Political noise seen adding to FDI uncertainty alongside energy crisis

By Beatriz Marie D. Cruz
Senior Reporter

FOREIGN INVESTMENT pledges in the coming months could dampened by the fighting in Iran, compounded by a flareup of domestic political uncertainty, analysts said.

"This might be a slower year (for foreign investment pledges) due to uncertainties and the higher base recorded in the first quarter, Diana R. Rueda, an economics professor at the University of Asia & the Pacific, said via Viber.

Despite this, she noted that rising oil prices will likely attract foreign investment in sustainable energy, logistics and storage.

In the first quarter, foreign investment pledges jumped 52.3% to P42.64 billion, according to preliminary data from the Philippine Statistics Authority.

However, this was well below the P105.66 billion in foreign investment pledges approved in the fourth quarter of 2025.

Foreign investment pledges during the period were also the lowest since the P27.99 billion recorded in the first quarter of 2025.

"The Q1 number is a statistical artifact of a low base — not an evidence of investor conviction," Leonardo A. Lanzona, an economics professor at the Ateneo De Manila University, said via Facebook Messenger.

In the coming months, foreign investment pledges will likely cater to industries like manufacturing, digital infrastructure, logistics, and export-oriented ecozone projects, he also said.

"The main downside risks are global slowdown, geopolitical tensions, and weaker FDI (foreign direct investment) appetite," Mr. Lanzona added.

He also noted that the recent turmoil surrounding the impeachment could further dampen investor sentiment.

"The Senate crisis adds a political risk premium on top of an already fragile external environment," Mr. Lanzona said.

Gunshots were reported inside the Senate building on May 13 after the chamber sheltered Senator Ronald M. dela Rosa, who is wanted by the International Criminal Court over his alleged involvement in the previous administration's drug war.

"For a country that needs structural FDI to close its investment gap, that's compounding damage it can ill afford," Mr. Lanzona added.

PHILIPPINE STAR FILE PHOTO/EDD GUMBAN

DA warns it can penalize violators of rice price cap without turning to courts

RICE IMPORTERS and retailers violating the government's temporary price cap on imported rice will be subject to administrative penalties on the Department of Agriculture's (DA) own authority, on top of criminal prosecution under Republic Act No. 7581, the DA said.

Agriculture Secretary Francisco P. Tiu Laurel, Jr., added on Friday that price controls will likely extend beyond the initial period of 30 days.

"The effects of the (Iran) crisis are not limited to 30 days," he said, noting the strong possibility of a one- to two-month extension.

President Ferdinand R. Marcos, Jr. capped prices for imported rice — specifically the main import variety containing 5% broken grains — claiming that dealers are imposing unwarranted retail markups despite falling global prices and reduced tariffs.

The DA warned in a statement that it has the power to impose administrative sanctions over and above court action, including shuttering non-compliant establishments temporarily or permanently, seizing non-compliant products, and revoking business permits and licenses. Administrative fines ranging from P1,000 to P1 million may be levied separately from the criminal charges.

The threat of penalties represents a step up from earlier voluntary pricing recommendations that relied on retailer cooperation.

Under the Price Act, violations involving basic necessities are subject to imprisonment of one to 10 years, and fines of between P5,000 and P1 million, or both at the court's discretion. Corporate officers can also be held personally liable for company violations. — **Pierce Oel A. Montalvo**

GOCC subsidies rise 70.8% in March led by irrigation agency

SUBSIDIES extended to government-owned and -controlled corporations (GOCCs) grew 70.8% year on year in March, the Bureau of the Treasury (BTr) reported.

The BTr said budgetary support to state-run firms was P18.15 billion in March, against P10.63 billion a year earlier.

Month on month, GOCC subsidies rose 240.3% from February.

State-owned firms receive monthly subsidies from the National Government to support their daily operations if their revenue is insufficient.

In March, the National Irrigation Administration (NIA) received P4.06 billion, accounting for 22.37% of the total.

This was the second month the NIA was the top subsidy recipient, after the P2.45 billion granted in February.

The National Electrification Administration (NEA) received P3.02 billion, followed by the Power Sector Assets and Liabilities Management Corp. with P2.5 billion and the Bases Conversion and Development Authority with P2.08 billion.

The Philippine Fisheries Development Authority received P1.76 billion, while the National Food Authority (NFA) got P1.26 billion.

In March, three agencies received subsidies between P300 million and P1 billion: the Philippine Rice Research Institute (P761 million), the Philippine National Railways (P324 million), and the Philippine Crop Insurance Corp. (P309 million).

Four agencies received at least P200 million: the National Power Corp. (P297 million), the Sugar Regulatory Administration (P283 million), the Tourism Infrastructure and Enterprise Zone Authority (P248 million), and the Philippine Heart Center (P202 million).

GOCCs that received at least P100 million in subsidies included the Philippine Coconut Authority (P155 million), the Development Academy of the Philippines (P134 million), the Philippine Children's Medical Center (P128 million), and the National Kidney and Transplant Institute (P126 million).

Four agencies received subsidies of at least P50 million — the Subic Bay Metropolitan Authority (P89 million), the Lung Center of the Philippines (P77 million), the Light Rail Transit Authority (P68 million), and the Center for International Trade Expositions and Missions (P59 million).

Agencies that received at least P11 million in subsidies included the National Dairy Authority (P44 million), the Philippine Institute for Development Studies (P41 million), the Cultural Center of the Philippines (P34 million), the Metropolitan Waterworks and Sewerage System (P17 million), the Philippine Institute for Traditional and Alternative Health Care (P12 million), and the People's Television Network, Inc. (P11 million).

BUREAU OF THE TREASURY OFFICIAL FACEBOOK ACCOUNT

Meanwhile, the Aurora Pacific Economic Zone and Freeport Authority received P10 million, followed by the Philippine Center for Economic Development (P9 million), the Intercontinental Broadcasting Corp. (P8 million), the Southern Philippines Development Authority (P7 million), the Philippine Tourism Authority (P5 million), and the Zamboanga City Special Economic Zone Authority (P4 million).

Receiving no subsidies in March were the Small Business Corp. and Philippine Postal Corp.

In the first three months of the year, GOCC subsidies rose 18.83% year on year to P26.84 billion.

The NIA was the top recipient during the quarter with P6.93 billion in subsidies, followed by the NFA with P3.87 billion and NEA with P3.02 billion. — **Justine Irish D. Tabile**

OPINION

Turning technology risk into strategic advantage

IN BRIEF:

- Technology risk has evolved into an enterprise leadership challenge, as decisions on governance, execution, cybersecurity, third-party ecosystems, and AI increasingly determine whether digital investments deliver value or erode trust.
- Technology risks are interconnected and life cycle-based, with gaps in governance cascading into execution failures, cybersecurity exposure, third party dependency, and amplified AI accountability risks.
- The goal of technology risk management is confidence — not control, enabling responsible innovation, resilient operations, and sustained trust in an increasingly complex digital environment.

SUITS THE *C*-SUITE
ELVIN N. MERCADER

Leading organizations embed risk awareness into strategy, execution, and oversight — recognizing that confidence, not control, is the objective.

Organizations that treat technology risk as a strategic input — rather than a compliance exercise — gain speed, resilience, and trust. Drawing on insights from the recent SGV thought leadership forum, "Transforming Risk into Strategic Advantage," held on May 6, this perspective reflects how leading organizations are reframing risk as a driver of value.

These benefits materialize only when leadership explicitly positions risk as an enabler of value, embeds risk into strategy and delivery, and applies governance mature enough to provide clarity rather than friction. Under these conditions, organizations gain speed not by reducing rigor but by making risk timely, proportional, and relevant to business decisions.

THE PARADOX OF DIGITAL TRANSFORMATION

As digital capability becomes a competitive differentiator, organizations are accelerating the adoption of new platforms, delivery models, and intelligent technologies. However, a critical leadership question persists: Are technology decisions truly driving advantage — or quietly increasing enterprise risk?

While technology enables growth, it also introduces operational, regulatory, and ethical complexity. In many organizations, innovation has outpaced the maturity of governance, risk oversight, and organizational readiness.

This creates a central paradox: technology is adopted to increase speed and resilience, yet unmanaged risk slows momentum and erodes trust. Artificial intelligence (AI) intensifies this challenge by amplifying long-standing concerns around cybersecurity, data quality, ethics, and accountability. Technology risk is no longer technical — it is a strategic leadership issue.

Crucially, these risks do not occur independently. They form a connected system where weaknesses in one area cascade across the enterprise. When managed intentionally, this complexity becomes a source of advantage.

Alignment and decision quality

Technology governance is often mistaken for bureaucracy. In practice, it ensures digital ambition translates into business value.

Without strong governance, priorities compete, costs rise, and leadership confidence diminishes — particularly as organizations introduce multiple platforms, vendors, and emerging technologies.

Effective governance aligns digital investments with strategy, clarifies expected benefits, and embeds risk considerations early in decision-making.

When enterprise architecture is reduced to documentation, it adds little value. When used as a strategic decision lens, it helps leaders make informed portfolio trade-offs, identify platform rationalization opportunities, and understand the implications of scaling, integration, or acquisitions before costs and complexity become entrenched.

In complex transformation environments, decision quality improves when organizations use structured governance reviews to evaluate how technology decisions, investments, and risks are overseen. The goal is insight, not additional layers of control — ensuring clarity on accountability, priorities, and exposure tied to business outcomes. Where governance lacks coherence, execution risk quickly follows.

TECHNOLOGY IMPLEMENTATION: VALUE REALIZATION

Even the strongest strategies fail without disciplined execution. Across large-scale transformation programs, execution challenges most often emerge when requirements lack clarity, data readiness is underestimated, access controls are not designed upfront, and users are insufficiently prepared for change.

These gaps drive workarounds, low adoption, and delayed value realization. Leadership oversight becomes effective when assurance is applied at key inflection points — before go-live to surface design and control risks while change is still feasible, and after implementation to confirm that execution, controls, and benefits align with business intent. This shift requires assurance teams to engage earlier and operate with greater business fluency, which enables faster escalation, fewer go-live surprises, and clearer accountability for executive sponsors.

CYBERSECURITY: TRUST AND RESILIENCE

Cybersecurity sits at the intersection of trust, continuity, and executive accountability. Leaders must confidently answer whether critical assets are protected, vulnerabilities are understood, and incidents are manageable.

When treated as a constraint, security slows innovation. When embedded early into digital design — rather than bolted on late — it introduces predictable friction upfront, reducing disruptive rework, incidents, and loss of confidence downstream. Clear ownership, asset visibility, security by design principles, and zero-trust approaches allow scale while reinforcing trust.

Cyber-resilient organizations strengthen confidence through cybersecurity program assessments complemented by vulnerability testing and penetration validation, enabling executives to prioritize based on business impact rather than technical noise.

THIRD-PARTY RISK: ECOSYSTEM RESILIENCE

Modern transformation depends on ecosystems of vendors and partners. While these relationships enable speed and specialization, they also introduce dependency and exposure.

Third-party risk is no longer confined to procurement or compliance; it is an enterprise resilience issue, as critical operations, data, and decision-making increasingly depend on a concentrated ecosystem of cloud, SaaS, and AI providers. As dependencies deepen, executives must consider exit and substitution risk — how quickly operations, data, or AI capabilities could be transitioned if a key vendor fails or changes terms.

AI: READINESS AND ACCOUNTABILITY

AI has moved from experimentation to expectation. While it offers significant productivity gains, many initiatives fall short due to insufficient readiness rather than technical limitation.

The greatest AI risk is not algorithm failure — it is unclear accountability when outcomes go wrong. Risk varies significantly across AI use cases — from predictive decision support to fully autonomous action — requiring boards and executive leadership to adjust oversight and accountability as automation increases.

Before scaling AI, leaders must assess governance maturity, data reliability, workforce preparedness, and incident readiness. AI governance readiness assessments help clarify oversight, ownership, and escalation across the AI lifecycle, providing boards and executives with the confidence to scale responsibly.

A STRATEGIC FRAMEWORK FOR REFRAMING TECHNOLOGY RISK

Across these domains, a clear pattern emerges: technology risks are interconnected and life cycle-based. Governance, implementation, cybersecurity, third-party risk, and AI are enterprise drivers of both value and risk — not separate conversations.

Across complex digital environments, three imperatives consistently separate confident decision-making from reactive risk management:

- Integrate risk intelligence into digital strategy to make intentional tradeoffs without sacrificing trust.
- Manage risk across the full technology lifecycle, enabling early detection and decisive response.
- Shift from control to confidence, ensuring innovation scales responsibly.

These principles are operationalized through targeted assessments across governance, execution, security, third-party ecosystems, and AI, providing leadership with continuous visibility and confidence. The starting point is not more controls, but better visibility.

Organizations that progress most effectively begin by establishing a single, enterprise view of technology risk and focusing leadership attention on the areas where gaps in ownership, execution, or trust could materially impact outcomes.

CONFIDENCE, NOT CONTROL

Overseeing technology risk is no longer a technical responsibility — it is a core executive mandate. Leading organizations embed risk awareness into strategy, execution, and oversight, recognizing that confidence, not control, is the objective.

Leaders are increasingly challenged to reflect on whether they have a single, integrated view of technology risk across the entire lifecycle, ensuring that risks are not assessed in isolation but understood holistically. Equally important is identifying where decisions may be occurring without sufficient visibility into downstream risk or clear accountability, as these blind spots can amplify exposure and weaken governance. Leaders must also consider which initiatives would be most vulnerable if trust in security, data integrity, or third-party resilience were suddenly compromised, recognizing that the strength of these critical foundations can directly determine whether key programs continue forward or stall under pressure.

Technology risk leadership does not slow organizations down. It enables leaders to move faster with intent without sacrificing resilience, trust, or value. For today's executives, the question is no longer whether technology risk should be addressed, but how deliberately it is shaped into strategic advantage.

This article is for general information only and is not a substitute for professional advice where the facts and circumstances warrant. The views and opinions expressed above are those of the authors and do not necessarily represent the views of SGV & Co.

ELVIN N. MERCADER is a technology risk senior director of SGV & Co.