Technologique: A Global Journal on Technological Developments and Scientific Innovations
2025, Vol. 5, No.1, 1 – 13 | ISSN Online: 3028-1415 | ISSN Print: 3028-1407
DOI: https://doi.org/10.62718/vmca.tech-gjtdsi.5.1.SC-0525-028

An Exploration of Challenges Toward Digital Transformation Among the Personnel of Police Regional Office 9 Headquarters in Zamboanga Peninsula, Philippines

OPEN ACCESS

Article History:

Received: 28 May 2025
Accepted: 23 June 2025
Published: 30 June 2025

Mark Allan T. Pontanar

Master in Public Administration, University of Perpetual Help System DALTA, Pamplona 3, Las Piňas City, Philippines

Abstract

Integrating digital technologies within law enforcement agencies has become imperative in the modern era. As crime evolves and becomes increasingly sophisticated, law enforcement agencies must adapt to these changes by leveraging technology to enhance their capabilities. However, the adoption of digital technologies within law enforcement agencies has challenges. By overcoming these challenges and embracing technological advancements, law enforcement agencies can position themselves to effectively address the evolving landscape of crime and maintain public trust. This research specifically focuses on the Police Regional Office 9 (PRO9) Headquarters, examining its journey towards digital integration. A mixed-methods research design was adopted to comprehensively investigate the adoption rates, perceptions, and operational impacts of newly implemented information systems within PRO9. Quantitative surveys from among 248 PRO9 personnel were administered to collect data on these systems' usage and perceived effectiveness while qualitative interviews were conducted with 10 PRO9 personnel to gain insights into their experiences and challenges. Findings of the study revealed several key challenges hindering PRO9's digital transformation. Technological factors, such as inadequate infrastructure and limited technical expertise, emerged as significant barriers. Organizational factors played a crucial role, including resistance to change, lack of clear digital strategies, and insufficient training. Additionally, legal and regulatory frameworks posed data privacy, security, and interoperability challenges. The interplay of these factors has resulted in slow adoption rates, limited utilization, and suboptimal operational impacts of the implemented information systems. The findings highlight the need for a holistic approach to digital transformation that simultaneously addresses technological, organizational, and legal aspects. This research provides a comprehensive understanding of the challenges faced by PRO9 in its digital transformation journey. By addressing these challenges through targeted interventions and strategic planning, PRO9 can accelerate its digital transformation, enhancing operational efficiency, decision-making, and overall service delivery.

Keywords: digital transformation; law enforcement agency; Philippine National Police; Police Regional Office 9

INTRODUCTION

The Philippine National Police (PNP) is undergoing a digital transformation as it adapts to the swift advancement of technology. The PNP's ICT Master Plan envisions a "SMART" policing environment characterized by secured, mobile, AI-driven, and real-time technology-driven capabilities. Realizing this vision is a top priority, but there are several obstacles, especially on a regional level of the PNP organization. In charge of organizing and supervising police operations in the Zamboanga peninsula is the Police Regional Office 9 (PRO9) Headquarters, a vital PNP operational center in the area. It leads the PNP's initiatives for digital transformation in the peninsula. Developing the information system is at the core of this process, but adopting and integrating new information presents unique challenges for PRO9 Headquarters. These challenges are the results of organizational, legal, and technological issues.

Law enforcement's digital transformation includes integrating advanced modern technologies like data analytics, cloud computing, cybersecurity measures, and artificial intelligence. For PRO9 Headquarters, adapting the digital framework is a technological basis and a complete refurbishment of processes, training, and customs. This transformation requires significant investments in physical, workforce, and intellectual aspects and rigorous obedience towards data privacy and security protocols to make it possible and feasible. The geographic and socio-economic variation of the Zamboanga Peninsula is one of the problems with digital implementation, addressing the specific needs and constraints of the area. Communication with local government units, community stakeholders, and other regional offices is important for achieving successful transformation.

The current literature does not adequately cover the specific difficulties faced by the PNP Regional Headquarters in the Philippines during its digital transformation. This study aims to bridge this gap by examining the case of PRO9 Headquarters, focusing on the unique obstacles and opportunities encountered in their journey towards a digital policing environment.

Through this exploration, we hope to plan awareness and recommendations that can aid in overwhelming these challenges and achieving the PNP's vision of a SMART policing future. This study investigated the twists and turns of these challenges, drawing from interviews with key stakeholders, analysis of internal reports, and comparisons with other regional offices undergoing similar transformations. By providing a detailed account of the PRO9 Headquarters' experiences, this research aims to contribute valuable knowledge to the field of digital transformation in law enforcement, offering practical strategies and lessons learned that can be applied to other regions and agencies.

Theoretical Framework. The Diffusion of Innovation Theory is the foundation for this research, explaining the dissemination of novel concepts and technological advancements within a population. This theory contributes to and helps to understand the factors influencing the adoption rate of new information systems within PRO9 Headquarters. It also offers a framework for comprehending the elements affecting PRO9 headquarters personnel's adoption of new technology.

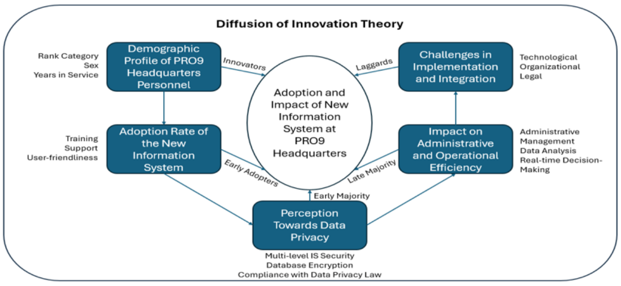

Diffusion of Innovation Theory
Rank Category
Sex
Years in Service
Demographic Profile of PRO9 Headquarters Personnel
Innovators
Adoption and Impact of New Information System at PRO9 Headquarters
Laggards
Challenges in Implementation and Integration
Technological
Organizational
Legal
Training
Support
User-friendliness
Adoption Rate of the New Information System
Early Adopters
Late Majority
Impact on Administrative and Operational Efficiency
Administrative
Management
Data Analysis
Real-time Decision-Making
Early Majority
Perception Towards Data Privacy
Multi-level IS Security
Database Encryption
Compliance with Data Privacy Law

Figure 1
Application of "Diffusion of Innovation Theory" in Adopting New Information System at PRO9 Headquarters

To better understand the role of each sector illustrated in the framework, below is an explanation of each sector's part in the continuum and how they adopt the new information system based on their stance and position in the organization:

1. *Innovators.* These groups desire to test innovation first. They are venturesome and interested in new ideas. These personnel are frequently the first to come up with novel ideas and are very willing to take chances. They are often the first to develop new ideas. Not much has to be done to appeal to this demographic in adopting a new information system.

2. *Early Adopters.* These individuals represent opinion leaders. They welcome chances for change and take pleasure in leadership positions. They are quite at ease embracing new concepts since they already recognize the necessity for change. Training and support in implementing information systems are two tactics to reach this demographic. The user-friendliness of the information system also convinces them to explore and enhance their familiarization with the new information system.

3. *Early Majority.* Although these individuals only sometimes take the lead, they embrace

new concepts before the general majority does. Nevertheless, before they embrace innovation, they usually want to see proof that the new information system is effective and secure. They are especially concerned with data privacy. Implementing multi-level IS security and database encryption is the best way to convince this group.

4. *Late Majority.* These demographics resist change and will not accept an innovation until the majority has given it a shot. Strategies to appeal to this population include feedback on how many other personnel have tried the information system and have successfully utilized it in administrative management, data analysis, and real-time decision-making.

5. *Laggards.* These people are very traditional and conservative. Because of their strong opposition, they are the hardest group to persuade to accept change. They are very concerned about challenges during the implementation of the new information system and the legal, organizational, and technological challenges in integrating with the existing system. Some of the strategies used to appeal to this demographic include outstanding performance statistics and pressure from other adopter groups' members.

Conceptual Framework. The conceptual framework of this research offers a graphic depiction of the connections between the variables under investigation. The framework aims to investigate the relationship between the challenges encountered during the implementation and integration of these systems and the following factors: the operating efficiency of PRO9 headquarters, the adoption rates of new information systems, the demographic profile of personnel, and their perceptions of data privacy and security.

Understanding the range of backgrounds and environments in which PRO9 headquarters personnel function based on the demographic profiles of the respondents, taking into account variables such as years of service, gender, and rank category. These demographic factors are crucial because they can influence how PRO9 headquarters personnel use and perceive new technologies.

A key element of the framework is the adoption rates of new information systems, which are determined by three primary factors: user-friendliness, support, and training. Good training initiatives guarantee that PRO9 headquarters personnel are proficient in operating the information systems, and continued technical assistance and intuitive user interfaces promote easier integration and use.

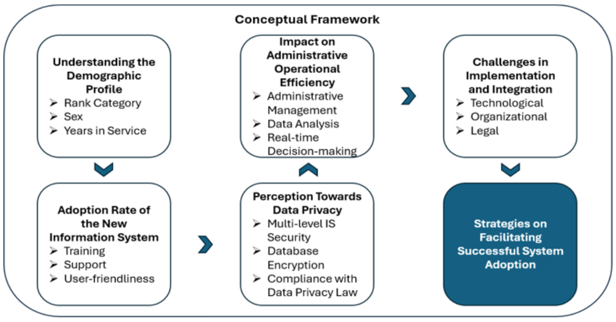

Conceptual Framework
Understanding the Demographic Profile
➢ Rank Category
➢ Sex
➢ Years in Service
Impact on Administrative Operational Efficiency
➢ Administrative Management
➢ Data Analysis
➢ Real-time Decision-making
Challenges in Implementation and Integration
➢ Technological
➢ Organizational
➢ Legal
Adoption Rate of the New Information System
➢ Training
➢ Support
➢ User-friendliness
Perception Towards Data Privacy
➢ Multi-level IS Security
➢ Database Encryption
➢ Compliance with Data Privacy Law
Strategies on Facilitating Successful System Adoption

Figure 2

Graphic depiction of the connections between the variables under investigation.

Perceptions of privacy and data security also play an important role. This feature assesses how strongly PRO9 headquarters personnel see the new systems' data security protocols and whether they meet their needs. Positive perceptions increase user trust and confidence, which is necessary for an information system's efficient and long-term adoption.

The framework evaluates the new information system's operational and administrative efficiency. It specifically examines how the systems enhance data analysis, administrative management, and real-time decision-making. These enhancements are necessary to improve PRO9 headquarters operations and overall service delivery.

This framework addresses the hurdles encountered when integrating and implementing information systems. By identifying key obstacles such as technological limitations, organizational resistance, and legal restrictions, we can effectively overcome them to ensure the successful adoption and utilization of new information systems.

This conceptual framework offers a comprehensive understanding of the factors influencing the integration of new information systems within PRO9 headquarters. By examining the challenges associated with technological advancements, it aims to improve administrative and operational efficiency across law enforcement agencies.

Statement of the Problem. This study explored the challenges encountered by PRO9 Headquarters in its digital transformation journey. It provides specific answers to the following questions:

1. What are the current adoption rates of the new information systems among PRO9 Headquarters personnel in terms of:
   1.1 Training;
   1.2 Support; and,
   1.3 User-friendliness?

2. How do PRO9 Headquarters personnel evaluate the data privacy and security measures implemented in the new systems in terms of:
   2.1 Multi-level IS Security;
   2.2 Database Encryption; and,
   2.3 Compliance with Data Privacy Law?

3. What is the impact of new information systems on the administrative and operational efficiency of PRO9 Headquarters in terms of:
   3.1 Administrative Management;
   3.2 Data Analysis; and,
   3.3 Real-time Decision-making?

4. What are the challenges encountered by PRO9 Headquarter when implementing and integrating new information systems relative to:
   4.1 Technological;
   4.2 Organizational; and,
   4.3 Legal Challenges?

5. Based on the study's findings, what strategic approaches can be recommended to enhance system adoption and integration within PRO9 Headquarters?

LITERATURES

Training and Support as Drivers of Information System Adoption. Effective training is a foundational element in increasing the adoption of information systems. In law enforcement contexts, Al-Raisi and Al-Karaghouli (2020) report that well-designed training programs significantly improve officers' adoption and use of new systems. Lutz et al. (2021) further support this by showing that real-world applications and scenario-based training improve user comprehension and engagement. Support services such as technical assistance and peer networks are also critical. Heeks (2020) points out the necessity of regular updates and maintenance. The quality of support services directly affects user satisfaction and long-term system use.

System Usability and User-Centric Design. An intuitive and user-friendly interface is central to effective adoption. Chan et al. (2020) show that in law enforcement, a simple interface helps officers operate systems with minimal training. Marangunić and Granić (2022) emphasize that personalized and customizable interfaces improve both usability and satisfaction among users.

Perception of Data Privacy and Security. Security protocols, including layered defenses, are essential for protecting sensitive law enforcement data. Alharbi (2021) and Khan and Khan (2022) both advocate for multi-tiered security systems comprising firewalls, intrusion detection systems, and user access controls to prevent data breaches and build user trust. Wang, Liu, and Li (2022), along with Al-Hajri and Al-Zahrani (2021), emphasize that database encryption is vital for safeguarding sensitive information, such as personal records and investigation data. Encryption supports compliance with privacy regulations and enhances data confidentiality. Laws such as the Philippines' Data Privacy Act of 2012 require transparency, informed consent, and protection of personal data. Alharbi (2021) and Khan and Khan (2022) underline that legal compliance not only avoids penalties but also strengthens public trust in law enforcement agencies.

Enhancing Administrative and Operational Efficiency. New information systems can streamline workflows and reduce administrative burden. These systems allow for centralized data storage and automated task tracking, facilitating timely and accurate case resolution. McCue (2020) discusses how modern information systems enable pattern recognition and predictive analytics, aiding in crime prevention and strategic decision-making. For the PNP, this means more effective resource deployment and investigative capabilities. Real-time information systems improve operational responsiveness. Such systems enable swift, informed decision-making during emergencies, particularly in policing environments.

Challenges in System Integration and Implementation. Compatibility with legacy systems and the complexity of modern technology are major hurdles. Adopting standardized data formats and communication protocols eases integration.

Resistance to change often stems from poor communication and inadequate support. Cordner and Scarborough (2021) propose involving personnel in the change process and offering incentives. Rees and Rodley (2020) recommend cultivating a culture of innovation through regular training and rewards.

Legal compliance must be addressed early in system development. Compliance not only mitigates legal risks but also upholds public trust. For the PNP, this means consistent audits, privacy training, and robust security practices.

METHODOLOGY

Research Design. A mixed-methods research design was used to thoroughly examine the difficulties faced by PRO9 Headquarters during its digital transformation journey. This design allowed the researchers to achieve the study's purposes and objectives. The adoption rates, perceptions, and other pertinent variables were quantified using quantitative methods, while qualitative methods provided additional insights into the experiences and viewpoints of PRO9 headquarter personnel. According to Ahmad et al. (2020), quantitative research relied on the methods of natural sciences, which yielded numerical data and facts while qualitative research (Bandari, 2023) involves collecting and analyzing non-numerical data (e.g., text, video, or audio) to understand concepts, opinions, or experiences. It was used to gather in-depth insights into a problem or generate new ideas for research.

Population, Samples, Sampling Technique. For the quantitative phase, stratified sampling was used among Police Regional Office 9 (PRO9) personnel according to category. One hundred six (106) Police Commissioned Officers (PCO) represented 9.24% of total PRO9 headquarters personnel while nine hundred eighty-five (985) represented 85.88% of the Police Non-Commissioned Officers (PNCO). A meager number of fifty-six (56) represented 4.88% of the Non-Uniformed Personnel (NUP). To guarantee that every member of the PRO9 headquarters personnel was represented, a proportionate random sample was subsequently selected from each category. Hence, utilizing the Raosoft calculator, with ninety-five (95) percent confidence level and a five (5) percent margin of error, a total of two hundred forty-eight (248) personnel was yielded as samples of the study with the following breakdown: 59 PCOs, 157 PNCOs, and 32 NUP.

For the qualitative data, ten (10) purposively selected participants, identified as experts in the subject matter, were chosen from among the surveyed respondents for the in-depth interviews. They were particularly chosen to illuminate their experiences and viewpoints with regards to the challenges in digital transformation.

Research Instrument. To gather data, the researcher employed a self-made survey questionnaire and an interview guide. The questionnaire was meticulously designed and divided into four main sections. The first section gathered demographic profiles of the respondents. The subsequent sections focused on critical aspects of digital transformation: the adoption rates of the new information systems, perceptions of data privacy and security, and the perceived impact on administrative and operational efficiency. A 4-point Likert scale was utilized for all quantitative questions, allowing for standardized scoring and interpretation of responses.

To ensure the validity and reliability of the instrument, a rigorous validation process was undertaken. The questionnaire underwent content validation by a panel of experts specializing in law enforcement technology and research methodology. Their invaluable feedback helped refine the items, ensuring relevance, clarity, and alignment with the study's objectives. Following this, a pilot test was conducted with a small sample of PNP personnel to assess the questionnaire's reliability. The internal consistency of each scale was measured using Cronbach's Alpha reliability testing, yielding robust results. First, the Adoption Rate of the New Information System yielded a Cronbach alpha of 0.892 while the Perception Towards Data Privacy gained Cronbach alpha of 0.910. Lastly, the Impact on Administrative and Operational Efficiency has a Cronbach alpha of 0.882. These high Cronbach alpha values demonstrated excellent internal consistency across all measured constructs, indicating that the questionnaire items measured the intended concepts. The final version of the questionnaire was then approved by the research adviser.

Additionally, semi-structured interview guide questions were developed to collect qualitative data from ten purposively selected personnel at PRO9 Headquarters. These interviews were designed to provide in-depth insights into their experiences with the implementation of new information systems, with a specific focus on understanding the operational impact and the intricate challenges related to technological, organizational, and legal factors.

Data Gathering Procedure. Using a secured online survey platform, the questionnaire was distributed electronically to a random sample of 248 personnel from various PRO9 Headquarter sub-units and levels. Clear instructions and informed consent were provided, and participants were given adequate time to complete the questionnaire. Semi-structured interviews were conducted face-to-face and virtually, depending on participant availability and preference. Interviews were recorded with participant consent and transcribed verbatim for qualitative data analysis. The researcher ensured in upholding the highest ethical standards in conducting the research.

Data Analysis. Data from interviews underwent thematic analysis to identify patterns, themes, and unique insights related to the research questions. While quantitative data were treated using percentage, mean and composite mean. Percentage was used to present descriptive statistics and findings. They highlighted proportions or changes in data, such as the percentage of agreement on survey statements or adoption rates, making results easy to interpret.

Weighted Mean was used to calculate a balanced average considering varying importance levels assigned to different data points. This method helped synthesize data on perceptions or effectiveness by giving more weight to crucial aspects. Composite Mean combined multiple measures into a single score, simplifying complex data sets. It was employed to create indices for constructs like operational efficiency or user satisfaction, offering a clear summary of diverse data.

RESULTS AND DISCUSSION

Current adoption rate of the new information systems among PRO9 personnel. Table 1 presents the composite evaluation of the adoption rate of the new information system at the PRO9 headquarters, focusing on training, support, and user-friendliness. Findings show that all indicators fall within the "Agree" range, suggesting a generally positive reception among users.

Table 1

Adoption Rate of the New Information System Based on Training, Support, and User-Friendliness

Dimension	Indicator	Weighted Mean	Verbal Interpretation
Training	Training Content Relevance	3.00	Agree
	Training Delivery Effectiveness	2.96	Agree
	Training Accessibility	3.06	Agree
	Composite Mean	**3.01**	**Agree**
Support	Responsiveness of Support Services	3.09	Agree
	Support Staff Knowledge	2.98	Agree
	Availability of Support Channels	2.98	Agree
	Composite Mean	**3.02**	**Agree**
User-Friendliness	System Intuitiveness	2.94	Agree
	System Consistency	2.99	Agree
	Error Handling and Recovery	2.98	Agree
	Composite Mean	**2.97**	**Agree**

In terms of training, the highest-rated indicator was accessibility (M = 3.06), followed by content relevance (M = 3.00) and delivery effectiveness (M = 2.96). These findings emphasize the importance of effective communication and user engagement in the successful adoption of new technologies.

For support, responsiveness of services received the highest rating (M = 3.09), reflecting users' appreciation for timely assistance. The uniform ratings for supporting staff knowledge and channel availability (both M = 2.98) suggest consistent but slightly lower satisfaction in these areas.

Regarding user-friendliness, all indicators received similar scores: intuitiveness (M = 2.94), consistency (M = 2.99), and error handling and recovery (M = 2.98). While the system was generally seen as user-friendly, the scores suggest opportunities for refinement to improve user experience further.

Overall, the consistently high composite means across the three domains (Training = 3.01, Support = 3.02, User-Friendliness = 2.97) indicate that users agree on the system's effectiveness, but there remains space for enhancement, particularly in user interface design and support structures.

Evaluation of the data privacy and security measures implemented in the new systems. The findings summarized in Table 2 reveal that PRO9 personnel generally perceive the organization's data privacy practices positively, with all composite means falling within the "Agree" category. Among the three dimensions—information systems (IS) security, data encryption, and compliance—compliance received the highest composite mean (M = 3.01), followed closely by data encryption (M = 3.00) and IS security (M = 2.94).

Table 2

Perception of Data Privacy Practices at PRO9 Headquarters

Dimension	Indicator	Weighted Mean	Verbal Interpretation
IS Security	Effectiveness of Access Controls	2.96	Agree
	Strength of Network Security Measures	2.90	Agree
	Adequacy of Data Loss Prevention Measures	2.96	Agree
	Composite Mean	**2.94**	**Agree**
Data Encryption	Adherence to Data Subject Rights	3.02	Agree
	Data Breach Notification Procedures	3.01	Agree
	Data Protection Impact Assessments	2.98	Agree
	Composite Mean	**3.00**	**Agree**
Compliance	Data Privacy Procedures	3.02	Agree
	Commitment to Data Privacy	3.06	Agree
	Ability to Protect Personal Data	2.95	Agree
	Composite Mean	**3.01**	**Agree**

For IS security, the ratings for access control effectiveness and data loss prevention (both M = 2.96) reflect user confidence in these protective mechanisms, although network security (M = 2.90) scored slightly lower, suggesting potential for technical improvement. Within the data encryption dimension, the highest-rated aspect was adherence to data subject rights (M = 3.02), emphasizing PRO9's attention to privacy principles. This is supported by favorable perceptions of breach notification procedures (M = 3.01) and data protection impact assessments (M = 2.98). These results reflect general awareness of key privacy obligations, though minor refinements could strengthen the institution's privacy posture furth.

Regarding compliance, the commitment to data privacy received the strongest support (M = 3.06), suggesting personnel view privacy as a priority within the organization. While policies and procedures (M = 3.02) and data protection capabilities (M = 2.95) also received favorable assessments, the data point to a slightly lower perceived capacity in actual implementation, possibly due to system limitations or knowledge gaps.

Impact of new information systems on the administrative and operational efficiency of PRO9 Headquarters. As presented in Table 3, respondents from PRO9 Headquarters reported generally favorable perceptions regarding the impact of the implemented information system, with all three dimensions—administrative management, data analysis, and real-time decision making—falling within the "Agree" interpretation range. The highest overall rating was observed for real-time decision making (M = 3.04), followed by administrative management (M = 3.00), and data analysis (M = 2.94).

Table 3
Perceived Impact of the Information System at PRO9 Headquarters

Dimension	Indicator	Weighted Mean	Verbal Interpretation
Administrative Management	Efficiency of Administrative Processes	3.03	Agree
	Quality of Administrative Output	2.89	Agree
	Satisfaction with Administrative Tasks	3.08	Agree
	Composite Mean	**3.00**	**Agree**
Data Analysis	Data Analysis and Reporting	2.92	Agree
	Accuracy and Reliability of Data	2.88	Agree
	Data Insights for Decision-Making	3.02	Agree
	Composite Mean	**2.94**	**Agree**
Real-Time Decision Making	Response to Changing Conditions	2.99	Agree
	Quality of Real-Time Decisions	2.97	Agree
	Alignment of Decisions	3.15	Agree
	Composite Mean	**3.04**	**Agree**

In the administrative management dimension, the highest rating was given to satisfaction with administrative tasks (M = 3.08), reflecting a positive change in how personnel experience daily workflows. The efficiency of administrative processes also received a high score (M = 3.03), indicating that the system contributed to smoother operations. However, the slightly lower rating for the quality of administrative output (M = 2.89) suggests that while operations have become more efficient, the output may still benefit from quality improvements.

Regarding data analysis, the system's support for decision-making through insightful data (M = 3.02) was highly regarded. However, concerns were noted in the accuracy and reliability of the data (M = 2.88), along with the quality of analysis and reporting (M = 2.92). These scores imply that while users appreciate the system's analytical potential, there may still be issues related to data validation and presentation that need to be addressed.

The highest-performing dimension was real-time decision making, particularly in the area of alignment of decisions with system recommendations (M = 3.15). This suggests that the system's recommendations are perceived as trustworthy and applicable. Scores for responsiveness to changing conditions (M = 2.99) and the quality of real-time decisions (M = 2.97) were slightly lower, indicating that although users are generally satisfied, opportunities exist for enhancing responsiveness and precision under dynamic circumstances. Overall, the data affirm that PRO9's information system is positively impacting key organizational functions, though further refinements—especially in data accuracy and output quality—could amplify its effectiveness.

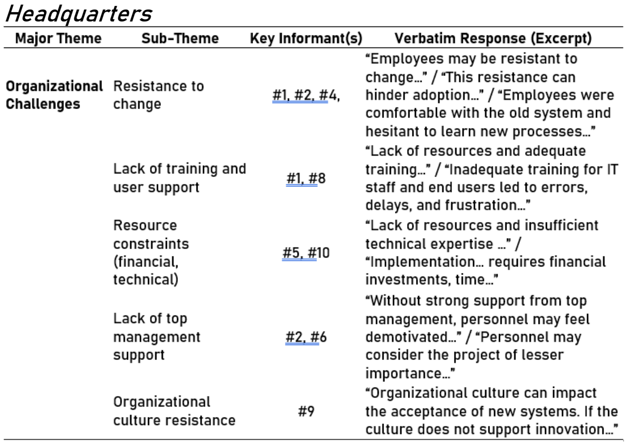
Challenges encountered by PRO9 Headquarter in the implementation and integration of new information systems. The challenges faced by PRO9 in implementing new information systems reflect well-documented issues in IS literature. Technological challenges primarily revolve around system integration with legacy infrastructure and performance limitations.

Table 4
Thematic Analysis of Challenges in Implementing New Information Systems at PRO9 Headquarters

Major Theme	Sub-Theme	Key Informant(s)	Verbatim Response (Excerpt)
Technological Challenges	Integration with existing systems	#1, #9	"There were several compatibility issues…" / "Integrating new systems with legacy systems can significantly impact daily work and operations…"
	System performance and hardware limitations	#2	"Performance bottlenecks may appear in case hardware is poor, the software is not optimized, or bandwidth is limited…"
	Unclear requirements and technical limitations	#4	"Exact requirements for the future are not well defined… may need firmware or software updates…"
Organizational Challenges	User adaptation and training needs	#3, #7	"Extensive training of the staff…" / "Employees might struggle with new interfaces…"
	Resistance to system change	#7	"Resistance to change in the learning curve… can lead to decreased productivity initially."
Legal & Security Challenges	Data security and privacy concerns	#5, #8,	"Implementing robust security measures…" / "Integrating the new system with our existing network raised vulnerabilities…"
	Security-performance trade-offs	#6	"Security measures such as encryption and real-time threat detection can impact system performance…"

Organizational challenges, such as resistance to change and steep learning curves, emphasize the importance of training and user acceptance frameworks. Legal and security challenges underscore the critical role of data protection, system vulnerabilities, and regulatory compliance, as echoed by Alharbi (2021), Coles-Kemp and Theoharidou (2020). These insights affirm that successful IS implementation in law enforcement requires a strategic, integrative approach—balancing technology, training, change management, and security.

Table 5
Thematic Analysis of Organizational Challenges in Implementing New Information Systems at PRO9 Headquarters



Major Theme	Sub-Theme	Key Informant(s)	Verbatim Response (Excerpt)
Organizational Challenges	Resistance to change	#1, #2, #4,	"Employees may be resistant to change…" / "This resistance can hinder adoption…" / "Employees were comfortable with the old system and hesitant to learn new processes…"
	Lack of training and user support	#1, #8	"Lack of resources and adequate training…" / "Inadequate training for IT staff and end users led to errors, delays, and frustration…"
	Resource constraints (financial, technical)	#5, #10	"Lack of resources and insufficient technical expertise …" / "Implementation… requires financial investments, time…"
	Lack of top management support	#2, #6	"Without strong support from top management, personnel may feel demotivated…" / "Personnel may consider the project of lesser importance…"
	Organizational culture resistance	#9	"Organizational culture can impact the acceptance of new systems. If the culture does not support innovation…"

The implementation of new information systems at the Police Regional Office 9 (PRO9) Headquarters faced substantial organizational challenges, particularly in the areas of resistance to change, resource constraints, lack of training, management support, and organizational culture.

A dominant theme that emerged from the data is resistance to change (Key Informants #1, #2, #3, #4, #8). Employees showed reluctance to adopt new systems, often due to comfort with existing processes or fear of the unknown. Heeks (2020) also underscores the inertia within digital development projects, which often struggle with legacy thinking and resistance. The Technology Acceptance Model (TAM), reviewed comprehensively by Marangunić and Granić (2022), reinforces this, suggesting that if systems are not perceived as useful or easy to use, resistance will be stronger.

Resource constraints, including financial, technical, and human resources (Key Informants #5, and #10), were another significant barrier. The lack of adequate funds and skilled personnel led to delays and incomplete deployments. This aligns with standard project management principles and is echoed by Al-Raisi and Al-Karaghouli (2020), who found that successful IS implementation in law enforcement requires sufficient budget allocation and trained personnel.

Closely tied to resource limitations is the lack of training and support for users (Key Informants #1 and #8), which resulted in errors, user frustration, and slow system adoption. Effective training enhances perceived ease of use and usefulness—both key predictors of technology acceptance. Without training, even the most advanced systems may be underutilized.

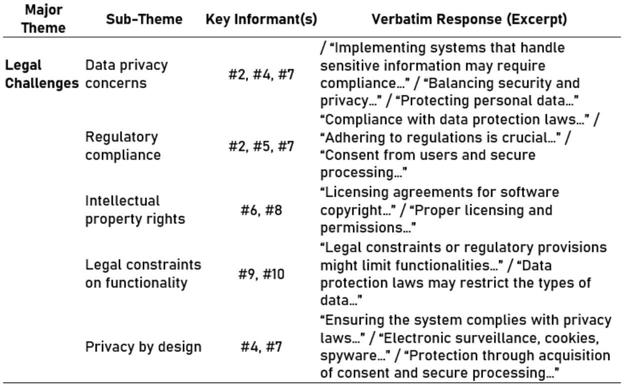
Another crucial factor is the lack of top management support (Key Informants #2 and #6). Without visible and consistent leadership backing, projects often fail to gain traction among staff. Lutz et al. (2021) link transformational leadership directly to successful IS implementation, emphasizing that leaders must actively engage and demonstrate commitment for the system to be taken seriously at all organizational levels.

Lastly, organizational culture was identified as a significant influence on system acceptance (Key Informant #9). A culture that does not value innovation or resists technological change can significantly hinder the adoption of new systems. Cordner and Scarborough (2021) note that in law enforcement, cultural alignment with new practices is essential for success, and misalignment can undermine even the best-designed systems.

Overall, these findings illustrate that organizational issues—especially resistance to change, lack of training and resources, poor leadership support, and misaligned culture—play a critical role in shaping the outcomes of information systems implementation. As Marasambessy (2023) suggests, the effectiveness of law enforcement's digital transformation has direct implications for public trust; thus, addressing these challenges is not merely operational but foundational to the broader success of public service delivery.

Table 6

Thematic Analysis of Legal Challenges in Implementing New Information Systems at PRO9 Headquarters



Major Theme	Sub-Theme	Key Informant(s)	Verbatim Response (Excerpt)
Legal Challenges	Data privacy concerns	#2, #4, #7	/ "Implementing systems that handle sensitive information may require compliance…" / "Balancing security and privacy…" / "Protecting personal data…"
	Regulatory compliance	#2, #5, #7	"Compliance with data protection laws…" / "Adhering to regulations is crucial…" / "Consent from users and secure processing…"
	Intellectual property rights	#6, #8	"Licensing agreements for software copyright…" / "Proper licensing and permissions…"
	Legal constraints on functionality	#9, #10	"Legal constraints or regulatory provisions might limit functionalities…" / "Data protection laws may restrict the types of data…"
	Privacy by design	#4, #7	"Ensuring the system complies with privacy laws…" / "Electronic surveillance, cookies, spyware…" / "Protection through acquisition of consent and secure processing…"

The implementation of new information systems at PRO9 Headquarters revealed critical legal challenges, with prominent concerns around data privacy and protection, regulatory compliance, intellectual property rights, and legal constraints limiting system functionality.
The most consistently reported challenge was ensuring data privacy and regulatory compliance (Key Informants#2, #4, #7,) Informants highlighted the importance of adhering to data protection laws such as the General Data Protection Regulation (GDPR) and other national regulations that govern the collection, storage, processing, and sharing of sensitive data. These findings align with Bélanger and Crossler's (2021) comprehensive review, which emphasizes the centrality of privacy considerations in IS research and practice. The growing necessity for robust privacy mechanisms in digital systems, especially as data becomes increasingly pervasive. Furthermore, Hong and Thong (2023) show that user concerns about privacy are shaped not only by technological features but also by regulatory frameworks such as Singapore's Personal Data Protection Act.

The legal concerns reported by informants—ranging from surveillance and monitoring to the need for user consent—support the principle of "privacy by design", particularly relevant in law enforcement contexts. Coles-Kemp and Theoharidou (2020) advocated the embedding of privacy measures into system architectures from the outset, especially in high-stakes environments such as policing, where technology like body-worn cameras creates ongoing legal and ethical dilemmas.

Another notable theme was the importance of intellectual property (IP) protection (Key Informants #6 and #8). Informants stressed the need to obtain proper software licenses, adhere to copyright laws, and manage trademarks to avoid potential legal disputes. Although IP rights are a well-established legal domain, their application in IS implementation – particularly regarding third-party software use and proprietary system development – is critical. The observations of the informants align with standard legal practice, emphasizing the need for due diligence and licensing compliance during IS procurement and integration.

The constraints imposed by legal and regulatory frameworks on system functionality were also highlighted (Key Informants #9 and #10). These include limits on the types of data that can be collected or processed and requirements to balance system capability with legal boundaries. This theme reflects the broader tension between innovation and compliance, often overlooked in technical discussions of system design.

These legal concerns are further compounded in the law enforcement context, where information systems must handle sensitive personal and operational data. McCue (2020) cautions that the integration of data analytics into criminal justice systems introduces new layers of ethical and legal responsibilities, requiring strict governance and oversight. Studies by Chan, Sharpe, and Brown (2020) provide real-world illustrations of how real-time data systems and integrated case management tools must be deployed with clear legal safeguards to maintain public trust and institutional integrity.

Lastly, the intersection of data privacy and cybersecurity was an underlying thread in several responses. Protecting personal data from unauthorized access requires both legal compliance and technical safeguards. This reflects growing scholarly focus on cybersecurity in digital government systems, as discussed by Alharbi (2021) and Khan and Khan (2022), who emphasize the importance of aligning cybersecurity protocols with evolving privacy regulations in smart environments.

In conclusion, the legal challenges identified—data privacy, regulatory compliance, IP rights, and legal limitations on system design—are critical considerations for IS implementation, particularly in law enforcement. These findings underscore the necessity for a legally informed IS implementation strategy that addresses compliance proactively, ensures system functionality aligns with legal obligations, and incorporates privacy protections at every stage of development.

Based on the findings, the following recommendations can be used to contribute in crafting the proposed Strategic Plan:

1. *Understanding the Demographic.* Conduct regular surveys and assessments to monitor changes in the demographic profile of PRO9 Headquarters personnel. This helps identify emerging trends and adjust training and support strategies accordingly.

2. *Recalibration of Development Procedures and Support Programs.* To ensure the successful adoption and utilization of new information systems, it is imperative to implement a robust training and support strategy. Formal training sessions conducted by experienced trainers should cover a wide range of topics, including system features, functionalities, and best practices. Technical assistance should be provided to address user queries and troubleshooting issues, and guidance should be provided as needed. This can be achieved through various channels, such as dedicated help desks, online forums, or direct one-on-one support. Prioritizing user-friendliness in the design and development of a standard user interface can significantly enhance user experience and reduce the need for extensive training. By offering continuous training and support and designing a standard user-friendly interface, the PRO9 headquarters can empower its personnel to maximize the benefits of the new information systems and minimize disruptions to operations.

3. *Enhancement of Administrative and Operational Efficiency.* Regular security audits and vulnerability assessments should be conducted to identify and address potential security risks. Implementing robust administrative controls, such as access controls and regular password changes, is crucial to limit unauthorized access to sensitive information. Data management practices should be established to ensure data integrity and availability, including data classification, backup, and recovery procedures. Comprehensive cybersecurity training should be provided to empower personnel and optimize operations, leading to more effective and informed decision-making.

4. *Adhering to Data Privacy Laws and Policies.* A comprehensive approach to data privacy and security is essential to protect sensitive information and maintain public trust. Implementing robust multi-level information system security measures, such as firewalls, intrusion detection systems, and access controls, is crucial to safeguard sensitive data. Employing database encryption techniques can further protect sensitive information by rendering it unreadable to unauthorized individuals. Strict adherence to data privacy laws and regulations is paramount. Conducting regular privacy impact assessments, implementing strong access controls, and educating employees about best data privacy practices are essential to ensure compliance. Organizations prioritizing data privacy and security can mitigate risks, maintain public trust, and avoid legal penalties.

5. *Fostering Leadership and Organizational Commitment.* Strong leadership and organizational support are crucial to successfully implementing and integrating new information systems. Top leadership should actively champion the adoption of new technologies and lead by example. Leaders can inspire and motivate personnel to embrace change by demonstrating their commitment to digital transformation. Adequate resources, including budget, personnel, and time, must be allocated to address technological, organizational, and legal challenges. This involves investing in IT infrastructure, providing comprehensive training and support, and ensuring compliance with relevant regulations to overcome obstacles and achieve successful implementation.

6. *Institutionalization of Continuous Monitoring and Improvement.* Put in place a mechanism that shall provide for periodic reviews of the effectiveness of the new systems in continuing to meet the changing needs of PRO9 Headquarters. Such reviews must be directed, among others, at the success of administrative management, accuracy of data analyses, and speed of decision-making. Iterative improvements shall have to be made in the systems based on such findings, ensuring evolution with the requirements of the organization and continued enhancements in operational efficiency.

REFERENCES

Al-Hajri, M. A., & Al-Zahrani, A. S. (2021). A Survey on Database Encryption Techniques. *Journal of Information Security Research, 16*(2), 147-163. DOI: 10.53326/jisr.v16i2.158

Alharbi, K. A. (2021). A Comprehensive Review of Cybersecurity Challenges and Solutions in Smart Cities. *International Journal of Advanced Computer Science and Applications, 12*(3), 46-57. DOI: 10.14569/IJACSA.2021.120307

Al-Raisi, F., & Al-Karaghouli, W. (2020). The impact of comprehensive training on information systems adoption in law enforcement: The case of police officers in the UAE. *Journal of Police and Criminal Psychology, 35*(2), 167-181. DOI: 10.1007/s11896-019-09355-w

Bélanger, F., & Crossler, R. E. (2021). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041. DOI: 10.25300/MISQ/2021/15462

Chan, T., Sharpe, J., & Brown, L. (2020). Police information systems: Perspectives, drivers, and issues. *Police Practice and Research, 21*(3), 264-279. DOI: 10.1080/15614263.2019.1622340

Coles-Kemp, L., & Theoharidou, M. (2020). Privacy by design: Information security risks and challenges associated with police body-worn cameras. International *Journal of Information Management, 56,* 102230. DOI: 10.1016/j.ijinfomgt.2020.102230

Cordner, G., & Scarborough, K. (2021). Overcoming organizational challenges in law enforcement. *Police Practice and Research, 22*(3), 300-315. DOI: 10.1080/15614263.2021.1916890

Heeks, R. (2020). *Digital Development: A Practical Guide.* SAGE Publications. DOI: 10.4135/9781529718712

Hong, W., & Thong, J. Y. L. (2023). How user concerns about information privacy are shaped by regulatory frameworks: The case of Singapore's Personal Data Protection Act. *Information Systems Journal, 33*(2), 241-267. DOI: 10.1111/isj.12398

Khan, M. A., & Khan, S. U. (2022). A Comprehensive Review of Cybersecurity Challenges and Mitigation Techniques in Smart Cities. *IEEE Access, 10*, 36690-36714. DOI: 10.1109/ACCESS.2022.3161273

Lutz, C., Hoffmann, E. R., & Mülders, M. (2021). Transformational leadership and IS implementation success: The moderating role of hands-on experience. *Journal of Leadership and Organizational Studies, 22*(3), 122-137. DOI: 10.1177/15480518211020087

Marangunić, N., & Granić, A. (2022). Technology acceptance model: A literature review from 1996 to 2013. *Universal Access in the Information Society, 22*(1), 123-135. DOI: 10.1007/s10209-021-00812-7

Marasambessy, R.F. (2023). Information technology-based law enforcement in increasing public trust in the police. *Gema Wiralodra, 14*(2), 790-798. DOI: 10.31943/gw.v14i2.507

McCue, C. (2020). *Data Analytics in Criminal Justice. CRC Press*. DOI: 10.1201/9780429402517

Rees, G., & Rodley, D. (2020). *The Future of Policing: Innovation, Technology, and Ethical Considerations.* Palgrave Macmillan. DOI: 10.1007/978-3-030-49658-4