ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

SECURITY GOVERNANCE IN PRIVATE SECURITY AGENCIES: A QUALITATIVE STUDY OF PHYSICAL, INFORMATION, AND PERSONNEL SECURITY

Pepito, Nestor T.
Philippine College of Criminology

Article DOI: https://doi.org/10.36713/epra31408
DOI No: 10.36713/epra31408

ABSTRACT

This phenomenological study explored the lived experiences of security professionals regarding security governance at the organizational level within private security agencies in Region IV-A (CALABARZON). The study sought to determine the participants' experiences in governing physical security, information security, and personnel security, including how they perceived governance practices, encountered organizational challenges, adapted to changing operational conditions, and interpreted the impact of governance on organizational security. Using a qualitative phenomenological design, data were gathered through in-depth, semi-structured interviews with 21 key informants who were selected through purposive sampling. The findings revealed that participants experienced physical security governance as a continuous process of safeguarding facilities through access control, surveillance, patrol operations, inspections, emergency preparedness, and incident response. Information security governance was experienced through the responsible handling of organizational information, confidentiality, controlled access, document management, and compliance with data protection policies. Personnel security governance was described as fostering competence, integrity, accountability, and professionalism through recruitment, background investigation, training, supervision, performance evaluation, and ethical discipline. They likewise described security governance as a dynamic organizational experience influenced by inconsistent policy compliance, manpower shortages, resource limitations, evolving security threats, information security risks, increasing client expectations, and regulatory requirements. They experienced these challenges by adopting risk-based deployment strategies, strengthening supervision, enhancing communication, implementing digital reporting systems, conducting continuous training, and promoting security awareness and organizational collaboration. Across these experiences, they perceived security governance as a shared organizational responsibility requiring effective leadership, accountability, continuous improvement, and adaptability. The essence of the lived experience revealed that security governance is an integrated organizational commitment that unites leadership, accountability, risk management, and professional responsibility in protecting people, information, and organizational assets while continuously adapting to emerging security challenges. Based on these findings, the study proposes a Context-Specific Security Governance Framework for Private Security Agencies in Region IV-A (CALABARZON) to strengthen governance practices across physical security, information security, and personnel security, thereby promoting organizational effectiveness, regulatory compliance, and sustainable security management.

KEYWORDS: *Security Governance, Physical Security Governance, Information Security Governance, Personnel Security Governance, Private Security Agencies*

INTRODUCTION

Security governance has become an increasingly important organizational concern as private security agencies operate within complex and evolving security environments. Security professionals are expected to respond not only to physical threats such as theft, sabotage, and workplace violence but also to information security risks, including unauthorized access, data breaches, and misuse of sensitive information, as well as personnel-related risks such as insider threats, misconduct, compromised integrity, and inadequate vetting. These expanding responsibilities have transformed the role of private security agencies from providers of physical protection into organizations expected to uphold effective governance through leadership, accountability, regulatory compliance, ethical practice, and continuous improvement.

Within private security agencies, security governance is experienced through the day-to-day implementation of organizational policies, supervisory practices, operational decision-making, risk management, and accountability mechanisms. Security managers, supervisors, and operational personnel continually interpret and apply governance principles while responding to operational demands, organizational expectations, client requirements, and regulatory obligations. Their experiences shape how security governance is understood and practiced across physical security, information security, and personnel security. From a phenomenological perspective, these lived experiences provide valuable insights into the essence of organizational security governance.

Globally, security incidents have demonstrated that many organizational failures are not solely caused by technological weaknesses or operational deficiencies but are often associated with how governance is experienced and

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

implemented within organizations. Data breaches, insider threats, unauthorized facility access, and internal security violations frequently reflect challenges in leadership, accountability, communication, supervision, and policy implementation rather than the absence of security technologies alone (Floyd & Croft, 2023; DCAF, 2024). These experiences highlight the importance of understanding security governance from the perspectives of those directly responsible for implementing security policies and maintaining organizational security.

Internationally, organizations continue to strengthen security governance through structured management systems and internationally recognized standards. Frameworks such as ISO/IEC 27001:2022 for Information Security Management Systems and ISO 31000:2018 for Risk Management emphasize leadership commitment, systematic risk management, continuous improvement, and organizational accountability (International Organization for Standardization [ISO], 2022). Likewise, international discussions on the governance of private security organizations emphasize transparency, oversight, professional responsibility, and respect for human rights (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2023; OHCHR, 2024). These developments underscore that effective security governance extends beyond compliance and operational procedures to include how governance is understood and practiced within organizations.

In the Philippine context, the private security industry continues to evolve under an expanding legal and regulatory framework. Republic Act No. 11917 (2022) strengthened the regulation and professionalization of private security agencies by promoting higher standards of accountability, competence, and organizational governance. Similarly, the Data Privacy Act of 2012 (Republic Act No. 10173) and the updated circulars issued by the National Privacy Commission reinforce the responsibility of organizations to safeguard personal information through appropriate governance mechanisms (NPC, 2024a; NPC, 2024b). These legal and regulatory developments provide the institutional context within which private security professionals carry out their governance responsibilities across physical, information, and personnel security.

Despite these developments, limited research has explored how security governance is actually experienced by individuals responsible for implementing it within private security agencies. Existing literature predominantly describes governance from the perspective of organizational policies, regulatory compliance, management systems, or operational performance. Comparatively few studies have examined the lived experiences of agency managers, supervisors, and operational security personnel regarding how they understand, implement, adapt, and give meaning to security governance in their everyday professional practice. Consequently, the human experiences underlying governance implementation remain insufficiently understood.

Recognizing this gap, the present study adopts a qualitative phenomenological approach to explore the lived experiences of security professionals regarding security governance at the organizational level in private security agencies in Region IV-A (CALABARZON). Specifically, the study seeks to understand how participants experience governance across the three interconnected domains of physical security, information security, and personnel security, how they perceive the challenges encountered in implementing governance, how they adapt to changing organizational and operational demands, and how they make meaning of their experiences in promoting organizational security.

By exploring the shared meanings and common essence of these lived experiences, the study is expected to contribute to the growing body of knowledge on organizational security governance while providing practice-based insights that may inform the development of a Context-Specific Security Governance Framework for Private Security Agencies in Region IV-A (CALABARZON). Ultimately, the findings aim to enhance leadership, accountability, risk management, and governance practices that support organizational effectiveness, regulatory compliance, and sustainable security management within the Philippine private security industry.

Theoretical Framework

This study is primarily anchored on **Governance Theory**, with **Agency Theory** and **Risk Management Theory** serving as supporting perspectives. Governance Theory provides the principal lens for examining how private security agencies establish leadership structures, formulate policies, allocate resources, enforce accountability, and monitor security functions. It views security governance as an organizational process involving strategic direction, coordination, oversight, and continuous improvement (Bigo, Isin, & Ruppert, 2021; Floyd & Croft, 2023). In this study, the theory guides the examination of how agencies govern physical, information, and personnel security and how these governance practices contribute to organizational effectiveness and crime prevention.

Agency Theory complements this perspective by explaining relationships of delegation, authority, and accountability among owners, managers, supervisors, security personnel, and client organizations. It highlights the importance of supervision, monitoring, reporting, and performance evaluation in reducing non-compliance, negligence, and misconduct. Meanwhile, **Risk Management Theory**, consistent with the principles of ISO 31000, explains how agencies identify, assess, treat, and monitor security risks. It supports the examination of physical, information, and personnel security controls designed to address evolving threats, vulnerabilities, and operational challenges.

The study is further informed by **Routine Activity Theory** and **Situational Crime Prevention Theory**, which explain how capable guardianship and appropriate environmental and procedural controls reduce opportunities for crime. Together, these perspectives position security governance as a multidimensional organizational function involving leadership, accountability, oversight, and risk control. They provide an interpretive foundation for examining the experiences and practices of security professionals and support the development

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

of a context-specific **Security Governance Framework for Private Security Agencies in Region IV-A (CALABARZON)**.

Statement of the Problem

This study examined the security governance in private security agencies in terms of physical security, information security, and personnel security. This qualitative study seeks to answer the following questions:

1. How is physical, information, and personnel security governed by private security agencies in Region IV-A (CALABARZON)?
2. What challenges affect security governance in private security agencies in Region IV-A (CALABARZON)?
3. How do the informants adapt their governance practices in response to operational or organizational constraints?
4. How do the informants address the challenges affecting the security governance in private security agencies?
5. How do the informants perceive the effectiveness and organizational impact of their security governance practices across physical, information, and personnel domains?
6. Based on the findings, what program may be proposed?

METHODOLOGY

This study employed a **qualitative phenomenological research design** to explore the lived experiences of security professionals regarding security governance in private security agencies in Region IV-A (CALABARZON). The qualitative approach was appropriate because the study sought to understand participants' experiences, perceptions, interpretations, and meanings concerning physical security, information security, and personnel security rather than measure variables or test hypotheses (Creswell & Poth, 2024). Data were gathered through **semi-structured, in-depth interviews** with selected key officials and security professionals, allowing participants to describe their experiences while providing opportunities for probing questions. The interview data were analyzed using **thematic analysis** to identify recurring patterns and themes related to security governance practices and challenges (Braun & Clarke, 2021). This approach enabled the study to develop a context-specific understanding of security governance grounded in the participants' lived experiences.

To capture the phenomenon from different organizational perspectives, the informants represented three levels of responsibility: seven (7) Managers, seven (7) Supervisors, and seven (7) Security Officers/Guards. This diversity of roles enabled the researcher to explore the common meanings and shared experiences of organizational security governance across strategic, supervisory, and operational levels. The population of the study were purposively selected from licensed private security agencies operating in Region IV-A (CALABARZON). Consistent with a qualitative phenomenological approach, participants were selected because they had direct, firsthand experience with organizational security governance and were able to provide rich descriptions of their lived experiences concerning physical security, information security, and personnel security within their respective agencies.

The study used a researcher-developed, semi-structured interview guide containing open-ended questions aligned with the Statement of the Problem to explore participants' lived experiences and perceptions of organizational security governance in terms of physical, information, and personnel security. The format allowed flexibility for participants to share experiences while enabling the researcher to probe and clarify responses. Before data collection, the guide underwent expert validation by two experts—a qualitative/criminology research expert and a security management practitioner—to assess its relevance, clarity, adequacy, and alignment with the study's objectives and frameworks. Minor revisions in wording, sequencing, and probing questions were incorporated based on their recommendations. The validated instrument was then used to obtain rich and in-depth narratives appropriate for the phenomenological inquiry.

The data from the in-depth, semi-structured interviews were analyzed using qualitative thematic analysis. No statistical treatment was applied, as the study focused on understanding participants' lived experiences and the meanings they attributed to organizational security governance. Interview recordings were transcribed verbatim, checked for accuracy, and organized according to the Statement of the Problem. The transcripts were repeatedly reviewed to identify significant statements, patterns, and common themes related to physical security, information security, and personnel security governance. The qualitative data from the in-depth interviews were analyzed using Braun and Clarke's (2006, 2021) reflexive thematic analysis. This approach was appropriate for identifying and interpreting patterns of meaning across participants' accounts of security risks, crime prevention practices, implementation challenges, and institutional support within community malls. It also complemented the phenomenological design by capturing common meanings and shared experiences among security personnel, mall administrators, and tenants.

Following the six-phase thematic analysis framework of Braun and Clarke (2021), the researcher first familiarized himself with the data, generated initial codes from significant statements, searched for patterns of meaning, reviewed and refined the emerging themes, defined and named the themes, and finally prepared the thematic narrative. The analysis emphasized participants' descriptions, interpretations, and meanings rather than the frequency of particular responses.

Overall, reflexive thematic analysis provided a systematic yet interpretive process for transforming participants' narratives into meaningful themes while recognizing the researcher's role in interpreting patterns within the data.

RESULTS AND DISCUSSIONS

This section presents, analyzes, and interprets the data gathered from the informants.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

Governance of Physical, Information, and Personnel Security by Private Security Agencies in Region IV-A (CALABARZON)

Using thematic analysis, the participants' narratives were coded, categorized, and synthesized into four emergent themes that reflect the shared meanings of organizational security governance in protecting facilities, assets, and persons.

Physical Security. The findings reveal that informants experienced physical security governance as a structured and coordinated organizational process guided by established policies, operational procedures, leadership oversight, and risk-informed decision-making. They described governance as extending beyond the implementation of security measures to include continuous supervision, accountability, and organizational commitment to protecting facilities, assets, and individuals. Participants also emphasized that effective governance relies on the integration of access control, patrol operations, surveillance, inspections, information protection, and personnel management. Collectively, these experiences illustrate that organizational security governance is sustained through policy-driven leadership, consistent implementation of security procedures, and the active participation of security personnel at different organizational levels.

The analysis generated four emergent themes: (1) Risk-Based and Policy-Driven Physical Security Governance; (2) Access Control, Patrol, Surveillance, and Inspection as Protective Governance Mechanisms; (3) Controlled Access, Confidentiality, and Secure Records Management in Information Security Governance; and (4) Personnel Reliability and Accountability Through Recruitment, Screening, Training, Monitoring, and Discipline.

Theme 1: Risk-Based and Policy-Driven Physical Security Governance. The findings show that physical security governance is guided by established policies, standard operating procedures, and risk-based decision-making to protect facilities, assets, and personnel. Participants emphasized that security decisions are based on risk assessments, site conditions, client requirements, and operational needs. As stated by I1, *"Our agency protects facilities, assets, and personnel through security policies, access control, patrols, inspections, and incident reporting."* Similarly, I4 noted that governance is implemented through post orders, supervisory inspections, patrol schedules, and incident reporting. These findings are consistent with Republic Act No. 11917 and Republic Act No. 5487, as amended, which emphasize professionalism, supervision, and appropriate security measures. The theme is supported by Governance Theory (Bevir, 2012), Risk Management Theory (ISO 31000:2018), and Braun and Clarke (2006, 2022), which emphasize governance, risk assessment, and meaningful patterns in participants' experiences.

Theme 2: Access Control, Patrol, Surveillance, and Inspection as Protective Governance Mechanisms. Participants described access control, patrols, CCTV surveillance, and inspections as essential mechanisms for preventing unauthorized access, detecting threats, and maintaining security. I13 stated, *"We implement access control and verify all personnel and visitors before entry,"* while I11 emphasized access control, patrols, CCTV monitoring, and routine inspections. These practices were viewed as practical expressions of security governance that strengthen situational awareness, accountability, and incident prevention. The findings are consistent with Republic Act No. 11917 and Republic Act No. 5487, as amended, and are supported by Routine Activity Theory (Cohen & Felson, 1979) and Situational Crime Prevention Theory (Clarke, 1997), which emphasize capable guardianship, surveillance, access control, and reduction of opportunities for security breaches.

Theme 3: Active Supervision and Accountability. The findings indicate that physical security governance is strengthened through continuous supervision, performance monitoring, and accountability. Participants reported that supervisors ensure compliance with policies, provide guidance, and address operational concerns. I3 stated, *"Supervisors monitor our compliance with security procedures and immediately address any issues,"* while I18 noted that personnel are regularly supervised and evaluated. Participants viewed supervision not merely as oversight but as supportive leadership that promotes discipline, responsibility, and continuous improvement. The findings are supported by Republic Act No. 11917, Republic Act No. 5487, as amended, Governance Theory (Bevir, 2012), Agency Theory (Jensen & Meckling, 1976), and Braun and Clarke (2006, 2022).

Theme 4: Risk-Based Decision-Making and Adaptation. Participants experienced physical security governance as a dynamic process requiring continuous risk assessment and adaptation. Security strategies were adjusted according to risk levels, operational requirements, client expectations, and emerging threats. I5 stated, *"We assess security risks and adjust our deployment based on operational needs,"* while I19 emphasized adapting procedures whenever new threats or concerns arise. The findings suggest that adaptive decision-making enables agencies to anticipate threats, allocate resources effectively, and maintain operational readiness. This theme is supported by Republic Act No. 11917, Republic Act No. 5487, Risk Management Theory (Hopkin, 2021), ISO 31000:2018, Governance Theory (Bevir, 2012), and Braun and Clarke (2006, 2022).

Theme 5: Collaborative Security Governance. The findings reveal that effective physical security governance depends on collaboration, communication, and shared responsibility among management, supervisors, security personnel, and clients. I6 stated, *"We coordinate with clients and security personnel to ensure effective security implementation,"* while I20 emphasized that governance becomes more effective when stakeholders understand their responsibilities and work together. Participants viewed collaboration as essential for timely information sharing, coordinated decision-making, and effective incident response.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

The findings are consistent with Republic Act No. 11917 and Republic Act No. 5487, as amended, and are supported by Governance Theory (Bevir, 2012), Agency Theory (Jensen & Meckling, 1976), and Braun and Clarke (2006, 2022).

Theme 6: Incident Management and Continuous Improvement. Participants described incident reporting, investigation, documentation, corrective action, and review as essential to effective physical security governance. I9 stated, *"All incidents are documented, reported, and followed by appropriate corrective actions,"* while I18 noted that incident reports are reviewed to improve security procedures. The findings show that incident management functions as a continuous learning process through which agencies identify weaknesses, improve procedures, and prevent recurrence. This theme is supported by Republic Act No. 11917, Republic Act No. 5487, ISO 9001:2015, ISO 31000:2018, Governance Theory (Bevir, 2012), Risk Management Theory (Hopkin, 2021), and Braun and Clarke (2006, 2022).

Information Security Governance. Most informants shared that their agencies protect records, reports, communications, and other confidential information by limiting access to authorized personnel, following standardized procedures, and ensuring compliance with organizational policies. They also emphasized the important role of supervisors in monitoring compliance, providing guidance, and strengthening personnel accountability through regular training and security awareness.

From their lived experiences, the participants viewed information security governance as a shared organizational responsibility built on confidentiality, accountability, and ethical practice. Overall, the findings suggest that effective information security governance strengthens information protection, regulatory compliance, organizational resilience, and the secure delivery of security services.

Theme 1: Controlled Access and Confidential Information Protection. The first theme, Controlled Access and Confidential Information Protection, reflects the participants' experiences that information security governance begins by limiting access to confidential records, reports, and sensitive information to authorized personnel. As stated by the informants, *"Only authorized personnel are allowed to access confidential records and reports"* (I1); *"We strictly control access to sensitive information and only share it with personnel who are authorized"* (I5); and *"Confidential documents are secured, and unauthorized access is not permitted"* (I9). These experiences show that controlled access is viewed as a shared professional and ethical responsibility that promotes confidentiality, accountability, and organizational trust.

The finding is supported by RA No. 10173 (Data Privacy Act of 2012), which requires appropriate safeguards against unauthorized access, use, or disclosure of personal and sensitive information, and RA No. 11917 (Private Security Services Industry Act), which promotes professionalism and accountability in private security services. It is also consistent with Governance Theory (Bevir, 2012) and ISO/IEC 27001:2022, which emphasize accountability, access control, and the protection of information assets. The recurring experiences identified through thematic analysis are consistent with Braun and Clarke (2006, 2022).

Theme 2: Secure Information and Records Management. The second theme emphasizes the proper handling, storage, maintenance, and disposal of physical and electronic records. Informants shared that *"We securely store physical and electronic records following company procedures"* (I4); *"Incident reports and confidential documents are properly filed and protected from unauthorized access"* (I8); and *"Records are organized, maintained, and regularly reviewed to ensure their security and accuracy"* (I12). These experiences indicate that records management is viewed not merely as an administrative task but as an essential governance practice that protects confidentiality, integrity, and availability while supporting accountability and decision-making.

The finding is supported by RA No. 10173 and RA No. 11917, which promote the protection and responsible management of sensitive information and security-related records. It is likewise consistent with ISO/IEC 27001:2022 and Governance Theory (Bevir, 2012), which emphasize appropriate information controls and organizational accountability. The recurring patterns identified among participants are consistent with Braun and Clarke (2006, 2022).

Theme 3: Confidentiality and Responsible Information Sharing. The third theme, highlights the importance of disclosing sensitive information only to authorized individuals through approved communication channels. The informants stated, *"Information is shared only with authorized personnel following company policies"* (I7); *"We ensure that confidential reports are released only to individuals with proper authorization"* (I10); and *"Sensitive information is communicated through secure and approved channels"* (I15). Participants viewed confidentiality as a professional and ethical responsibility that protects sensitive information, strengthens trust, and supports operational coordination.

This finding is supported by RA No. 10173, which requires the lawful and secure processing of personal information, and RA No. 11917, which promotes professionalism, confidentiality, and accountability in private security services. It is also consistent with Governance Theory (Bevir, 2012) and ISO/IEC 27001:2022, particularly regarding confidentiality, information classification, and secure communication. The recurring experiences of participants reflect shared meanings consistent with Braun and Clarke (2006, 2022).

Theme 4: Leadership Oversight and Information Security Compliance. The fourth theme, demonstrates that effective information security governance requires active leadership, supervision, and monitoring of policy compliance. Informants reported that *"Supervisors regularly monitor how confidential information is handled and stored"* (I11); *"Management reviews*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

reports and ensures compliance with information security policies" (I14); and *"We conduct regular inspections and immediately address any information security concerns"* (I18). These experiences indicate that leadership provides guidance, reinforces accountability, and ensures consistent implementation of security policies.

The finding is supported by RA No. 11917 and RA No. 10173, which emphasize professionalism, accountability, supervision, and organizational measures for data protection. It is consistent with Governance Theory (Bevir, 2012) and ISO/IEC 27001:2022, which highlight management commitment, oversight, and continual monitoring as essential elements of information security governance. Braun and Clarke (2006, 2022) further support the identification of recurring patterns in participants' experiences.

Theme 5: Security Awareness and Personnel Accountability. The fifth theme emphasizes the role of employee awareness, training, and individual responsibility in protecting organizational information. Participants shared that *"We receive regular orientation on confidentiality and proper handling of sensitive information"* (I16); *"Personnel are reminded to protect confidential records and follow information security procedures"* (I17); and *"Training helps us understand our responsibilities in safeguarding organizational information"* (I20). These experiences show that information security is perceived as a shared responsibility requiring continuous learning, ethical conduct, and accountability.

The finding is supported by RA No. 10173, which requires organizational measures to safeguard personal information, and RA No. 11917, which emphasizes professionalism and competence among private security personnel. It is further supported by Agency Theory (Jensen & Meckling, 1976) and ISO/IEC 27001:2022, which recognize individual accountability, competence, awareness, and training as important components of effective information security governance. The shared experiences identified are consistent with Braun and Clarke (2006, 2022).

Theme 6: Continuous Improvement in Information Security Governance. The sixth theme reflects the participants' experiences of regularly reviewing policies, monitoring practices, evaluating risks, and implementing corrective actions. Informants stated, *"We regularly review our information security procedures and update them when necessary"* (I20); *"Audit findings and incident reports help us improve our information security practices"* (I19); and *"We implement corrective actions to prevent similar information security issues from happening again"* (I21). These experiences demonstrate that information security governance is viewed as an ongoing process of learning, adaptation, and improvement.

The finding is supported by RA No. 11917 and RA No. 10173, which promote professional standards and the continual strengthening of information protection measures. It is also consistent with Risk Management Theory (Hopkin, 2021) and ISO/IEC 27001:2022, which emphasize risk assessment, monitoring, audits, management review, and corrective action. The recurring experiences of evaluation and adaptation identified in the data are consistent with Braun and Clarke (2006, 2022).

Personnel Security Governance. Most of the 21 informants shared that their agencies promote personnel reliability through careful recruitment and background screening, proper deployment based on operational requirements, continuous supervision, regular performance evaluation, ongoing training, and fair disciplinary measures. They emphasized that these governance practices strengthen competence, integrity, professionalism, and compliance with organizational standards.

From their lived experiences, the participants perceived personnel security governance as more than managing human resources. They viewed it as a shared organizational responsibility that fosters trust, ethical conduct, accountability, and professional growth while ensuring that security personnel are capable of performing their duties effectively.

Theme 1: Recruitment and Background Screening for Personnel Reliability. The first theme highlights recruitment and screening as the foundation of personnel security governance. Participants described qualification verification, background checks, interviews, and documentary requirements as essential in selecting competent, trustworthy, and ethical personnel. As stated by the informants, *"Applicants undergo background checks before they are hired"* (I1); *"We verify the applicant's qualifications and previous employment before deployment"* (I4); and *"Only those who meet the agency's standards are accepted because reliability is very important in security work"* (I9). These practices were viewed as the organization's first safeguard against personnel-related risks and as a means of strengthening trust, accountability, and professionalism.

The findings are supported by RA No. 11917 (Private Security Services Industry Act) and RA No. 5487, as amended, and its Implementing Rules and Regulations, which establish qualification, screening, licensing, and professional requirements for private security personnel. They are consistent with Agency Theory (Jensen & Meckling, 1976), which emphasizes selecting reliable individuals to fulfill organizational responsibilities, and Governance Theory (Bevir, 2012), which highlights accountability, integrity, and responsible leadership as foundations of effective governance.

Theme 2: Strategic Deployment and Role Assignment. The second theme emphasizes matching personnel competencies with operational requirements, client expectations, and security risks. Participants explained that deployment decisions consider qualifications, experience, site conditions, and operational needs. Informants stated, *"Personnel are assigned based on their qualifications, experience, and client requirements"* (I7); *"Deployment depends on operational needs and the security requirements of each area"* (I10); and *"Supervisors consider the risk level of the assignment before deploying personnel"* (I14). These experiences show that proper deployment maximizes

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

personnel capability, improves operational efficiency, and strengthens the agency's response to security challenges.

The findings support RA No. 11917, which promotes competency, professional management, and effective delivery of private security services. They are also consistent with Risk Management Theory (Hopkin, 2021), which emphasizes allocating resources according to identified risks and priorities, and Governance Theory (Bevir, 2012), which recognizes strategic decision-making and responsible resource management as essential to effective governance.

Theme 3: Continuous Supervision and Performance Monitoring. The third theme reflects supervision as an ongoing governance practice that promotes compliance, accountability, and consistent performance. Participants described regular inspections, performance reviews, incident-report monitoring, and feedback as important mechanisms for maintaining professional standards. Informants shared, *"Supervisors regularly monitor our performance and ensure that we follow security procedures"* (I12); *"Our work is evaluated through inspections, reports, and regular performance reviews"* (I15); and *"We receive guidance whenever improvements are needed"* (I18). Supervision was therefore viewed not only as monitoring but also as guidance that supports professional improvement.

The findings are supported by RA No. 11917 and the IRR of RA No. 5487, which emphasize supervision, accountability, and compliance with operational standards. They are consistent with Governance Theory (Bevir, 2012), which identifies monitoring and leadership oversight as governance functions, and Agency Theory (Jensen & Meckling, 1976), which emphasizes supervision to ensure responsible fulfillment of organizational duties.

Theme 4: Competency Development and Professional Growth. The fourth theme emphasizes continuous training, refresher programs, and professional development as essential to maintaining personnel competence and operational readiness. Participants stated, *"We regularly attend training and refresher courses to improve our skills"* (I17); *"Training helps us perform our duties more effectively and confidently"* (I18); and *"Continuous learning prepares us for new security challenges"* (I20). These experiences indicate that professional development strengthens personnel confidence, competence, and capacity to respond to changing security threats and operational demands.

The findings are supported by RA No. 11917 and the IRR of RA No. 5487, which promote competency development, professional standards, and appropriate training for security personnel. They are consistent with Governance Theory (Bevir, 2012), which recognizes capacity building as an important governance function, and Risk Management Theory (Hopkin, 2021), which emphasizes developing organizational capabilities to address emerging risks.

Theme 5: Discipline, Accountability, and Ethical Conduct. The fifth theme highlights the importance of clear rules, fair disciplinary procedures, and ethical behavior in maintaining personnel security governance. Participants shared, *"Personnel who violate policies are investigated and given appropriate disciplinary action"* (I20); *"We are expected to follow ethical standards and remain accountable for our actions"* (I21); and *"Discipline helps maintain professionalism and public trust"* (I14). Their experiences indicate that discipline serves not only to correct misconduct but also to reinforce integrity, responsibility, professionalism, and organizational trust.

The findings are supported by RA No. 11917, which promotes professionalism, accountability, and ethical standards in private security services, and RA No. 6713 (Code of Conduct and Ethical Standards for Public Officials and Employees), whose principles of integrity and accountability provide relevant guidance for professional conduct. The findings further support Governance Theory (Bevir, 2012), which emphasizes accountability and ethical leadership, and Agency Theory (Jensen & Meckling, 1976), which stresses responsible behavior in fulfilling organizational roles.

Theme 6: Collaborative Personnel Security Governance. The sixth theme emphasizes that personnel security is a shared responsibility involving managers, supervisors, security personnel, clients, and other stakeholders. Participants highlighted communication, teamwork, and coordinated decision-making as important in maintaining accountability and addressing operational concerns. Informants stated, *"Managers, supervisors, and guards work together to ensure that security policies are properly implemented"* (I8); *"Everyone has a responsibility to maintain discipline and support one another"* (I13); and *"Regular coordination helps us respond effectively to operational concerns"* (I16). These experiences show that collaboration strengthens trust, communication, collective accountability, and the consistent implementation of security practices.

The finding is supported by RA No. 11917, which promotes professional management, effective supervision, coordination, and responsible delivery of private security services. It also reflects Governance Theory (Bevir, 2012), particularly its emphasis on cooperation, accountability, shared responsibility, and coordinated decision-making. Overall, the theme demonstrates that personnel security governance is strengthened when organizational stakeholders work collectively toward common security objectives.

Challenges Affecting Security Governance in Private Security Agencies in Region IV-A (CALABARZON)

The informants shared their experiences regarding the organizational, operational, and external factors that affect the effective governance of physical, information, and personnel security. Their narratives describe the realities they face in maintaining security standards, ensuring regulatory compliance, managing personnel, protecting sensitive information, and responding to evolving security risks within their organizations.

The shared meanings drawn from the participants' lived experiences provide a deeper understanding of the challenges influencing organizational security governance. These findings

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

reveal the essence of the phenomenon by showing that security governance is a dynamic and continuous process shaped by both internal and external challenges, requiring organizational adaptability, effective leadership, collaboration, and a sustained commitment to strengthening security governance practices.

Theme 1: Inconsistent Compliance and Uneven Implementation Across Sites. The first theme reflects participants' experiences that established security policies are not always implemented uniformly across deployment areas. Differences in site conditions, client requirements, personnel assignments, turnover, and supervisory presence affect the consistent application of security standards. Informants stated, *"One of the main challenges is maintaining consistent compliance with security policies across different sites and personnel"* (I1); *"Our agency faces several key challenges: ensuring consistent compliance with security policies; managing high personnel turnover, which affects training and awareness"* (I3); and *"Ensuring consistent compliance with security procedures, maintaining security awareness, preventing unauthorized access, and addressing manpower shortages during critical operations"* (I5). Informants 9 and 10 likewise emphasized the difficulty of maintaining consistent security practices and policy compliance across sites.

The findings indicate that policies alone do not guarantee consistent governance. Continuous supervision, communication, training, and accountability are necessary to maintain uniform security practices despite varying operational environments. The findings are consistent with RA No. 11917 (Private Security Services Industry Act), Governance Theory (Bevir, 2012), and Agency Theory (Jensen & Meckling, 1976), which emphasize professional standards, policy implementation, supervision, and accountability. Consistent with Creswell and Poth (2024), the participants' shared narratives reveal that consistent implementation is a fundamental lived experience shaping security governance.

Theme 2: Manpower Shortages, Turnover, and Personnel Continuity Problems. The second theme highlights workforce-related challenges affecting the continuity and effectiveness of security governance. Participants reported that personnel shortages, frequent turnover, and reassignment increase workloads and make it difficult to maintain adequate security coverage and consistent implementation of policies. Informants shared, *"Our agency faces several key challenges: managing high personnel turnover, which affects training and awareness"* (I3); *"Addressing manpower shortages during critical operations"* (I5); and *"Frequent personnel movements and varying levels of security awareness also contribute to governance challenges"* (I1). Informants 9 and 10 similarly identified manpower shortages, turnover, and limited resources as recurring concerns.

The findings suggest that personnel stability, competence, and continuity are essential to effective security governance. Frequent turnover requires repeated orientation, training, and supervision, while manpower shortages may increase workload and operational vulnerabilities. The findings are supported by RA No. 11917, Governance Theory (Bevir, 2012), and Agency Theory (Jensen & Meckling, 1976), which emphasize professional competence, organizational support, supervision, and accountability. Patterson et al. (2020) further highlight the importance of competence, training, supervision, and organizational support in strengthening workforce performance. These lived experiences are consistent with the phenomenological perspective of Creswell and Poth (2024).

Theme 3: Evolving Physical, Information, and Technological Security Threats. The third themereflects participants' experiences of an increasingly complex and changing security environment. Informants identified unauthorized access, information breaches, cyber risks, technological changes, human error, and varying personnel competencies as challenges requiring continuous adaptation. Informant 1 noted that the agency faces risks involving *"unauthorized access, information handling, employee turnover, and adapting to evolving security threats,"* while Informant 3 emphasized the need to protect sensitive information from breaches and respond to technological vulnerabilities. Informants 5 and 9 likewise highlighted technological and regulatory changes as factors requiring continuous improvement.

The findings indicate that physical, information, and technological risks are interconnected and require an integrated, adaptive, and risk-based governance approach. Traditional security practices alone may be insufficient without continuous risk assessment, technological awareness, personnel development, and policy enhancement. The findings are supported by RA No. 10173 (Data Privacy Act of 2012), Governance Theory, Routine Activity Theory, and ISO/IEC 27001:2022, which emphasize protection against unauthorized access, effective guardianship, risk-based controls, and continual improvement.

Theme 4: Resource, Regulatory, and Operational Pressures. The fourth theme captures participants' experiences of balancing limited resources with increasing client expectations, operational demands, technological changes, and regulatory requirements. Informants reported that financial and manpower limitations can restrict training, technology investments, supervision, and other security improvements. Informant 3 stated, *"Limited financial and human resources, together with high operational demands, often require us to prioritize immediate operational needs over long-term security improvements"*; Informant 5 noted the challenge posed by *"increasing client requirements, evolving security threats, varying personnel experience, operational demands, and continuous technological and regulatory changes"*; while Informants 9 and 10 similarly identified limited resources, client requirements, and regulatory changes as factors affecting implementation.

The findings demonstrate that security governance is shaped by the organization's capacity to balance competing priorities and available resources. These pressures may increase workloads, delay improvements, and affect the consistent

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

implementation of security standards. The findings are supported by RA No. 11917, Governance Theory (Bevir, 2012), and the OECD Framework on Risk Governance and Risk Management (2020), which emphasize accountability, strategic resource allocation, risk prioritization, and adaptability.

Theme 5: Continuous Monitoring and Governance Oversight. The fifth theme emphasizes regular inspections, supervisory visits, incident reviews, performance evaluations, and compliance checks as mechanisms for maintaining effective security governance. Participants stated, *"Supervisors regularly inspect our posts and monitor whether security procedures are properly followed"* (I5); *"Incident reports and compliance checks help us identify problems and improve our operations"* (I12); and *"Regular monitoring keeps everyone accountable and helps prevent recurring security issues"* (I18). These experiences show that monitoring provides not only control but also guidance, feedback, and opportunities for improvement.

The findings indicate that continuous oversight promotes policy compliance, operational consistency, accountability, and timely corrective action. They are supported by RA No. 11917 and the IRR of RA No. 5487, which emphasize supervision and compliance with professional and operational standards. They are also consistent with Governance Theory (Bevir, 2012) and Risk Management Theory (Hopkin, 2021), which recognize monitoring, accountability, risk assessment, and corrective action as essential governance processes.

Theme 6: Organizational Capacity Building and Continuous Improvement. The sixth theme reflects participants' experiences of continuous training, leadership support, policy review, and organizational adaptation as mechanisms for strengthening security governance. Informants stated, *"Continuous training helps us improve our knowledge and adapt to new security challenges"* (I7); *"We review our procedures after incidents so that we can improve future operations"* (I15); and *"Management encourages us to learn from our experiences and strengthen our security practices"* (I21). Participants viewed continuous improvement as an organizational culture that promotes learning, professional growth, innovation, and resilience.

The findings indicate that capacity building and continuous improvement strengthen personnel competence, organizational adaptability, and institutional resilience. The findings are supported by RA No. 11917 and PNP-SOSIA standards, which promote professional development, training, compliance, and professionalization. They are further consistent with Governance Theory (Bevir, 2012), which emphasizes adaptive leadership and organizational learning, and Risk Management Theory (Hopkin, 2021), which highlights capacity building, learning from experience, and continuous improvement in managing emerging risks.

Synthesis. Overall, the six themes reveal that participants experienced security governance challenges as interconnected organizational and operational concerns rather than isolated problems. Inconsistent policy implementation, manpower shortages and turnover, evolving security threats, resource and regulatory pressures, insufficient oversight, and the continuing need for capacity building collectively influence the effectiveness of physical, information, and personnel security. The findings demonstrate that effective security governance requires consistent policy implementation, adequate and competent personnel, continuous monitoring, adaptive risk management, strategic resource allocation, leadership support, and organizational learning. From a phenomenological perspective, these shared experiences portray security governance as a dynamic and continuously evolving process shaped by the everyday realities of private security agencies.

Informants Adapting their Governance Practices in Response to Operational or Organizational Constraints

The informants shared that responding to these limitations requires practical and adaptive governance strategies to ensure the continuity of security operations. They explained that when resources become limited, their agencies adjust by prioritizing critical security functions, strategically deploying available personnel, strengthening supervisory oversight, maximizing existing resources, and utilizing technology such as CCTV monitoring and digital reporting systems. They also emphasized the importance of cross-training personnel, enhancing security awareness, improving coordination, and maintaining continuous communication to sustain operational effectiveness despite organizational constraints. These adjustments enable agencies to continue implementing physical security, information security, and personnel security measures while minimizing the impact of limited resources on daily operations.

Based on their lived experiences, the informants viewed security governance as a flexible and responsive process that requires continuous assessment, sound leadership, effective resource management, and organizational collaboration. They emphasized that the ability to adapt through strategic planning, personnel development, technological support, and continuous improvement enables private security agencies to maintain service continuity, comply with regulatory requirements, and respond effectively to changing operational conditions. Overall, the findings suggest that adaptive security governance is essential for sustaining organizational resilience and ensuring the consistent delivery of security services despite operational and organizational limitations.

Theme 1: Risk-Based Prioritization of Critical Security Functions. This theme reflects the informants' experiences of adapting security governance to limited manpower, budget constraints, increasing demands, and resource shortages. Rather than distributing resources equally, participants described identifying high-risk areas and prioritizing critical security functions. Informant 1 stated, *"When resources are limited, we prioritize critical security operations, optimize manpower deployment, strengthen supervision, and focus on high-risk areas."* Informant 2 similarly shared, *"We prioritize critical security functions, optimize manpower deployment, and focus on high-risk areas to maintain security operations despite resource*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

constraints." Informants 9 and 10 likewise emphasized prioritizing critical functions, strengthening supervision, and maximizing available resources.

The findings indicate that risk assessment enables agencies to protect critical assets and sustain essential operations despite constraints. Participants applied prioritization across physical, information, and personnel security by focusing personnel and supervisory attention on vulnerable locations, sensitive information, and critical assignments. However, they recognized that concentrating resources on high-risk areas may leave lower-risk locations with reduced protection, highlighting the need for adequate staffing, funding, and organizational support.

The findings are consistent with RA No. 11917 (Private Security Services Industry Act), Situational Crime Prevention Theory, which emphasizes strengthening guardianship in high-risk environments, and the OECD Risk Management Framework, which advocates identifying, assessing, and prioritizing risks. Overall, participants experienced risk-based prioritization as a central adaptive governance practice that promotes continuity, resilience, and responsible resource allocation.

Theme 2: Optimized Manpower Deployment and Resource Maximization. The second theme highlights participants' experiences of making efficient use of available personnel, equipment, and security systems despite manpower and budget limitations. Informant 1 explained, *"When resources are limited, we prioritize critical security operations, optimize manpower deployment, strengthen supervision, and focus on high-risk areas."* Informant 9 similarly stated, *"We prioritize critical security functions, optimize personnel deployment, strengthen supervision, maximize available resources, and implement practical risk-based security measures."* Informants 9 and 10 also described cross-training, digital reporting, adjusted deployment schedules, enhanced communication, and stronger coordination with clients and supervisors.

The findings demonstrate that resource maximization extends beyond personnel deployment to include flexible scheduling, technological utilization, communication, supervision, and coordination. Participants viewed optimization as a continuous process of reallocating responsibilities and resources to maintain essential security functions. However, they acknowledged that excessive reliance on limited personnel may increase workloads, fatigue, and dependence on experienced personnel, emphasizing the importance of sustainable staffing and long-term resource planning.

The findings are supported by RA No. 11917, which promotes professional and effective management of private security agencies, and Governance Theory, which emphasizes the strategic coordination of resources, leadership, authority, and accountability. Overall, the participants' experiences demonstrate that adaptive governance depends not only on the availability of resources but also on how effectively existing resources are organized and utilized.

Theme 3: Technology-Supported Monitoring and Digital Reporting

The third theme, **Technology-Supported Monitoring and Digital Reporting**, reflects participants' experiences of using technology to compensate for manpower limitations, strengthen monitoring, improve documentation, and support timely decision-making. Informant 1 stated, *"We have implemented risk-based deployment, increased the use of CCTV monitoring, strengthened security awareness programs, and cross-trained personnel."* Informant 2 similarly noted the use of risk-based deployment, enhanced CCTV monitoring, security awareness, and cross-training. Informants 9 and 10 highlighted the digitization of reporting processes, improved communication systems, digital reporting, and stronger monitoring and coordination.

The findings indicate that technology serves not only as a surveillance tool but also as a governance mechanism that enhances accountability, information flow, documentation, and operational coordination. CCTV supports physical security, digital reporting strengthens information management, while communication technologies improve personnel supervision and coordination. Participants nevertheless recognized the need for responsible management of electronic information to prevent unauthorized access, misuse, and privacy violations.

The findings are consistent with RA No. 10173 (Data Privacy Act of 2012), which requires appropriate organizational, physical, and technical safeguards for personal and sensitive information. They are also supported by Governance Theory and ISO/IEC 27001:2022, which emphasize responsible technology use, information security controls, monitoring, documentation, and accountability. Overall, technology was experienced as an important adaptive resource that strengthens security governance when supported by appropriate policies, supervision, and responsible information management.

Theme 4: Capacity Building, Cross-Training, Security Awareness, and Service Continuity.

The fourth theme emphasizes the importance of developing a flexible and competent workforce capable of sustaining operations despite organizational constraints. Informant 1 stated, *"We have implemented risk-based deployment, increased the use of CCTV monitoring, strengthened security awareness programs, and cross-trained personnel to perform multiple security functions when necessary."* Informant 2 similarly explained that cross-training and security awareness improve operational flexibility. Informant 9 reported that the agency combines cross-training with digital reporting, adjusted deployment, improved communication, and stronger monitoring. Informant 1 further noted that these adaptations help maintain operations, reduce vulnerabilities, and ensure service continuity.

The findings show that capacity building is a continuous process involving training, cross-training, security awareness, supervision, coordination, and organizational learning. Cross-trained personnel can assume multiple responsibilities during manpower shortages, while security awareness strengthens compliance, information protection, and professional responsibility. Participants also emphasized that expanded responsibilities require clear policies, defined authority, effective

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

supervision, and performance evaluation to prevent role confusion and excessive workloads.

The findings are supported by RA No. 11917, which promotes competence, accountability, and professional development among private security personnel, and Situational Crime Prevention Theory, which emphasizes capable and knowledgeable guardianship. They are also consistent with literature on personnel security and organizational governance emphasizing continuous professional development, effective supervision, and organizational learning. Overall, participants viewed capacity building as essential to workforce flexibility, service continuity, organizational resilience, and effective adaptive security governance.

Synthesis. The four themes collectively demonstrate that adaptive security governance is a continuous process of prioritizing risks, maximizing resources, utilizing technology, and developing personnel capabilities. Participants' experiences show that private security agencies respond to manpower shortages, financial limitations, technological changes, and increasing security demands by concentrating resources on critical risks, optimizing personnel deployment, strengthening technological monitoring, and investing in cross-training and security awareness. These strategies enable agencies to maintain essential physical, information, and personnel security functions despite operational constraints. However, the findings also indicate that adaptive practices are most sustainable when supported by adequate resources, effective leadership, continuous supervision, clear policies, and long-term organizational investment. Thus, adaptive governance is not merely a response to constraints but a strategic and continuous process that strengthens service continuity, organizational resilience, and overall security effectiveness.

Informants Addressing the Challenges Affecting Security Governance in Private Security Agencies

The findings reveal that addressing security governance challenges requires a combination of strategic leadership, operational planning, technological support, personnel development, and collaborative coordination. They explained that their agencies respond to manpower shortages, budget constraints, operational demands, and evolving security risks by implementing risk-based deployment, strengthening supervisory oversight, optimizing personnel assignments, enhancing communication and coordination, expanding the use of CCTV and digital reporting systems, and conducting continuous training and cross-training programs. These interventions enable agencies to sustain the implementation of physical security, information security, and personnel security despite organizational and operational limitations.

Theme 1: Strategic Leadership and Risk-Based Governance. The first theme reflects participants' experiences that effective security governance depends on proactive leadership, risk assessment, security audits, policy reviews, and strengthened supervision. Informants described these practices as mechanisms for identifying vulnerabilities, prioritizing risks, and addressing concerns before they escalate. Informant 1 stated, *"Our agency addresses security challenges through regular risk assessments, security audits, refresher training, policy reviews, coordination meetings, strengthened supervision, improved reporting procedures, and corrective actions."* Informant 2 similarly noted that *"Regular assessments, training, audits, and corrective actions strengthen our security controls."* Informants 5, 9, and 10 likewise emphasized inspections, policy reviews, audits, risk assessments, monitoring, and stakeholder coordination.

The findings indicate that leadership serves as the driving force behind proactive and adaptive security governance. Through continuous assessment, supervision, and policy improvement, leaders can make informed decisions and maintain physical, information, and personnel security despite organizational constraints. The findings are supported by RA No. 11917 (Private Security Services Industry Act) and ISO 31000:2018, which emphasize professional management, risk assessment, leadership commitment, and continuous improvement. They are also consistent with Governance Theory (Rhodes, 1996; OECD, 2015) and Enterprise Risk Management principles (COSO, 2017), which highlight leadership, accountability, risk-based decision-making, and organizational resilience.

Theme 2: Resource Optimization and Operational Management. The second theme highlights participants' experiences of maximizing available personnel, equipment, and organizational resources in response to manpower shortages, budget limitations, and increasing operational demands. Informant 1 shared, *"When resources are limited, we prioritize critical security operations, optimize manpower deployment, strengthen supervision, focus on high-risk areas, maximize existing security systems, and coordinate closely with clients."* Informant 2 similarly stated that agencies prioritize critical functions and high-risk areas, while Informants 5, 9, and 10 emphasized optimizing manpower, strengthening supervision, and maximizing available resources.

The findings demonstrate that effective resource management involves strategic personnel allocation, prioritization of critical assignments, and efficient operational planning. Participants viewed resource constraints as conditions requiring flexibility and sound decision-making rather than barriers to governance. These practices enable agencies to maintain service continuity across physical, information, and personnel security. The findings are supported by RA No. 11917 and ISO 31000:2018, which promote professional management and risk-based resource allocation. They are also consistent with Governance Theory (Rhodes, 1996), Resource-Based Theory (Barney, 1991), and COSO Enterprise Risk Management (2017), which emphasize strategic resource utilization, coordination, and resilience.

Theme 3: Technology-Enabled Security Governance. The third theme reflects the informants' experiences of integrating CCTV surveillance, digital reporting, electronic communication, and technology-supported monitoring into daily security

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

operations. Informant 1 stated, *"We have implemented risk-based deployment, increased the use of CCTV monitoring, strengthened security awareness programs, and cross-trained personnel."* Informant 2 similarly highlighted CCTV monitoring and cross-training, while Informants 9 and 10 described digitized reporting, enhanced communication systems, and strengthened monitoring and coordination.

The findings indicate that technology functions not only as an operational tool but also as a governance mechanism that improves surveillance, documentation, information sharing, accountability, and decision-making. Technology supports physical security through monitoring, information security through digital documentation and communication, and personnel security through improved supervision and coordination. However, participants recognized the need for responsible management of electronic information to prevent unauthorized access and misuse.

The findings are supported by RA No. 10173 (Data Privacy Act of 2012), RA No. 11917, and ISO/IEC 27001:2022, which emphasize information protection, accountability, secure information management, and risk-based controls. They are also consistent with Governance Theory (Rhodes, 1996) and Information Security Governance principles (Von Solms & Von Solms, 2004), which stress leadership, policies, accountability, and effective technology management.

Theme 4: Personnel Development and Collaborative Governance. The fourth theme emphasizes continuous training, cross-training, security awareness, supervision, and coordination with clients and stakeholders as strategies for strengthening security governance. Informant 1 shared, *"Our agency conducts refresher training, coordination meetings, strengthens supervision, and continuously improves reporting procedures to maintain security standards."* Informant 5 highlighted security awareness and site inspections, while Informants 9 and 10 emphasized training, performance monitoring, coordination, and supervision. Informant 11 further stated, *"Continuous training and active supervision strengthen personnel competence, discipline, and compliance with security procedures."*

The findings demonstrate that continuous personnel development enhances competence, adaptability, accountability, and operational flexibility, while collaboration strengthens communication, shared responsibility, and coordinated decision-making. Participants viewed a competent and well-supported workforce as essential to maintaining physical, information, and personnel security under changing conditions. The findings are supported by RA No. 11917, which promotes professional competence and accountability, and RA No. 11058 (Occupational Safety and Health Standards Act), which emphasizes training, instruction, and supervision. The findings are also consistent with Governance Theory (Rhodes, 1996), Human Capital Theory (Becker, 1964), and Senge's Learning Organization Theory (1990), which emphasize collaboration, continuous learning, knowledge development, and organizational resilience.

Synthesis. Collectively, the four themes reveal that effective security governance is achieved through strategic leadership, efficient resource management, technological integration, and continuous personnel development and collaboration. Participants' lived experiences demonstrate that agencies respond to security challenges by proactively assessing risks, prioritizing critical functions, maximizing available resources, adopting technology, strengthening personnel competencies, and coordinating with stakeholders. These practices enable agencies to sustain physical, information, and personnel security despite operational constraints and changing security conditions.

Overall, the findings portray security governance as a proactive, adaptive, and continuously improving process rather than merely the implementation of policies. Leadership provides direction, risk assessment guides priorities, resources are strategically managed, technology strengthens operational capacity, and personnel development sustains organizational competence. When these elements are integrated, private security agencies are better positioned to maintain service continuity, regulatory compliance, accountability, and organizational resilience.

Output of the Study

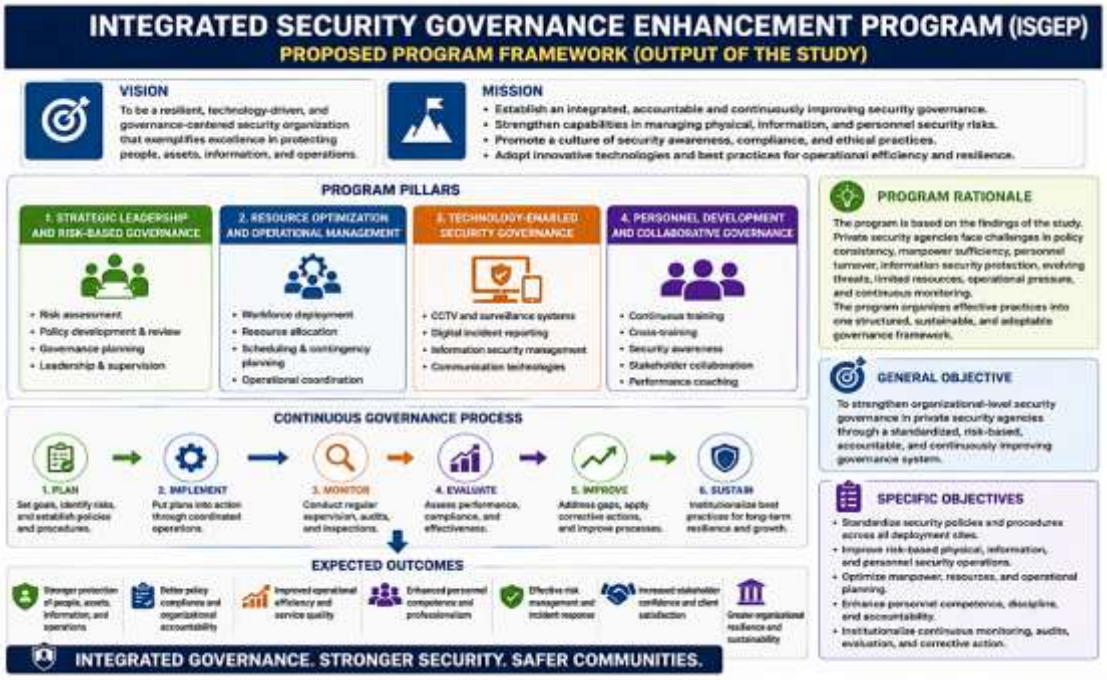
Based on the findings of the study, the program below is proposed.

Program Title: Integrated Security Governance Program for Private Security Agencies (ISGEP)

The proposed framework consists of five interconnected governance pillars:

1. Security Governance Policy Standardization
2. Risk-Based Physical Security Governance
3. Information Security and Records Protection
4. Personnel Reliability and Accountability Development
5. Continuous Monitoring, Evaluation, and Improvement

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188



Together, these pillars promote adaptive leadership, evidence-based decision-making, organizational accountability, and continuous improvement to strengthen security governance across physical, information, and personnel security.

Program Rationale

Considering the findings, this study proposes the **Integrated Security Governance Enhancement Program (ISGEP)** as a practical and evidence-based framework for strengthening organizational security governance in private security agencies in Region IV-A (CALABARZON). The program was developed from the lived experiences and perspectives of the twenty-one (21) key informants, who described the realities, challenges, adaptive practices, and effective governance strategies implemented across the physical, information, and personnel security domains.

The findings revealed that private security agencies continue to face challenges related to policy implementation, manpower limitations, personnel turnover, information security protection, evolving security threats, limited resources, operational pressures, and the need for continuous monitoring and evaluation. Despite these constraints, the informants shared that their agencies sustain effective security governance through strategic leadership, risk-based decision-making, resource optimization, technology integration, personnel development, policy review, security audits, supervision, corrective actions, and collaborative coordination. These experiences demonstrate that effective security governance extends beyond policy compliance and requires adaptive leadership, organizational learning, technological innovation, and continuous improvement.

The **Integrated Security Governance Enhancement Program (ISGEP)** serves as the practical output of this qualitative phenomenological study. It consolidates the adaptive governance practices identified by the participants into a unified, adoptable, and sustainable program that supports continuous organizational improvement. By integrating strategic leadership, risk-based governance, technology-enabled security management, resource optimization, and personnel capability development, the program aims to strengthen the long-term effectiveness of private security agencies while ensuring the continuous protection of people, assets, information, and organizational operations.

Vision

To become a resilient, technology-enabled, and governance-driven private security organization that demonstrates excellence in physical, information, and personnel security through continuous improvement, professionalism, and organizational accountability.

Mission

1. To establish an integrated security governance framework founded on accountability, professionalism, and continuous improvement.

2. To strengthen organizational capability in managing physical, information, and personnel security risks through risk-based governance.

3. To promote a culture of security awareness, ethical conduct, collaboration, and regulatory compliance among all personnel.

4. To leverage technology, innovation, and best security practices to enhance organizational resilience, operational efficiency, and service excellence.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

General Objective

To strengthen organizational-level security governance in private security agencies through a standardized, risk-based, accountable, and continuously improving governance framework that enhances physical, information, and personnel security.

Specific Objectives

The program specifically aims to:

1. Standardize security governance policies, procedures, and operational practices across all deployment sites.
2. Strengthen risk-based physical, information, and personnel security management.
3. Optimize manpower deployment, resource utilization, and operational planning.
4. Enhance personnel competence, ethical conduct, and professional accountability through continuous training and leadership development.
5. Expand the use of technology-enabled security systems, digital reporting, communication platforms, and information management.
6. Institutionalize continuous monitoring, security audits, performance evaluation, stakeholder collaboration, and corrective action to sustain organizational resilience and governance effectiveness.

Conclusions

Based on the findings of the study, the following conclusions are drawn:

Based on the findings, the study concludes that security governance in private security agencies is a comprehensive organizational function that integrates physical security, information security, and personnel security. These interconnected domains collectively strengthen the protection of people, assets, information, and organizational operations.

The findings indicate that effective security governance is founded on well-defined policies, competent leadership, risk-based decision-making, continuous supervision, personnel accountability, and systematic monitoring. However, its effectiveness depends not only on the existence of governance mechanisms but also on their consistent implementation across different operational environments.

The study further concludes that private security agencies encounter various governance challenges, including inconsistent policy implementation, manpower shortages, resource constraints, evolving security threats, and increasing regulatory and operational demands. Despite these challenges, agencies demonstrate adaptability by employing risk-based deployment, technology-supported monitoring, continuous training, collaborative coordination, and proactive leadership to sustain effective governance.

Moreover, the findings reveal that security governance is strengthened through continuous assessment, security audits, policy review, corrective action, and organizational learning. These practices enable agencies to improve compliance, enhance personnel competence, strengthen accountability, and promote continuous organizational improvement.

Finally, the study concludes that the proposed **Integrated Security Governance Enhancement Program (ISGEP)** provides a practical, findings-based framework for strengthening governance practices among private security agencies. By integrating policy standardization, risk-based security management, technology utilization, personnel development, and continuous monitoring, the program supports organizational resilience, operational excellence, and long-term governance sustainability.

4.3 Recommendations

Based on the findings and conclusions, the following recommendations are proposed:

1. For the governance of physical, information, and personnel security, private security agencies should strengthen integrated security governance by aligning these three security domains under a unified governance framework. Agencies should standardize policies, operating procedures, supervisory inspections, compliance monitoring, and performance evaluation across all deployment sites to ensure consistent implementation. Security governance should also be supported by risk-based planning, appropriate personnel deployment, secure information management, and clear accountability mechanisms.
2. To address the challenges affecting security governance, agencies should strengthen resource and capacity management by improving workforce planning, personnel retention, contingency deployment, equipment provision, and allocation of financial and human resources. Particular attention should be given to manpower shortages, personnel movement, increasing workloads, limited equipment, and differences in personnel competency and security awareness. Agencies should also regularly review policies and procedures to respond to changing regulations, client requirements, technological developments, and emerging physical and information security threats.
3. To support adaptation to operational and organizational constraints, agencies should institutionalize flexible and risk-based governance practices. When faced with manpower shortages, changing schedules, emergencies, increased workloads, or limited resources, management should prioritize high-risk areas, optimize personnel deployment, cross-train personnel, establish contingency arrangements, and adjust operational procedures based on assessed risks. These adaptations should be documented and reviewed to ensure that short-term adjustments do not compromise established security standards.
4. To address identified security governance challenges, agencies should strengthen continuous monitoring, coordination, and corrective action mechanisms. Regular inspections, compliance checks, incident reporting, security audits, and post-incident reviews should be conducted to identify weaknesses and determine appropriate interventions. Management should also strengthen communication among managers, supervisors, security personnel, and clients to minimize unclear instructions, human error, and coordination problems. Corrective actions should be documented, assigned to responsible personnel, monitored, and evaluated for effectiveness.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

5. To improve the perceived effectiveness and organizational impact of security governance practices, agencies should adopt measurable governance performance indicators covering physical, information, and personnel security. These may include compliance rates, incident trends, audit findings, response performance, personnel performance, training completion, corrective action implementation, information security incidents, and client feedback. The results should be regularly reviewed by management to determine whether governance practices are improving security performance, operational efficiency, personnel accountability, and client confidence. Technology such as CCTV systems, digital incident reporting, electronic records management, and secure communication platforms should also be maximized where appropriate to improve monitoring, documentation, coordination, and response.

6. Based on the findings of the study, private security agencies in Region IV-A (CALABARZON) are recommended to adopt the proposed ***Integrated Security Governance Enhancement Program (ISGEP).*** The program should provide a practical organizational framework that integrates policy standardization, risk-based security management, resource and manpower planning, personnel development and accountability, technology integration, continuous monitoring, and organizational improvement. The program should include regular security policy reviews, competency-based training, leadership and supervisory development, security awareness activities, governance audits, incident analysis, corrective action tracking, and periodic evaluation of client and organizational feedback. Its implementation should be supported by adequate organizational resources and management commitment to ensure sustainability across deployment sites.

In addition, private security agencies and academic institutions are encouraged to support future research and evaluation of the ISGEP by involving broader participant groups, other regions, and different organizational settings. Comparative qualitative, quantitative, or mixed-methods studies may be conducted to validate the findings, measure the effectiveness of the proposed program, and further refine the integrated security governance framework.

REFERENCES

1. *Bevir, M. (2012). Governance: A very short introduction. Oxford University Press. (Supports Governance Theory used as your primary theoretical framework.)*
2. *Braun, V., & Clarke, V. (2022). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. International Journal of Transgender Health, 24(1), 1–6.*
3. *Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. Sage.*
4. *Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.*
5. *Clarke, R. V. (2021). Situational crime prevention: Successful case studies (3rd ed.). Harrow and Heston.*
6. *Creswell, J. W., & Poth, C. N. (2024). Qualitative inquiry and research design: Choosing among five approaches (5th ed.). Sage.*
7. *DCAF – Geneva Centre for Security Sector Governance. (2024). Addressing new challenges of private military and security companies. DCAF.*
8. *DCAF – Geneva Centre for Security Sector Governance. (2024). Governance of privatesecurity in the South Asia region. DCAF.*
9. *Floyd, R., & Croft, S. (2023). Governance, security, and responsibility. Security Dialogue, 54(2), 139–156. https://doi.org/10.1177/09670106221139752*
10. *Hopkin, P. (2021). Fundamentals of risk management (6th ed.). Kogan Page.*
11. *International Code of Conduct Association. (2025). Ensuring responsible security in the digital age: The application of the International Code of Conduct for Private Security Service Providers to advanced technologies.*
12. *International Organization for Standardization. (2022a). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection – Information security management systems – Requirements.*
13. *International Organization for Standardization. (2022b). ISO/IEC 27002:2022 information security, cybersecurity and privacy protection – Information security controls.*
14. *Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.*
15. *National Privacy Commission. (2024). NPC Circular No. 2024-02: Closed-circuit television (CCTV) systems. NPC.*
16. *National Privacy Commission. (2024b, April 1). NPC issues circulars to strengthen personal data protection in PH. NPC.*
17. *National Privacy Commission. (2025). NPC Circular No. 2025-01: Guidelines on the processing of personal data collected using body-worn cameras. NPC.*
18. *Office of the United Nations High Commissioner for Human Rights. (2024). A/HRC/57/45: Report of the Working Group on the use of mercenaries. OHCHR.*
19. *Office of the United Nations High Commissioner for Human Rights. (2024). Fourth draft instrument on an international regulatory framework on the regulation, monitoring of and oversight over the activities of private military and security companies. OHCHR.*
20. *Office of the United Nations High Commissioner for Human Rights. (2025). Role of mercenaries, mercenary-related actors and private military and security companies in the exploitation of natural resources: Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (A/HRC/60/27). OHCHR.*
21. *Organisation for Economic Co-operation and Development. (2020). OECD risk management framework. OECD Publishing.*
22. *Republic Act No. 10173. (2012). Data Privacy Act of 2012. Official Gazette of the Republic of the Philippines.*
23. *Republic Act No. 11917. (2022). Private Security Services Industry Act. Official Gazette of the Republic of the Philippines.*
24. *Rhodes, R. A. W. (1997). Understanding governance: Policy networks, governance, reflexivity and accountability. Open University Press.*
25. *United Nations Office on Drugs and Crime. (2021). Handbook on police accountability, oversight and integrity. UNODC.*
26. *von Solms, R., & van Niekerk, J. (2021). From information security to cybersecurity. Computers & Security, 101, 102–109. https://doi.org/10.1016/j.cose.2020.102109*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

Research Instrument

SOP 1. How is physical, information, and personnel security governed by private security agencies in Region IV-A (CALABARZON)?

Probing Questions

1. Please describe how your agency governs *physical security*, including the policies, procedures, supervision, and decision-making practices used to protect facilities, assets, and persons. (*Pakilarawan kung paano pinamamahalaan ng inyong ahensiya ang physical security, kabilang ang mga polisiya, pamamaraan, pangangasiwa, at mga paraan ng pagpapasya na ginagamit upang maprotektahan ang mga pasilidad, ari-arian, at mga tao.*)

2. Please describe how your agency governs *information security*, particularly in the handling, storage, sharing, and protection of records, reports, communications, and other sensitive organizational information. (*Pakilarawan kung paano pinamamahalaan ng inyong ahensiya ang information security, lalo na sa paghawak, pag-iimbak, pagbabahagi, at pagprotekta ng mga rekord, ulat, komunikasyon, at iba pang sensitibong impormasyong pang-organisasyon.*)

3. Please describe how your agency governs *personnel security*, including recruitment, screening, deployment, monitoring, discipline, and other measures used to ensure the reliability and accountability of personnel. (*Pakilarawan kung paano pinamamahalaan ng inyong ahensya ang personnel security, kabilang ang pagre-recruit, pagsasala, pagde-deploy, pagmamanman, disiplina, at iba pang mga hakbang upang matiyak ang pagiging maaasahan at may pananagutan ng mga tauhan.*)

SOP 2. What challenges affect security governance in private security agencies in Region IV-A (CALABARZON)?

Probing Questions

1. What major challenges or difficulties does your agency experience in governing *physical, information, and personnel security*? (*Ano ang mga pangunahing hamon o suliraning nararanasan ng inyong ahensiya sa pamamahala ng physical security, information security, at personnel security?*)

2. In your view, what organizational, operational, or external factors contribute to these challenges in security governance? (*Sa inyong pananaw, anu-anong mga salik na pang-organisasyon, pang-operasyon, o panlabas ang nag-aambag sa mga hamong ito sa security governance?*)

3. How do these challenges affect the implementation, consistency, or effectiveness of your agency's security governance practices? (*Paano naaapektuhan ng mga hamong ito ang pagpapatupad, pagiging pare-pareho, o pagiging epektibo ng mga kasanayan ng inyong ahensiya sa security governance?*)

SOP 3. How do the informants adapt their governance practices in response to operational or organizational constraints? (*Paano inaangkop ng mga impormante ang kanilang mga kasanayan sa pamamahala bilang tugon sa mga limitasyong pang-operasyon o pang-organisasyon?*)

Probing Questions

1. When your agency faces limitations such as lack of personnel, budget constraints, operational demands, or policy restrictions, how do you adjust your security governance practices? (*Kapag humaharap ang inyong ahensiya sa mga limitasyon tulad ng kakulangan sa tauhan, limitadong badyet, matataas na pangangailangang pang-operasyon, o mga restriksiyon sa polisiya, paano ninyo inaangkop ang inyong mga kasanayan sa security governance?*)

2. Can you describe specific changes or adaptations your agency has made in governing *physical, information, or personnel security* in response to these constraints? (*Maaari ba ninyong ilarawan ang mga tiyak na pagbabagong ginawa o mga pag-aangkop na isinagawa ng inyong ahensiya sa pamamahala ng physical security, information security, o personnel security bilang tugon sa mga limitasyong ito?*)

3. Based on your experience, how effective are these adaptations in helping the agency continue its security governance responsibilities despite existing limitations? (*Batay sa inyong karanasan, gaano kaepektibo ang mga pag-aangkop na ito sa pagtulong sa ahensiya upang maipagpatuloy nito ang mga tungkulin nito sa security governance sa kabila ng umiiral na mga limitasyon?*)

SOP 4. How do the informants address the challenges affecting the security governance in private security agencies? (*Paano tinutugunan ng mga impormante ang mga hamong nakaaapekto sa security governance sa mga pribadong ahensiyang panseguridad?*)

Probing Questions

1. What actions, strategies, or interventions does your agency undertake to address the challenges affecting its security governance practices? (*Ano-anong mga hakbang, estratehiya, o interbensiyon ang isinasagawa ng inyong ahensiya upang matugunan ang mga hamong nakaaapekto sa mga kasanayan nito sa security governance?*)

2. How do agency leaders, supervisors, or concerned personnel respond when problems arise in *physical, information, or personnel security*? (*Paano tumutugon ang mga pinuno ng ahensiya, mga superbisor, o mga kinauukulang tauhan kapag may lumilitaw na suliranin sa physical security, information security, o personnel security?*)

3. Which of these responses or corrective measures have been most helpful in improving security governance, and why? (*Alin sa mga tugon o mga hakbang na pagwawasto ang pinakanakatulong sa pagpapabuti ng security governance, at bakit?*)

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

SOP 5. How do the informants perceive the effectiveness and organizational impact of their security governance practices across physical, information, and personnel domains? (*Paano nakikita ng mga impormante ang pagiging epektibo at epekto sa organisasyon ng kanilang mga kasanayan sa security governance sa larangan ng physical, information, at personnel security?*)

Probing Questions

1. How do you assess the effectiveness of your agency's security governance practices in the areas of *physical, information, and personnel security*? (*Paano ninyo sinusuri ang pagiging epektibo ng mga kasanayan ng inyong ahensiya sa security governance sa mga larangan ng physical security, information security, at personnel security?*)

2. What positive or negative effects have these security governance practices had on your agency's operations, personnel, and overall organizational performance? (*Ano-ano ang mga positibo o negatibong epekto ng mga kasanayang ito sa security governance sa operasyon ng inyong ahensiya, sa mga tauhan nito, at sa kabuuang pagganap ng organisasyon?*)

3. From your perspective, what signs or experiences show that your agency's security governance practices are either working well or need further improvement? (*Mula sa inyong pananaw, anu-anong mga palatandaan o karanasan ang nagpapakita na ang mga kasanayan ng inyong ahensiya sa security governance ay maayos na gumagana o nangangailangan pa ng karagdagang pagpapabuti?*)

SOP 6. Based on the findings, what program may be proposed?

Probing Questions

1. Based on your experience, what kind of program, policy initiative, or institutional support would help strengthen security governance in private security agencies? (*Batay sa inyong karanasan, anong uri ng programa, panukalang polisiya, o suportang institusyonal ang makatutulong upang mapalakas ang security governance sa mga pribadong ahensiyang panseguridad?*)

2. What important components, activities, or focus areas should be included in a proposed program intended to improve *physical, information, and personnel security governance*? (*Ano-anong mahahalagang bahagi, gawain, o pokus na larangan ang dapat isama sa isang ipinanukalang programa na naglalayong mapabuti ang pamamahala ng physical, information, at personnel security?*)

3. What recommendations can you offer to ensure that such a proposed program will be practical, responsive, and effective for private security agencies in *Region IV-A (CALABARZON)*? (*Ano-anong mga rekomendasyon ang maaari ninyong ibigay upang matiyak na ang ganitong ipinanukalang programa ay magiging praktikal, tumutugon sa pangangailangan, at epektibo para sa mga pribadong ahensiyang panseguridad sa Region IV-A (CALABARZON)?*)

Optional Probing Questions for the Interviewer. May you please elaborate further? Can you give a specific example? What led to that situation? How was it handled in your agency? What was the outcome? (*Opsyonal na Follow-up Questions para sa Tagapanayam. Maaari po ba ninyong ipaliwanag pa nang mas detalyado? Maaari po ba kayong magbigay ng tiyak na halimbawa? Ano po ang naging dahilan ng sitwasyong iyon? Paano po ito hinarap sa inyong ahensiya? Ano po ang naging kinalabasan?*)

CLOSING SCRIPT (*PANGWAKAS NA PAMBUNGAD*)

Thank you very much for your time, participation, and valuable insights. Your responses will greatly contribute to the completion of this dissertation and to a better understanding of *security governance* practices in private security agencies. Rest assured that the information you have shared will be handled responsibly and ethically. (*Maraming salamat po sa inyong oras, pakikilahok, at mahahalagang pananaw. Malaki po ang maitutulong ng inyong mga sagot sa pagkumpleto ng disertasyong ito at sa mas malalim na pag-unawa sa mga kasanayan sa security governance sa mga pribadong ahensiyang panseguridad. Makatitiyak po kayo na ang impormasyong inyong ibinahagi ay hahawakan nang may pananagutan at ayon sa etika.*)

If needed, the researcher may contact you again only for clarification or validation of certain points related to your responses. Thank you once again for your participation. (*Kung kinakailangan, maaari kayong muling kontakin ng mananaliksik para lamang sa paglilinaw o beripikasyon ng ilang bahagi ng inyong mga sagot. Maraming salamat pong muli sa inyong pakikilahok.*)