



JUMP+ Plan



SIAMRAJATHANEE PUBLIC COMPANY LIMITED

(SO)

Year 2026 - 2028

This report was approved by the board of directors on 26/02/2026
and disseminated on 31/03/2026

Disclaimer

This document has been prepared by SIAMRAJATHANEE PUBLIC COMPANY LIMITED ("SO") based on information, assumptions, and projections of the Company as of the document preparation date. All plans, projects, proposals, opinions, forecasts, projections, or statements contained herein are provided solely for disclosure to interested parties.

The Company reserves the right to amend, modify, or update any project plans, including targets of the plans or projects described in this document at its sole discretion. The Company makes no representation or warranty regarding the accuracy, completeness, or validity of information contained herein, nor does it guarantee that the plans or projects outlined herein will successfully deliver outcomes according to the established targets or estimated timelines. All proposals, opinions, forecasts, projections, and forward-looking statements specified herein reflect the Company's views as of the document preparation date which are subject to risks and uncertainties and may change in the future according to changing economic conditions, competition, business-related factors, or any other factors. The Company assumes no obligation to update or revise such information or statements, except where the Company's Board of Directors approves any revisions to plans, targets, or other information that require the Company to disclose such changes through the system provided by The Stock Exchange of Thailand ("SET").

This document is intended only for disclosure to investors and related parties in general without the intent to solicit, recommend, induce, or offer opinions on investments in securities issued by the Company, nor shall it be construed as investment advice, an offer to buy or sell, or a solicitation for offers to buy or sell securities, or an inducement to engage in any transactions related to securities issued by the Company, particularly in any countries or special administrative regions where such acts may violate their applicable laws. No part of this document should be relied upon as a determining factor in making any decisions concerning the execution of contracts, agreements, or investments whatsoever. The Company and its directors, executives, and employees shall not be liable for any losses or damages, whether direct, indirect, compensatory, or consequential (including but not limited to loss of profits), arising from the use of or reliance on information contained herein, or from any variance between actual outcomes and the Company's forecasts or projections.

Investors are advised to exercise careful judgement and discretion in making investment decisions and to regularly review the Company's public disclosures such as information releases on material events, financial statements, Form 56-1 One Report, to support their prudent investment decisions with appropriate due diligence.

The role of The Stock Exchange of Thailand ("SET") is solely to initiate and facilitate the JUMP+ program which is intended to enable the growth and enhance the attractiveness of participating listed companies. SET does not participate or engage in the identification of the targets, forecasts, projections, and expected outcomes contained herein, nor does SET endorse the validity, accuracy, feasibility, and reasonableness thereof. The decision to rely on such information solely depends on the judgment and at the discretion of investors and related parties. SET and its directors, executives, and employees shall not be liable for any losses or damages, whether direct, indirect, compensatory, or consequential (including but not limited to loss of profits), arising from the use of or reliance on information contained herein, or from any variance between actual outcomes and the Company's forecasts or projections.

Table of Contents

	Page
Executive Summary	1
Section 1 Business Plan	2
Target in 2028	3
Strategic Plan : SMARTOPS 2.0 : ERP Development for Enhanced Organizational Capability	3
Section 2 Governance Plan	7
Enhancing anti-corruption and fraud prevention efforts	8
Enhancing the prevention of insider information	10
Enhancing business continuity management	12
Attachment	15



SIAMRAJATHANEE PUBLIC COMPANY LIMITED

SET
Services / Professional Services

CG Report :

SET ESG Ratings: **BBB**

Anti-Corruption Certification (CAC): -

Business Type

The Company operates 2 main businesses which are; 1. Outsourcing Services, divided into 2 types: (1) Management service businesses including driver, office staff, technician staff and data entry services (2) Landscape management services 2. Rental and services business including automobile rental and property rental.

Financial Statement

Year	2025	2024	2023	2022
------	------	------	------	------

Income Statement (MB)

Revenues	2,845.80	2,584.64	2,382.47	2,318.78
Expenses	2,617.46	2,391.34	2,154.75	2,108.01
Net Profit	227.87	153.40	183.50	168.77

Balance Sheet (MB)

Assets	2,523.38	2,351.48	2,074.34	1,917.75
Liabilities	1,403.68	1,267.34	1,043.70	874.89
Shareholders' Equity	1,119.70	1,084.14	1,030.64	1,042.86

Cash Flow (MB)

Operating	489.11	327.32	350.44	259.98
Investing	146.94	30.84	71.84	140.54
Financing	-636.57	-485.48	-463.78	-336.99

Financial Ratio

EPS (Baht)	0.48	0.32	0.41	0.38
GP Margin (%)	15.65	16.11	17.52	17.12
NP Margin (%)	8.01	5.94	7.70	7.28
D/E Ratio (Times)	1.25	1.17	1.01	0.84
ROE (%)	20.68	14.51	17.70	16.92
ROA (%)	11.79	8.73	11.41	12.19

JUMP+ Plan

Business Plan

Target in 2028

Net Profit **299.12** Million Baht

Strategic Plan	Growth	Profitability & Efficiency	Stability
----------------	--------	----------------------------	-----------

1. Strategic Plan : SMARTOPS 2.0 : ERP



Development for Enhanced
Organizational Capability

Governance Plan

1. Enhancing anti-corruption and fraud prevention efforts
2. Enhancing the prevention of insider information
3. Enhancing business continuity management

Remark : This document has been prepared by the listed company for the purpose of disseminating corporate information to investors solely for their investment decision-making. The listed company does not provide any investment advice or recommendations regarding its securities. Investors are advised to conduct further research and consult with qualified professionals before making any investment decisions. The listed company shall not be held liable for any damages or losses arising from the use of information contained in this document under any circumstances. The listed company reserves the right to amend the information presented herein without prior notice. Reproduction, modification, or dissemination of this document or any part thereof is prohibited unless prior permission has been obtained from the listed company. For additional information, investors may refer to the reports or disclosures made available through the Office of the Securities and Exchange Commission and/or the Stock Exchange of Thailand.

Section 1
Business Plan

Section 1 Business Plan

Target in 2028

Topic	YE/2023	YE/2024	YE/2025	Target in 2028
Net Profit (Million Baht)	183.50	153.40	227.87	299.12

The company focuses on developing an internal information system (SmartOps 2.0) to replace the existing ERP system that has been in use for over 10 years. This involves developing 21 new cloud-based web application systems covering all core business processes within a 3-year period (2026–2028). The initiative is expected to reduce IT costs by up to 85 million THB compared to implementing SAP S/4HANA Cloud, or increase net profit by approximately +28 million THB per year.

Growth plan/Increase business value

Strategic Plan : SMARTOPS 2.0 : ERP Development for Enhanced Organizational Capability

The company is developing a new ERP system in-house, transitioning from a legacy Windows application (PowerBuilder) that has been in use for over 10 years to a modern, secure, and flexible cloud-based web application. This transformation is designed to support business operations in the digital era.

This approach was chosen over adopting a packaged solution such as SAP S/4HANA Cloud because the total cost over three years is significantly lower (15 million THB compared to over 100 million THB for SAP). In addition, the company retains full ownership of the system, allowing unlimited customization and avoiding dependency on any specific vendor.

This plan will promote and develop the organization in the following dimensions

- Profitability & Efficiency

Targets

- Corporate Financial Targets

Topic	Latest data		Targets		
	YE/2024	YE/2025	2026	2027	2028
Net Profit : Owners Of The Parent (MILLION BAHT)	153.40	227.87	207.64	252.15	299.12

- Other Targets

Topic	Baseline	Targets		
	YE/2025	2026	2027	2028
Cumulative number of developed and Go-Live systems	Not yet implemented	6 system	16 system	19 system
System supports Work from Anywhere (Web-based)	Not yet implemented	In development	Ready for use (16 systems)	Fully operational (100%)
PDPA & Cybersecurity Compliance	Not yet implemented	Establish standards & policy	Review and fix Go-Live systems	Passed PDPA & Security audit

Topic	Baseline	Targets		
	YE/2025	2026	2027	2028
Decommission PowerBuilder (Legacy ERP) system	In operation	parallel Run (6 system)	parallel Run (16 system)	System decommission (after ≥ 1 year of stability)

Strategic Initiative

Strategic Initiative	Year	Expected Outcomes
Work Plan 1: Development of Operational & HR Systems (2026)	2026	<ul style="list-style-type: none"> 1. Site Employee Management System 2. Vehicle Rental and Maintenance System 3. Recruitment and Selection System 4. Project Management System 5. Administrative System 6. Procurement System
Work Plan 2: Development of Finance & Compliance Systems (2027)	2027	<ul style="list-style-type: none"> 1. Leasing System 2. Accounts Payable System 3. Accounts Receivable System 4. Tax System 5. Billing System 6. Expense / Prepayment System 7. Payment Voucher System 8. Budget Planning System 9. Letter of Guarantee (LG) System 10. Travel and Expense Management System
Work Plan 3: Development of HR Core & Asset Systems (2028)	2028	<ul style="list-style-type: none"> 1. Human Resource Management System 2. Accounting System 3. Asset Management System

Risk Management

Risk 1 : Risk of delays in system development

- **Risk Characteristic**

- Large-scale in-house development projects (21 systems) often take longer than initially estimated
- The internal development team may have insufficient capacity if multiple systems are developed simultaneously
- User requirements may change during the implementation phase

- **Risk Impact**

- If delayed by 1 year, the opportunity to save costs of 28 million THB per year will be lost.
- Management and employee confidence in the project will decrease.
- The budget may exceed the approved limit of 15 million THB.

- **Risk Management Measures**

- Use Agile methodology (Scrum) with short sprints and regular demos.
- Establish GO/NO-GO gates every quarter, governed by the Steering Committee.
- Implement a phased development approach based on priorities, rather than developing all systems simultaneously.
- Allocate a contingency reserve of 3.4 million THB to mitigate risks related to timeline and resources.

Risk 2 : Change Resistance

- **Risk Characteristic**

- 250 employees have been familiar with the legacy system (PowerBuilder) for over 10 years.
- Some employees may not be comfortable with new technology.

- **Risk Impact**

- Low user adoption rate, resulting in not fully realizing the benefits of the new system.
- Employees continue using old workarounds (Excel, email), leading to a loss of expected efficiency gains.

- **Risk Management Measures**

- CEO sponsorship: communicate the vision through a Town Hall meeting.
- Super User Program: select power users to act as champions in each department.
- Provide role-based training and use gamification to encourage adoption.
- Link executives' KPIs to the success of the project.

Risk 3 : Data Migration & Quality

- **Risk Characteristic**

- Data in the legacy system has accumulated over 10 years and may be duplicated, incomplete, or outdated.
- The database structure of the legacy system (PowerBuilder) differs from the new system, making migration complex and potentially redundant.

- **Risk Impact**

- Incorrect data in the new system can impact credibility and business decision-making.
- If the data is incomplete, the new system may not be fully usable, forcing a return to the legacy system.

- **Risk Management Measures**

- Perform data cleansing and data audits for all systems before go-live.
- Conduct parallel runs for all systems: operate both legacy and new systems simultaneously to validate data accuracy.
- Establish a rollback plan and complete backups for every sprint, enabling immediate recovery if needed.

Risk 4 : Risk related to security and PDPA compliance

- **Risk Characteristic**

- Developing a new web application introduces higher cybersecurity risks compared to the legacy system.
- The system will store sensitive data (employee, customer, and financial information), which is subject to PDPA regulations.

- **Risk Impact**

- Non-compliance with PDPA may result in fines of up to 5 million THB per case.
- Data breaches or cyberattacks can impact trust and disrupt business operations.

- **Risk Management Measures**

- Security by Design: define security standards from the design phase, not as an afterthought.
 - Implement Role-Based Access Control (RBAC) and data encryption for sensitive information.
 - Conduct penetration testing before go-live for all systems handling sensitive data.
 - Appoint a Data Protection Officer (DPO) to oversee PDPA compliance.
 - Perform PDPA and security audits after go-live for all 21 systems (by 2028).
-

Section 2

Governance Plan

Section 2 Governance Plan

Accountability and Transparency Governance

Enhancing anti-corruption and fraud prevention efforts

At present, the Company recognizes the importance of promoting transparency and ethical conduct in its operations. Siamrajathanee Public Company Limited, as a provider of outsourcing services in workforce and operational management for numerous corporate clients, has therefore developed an enhancement plan for anti-corruption efforts. This plan focuses on strengthening preventive measures and internal controls, along with improving monitoring and evaluation mechanisms for compliance with anti-corruption policies. It aligns with the CG Code 2017 and the regulations of the Securities and Exchange Commission (SEC). In addition, the Company aims to actively drive awareness and communication of its anti-corruption policy in a concrete manner, in order to sustain and foster an organizational culture rooted in integrity and ethical conduct.

Targets

Topic	Current Status	Targets		
		2026	2027	2028
The company has established an anti-corruption policy and practices.	In Progress	Success	Success	Success
<ul style="list-style-type: none"> An anti-corruption and anti-bribery policy has been developed to comprehensively cover the organization's business operations, formally approved by the Board of Directors, and supported by clear and practical implementation guidelines 	In Progress	Success	Success	Success
<ul style="list-style-type: none"> The company conducts regular monitoring and evaluation of compliance with its anti-corruption and anti-bribery policy and procedures. Audit results are reported by internal auditors to the Board of Directors at least annually. In the event of any violations, corrective actions and preventive measures are clearly defined to prevent recurrence 	In Progress	Success	Success	Success
<ul style="list-style-type: none"> The company conducts an annual review of its anti-corruption and anti-bribery policy and practices with the Board of Directors 	In Progress	Success	Success	Success
Achieve CAC certification from the Thai Institute of Directors (Thai IOD)	Not Started	Not Started	Not Started	Certified
Enhance awareness and communicate the anti-corruption policy in a concrete and tangible manner.	-	In Progress	Success	Success

Strategic Initiative

Strategic Initiative	Year	Expected Outcomes
Monitoring and continuous improvement of anti-corruption policies and practices	2026	<ul style="list-style-type: none"> Review and update the anti-corruption policy to ensure alignment with CG Code and CAC standards Establish a Compliance Unit to oversee adherence to policies. Establish practical guidelines for employees at all levels, along with training at least once per year.
	2027	<ul style="list-style-type: none"> Conduct internal audits on anti-corruption measures at least once per year Continuously review policies and practices, and report to the Audit Committee
	2028	<ul style="list-style-type: none"> Conduct internal audits on an ongoing basis and prepare a report to be submitted to the Board of Directors at least once per year Update policies based on audit findings
Enhance awareness and communicate the anti-corruption policy in a concrete and tangible manner.	2026	<ul style="list-style-type: none"> Develop clear Anti-Corruption Guidelines for employees at all levels. Communicate the policy through internal channels such as email and infographics.
	2027	<ul style="list-style-type: none"> Ensure the policy is communicated to employees at all levels at least once per year. Communicate the policy to key customers (Critical Tier 1 Suppliers)
	2028	<ul style="list-style-type: none"> Monitor outcomes and evaluate the effectiveness of implementation. Prepare an annual summary report for submission to the Board of Directors.

Risk Management

Risk 1 : Risk that internal audit processes and CAC certification do not comply with the prescribed timeline and standards.

- **Risk Characteristic**

- The Company may need to allocate significant resources to improve systems in order to comply with CAC standards.
- The complexity of the outsourcing business, with its diverse contractual arrangements, may result in a lengthy audit process.

- **Risk Impact**

- Failure to achieve CAC certification within the specified timeframe may negatively impact the Company's reputation and business opportunities.
- It may also result in a loss of confidence among investors and customers.

- **Risk Management Measures**

- Establish a structured assurance framework by appointing a dedicated task force responsible for CAC audit implementation.
- Engage external consultants with CAC certification expertise to provide guidance and review the completeness of documentation.

- Conduct periodic gap analyses to monitor progress and ensure alignment with requirements.-

Risk 2 : Risk arising from a lack of continuity and understanding in complying with the anti-corruption policy among employees and business partners.

• **Risk Characteristic**

Employees and key business partners may be unable to fully and correctly implement the anti-corruption policy guidelines.

• **Risk Impact**

This may pose reputational risks and could result in the Company’s failure to fully comply with CAC standards.

• **Risk Management Measures**

- The Company requires employees at all levels to attend training at least once per year, with a participation target of no less than 70%.

- Regular internal communications are conducted, and anti-corruption policies are incorporated into contracts with key business partners.

Enhancing the prevention of insider information

The Company is committed to elevating its standards of good corporate governance, placing strong emphasis on transparency and accountability, particularly in the management of undisclosed internal information. This is to prevent the misuse of such information for personal gain or its disclosure to unauthorized parties. During the implementation of the SmartOps 2.0 project, which involves a significant amount of information that may materially affect securities prices, the Company places great importance on having clear data control measures in place as a proactive approach to risk prevention.

Targets

Topic	Current Status	Targets		
		2026	2027	2028
The company has established a policy and procedures to prevent the misuse of insider information.	In Progress	Success	Success	Success
• A Board-approved written policy on insider information prevention has been clearly defined and implemented	In Progress	Success	Success	Success
• A structured process is implemented to regularly monitor and review compliance with the insider trading prevention policy,with audits conducted at least annually.	Not Started	Success	Success	Success
• The implementation of the insider information prevention policy is reviewed and reported to the Board of Directors at least annually. If any violations are detected,corrective actions and preventive measures are clearly outlined to prevent recurrence	Not Started	Success	Success	Success
Announcement: Designation of persons who hold positions or duties that grant access to the company’s inside information.	-	Success	Success	Success

Strategic Initiative

Strategic Initiative	Year	Expected Outcomes
Review and revision of policies and practices for the prevention of insider information misuse.	2026	• Review and update the insider trading prevention policy to align with SEC standards.
		• Establish Non-Disclosure Agreements (NDAs).
		• Provide training on relevant practices for executives and employees at least once per year.
	2027	• Conduct internal audits on insider information prevention at least once per year.
		• Review access logs on a quarterly basis and report the findings to the Audit Committee.
		• Continuously review and update policies and practices.
2028	• Conduct internal audits and prepare a summary report for submission to the Board of Directors on an annual basis.	
	• Assess data security and develop corrective action plans if any deficiencies are identified.	
Control of access to internal information and maintenance of confidentiality.	2026	• Review and strengthen the data access management process (Change Management Procedure).
		• Prepare Non-Disclosure Agreements (NDAs) for relevant internal and external personnel.
		• Review the Data Center system and access rights management (Access Governance Review).
	2027	• Implement logging systems to monitor access to critical data and enable audit trails for retrospective review.
		• Review or update the Change Management Procedure at least once per year.
		• Provide training on data privacy for relevant personnel at least once per year.
	2028	• Continuously review and improve systems.
		• Conduct internal audits on data security, with corrective action plans implemented if any deficiencies are identified.

Risk Management

Risk 1 : Risk arising from the misuse or unauthorized disclosure of insider information.

- **Risk Characteristic**

- Personnel with access to insider information may disclose such information prior to public release.
- During the SmartOps 2.0 period, the Company will handle a significant volume of sensitive material information.

- **Risk Impact**

- Relevant operational processes may be delayed or temporarily suspended to review approaches and implement corrective actions.
- This may negatively impact investor and customer confidence, as well as business opportunities.

• **Risk Management Measures**

- Establish and publish a policy and guidelines to prevent the misuse of inside information, with clearly defined scope of what constitutes inside information.
- Implement role-based access control (RBAC) and require non-disclosure agreements (NDAs) for all relevant parties.

Risk 2 : Risk arising from incomplete or outdated access control management.

• **Risk Characteristic**

- Employees who have resigned or changed roles may still retain access to internal information.
- The system for recording access approvals or user timestamps may be incomplete.

• **Risk Impact**

Unauthorized access to information may occur, affecting the organization’s data security and credibility.

• **Risk Management Measures**

- Conduct the Change Management Procedure and Access Governance Review at least once per year.
- Update access rights promptly upon any personnel changes and report to the Audit Committee.

Governance of Risk and Management Compliance

Enhancing business continuity management

The Internal Audit (IA) function identified that the current Business Continuity Plan (BCP) requires enhancement to align with the Company’s current operations. This includes the need to strengthen the Business Impact Analysis (BIA), Recovery Time Objective (RTO), Recovery Point Objective (RPO), and crisis communication processes. The risk level assessed by IA is moderate across several areas. In addition, the 2026 risk assessment identified natural disasters and cybersecurity as enterprise-level risks. The transition of the ERP system to a cloud platform during 2026–2031 also introduces continuity risks during the transition period. Therefore, strengthening BIA, BCM, and BCP is essential and should be carried out in parallel with the SmartOps 2.0 project.

Targets

Topic	Current Status	Targets		
		2026	2027	2028
The company has developed, reviewed, and conducted drills for its Business Continuity Plan (BCP) and crisis response protocols.	In Progress	Success	Success	Success
• Prepare and conduct the annual review of the business continuity management plan.	In Progress	Success	Success	Success
• Organize Crisis Management Drills	In Progress	Success	Success	Success
The BCP covers risks related to cybersecurity and the transition of the ERP system to the cloud.	-	In Progress	Success	Success

Strategic Initiative

Strategic Initiative	Year	Expected Outcomes
Enhancement of Business Impact Analysis (BIA) and Business Continuity Plan (BCP).	2026	<ul style="list-style-type: none"> Conduct BIA across all critical processes and clearly define RTO and RPO. Enhance the BCP to cover crisis communication and cybersecurity scenarios. Conduct the first BCP test and report the results to the Audit Committee.
	2027	<ul style="list-style-type: none"> Conduct BCP testing on a regular basis, at least once per year. Enhance the BCP to support the transition of the ERP system to the cloud (SmartOps 2.0). Summarize the test results and submit a report to the Board of Directors.
	2028	<ul style="list-style-type: none"> Review and update the BCP to align with the new ERP system following its successful go-live. Conduct BCP testing at least once per year and report the results to the Board of Directors.
Enhance the BCP to cover crisis communication and cybersecurity scenarios.	2026	<ul style="list-style-type: none"> Assess cybersecurity risks during the SmartOps 2.0 system transition. Establish preventive measures and a dedicated cybersecurity incident response plan. Develop an Incident Response Plan specifically for the data migration phase.
	2027	<ul style="list-style-type: none"> Implement a parallel run (operating legacy and new systems concurrently) along with risk mitigation plans. Conduct penetration testing prior to the SmartOps 2.0 system go-live.
	2028	<ul style="list-style-type: none"> Review cybersecurity measures after successful go-live. Prepare a summary report and continuous improvement recommendations for submission to the Board of Directors.

Risk Management

Risk 1 : Risk of business disruption during the ERP system transition.

• **Risk Characteristic**

- During the data migration and SmartOps 2.0 go-live phases, operational processes may be disrupted.
- The current BCP may not fully cover cloud transition scenarios.

• **Risk Impact**

- Customer service operations may be disrupted, affecting revenue and the Company’s reputation.

• **Risk Management Measures**

- Implement a parallel run strategy (running legacy and new systems concurrently) for at least 1–6 months.
- Develop a clear rollback plan to enable immediate reversion to the legacy system in case of critical issues.

- Conduct BCP testing specifically for ERP transition scenarios prior to go-live.

Risk 2 : Increased cybersecurity risks during the transition to the cloud.

- **Risk Characteristic**

- Cloud-based web applications have a larger attack surface than traditional on-premise systems.
- During data migration, a significant volume of sensitive data is transferred, increasing the risk of data leakage.

- **Risk Impact**

- Sensitive data may be leaked or compromised, potentially causing business disruption and damaging the Company's credibility.

- **Risk Management Measures**

- Use cloud providers certified with ISO 27001 and SOC 2, and conduct penetration testing prior to go-live.
 - Develop a dedicated incident response plan for cybersecurity scenarios.
 - Encrypt all data during migration (both in transit and at rest).
-

Attachment

Attachments

Attachments

URL Link to the Document : <https://jumpplusmedia-setlink.setgroup.or.th/SO/1774925581277.pdf>

