffing Level	Staff shortfall not exceeding	Staff shortfall 10%–15% of plan	Staff shortfall 15%–20% of plan	Staff shortfall 20%–25% of plan	Staff shortfall exceeding 25% of plan

		10% of plan				
3	Construction Quality Area - Number of unit repair (defect) requests	Zero Defect > 70% of all units	Zero Defect 60%–70% of all units	Zero Defect 50%–60% of all units	Zero Defect 40%–50% of all units	Zero Defect < 40% of all units
4	Corruption Area *	Never occurs (0%) when such transactions must be conducted	Occurs very rarely (<20%) when such transactions must be conducted	Occurs occasionally (20%–50%) when such transactions must be conducted	Occurs frequently (>50%) when such transactions must be conducted	Occurs every time (100%) when such transactions must be conducted
5	Technology Area	No Notification Incident Ticket **	Notification Incident Ticket — fully controlled and resolved (100%)	Notification Incident Ticket at Low level — not controlled/resolved	Notification Incident Ticket at Medium level — not controlled/resolved	Notification Incident Ticket at High/Critical level — not controlled/resolved

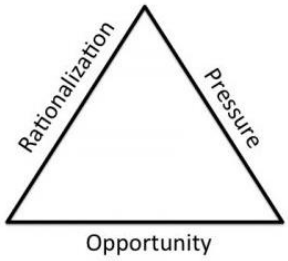
*** Notification Incident Ticket generated by the Security Information & Event Management (SIEM) system*

Note: * In assessing the likelihood of corruption risk, the following risk factors should be considered:

1. Pressure/Incentive

2. Opportunity arising from weaknesses or gaps in internal controls

3. Rationalization



(See example of corruption risk patterns in the Appendix)

Impact Assessment Criteria — Enterprise-Level Risk

In assessing risk impact, both Financial Impacts and Non-Financial Impacts should be considered.

No.	Indicator	1	2	3	4	5
1	Financial Impact (Financial Loss)	Impact on assets < 5 million baht	Impact on assets 5–10 million baht	Impact on assets 10–50 million baht	Impact on assets 50–100 million baht	Impact on assets ≥ 100 million baht
2	Operational Target Impact	Impact on organizational goals < 1%	Impact on organizational goals 1%–3%	Impact on organizational goals 3%–5%	Impact on organizational goals 5%–10%	Impact on organizational goals > 10%
3	Occupational Safety Impact	Minor injury requiring basic first aid, or minor illness not affecting work	Injury/illness requiring work stoppage of less than 3 days	Injury/illness requiring work stoppage of less than 1 month	Injury/severe illness requiring work stoppage of more than 1 month	Injury/severe illness resulting in permanent disability or death
4	Reputation and	Very minor	Reputation: news	Reputation: social	Reputation: continuous	Reputation: Company is

	Image Impact	likelihood of negative news about reputation/image, and controllable	appears that could implicate individuals within the Company or the Company itself. Customers/ Shareholders: concerns begin and inquiries are made	media spreads news or information on a corruption case involving the Company. Customers/ Shareholders: questions raised to the Board of Directors	news coverage and society begins to pay attention. Customers/Shareholders: the Board and management must clarify and explain the facts	blacklisted / negatively portrayed regarding good corporate governance. Customers/Shareholders: lawsuit filed for damages incurred
5	Regulatory / Legal / Government Requirement Compliance Impact	Able to fully comply with internal and external regulations	Warned, or fined an insignificant amount	May need to submit evidence and clarify if a government agency investigates and accepts a complaint	Investigated by a government agency and required to clarify and identify wrongdoing	Business license/permit revoked; executives and senior management imprisoned
6	Environmental Impact	Minor impact, self-remediating naturally, not affecting surrounding	Minor impact on surrounding community; Company can resolve quickly within 24 hours using	Impact on community; Company can control quickly within 24 hours, requiring external personnel	Company cannot control within 24 hours, or remediation takes less than 1 year and/or requires	Widespread environmental impact, or remediation takes more than 1 year and/or cannot be remediated and/or no

		communities	its own staff	to assist but not affecting Company operations, or a formal written complaint is received	technology for treatment/recycling, or affects operations causing project delay not exceeding 3 months, or a warning/fine from a government agency	appropriate remediation technology yet exists, or affects operations causing project delay exceeding 3 months, or may result in construction suspension or criminal penalty

Note: Impact assessment should evaluate all impact areas arising from a given risk factor. If a risk factor has an impact in more than one area, the highest value shall be used as the impact level for that risk.

4.2) Risk Prioritization (Severity)

Risk prioritization helps ensure the Company's risk management is effective, with Company resources allocated appropriately according to the significance level of each risk, using the Risk Map illustrated below:

Risk Map: showing the relationship between the likelihood of a damaging event occurring and the impact of each risk

Risk Map - Risk Assessment

Impact	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Very High (5)	5 (C)	10 (B)	15 (B)	20 (A)	25 (A)
High (4)	4 (C)	8 (C)	12 (B)	16 (A)	20 (A)
Medium (3)	3 (D)	6 (C)	9 (C)	12 (B)	15 (B)
Low (2)	2 (D)	4 (C)	6 (C)	8 (C)	10 (B)
Very Low (1)	1 (D)	2 (D)	3 (D)	4 (C)	5 (C)
	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)

Likelihood

Risk prioritization (severity level) is determined from the score shown in the Risk Map grid, divided as follows:

Score Range	Significance (Severity) of Risk	Symbol
16-20	Very high severity/significance level — requires immediate management	**A**
10-15	Relatively high severity/significance level — requires urgent management	**B**
4-9	Moderate severity/significance level — requires regular monitoring	**C**
Below 3	Low severity/significance level — risk is at a level the Company can accept	**D**

5) Determining Risk Treatment Measures (Risk Treatment)

To ensure risk management is carried out continuously and effectively, the Company has established responsibility for risk management and guidelines for managing risk as follows:

5.1) Levels of Responsibility (Risk Owner) and Actions According to Risk Significance Level

Level	Significance	Action	Risk Owner Level
A	High severity level	Must have a risk-reduction plan, allocating sufficient resources and measures to reduce risk immediately, with actions completed within a specified time frame, or risk transfer where necessary	C Level
B	Relatively high severity level	Must have a risk-reduction plan, allocating sufficient resources and measures to bring risk down to an acceptable level	C Level

C	Moderate severity level	Must have risk controls in place, with appropriate and sufficient control measures, such as improving operating processes or establishing control standards	SEVP / EVP
D	Low severity level	Regularly monitor risk status as part of normal operating procedures	SVP / VP / AVP

Risk management plans are presented to the management meeting for consideration and approval of any necessary resource allocation. The most appropriate risk management approach is selected with regard to the cost involved compared to the expected benefit, relevant laws and other requirements, and social responsibility.

5.2) Risk Management Approaches (4T)

- Terminate: Stopping or cancelling the activity that causes the risk. Used when the risk is highly severe and there is no way to reduce or manage it to an acceptable level.
- Transfer: Transferring all or part of the risk to a third party or external organization to share the risk burden, such as purchasing an insurance policy.
- Treat: Putting management measures in place to reduce the likelihood of a risk event occurring or to reduce its potential impact, such as preparing a Contingency Plan.
- Take: Accepting existing risk without taking any action. Typically used for risks where the cost of management measures is high and not commensurate with the benefit gained.

6) Monitoring and Reporting Risk Management Results:

6.1). The risk management unit coordinates with the management responsible for each risk to report risk assessment results and risk management performance to the management meeting, the Risk Management Working Group, and the Board of Directors for further consideration. Where the risk management results indicate a high level of significance, the responsible management (Risk Owner) shall report the risk status and prepare a management plan to reduce the risk to an acceptable level, presenting it to the Risk Management Committee for consideration and to the Board of Directors for approval, until the risk severity has been reduced to an acceptable level.

6.2). Management shall analyze and monitor changes in the internal and external

environment in order to assess risks that may materially affect the Company's stated goals. This may result in the need to review risk management and prioritization, and may also be used to review the overall risk management framework — at least once a year — with the results presented to the Risk Management Committee for consideration and to the Board of Directors for approval.

_____

(Mr. Chartchai Payuhanaveechai)
Chairman of the Board of Directors,
Origin Property Public Company Limited (Public)

Appendix

Example of Corruption Risk Patterns

- Government officials demanding payment, particularly in connection with permits for building/condominium/housing development construction
- Conflict of interest: taking on design drawing work and then inspecting one's own work (even though the government provides standard forms to facilitate the public, permit applications require accompanying site plans, so inspectors or approving officers are hired to make approval easier)
- Government officials colluding with, or being complicit in, individuals or juristic persons unlawfully constructing, modifying, demolishing, or relocating buildings
- Government officials colluding with, or being complicit in, individuals or juristic persons using buildings inconsistent with the permit certificate or notification filed with local officials
- Under-assessment of taxes
- Paying bribes through intermediaries, or paying monthly “protection” fees
- Employees, officials, or contracted staff acting as agents for registration/permit applications, demanding benefits or fees in exchange for special privileges
- Permit application processes lacking a clear timeframe, which may lead to bribery demands in exchange for faster approval
- Inconsistent use of discretion when checking the completeness of documents
- Incomplete document review relative to what is specified in the application, yet the application is still accepted
- Withholding a matter without notifying the applicant, in order to demand a benefit
- Review, verification, and recommendation of approvals/permits not processed in the order applications were received
- Under normal procedures, review takes 1 day, but in some cases review may take longer — for example, when it is necessary to schedule a site inspection with the permit applicant before issuing the permit. There is a risk that officials may exploit this gap to seek improper benefits or demand payment during the review process

- Processing of applications by “jumping the queue”
- Inspection of a proposed business location may favor the applicant in cases where the location does not meet the required criteria
- Bribing officials to gain favorable treatment on permit applications where the business location does not meet the required criteria
- Inspecting or visiting operator premises, such as construction sites, with the intent of leading to a demand for monthly special payments
- Changing the classification of an offense from severe to minor, or from minor to severe
- Concealing facts within criminal investigation case files
- Fabricating an anonymous complaint alleging a grievance against an operator, in order to conduct an inspection or search, where that operator does not pay monthly special fees
- Using intermediaries to collect special payments or monthly fees from various operators
- Using discretion to approve or exempt regulations in a manner that provides a benefit involving a conflict of interest
- Issuing regulations, rules, or directives that provide a benefit involving a conflict of interest
- Granting education or research scholarships to associates, reflecting cronyism or patronage systems