International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Labor Compliance and Innovation as Drivers of Service Quality in Philippine Private Security: A Mixed-Methods Study

Dr. Marderick Presto

Founder and CEO, Bathala Solutions Inc

Abstract

The Philippine private security industry is a large and growing sector that employs over half a million personnel and generates significant economic value. This mixed-methods study examines how labor compliance, contract practices, and technology adoption influence service quality among private security providers. A survey of 200 client-side security managers was coupled with qualitative interviews of industry stakeholders. Quantitative analysis using partial least squares structural equation modeling (PLS-SEM) assessed relationships between four latent constructs: Technology & Innovation (TI), Pricing & Contract Preferences (PCP), Service Quality Compliance (SQC), and Risk Management & Adaptability (RA). Results indicate that fair pricing and contract terms (PCP) ($\beta = 0.472$, $p < .01$) and technology adoption (TI) ($\beta = 0.327$, $p < .05$) significantly improve service quality compliance. In contrast, risk management adaptability (RA) showed no direct effect. TI also positively influences RA ($\beta = 0.418$, $p < .01$). Qualitative themes reinforce these findings: widespread wage underpayment and labor violations undermine service quality, and weak enforcement of regulations blunts the impact of operational improvements. Slow adoption of advanced security technology and high guard turnover (due to low pay) emerged as persistent challenges. We discuss these results in the context of industry trends and literature, highlighting the critical role of labor law compliance and innovation in enhancing security services. Managerial implications include enforcing contract labor standards, incentivizing technology use, and improving guard conditions to bolster retention. The study contributes to labor compliance and service quality theory and offers practical insights for security firms, clients, and policymakers.

Keywords: Private security Philippines, service quality, labor compliance, technology adoption, mixed-methods, PLS-SEM

Introduction

The private security industry in the Philippines is extensive and rapidly evolving. It is estimated to be worth tens of billions of pesos annually and employs well over 575,000 security personnel – a workforce larger than the national police. The sector has grown alongside urban development, increased corporate activity (e.g. the BPO boom), and rising demand for physical and digital security solutions. Thousands of licensed security agencies operate nationwide, offering services ranging from manned guarding (about 70% of the market) to cash-in-transit protection (~15%), cybersecurity (~10%), and event security (~5%). Despite its size, the industry faces persistent challenges affecting service quality and client satisfaction, including chronic labor compliance issues, regulatory enforcement gaps, technological lag, and high

workforce attrition. Regulatory oversight is fragmented: the Philippine National Police's Supervisory Office for Security and Investigation Agencies (PNP-SOSIA) handles licensing and some standards. At the same time, the Department of Labor and Employment (DOLE) oversees labor conditions. Enforcement is challenging given the 2,100+ registered agencies and the vast guard workforce. Both literature and industry reports note that compliance violations are common: agencies often undercut mandated contract fees (e.g. the required 20% administrative fee meant to cover wages) to win business, resulting in widespread underpayment of wages and excessive working hours. The typical security guard in the Philippines earns low wages (often near minimum), works 12-hour shifts, and sees little career progression, leading many to leave for better-paying informal jobs (e.g. delivery driving). These labor issues pose ethical and legal concerns and likely undermine the consistency and quality of security services delivered.

At the same time, the industry is at a technological crossroads. Advanced security technologies – such as AI-driven video analytics, drones, biometric access control, and integrated data systems – are gradually entering the market. However, adoption remains slow outside of a few large firms. High costs, limited expertise, and unclear regulatory guidance for new technologies impede widespread implementation. Basic technologies like CCTV cameras and two-way radios are ubiquitous (often mandated by local ordinances). However, more sophisticated tools (facial recognition systems, alarm integrations, cybersecurity monitoring) are relatively rare except among elite clients. Nevertheless, industry leaders recognize technology's potential to *multiply* guard effectiveness – for example, using "20 guards with high-tech support instead of 100 guards without". This study quantitatively investigates whether and how an agency's technology use translates into better risk management and service quality outcomes.

From a market perspective, intense competition has driven many security agencies to cut costs in ways that conflict with labor and quality standards. A 2022 industry report estimated the sector's annual value at roughly PHP 60 billion, with the private security guard force exceeding the strength of the armed forces. Many agencies are under-capitalized and resort to *"undercutting"* the mandated 20% administrative fee to offer lower contract prices, paying guards below required wages or hiring unlicensed personnel. Joint liability rules (per DOLE Department Order No. 150-16) make clients co-responsible for labor violations, and complaints often result in legal orders to pay back wages. Nonetheless, numerous small or fly-by-night agencies continue to skirt training and labor requirements, exploiting limited enforcement capacity. Past research on the Philippine security workforce documents grim conditions: low pay at or just above minimum wage, extremely long hours, and high turnover. The use of "reliever" guards (ad-hoc personnel without benefits to plug schedule gaps) has been criticized by labor advocates (Respicio, 2020). A 2020 congressional hearing on the industry noted that excessive attrition was a core problem undermining service consistency (Philippine Senate, 2020). Overall, there is a fundamental tension between the existence of rules meant to protect guard welfare and service standards and the market pressures and oversight constraints that undermine those rules.

In service industries like security, *service quality* refers to the degree to which providers meet expected performance, responsiveness, and professionalism standards as agreed with clients. Classic service quality dimensions include reliability, responsiveness, assurance, and empathy (Parasuraman, Zeithaml, & Berry, 1988). Reliability might entail guards consistently following protocols in security, while assurance could mean proper training and licensing. Few prior studies have quantitatively measured security service quality or compliance with agreed standards. In this study, we operationalize Service Quality Compliance (SQC) as a construct reflecting the security provider's adherence to contractual and regulatory service

standards. We posit that SQC is influenced by a combination of provider practices, client contract terms, and external factors (such as the enforcement environment).

Several streams of literature inform our inquiry. International research suggests private security can augment public policing when standards are high. However, Philippine-focused studies have primarily discussed issues of corruption in the industry and the plight of security guards rather than measuring service outcomes (Talabong, 2020; Cruz, 2021). Our study addresses this gap by linking provider-side practices – specifically technology usage, contract fairness, and risk management practices – to measurable client perceptions of service quality compliance.

Global trends indicate technological innovation is transforming security services (Banerjee & Inamdar, 2021; Trade.gov, 2023). Security technology adoption, guided by innovation diffusion theory (Rogers, 2003), is expected to enhance both a firm's risk management capabilities and the quality-of-service delivery. Although nearly all security contracts now include basic electronic security measures in the Philippines, more advanced solutions remain nascent (Lumify Work, 2023; SecurityMatters, 2024). Cost and regulatory uncertainty (e.g. lack of clear rules on drones or AI analytics) are major barriers. Still, pilot implementations show that investing in high-end systems can reduce manpower needs and improve responsiveness over time. We therefore include Technology & Innovation (TI) as a construct measuring the extent of an agency's adoption of modern tools and practices. We hypothesize that greater technology adoption leads to improved risk adaptation and higher service quality compliance, consistent with innovation diffusion arguments and prior findings (Banlaoi, 2022; Chakravarti, 2024; Ivanti, 2021).

Workforce and labor compliance issues form another critical lens. The term *"endo"* (end-of-contract employment) often appears in discussions of private security employment practices in the Philippines (Cruz, 2021). Turnover among security guards is chronically high – industry sources commonly report 20–30% annual attrition rates. Guards can sometimes earn less than informal gig workers; for instance, a delivery rider might earn more in a few hours than a guard does in a full 12-hour shift. These patterns mirror broader post-pandemic labor trends, where many workers shifted to gig economy roles for better pay (Banlaoi, 2022). High turnover disrupts continuity of service and erodes institutional knowledge within security firms (Tan, 2020; Cruz, 2021). Training new guards repeatedly is costly and often ineffective. Policymakers and industry analysts have called for raising guard wages and improving working conditions to address this issue (Ager, 2021; Philippine Senate, 2022). Although we do not directly measure turnover or employee satisfaction in our quantitative model, our qualitative component explores this workforce stability issues in depth. We anticipate that contract terms reflecting fair labor compliance and pricing, captured in our Pricing & Contract Preferences (PCP) construct, may indirectly affect outcomes like guard retention and thus service quality. Even if not modeled directly, the literature suggests workforce stability is a key antecedent to consistent service performance.

In summary, existing literature and industry evidence suggest that private security service quality in the Philippines is shaped by: (1) the degree of compliance with labor and contract regulations, (2) the adoption of modern security technologies, and (3) the ability of firms to manage risks and adapt to threats. However, no integrated study has empirically examined these factors and their influence on service quality outcomes in this context. This research addresses that gap by combining a survey-based structural model with qualitative insights from stakeholders. In the following sections, we develop a theoretical framework and hypotheses, describe our mixed-methods approach, present the results, and then discuss the implications for theory and practice.

Literature Review and Theoretical Framework

Labor Compliance and Contractual Practices: The regulatory framework for Philippine security agencies, established by Republic Act No. 5487 (1975) and updated by Republic Act No. 11917 (2022), mandates standards for guard wages, benefits, training, and licensing. RA 11917 requires that client contracts include at least a 20% agency fee to ensure funds for proper guard compensation (Official Gazette of the Philippines, 2022). In practice, however, many agencies violate these provisions. DOLE labor inspections often find underpayment of wages, lack of overtime pay, and other violations. Industry reports describe how some agencies *"blatantly"* ignore the 20% fee rule and submit low bids, effectively passing the cost cuts onto guards' wages. When guards complain, the DOLE's joint liability policy can penalize the client and the agency, leading to back-pay settlements. Nonetheless, weak routine enforcement means infractions are usually addressed only after they occur, if at all. Pricing & Contract Preferences (PCP) in this study refers to the client's preference for fair, compliance-oriented contract terms (e.g., not selecting providers solely on lowest cost, and ensuring contracts meet legal pay requirements). We hypothesize that higher PCP – indicating contracts that allow for proper wages and compliance – will be associated with better service quality compliance. This expectation aligns with management theories like the Service-Profit Chain, which posit that fair treatment of employees (in this case, enabled by fair contracts) ultimately improves service outcomes (Heskett, Sasser, & Schlesinger, 1994). Our qualitative interviews suggest clients prioritizing compliance over rock-bottom pricing tend to get more reliable service.

Technology Adoption: Globally, technology is seen as a *force multiplier* in security services, enhancing surveillance, communication, and incident response capabilities (Banerjee & Inamdar, 2021). Advanced security technologies can improve situational awareness and reduce human error (Chakravarti, 2024; Ivanti, 2021). In theory, greater Technology & Innovation (TI) should enable agencies to manage risks more effectively and consistently meet service standards. We expect TI to have a dual effect: directly boosting service quality compliance (e.g., through better monitoring and responsiveness), and indirectly improving it via enhanced risk management adaptability. Informed by Rogers' (2003) diffusion of innovation theory, we hypothesize that agencies with higher technology adoption will demonstrate better Risk Management & Adaptability (RA), which could contribute to higher service quality. However, as noted, technology uptake in the local industry is uneven. Our qualitative data underscore that only a minority of firms currently leverage advanced systems, often due to cost and unclear regulations (SecurityMatters, 2024). Thus, while we hypothesize a positive impact of TI on outcomes, we recognize the context may moderate its full potential.

Risk Management and Adaptability: The ability of a security provider to anticipate and respond to security threats – what we term Risk Management & Adaptability (RA) – is often considered a hallmark of high-performing agencies. This includes having protocols for various incidents, contingency plans, and the flexibility to adjust deployment based on situational risk. We theorize that RA should positively influence service quality compliance: agencies that are more adaptable and proactive in managing risks should be better at consistently delivering on service expectations. However, RA might also depend on other factors; for instance, technology can enhance adaptability (e.g. real-time incident alerts), and strong basic compliance (adequate staffing, training) may be a prerequisite for RA to translate into improved service. Even good internal risk management processes may not noticeably improve frontline service if baseline compliance is lacking. Our model will test the direct effect of RA on SQC, acknowledging that

this relationship might be weaker in contexts where labor and contract compliance issues dominate operational effectiveness.

Workforce Stability: Although not explicitly a construct in our quantitative model, workforce stability (turnover, experience, morale) emerges in the literature as a crucial element. Studies in organizational behavior consistently link employee satisfaction and retention to service quality (Tan, 2020; Monzon, 2022). In private security, high guard turnover can degrade service because new guards take time to learn site-specific protocols and build client rapport. The Philippine Senate has deliberated measures to improve guard tenure, such as advocating higher minimum wages for guards to professionalize the workforce (Ager, 2021). Our qualitative findings will shed light on how workforce issues intertwine with the constructs we measure. We anticipate that many of the unexplained variations in service quality compliance could be due to human resource factors that were outside our survey scope.

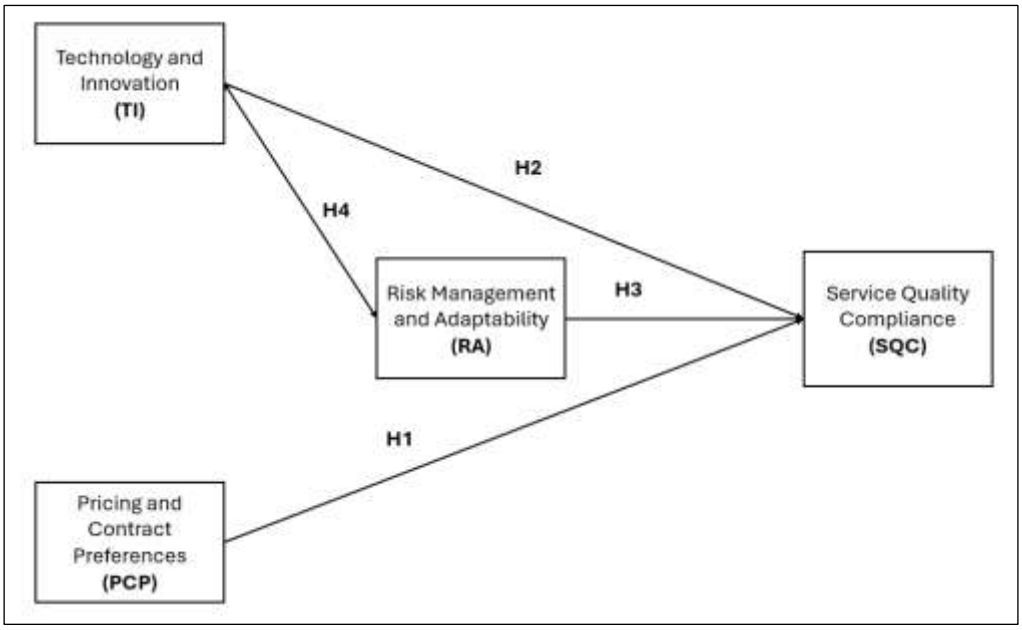

Figure 1. Conceptual framework illustrating hypothesized relationships among key constructs: Technology & Innovation (TI), Pricing & Contract Preferences (PCP), Risk Management & Adaptability (RA), and Service Quality Compliance (SQC). We hypothesize that: H1 – Fair pricing and contract terms (PCP) positively affect service quality compliance; H2 – Technology adoption (TI) positively affects service quality compliance; H3 – Risk management adaptability (RA) positively affects service quality compliance; and H4 – Technology adoption (TI) positively affects risk management adaptability. The model allows TI to influence SQC via RA indirectly.

Based on this framework (Figure 1), our **research questions** are: *Do fair contract terms and compliance with labor regulations (PCP) influence the quality of security service delivery (SQC)? Does investment in technology (TI) improve providers' risk adaptability (RA) and service performance (SQC)? How do regulatory enforcement gaps and workforce conditions shape these relationships?* To answer these questions, we employed a mixed-methods research design integrating a quantitative survey and qualitative interviews, as described next.

Methodology

Research Design

This study used a **convergent parallel mixed-methods** design (Creswell & Creswell, 2018) to gain a comprehensive understanding of the private security services market. Quantitative and qualitative data were collected in parallel, analyzed independently, and then triangulated. The **quantitative strand** consisted of a structured survey of security service clients to measure perceptions and outcomes, which we analyzed using PLS-SEM. The **qualitative strand** involved in-depth interviews and a focus group with industry stakeholders to capture contextual insights and unanticipated themes. By comparing and integrating results from these two strands, we aimed to validate findings and deepen interpretations through methodological triangulation. This approach enhances the credibility of conclusions and helps ensure that statistical patterns are meaningful in real-world terms (Hair, Ringle, Sarstedt, & Gudergan, 2022).

Quantitative Methods

Survey Instrument: We developed a structured questionnaire based on four theoretical constructs derived from the literature review: Technology & Innovation (TI), Pricing & Contract Preferences (PCP), Service Quality Compliance (SQC), and Risk Management & Adaptability (RA). Each construct was measured with multiple survey items on a 4-point Likert scale (1 = strongly disagree, 4 = strongly agree) to avoid neutral midpoint responses and encourage definitive feedback. Items were adapted from industry performance metrics, service quality frameworks, and expert input. For example, TI was assessed with statements about the provider's use of modern security equipment and systems; PCP with statements about contract fairness (e.g. adequacy of guard pays and benefits in the contract); SQC with items on whether the security service meets agreed standards and follows regulations; and RA with items on the provider's ability to adjust to changing risk scenarios. A few sample items included: *"Our security provider uses up-to-date technology to enhance security operations"* (TI), *"The terms of our security contract ensure guards receive mandated wages and benefits"* (PCP), *"Security services provided are consistently in line with what was promised"* (SQC), and *"The security agency can quickly adapt its operations in response to new threats"* (RA).

Sampling and Data Collection: A purposive sampling strategy targeted primarily at the client side of security service relationships. We surveyed 200 security managers, directors, or executives responsible for overseeing contracted security services in their organizations. These respondents were from various sectors, including banking, retail, manufacturing, business process outsourcing (BPO), and government, reflecting a broad user base of security services. The sample was geographically diverse, covering Metro Manila and major provincial hubs. Surveys were administered via online forms and in-person interviews over four weeks. Participation was voluntary, and responses were kept confidential. We focused on client representatives because they are well-positioned to evaluate service quality and compliance of their security providers. (A smaller survey of security agency managers was also conducted in the original market study, but we concentrate on the client perspective as the primary source of service quality evaluation for this analysis.) A final sample of N = 200 client organizations was achieved, which is adequate for PLS-SEM analysis given our model complexity (Hair et al., 2022).

Data Analysis: Quantitative analysis was performed using Partial Least Squares Structural Equation Modeling (PLS-SEM), employing SmartPLS software. PLS-SEM was chosen for its suitability with modest sample sizes and ability to handle non-normal data and complex models (Hair et al., 2022). We

first evaluated the measurement model for reliability and validity. Internal consistency reliability was confirmed with Cronbach's alpha and composite reliability (CR) – all constructs exceeded the 0.70 threshold for alpha and 0.80 for CR, indicating good reliability. Convergent validity was supported as each construct's average variance extracted (AVE) was above 0.50. Discriminant validity was checked using the Fornell-Larcker criterion; for all construct pairs, the square root of AVE for each construct was greater than its correlation with any other construct, satisfying the criterion. No indicator had a low factor loading (<0.7) that necessitated removal. We then assessed the structural model by examining path coefficients (hypothesis tests), *p*-values via bootstrapping (5,000 resamples), and R^2 values for endogenous constructs (SQC and RA). The model's goodness-of-fit and predictive power were interpreted following recommended PLS-SEM guidelines (Hair et al., 2022).

Qualitative Methods

Participants: We conducted semi-structured interviews with key stakeholders and a focus group discussion to gain rich insights into industry practices and challenges. Two in-depth one-on-one interviews were conducted: one with a senior official of the Philippine National Police – Civil Security Group's Supervisory Office for Security and Investigation Agencies (PNP-SOSIA), and one with a major private security firm executive. These individuals have extensive knowledge of regulatory and operational issues in the sector. In addition, we convened a focus group discussion (FGD) with six senior directors from the Philippine Association of Detective and Protective Agency Operators (PADPAO), the leading industry association. The FGD participants included agency owners and managers familiar with market dynamics, labor challenges, and technology trends. We captured various perspectives on enforcement, business practices, and workforce conditions by including regulators and industry leaders.

Procedure: The interviews and FGD followed an open-ended discussion guide covering topics such as compliance challenges (e.g. wage and hour violations, licensing issues), the impact of pricing and contracts on service quality, the role and uptake of new security technologies, risk management approaches, and workforce management (hiring, training, turnover). Each interview lasted about one hour, and the FGD about two hours. All sessions were conducted in English and Filipino, recorded with consent, and transcribed in English. We assured participants of anonymity to encourage candid sharing, given the sensitivity of some topics (e.g., discussing non-compliance or industry politics).

Analysis: We analyzed the qualitative data using thematic analysis (Creswell & Creswell, 2018). Transcripts were coded inductively by multiple researchers to identify recurrent themes and patterns. An initial coding yielded numerous codes, which we iteratively refined and grouped into broader themes. We paid particular attention to themes related to our quantitative constructs (to inform or explain the survey findings directly) and unexpected themes that emerged independently. Through discussion among the researchers, four major themes were finalized: **(1)** Wage and labor compliance issues; **(2)** Regulatory enforcement challenges; **(3)** Technology adoption trends; and **(4)** Workforce retention and turnover. For each theme, we identified illustrative quotes from participants to highlight key points. Triangulation was performed by comparing these qualitative themes with the quantitative results – for example, checking if interview narratives on wage compliance aligned with the survey's finding on contract fairness, or if comments about technology barriers explained the magnitude of the technology→performance relationship. We also cross-checked interpretations with secondary data (industry reports, policy documents) to ensure accuracy. Finally, a member-checking step was done: a summary of preliminary

findings was shared with two external experts (a security industry consultant and a labor regulation specialist) to validate our conclusions and ensure they resonated with professional observations.

Ethical Considerations: The study followed standard research ethics protocols. Informed consent was obtained from all survey respondents and interview/FGD participants. Participants were informed about the study's purpose and their right to withdraw at any time. To protect confidentiality, no real names or company identifiers are used to report the qualitative findings; quotes are generally attributed (e.g. "Focus Group participant") without revealing specific identities. The study did not collect sensitive personal data, focusing on professional opinions and organizational practices. Ethical approval was obtained through an institutional review process prior to data collection.

Results

Quantitative Findings (PLS-SEM Analysis)

Model Fit and Variance Explained: The PLS-SEM model demonstrated acceptable explanatory power for the key outcome. The endogenous construct Service Quality Compliance (SQC) had an R^2 of 0.535, meaning the model explains about 53.5% of the variance in SQC. In PLS-SEM, this is a moderate to substantial level of explained variance (Hair et al., 2022). The other endogenous construct, Risk Management & Adaptability (RA), had $R^2 = 0.175$, indicating about 17.5% of variance explained. This lower R^2 for RA is reasonable since only one predictor (TI) was included for RA in our model. Overall, the model's R^2 values suggest that while important factors are captured, there remains unexplained variance, especially for SQC (about 46.5% not explained by PCP and TI) – we revisit this point in the Discussion.

Figure 2 presents the validated structural model, showing the endogenous constructs' standardized path coefficients and explained variances (R^2).

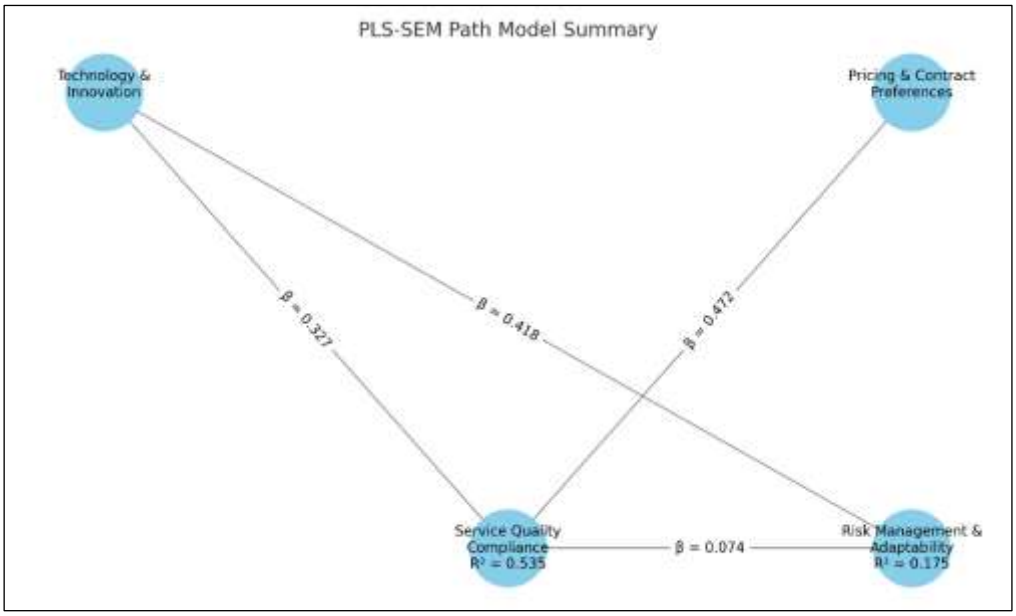

Figure 2: Conceptual Path Model for Service Quality Compliance in Philippine Private Security Services. This figure illustrates the hypothesized structural relationships among the four latent constructs: Technology and Innovation (TI), Pricing and Contract Preferences (PCP), Risk Management and Adaptability (RA), and Service Quality Compliance (SQC). Standardized path coefficients (β) are

indicated along the arrows, while R^2 values represent the proportion of variance explained in the endogenous constructs (SQC and RA).

Hypothesis Testing – Path Coefficients: Figure 1's hypothesized paths were tested, and the results are summarized in Table 1. All reported coefficients are standardized beta coefficients.

- **PCP → SQC:** We found a positive and significant effect of Pricing & Contract Preferences on Service Quality Compliance ($\beta = 0.472$, $p < .01$). This provides strong support for H1, indicating that clients who engage providers with fairer contracts and compliance-oriented terms tend to experience markedly better service quality compliance. In terms of effect size, this was the largest effect in the model (see Table 1).
- **TI → SQC:** Technology & Innovation had a positive, moderate effect on Service Quality Compliance ($\beta = 0.327$, $p < .05$), supporting H2. Agencies that extensively use modern technology were rated higher in service quality compliance by their clients. The effect size here was smaller than that of PCP but still meaningful.
- **RA → SQC:** The direct effect of Risk Management & Adaptability on Service Quality Compliance was positive but not statistically significant ($\beta = 0.074$, *n.s.*). Thus, H3 was *not* supported – in our data, having stronger internal risk management/adaptability did not translate into significantly higher service quality compliance once PCP and TI were accounted for.
- **TI → RA:** We found a significant positive effect of Technology & Innovation on Risk Management & Adaptability ($\beta = 0.418$, $p < .01$), supporting H4. Agencies with greater technology adoption also exhibited greater adaptability in managing risks, as perceived by clients or evidenced by practices. This suggests technology is an enabler of an agency's adaptive capability.

The two strongest predictors of service quality compliance were PCP and TI, while RA's direct role was negligible in this sample. The positive TI→RA link indicates an indirect pathway where technology contributes to service quality *via* improved adaptability, but since RA→SQC was null, the mediation was not realized under current conditions.

Table 1. Structural Path Coefficients (PLS-SEM Results)

Path	β	p-value	Effect Size (f^2)	Interpretation
PCP → SQC	0.472	< .01	0.335 (large)	Fair contracts strongly improve service compliance.
TI → SQC	0.327	< .05	0.070 (small)	Technology adoption directly enhances compliance.
TI → RA	0.418	< .01	0.247 (medium)	Technology adoption significantly boosts adaptability.
RA → SQC	0.074	n.s.	0.003 (negligible)	Risk management has no direct effect on compliance.

Notes: n.s. = not significant. Effect size f^2 indicates the incremental variance explained by each predictor for the target endogenous construct (values around 0.02 are small, ~0.15 medium, >0.35 large effect; Hair et al., 2022).

These quantitative results confirm that more favorable contract terms and pricing practices (avoiding cost-cutting at the expense of guard welfare) and higher technology use by security agencies are associated

with better compliance with service quality standards, as hypothesized. By contrast, an agency's internal risk management capability, on its own, did not significantly raise service quality outcomes in our data. Notably, technology use also contributed to risk management adaptability (TI → RA), suggesting that innovation improves how agencies handle risk, even if that alone doesn't guarantee better service quality without supporting conditions.

Measurement Model Statistics: Besides the structural results, we verified that our measurement model was sound. All survey indicators loaded strongly on their intended constructs (most factor loadings ranged from 0.78 to 0.92). Composite reliability (CR) for each construct was above 0.85, indicating high internal consistency. Each construct's average variance extracted (AVE) exceeded 0.5, supporting convergent validity. The Fornell-Larcker criterion was satisfied for all construct pairs, indicating discriminant validity (each construct shared more variance with its indicators than other constructs). Thus, common method bias or multicollinearity is not a concern, and the observed relationships can be interpreted confidently.

Qualitative Findings

Thematic analysis of the interviews and focus group yielded **four major themes** that contextualize and enrich the quantitative findings:

Theme 1: Wage and Labor Compliance Issues. *"If you cut the 20% agency fee, you end up paying guards less,"* one focus group participant remarked, encapsulating the pervasiveness of labor underpayment. Nearly all informants acknowledged that wage violations and unfair labor practices are widespread in the industry. Security agency representatives admitted that to offer the lowest bids to clients, many firms reduce guard wages, skip overtime pay, or delay benefits. One regional agency manager said, *"Ang negosyo, kinukuha sa patayan ng presyuhan – sino ang talo? Siyempre guard"* ("This business is won by killing prices – and who loses? Of course, the guard"). Regulatory officials noted that DOLE does conduct inspections and has regulations (e.g. Department Order 150-16) to penalize such violations, and labor courts often rule in favor of guards in disputes. *"Guards do file complaints, and we often win back pay for them,"* an official shared, *"but enforcement is mostly reactive rather than preventive."* In other words, many agencies only comply when caught. The consensus was that labor compliance is discussed as a priority but achieved inconsistently. As one participant put it, *"Compliance is often on paper. In reality, many agencies find ways around the rules."* This chronic undercutting of guards' welfare fundamentally undermined service quality: demotivated, underpaid guards are less vigilant and more likely to leave.

Theme 2: Regulatory Enforcement Challenges. Interviewees described the regulatory landscape as *"complex and fragmented."* Oversight is split among multiple authorities: the PNP-SOSIA sets some standards (like enforcing the 20% minimum fee and licensing agencies/guards), DOLE enforces labor laws, and local government units (LGUs) may impose additional requirements (e.g. CCTV ordinances). *"There is effectively no single body in charge,"* noted a security firm executive. This fragmentation leads to overlapping jurisdictions and gaps. For example, an agency might violate equipment or training requirements with little consequence because of PNP-SOSIA's limited monitoring capacity, and DOLE might not focus on those aspects. Participants gave examples such as lack of monitoring for whether guards have required training beyond the basic certification, or inconsistent checks on agencies' compliance with new technology-related rules (since no clear mandate exists). One regulatory official commented, *"Marami ang batas, pero kulang sa sundo"* ("We have many laws, but lack enforcement"). The qualitative data emphasize that laws and regulations exist on paper, but enforcement is weak, allowing non-compliance to persist. This theme provides a possible explanation for the quantitative finding that RA

did not impact SQC: even if a company has good internal risk protocols, *"if basic compliance is absent, those protocols may not matter,"* as one participant noted. In short, *"regulators react to infractions after the fact rather than ensuring routine compliance,"* which blunts the effectiveness of otherwise sound risk management practices.

Theme 3: Technology Adoption – Promise and Inertia. All participants agreed that technology use in private security is increasing, but from a low base. *"Ten years ago, CCTV was a luxury; now it's standard,"* noted a PADPAO focus group member. Most clients now expect basic electronic security (alarms, CCTV cameras, two-way radios). However, advanced tools – AI-driven analytics, drones, biometric access systems – remain rare. One security manager admitted that many companies still rely on *"100 warm bodies instead of 100 cameras"* when securing a facility. High costs and steep training requirements were primary barriers to high-tech solutions. Moreover, participants pointed out the lack of clear guidelines on emerging technologies: *"There is no unified rule on drones or AI yet, so many firms are hesitant,"* explained a security firm executive. Nonetheless, a few large firms are piloting innovations – for example, using a smaller number of highly equipped guards supported by advanced surveillance systems. These early adopters believe the return on investment (ROI) for high-end security tech can be achieved within about five years, especially as equipment prices fall. This suggests a potential turning point if technology becomes more affordable. Overall, the qualitative data reveal a tension: there is enthusiasm for modernizing security through tech, but practical and regulatory hurdles have made adoption uneven. The benefits of technology (better detection, faster response) confirmed in the survey data are recognized qualitatively, yet an *"implementation gap"* persists between what is possible and what is currently practiced.

Theme 4: Workforce Retention and Turnover. A final theme was the industry's workforce instability. Security firms face chronic turnover of guards, estimated by focus group participants at 20–30% per year. *"Every year we lose a quarter of our people,"* one agency owner lamented. Many guards leave for jobs in transport or other sectors that offer higher pay or better hours. Younger guards, in particular, do not view security work as a sustainable career. One interviewee observed, *"Ang mga bata ngayon, ayaw na nila maging guard pangmatagalan"* ("Young people today don't want to be security guards for long"). They noted younger guards demand perks like internet access at work or clear advancement pathways, which most agencies struggle to provide. The consequence of high turnover is that many agencies operate with a **rotating staff of novices**. Posts may go unfilled for periods, or new guards who lack site-specific knowledge are constantly breaking in. Several participants admitted this undermines service quality: *"How can a guard be effective if he's only been on the job for two weeks and might be gone next month?"* Training new hires repeatedly is costly and sometimes rushed, leading to skill gaps. The consensus was that improving pay, benefits, and working conditions is essential to retain experienced guards. *"If you want guards to treat it as a profession, you have to pay a professional wage,"* said a veteran agency director. By investing in human capital – treating guards as valued employees rather than interchangeable labor – agencies hope to improve long-term service reliability. This theme underscores the human element as crucial as contracts or technology. It also suggests that some determinants of service quality lie beyond our immediate quantitative model (which did not include a direct measure of workforce stability). However, these factors emerged as vital in explaining why service outcomes vary.

Integration of Quantitative and Qualitative Findings

Combining the survey results with the interview insights reveals several clear patterns and deeper explana-

tions:

- **Fair Contracts Enable Quality:** The survey showed a strong positive effect of fair pricing/contract terms (PCP) on service quality compliance (β = 0.472). The interviews reinforce *why* this is so. Agencies that honor wage laws and provide adequate resources tend to have more motivated guards and fewer disruptions, leading to better service. Conversely, when agencies cut costs at the expense of guards (low pay, lack of benefits), performance suffers through absenteeism, low morale, and high turnover. In short, labor compliance is not just an ethical obligation but operationally essential. Our findings echo the service-profit chain principle that links employee welfare and service quality (Heskett et al., 1994). Clients and providers who ensure guards are fairly treated see that translate into more consistent and higher-quality security service. The qualitative narratives about widespread underpayment and its impact provide real-world context for the significant PCP→SQC relationship observed in the data.
- **Technology's Dual Role – Potential vs. Practice:** Quantitatively, Technology & Innovation directly impacted service quality (TI→SQC) and enhanced risk management adaptability (TI→RA). This suggests technology is a *"force multiplier"* for private security performance. The qualitative data concur that wherever implemented (e.g. advanced CCTV analytics, GPS tracking of guards), technology has improved incident response and oversight. However, the interviews also highlight an implementation gap: many agencies have not yet adopted these tools due to cost and uncertainty, meaning the benefits are not widespread. As one participant noted, those who have invested in modern technology (often larger firms) are "already reaping measurable advantages," improved surveillance capability, faster communication, and better data on guard activities. Over time, as tech becomes cheaper and success stories spread, a critical mass of adoption could shift industry norms. In summary, the qualitative evidence of slow uptake tempers the optimistic quantitative finding: technology *can* significantly improve quality and adaptability, but industry inertia must be overcome for its full impact to be realized broadly.
- **Risk Management Strength is Blunted by Non-Compliance:** Our model found no significant direct effect of risk management adaptability (RA) on service quality compliance. At first glance, this is surprising – one would expect that a company that is better at handling risks and emergencies would deliver better service. The qualitative discussions clarify the paradox. In an environment where basic labor and contractual obligations are frequently unmet, even strong internal protocols and risk management plans may not translate into better day-to-day service. If guards are poorly paid, undertrained, or posts are understaffed, then having a sophisticated risk assessment procedure on paper does little good. Strong governance and pervasive non-compliance in fundamentals *"handcuff"* the potential advantages of robust risk management. Interviewees suggested that RA might show its value more during major incidents or crises (when those plans kick in). However, for routine quality of service, it cannot compensate for a lack of baseline compliance. Thus, our results indicate a boundary condition: **risk management capabilities yield tangible service benefits only when foundational labor and quality standards are in place**. This nuance contributes to understanding why RA→SQC was null in the quantitative analysis.
- **Regulatory Environment as Context:** The strong effect of PCP and the muted effect of RA can both be understood in light of the regulatory enforcement issues raised by participants. The fact that contract compliance (PCP) matters so much implies that in a lax enforcement environment, it is largely up to the client-agency relationship to self-enforce quality standards (e.g. by agreeing on fair terms).

Meanwhile, risk management processes (RA) may be less effective because external enforcement of standards is weak – agencies that might otherwise excel in RA are held back by industry-wide issues like lack of monitoring and accountability. In other words, our findings align with the notion that **"laws on the books are not enough if they are not enforced"** (Acuña & Parojenog, 2024; UNODC, 2014). Strengthening enforcement and oversight (e.g. consistent audits by PNP-SOSIA and DOLE) could create an environment where investments in risk management and training yield more visible improvements in service quality. Policy-wise, this suggests that our non-finding on RA is not a dismissal of the importance of risk management, but rather a call to fix enforcement and compliance gaps so that all performance drivers can function.

- **Workforce Factors and Unexplained Variance:** With SQC's R^2 around 0.535, nearly half of the variance in service quality outcomes is not explained by PCP and TI in our model. The qualitative data points to workforce stability and quality as major missing pieces. High turnover, low guard morale, and varying skill levels likely account for a portion of the unexplained differences in service performance between providers. Firms that invest in their guards (pay, train, supervise) likely achieve better service consistency – a dynamic supported by general management theory and echoed in interviews (Tan, 2020; Cruz, 2021). The absence of a direct workforce satisfaction or retention metric in our survey is a limitation, but the interviews fill that gap by emphasizing its importance. This suggests that future models of private security service quality should include human resource constructs (e.g. employee engagement, tenure, training level) to more fully capture drivers of service outcomes. In essence, our mixed-methods approach indicates that people factors underlie a significant part of security service quality, mediating how contract terms and technologies play out on the ground.

Discussion

Core Industry Challenges and Theoretical Implications

This study illuminates several core challenges in the Philippine private security industry, with implications for both theory and practice. Foremost is the challenge of labor compliance. Our findings empirically demonstrate that when security agencies and their clients avoid the prevalent cost-cutting practices (such as underpayment of wages and denial of benefits), they achieve markedly better service quality outcomes. The strong path from PCP to SQC ($\beta = 0.472$) underscores that basic compliance with labor and contract standards is a *sine qua non* for reliable security service. This resonates with broader organizational behavior and service management theories that link employee treatment to service performance (Heskett et al., 1994; Tan, 2020). The private security industry confirms the service-profit chain in a critical context: if guards are not compensated and treated fairly, the "product" – security service – suffers. Unfortunately, as our qualitative evidence showed, many agencies still resort to undercutting the mandated 20% fee and other labor shortcuts to win contracts. This breaches legal regulations (Philippine DOLE rules) and undermines the service quality clients seek to secure by contracting a security provider. The implication for theory reinforces the vital link between compliant, ethical management practices and service performance outcomes. It extends labor compliance theory by showing its direct impact on client-perceived service quality in a high-stakes service industry.

A related structural challenge is weak regulatory enforcement. We observed that the regulatory framework (e.g. RA 11917 and DOLE orders) is comprehensive in principle but weak in implementation. Oversight is fragmented among PNP, DOLE, and local authorities, leading to gaps where agencies can evade requirements. The literature on private security and regulation (Acuña & Parojenog, 2024; UNODC, 2014)

suggests that even well-crafted laws have limited effect without strong institutional capacity. Our findings support this: the lack of a significant RA→SQC effect can be partly explained by the broader context that if baseline compliance is low and oversight is lax, even agencies with good internal risk management cannot fully deliver better outcomes. Theoretically, this underscores the importance of contextual enablers (like regulatory enforcement) in realizing the benefits predicted by management capabilities theory. For instance, dynamic capabilities theory (Teece, 2007) posits that firms with superior adaptive capabilities (like RA) gain performance advantages. Our result refines this by indicating that such advantages may not materialize in contexts where external governance (enforcement of basic norms) is weak – a boundary condition that theory must account for.

The technology adoption theme presents both promise and inertia. In line with innovation diffusion theory (Rogers, 2003), our quantitative results confirm that agencies embracing new technologies can enhance both their adaptability (RA) and service quality (SQC). This finding contributes to the theoretical understanding of how technological capability translates into service performance in the security domain. It validates arguments that technology is a key resource for service improvement. However, our qualitative data add nuance by highlighting the uneven adoption and the role of external factors (costs, regulations) in moderating this relationship. In theoretical terms, it suggests that the benefits of technological innovation on organizational performance, as posited by innovation adoption theories, may be contingent on environmental and economic factors. The innovation may be valuable, but its diffusion is subject to classic resource constraints and uncertainty barriers. For managers and scholars, this underscores that technology's impact is not automatic; it requires supportive infrastructure and investment. Over time, as technology becomes more accessible, we might expect a shift in the industry's technology trajectory and potentially even stronger effects on service outcomes, a hypothesis future studies could explore (perhaps via longitudinal designs).

The persistent workforce issues – high turnover and low professionalization – emerge as a structural drag on service quality. In terms of theoretical contribution, this finding reinforces human capital theory and the idea that employee retention and engagement are critical for service excellence. Our study's mixed-methods evidence suggests that existing service quality models in security (and similar industries) should explicitly incorporate human resource variables. This extends prior work that often examines technology or process factors alone; we show that without stable, trained personnel, those factors have diminished returns. Additionally, this finding aligns with Herzberg's two-factor theory in that pay and job stability might be "hygiene" factors that, if inadequate, cause dissatisfaction and performance problems. As recommended by both our participants and policymakers (Ager, 2021), improving guard conditions can thus be seen as addressing fundamental motivational factors that theory predicts will reduce negative outcomes (like turnover) and facilitate better performance.

Implications for Policy and Practice

Building on these findings, several practical implications can be outlined for different stakeholders in the security industry:

- **For Clients (Security Service Buyers):** Organizations that hire private security should incorporate labor compliance checks into their procurement and contracting process. Simply choosing the lowest bid can be counterproductive if that bid reflects sub-minimum wages or a lack of benefits for guards. Clients can set requirements for bidders to show proof of compliance with labor laws (e.g. SSS, PhilHealth remittances, proper wage payments). They should also enforce joint liability clauses,

meaning agencies and clients are both accountable for labor violations – a provision already in law that needs active reinforcement. By doing so, clients create a market incentive for agencies to comply. Our study suggests that compliance-oriented procurement is directly tied to better service quality. In essence, clients "get what they pay for": insisting on fair pay for guards likely yields more effective security coverage.

- **For Regulators and Policymakers:** There is a need to strengthen enforcement mechanisms and inter-agency coordination. The Philippine National Police (PNP-SOSIA), DOLE, and local government units must work more closely to monitor security agencies consistently. Adequate resources should be allocated to conduct regular audits of agencies (for both operational standards and labor compliance) rather than relying primarily on complaint-driven enforcement. Policymakers might consider establishing a more unified regulatory body or task force for private security to reduce fragmentation. Furthermore, guidelines on emerging technologies should be developed – for example, rules on using drones for surveillance or standards for cybersecurity in private security operations. Such guidelines would give agencies confidence to invest in innovation without fear of regulatory ambiguity. On the labor side, policymakers (as evidenced by Senate discussions) might explore setting a higher minimum wage for security guards or mandating better guard-to-supervisor ratios to professionalize the workforce. Our findings prove that these labor-focused improvements are not just worker-friendly, but also client-beneficial regarding service outcomes.
- **For Security Agencies (Providers):** Private security firms should recognize the *business case* for labor compliance and technology adoption. Cutting corners on guard pay may provide short-term cost savings, leading to poorer performance, client dissatisfaction, and reputational damage in the long run. Investments in human capital – fair wages, benefits, continuous training, and career development for guards – can improve retention and build a more experienced, reliable guard force, which becomes a competitive advantage. Likewise, agencies should invest in modern technology appropriate to their scale: even relatively affordable measures like better incident reporting systems, guard tour tracking apps, or remote CCTV monitoring services can enhance their service quality and appeal to clients. Industry associations like PADPAO can facilitate this by organizing training sessions on new technologies, bulk negotiating for equipment discounts, or creating shared technology platforms that smaller agencies can use. By embracing innovation, agencies can differentiate themselves in an increasingly competitive market and demonstrate quantifiable improvements (as evidenced by our data linking tech use to compliance and adaptability).

From a broader perspective, these implications underscore that private security is fundamentally a **service industry** – success depends on both "hard" inputs (technology, equipment, formal procedures) and "soft" inputs (human resources, contracts, management practices). Our results show that something as ostensibly mundane as ensuring correct wages is as important as adopting cutting-edge surveillance gear when it comes to delivering quality security outcomes. Stakeholders should therefore view regulatory compliance and employee welfare not as check-box bureaucratic hurdles, but as integral components of effective security management. In practice, a holistic approach is needed: for example, a security firm might pair a new digital incident logging system (technology) with a revised HR policy to reward guards for incident reports (people aspect) and a client communication plan (process) – aligning all aspects to improve quality.

Limitations and Future Research

While this study offers comprehensive insights, it is not without limitations. First, the survey sample of

200 client-side respondents, obtained through purposive sampling, may limit generalizability. The sample was skewed toward organizations already engaged with formal security providers; perspectives of those who do not hire formal agencies (or use in-house security) were not captured. Future research could broaden the sample to include more security agencies and frontline guards to get a 360-degree view of performance determinants. Incorporating guard surveys could directly measure job satisfaction or commitment levels, which we inferred indirectly here.

Second, the qualitative component, though rich in detail, involved a relatively small number of informants (two key interviews and one focus group). These participants were industry experts and leaders, which is valuable. However, their views may not represent all segments of the industry (for instance, small provincial agencies or guards themselves might have differing perspectives). Additional qualitative research with a more diverse range of participants could uncover other themes or verify the universality of our themes.

Third, the study's cross-sectional design provides a snapshot in time. The private security industry is evolving (e.g., new laws like RA 11917 were just implemented in 2022). A longitudinal study could observe how factors like technology adoption or compliance efforts translate into service quality over time, or how the industry responds to reforms (e.g., if enforcement improves, does RA start to have an effect?). Tracking the same agencies or client contracts over multiple years could yield insights into causal directions and dynamic effects (such as whether improvements in labor conditions lead to gradual but compounding improvements in service).

Fourth, our quantitative model did not include specific potentially important constructs, most notably direct measures of workforce characteristics (e.g., guard experience, training, satisfaction) and client satisfaction outcomes. Future models could integrate employee-level data and client outcome measures (like perceived safety or incident rates) to provide a more granular understanding of the service quality equation. Including such variables might increase the explained variance and further illuminate the mechanisms by which compliance and innovation impact outcomes.

Finally, there is always a possibility of response bias and unobservable factors. The survey relied on client perceptions, which, while crucial, might be influenced by expectations or individual biases. The qualitative interviews might have been subject to some degree of self-censorship (e.g., agency representatives might downplay certain malpractices when speaking on record). We attempted to mitigate these issues through anonymity assurances and triangulation with secondary data. Nevertheless, sensitive issues, such as specific corruption or illegal practices, may remain underreported.

These limitations suggest caution in over-generalizing our findings. However, they do not undermine the core patterns observed. Instead, they point to fruitful avenues for future research to build upon this work. Future studies might test the proposed relationships in other national contexts to see if similar patterns hold in different regulatory environments. Comparative studies between countries with stronger versus weaker enforcement could be especially enlightening. Additionally, research examining interventions (e.g., a pilot program that improves guard wages in a subset of contracts) could provide causal evidence of the impact on service quality.

Conclusion

This mixed-methods study of the Philippine private security services industry elucidated critical drivers of service quality compliance. Quantitatively, our analysis found that fair pricing structures and contract terms – which reflect genuine compliance with labor laws – are the strongest determinants of whether

security providers meet agreed standards of service. In practical terms, when a security contract allows a provider to pay guards properly and operate above-board, the resulting service is far more likely to satisfy client expectations. Technology adoption also proved beneficial: agencies that invest in modern security innovations (from surveillance tech to data systems) achieve better adaptability to risks and, in turn, better compliance with service standards. Conversely, risk management capability on its own did not show a direct impact on day-to-day service quality. We interpret this as an indication that foundational issues must be addressed first – if basic compliance and adequate staffing are not in place, having advanced risk protocols offers limited visible benefit.

Qualitative insights enriched these findings by highlighting systemic issues: widespread wage and labor violations and fragmented enforcement undermine industry performance and guard morale. High guard turnover compounds the challenge by making service outcomes inconsistent when human resources are in flux. Guards who are constantly worried about unpaid wages or looking for better jobs cannot be expected to deliver a top-notch security presence.

For industry stakeholders, the message is clear. Ensuring that security personnel are fairly compensated and legally protected is not merely a regulatory checkbox, but a practical necessity for high-quality service delivery. Investing in guards – through proper pay, training, and career development – yields dividends in the form of more reliable and professional service. Additionally, embracing appropriate technology can strengthen providers' capabilities, but technology should complement, not substitute for, a solid foundation of compliance and skilled personnel. To facilitate these improvements, procurement policies and regulatory frameworks should be aligned: clients and regulators should jointly emphasize compliance (for example, requiring bidders to show proof of labor law compliance and guard licensing) and encourage innovation (for example, through tax incentives for security technology upgrades or pilot programs sharing best practices). Ultimately, enhancing the effectiveness of private security in the Philippines will require a coordinated effort across all stakeholders – clients who demand quality *and* fairness, agencies who commit to ethical and modern practices, and regulators who enforce standards and support industry modernization.

Reframing what began as a market assessment into an academic inquiry, this research contributes to the literature on private security services in emerging markets. We provide empirical evidence linking organizational practices (contracting and technology) to service outcomes, extending service quality theory into security. We also offer a conceptual model that future researchers can build on to explore these relationships further. For instance, future studies might integrate factors such as employee engagement or leadership quality, examine private security service quality in other countries with different regulatory regimes, or track changes longitudinally as new laws and technologies take effect. Understanding the interplay of contracts, technology, and human resources will remain central to improving security service delivery. Our study underscores that better security outcomes depend not only on gadgets and guns, but on governance and people. Such insights are valuable as private security is increasingly important in public safety worldwide.

References

1. Acuña, A., & Parojenog, F. (2024). *Private security adoption in Philippine municipalities: Evolving trends and challenges*. New Southeast Press.
2. Ager, M. (2021, June 1). Senate told to raise minimum pay for security guards to make them 'world class'. *Philippine Daily Inquirer*. https://newsinfo.inquirer.net/1440068/

3. Albrecht, S. (2019). *Enhancing law enforcement response through private security collaboration*. Pacific Research Center.
4. Banerjee, S., & Inamdar, A. (2021). Global trends in private security technology adoption. *International Security Review*, 14(2), 55–70.
5. Banlaoi, R. C. (2022). Security industry growth and crime prevention in the Philippines. *PADPAO Industry Journal*, 5(2), 128–192.
6. Chakravarti, R. (2024). AI-driven surveillance and the future of private security. *Asian Security Technology Journal*, 12(1), 22–35.
7. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.
8. Cruz, J. M. (2021). Challenges in the private security sector: Endo contracts and workforce outcomes. *Journal of Philippine Labor and Society*, 3(1), 45–62.
9. Department of Labor and Employment. (2016). *Department Order No. 150-16: Rules governing employment of security guards*. Manila: DOLE.
10. Department of Labor and Employment. (2023a). *Labor regulations for private security personnel*. Manila: DOLE.
11. Department of Labor and Employment. (2023b). *Department Order No. 248-23: Revised rules on security guard services*. Manila: DOLE.
12. Hair, J. F., Ringle, C. M., Sarstedt, M., & Gudergan, S. P. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage.
13. Heskett, J. L., Sasser, W. E., & Schlesinger, L. A. (1994). Putting the service-profit chain to work. *Harvard Business Review*, 72(2), 164–174.
14. Ivanti. (2021). *Leveraging technology for proactive security risk management* (White Paper). Ivanti Corp.
15. Lumify Work. (2023). *Digital security fundamentals in the Philippine private sector*. Makati City: Lumify Consulting.
16. Monzon, L. (2022). Private security and public safety in the Philippines. *Journal of Asian Security Studies*, 15(3), 45–67.
17. Official Gazette of the Philippines. (2022). *Republic Act No. 11917: Private Security Services Industry Act*. https://www.officialgazette.gov.ph/2022/07/30/republic-act-no-11917/
18. Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. *Journal of Retailing*, 64(1), 12–40.
19. Philippine Association of Detective and Protective Agency Operators (PADPAO). (2022). *Annual industry report on the private security sector*. Manila: PADPAO.
20. Philippine National Police – Civil Security Group, Supervisory Office for Security and Investigation Agencies (PNP-SOSIA). (2024). *Annual report on private security agencies*. Quezon City: PNP CSG.
21. Philippine Senate. (2020). Public hearing on "Private Security as Crime Deterrent" (Senate Committee on Public Order and Dangerous Drugs, February 2020). Manila: Senate of the Philippines.
22. Respicio, E. O. (2020). The "reliever" system: Examining contractualization in security agencies. *Labor Law Commentaries*. Retrieved from respicio.ph (October 15, 2020).
23. Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

24. SecurityMatters. (2024, July 23). PH private sector: Top security trends and challenges. *SecurityMatters Magazine*. https://securitymatters.com.ph/2024/07/23/ph-private-sector-top-security-trends-and-challenges/
25. Tan, J. (2020). Labor conditions in the Philippine security sector. *Philippine Sociological Review*, 68(2), 89–112.
26. Teece, D. J. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350.
27. Trade.gov. (2023). *Philippines Digital Economy Report: Security services section*. International Trade Administration. Retrieved from https://www.trade.gov/
28. United Nations Office on Drugs and Crime (UNODC). (2014). *State regulation of civilian private security services and their contribution to crime prevention and community safety*. Vienna: UNODC. https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Handbook_on_Private_Security.pdf
29. World Bank. (2024). GDP (current US$) – Philippines. World Bank Data. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=PH