



USE OF TECHNOLOGIES IN THE DETECTION OF THREATS ON AVIATION SECURITY: ACTION PLAN TOWARDS ENHANCING PASSENGERS' SAFETY

Manatad, Camilo Jr. L.
Philippine College of Criminology

Article DOI: <https://doi.org/10.36713/epra31470>
DOI No: 10.36713/epra31470

ABSTRACT

Aviation security serves as a cornerstone of the global transportation infrastructure, requiring continuous modernization to counter increasingly sophisticated physical and digital threat vectors. This study evaluated the use of technologies in the detection of threats on aviation security. Utilizing an explanatory sequential mixed-methods research design, the investigation gathered multi-stakeholder perspectives from technical and regulatory experts, operational security personnel, and traveling beneficiaries to assess key technological dimensions. The study found that aviation security technologies – including sensor systems, data analysis tools, automated monitoring, cybersecurity measures, passenger behavior analysis, and regulatory adaptations – are generally perceived as less efficient in detecting threats. Significant differences were also identified in efficiency ratings across technical and regulatory experts, operational stakeholders, and beneficiaries, indicating varying perspectives based on role and experience. In terms of issues affecting technology use, false alarm rates and training requirements were rated as serious concerns, while privacy protection, budget constraints, technology integration, and technological reliability were generally considered less serious. Significant differences in perceptions of issue severity were also observed across respondent groups. Qualitative findings revealed that cybersecurity alerts and passenger behavior sometimes do not align, requiring verification procedures, multi-agency collaboration, and professional objectivity. Challenges in using both technology and human judgment include conflicting system outputs and behavioral observations, cognitive overload in real-time operations, and uncertainty in interpreting passenger behavior. Regarding regulatory influences, findings showed that regulations both support system standardization and security while also limiting operational flexibility and affecting response speed due to compliance requirements. Finally, recommended improvements include enhancing system integration and interoperability, advancing AI and predictive analytics, strengthening training and human capacity development, improving cybersecurity and system maintenance, and promoting coordinated organizational and regulatory approaches to improve overall aviation security effectiveness.

KEYWORDS: Aviation Security, Threat Detection Technology, Cybersecurity Precautions, Behavioral Analysis, Operational Efficiency.

INTRODUCTION

Aviation security has become a cornerstone of global air transportation due to the persistent and increasingly complex evolution of threats confronting the aviation industry. These threats extend beyond conventional acts of terrorism to include organized crime, insider threats, cyber intrusions, and the misuse of emerging technologies. As air travel continues to grow in volume and connectivity, airports and airlines remain attractive targets because of their symbolic value, economic importance, and potential for mass casualties.

Consequently, ensuring the safety of passengers, crew, and critical aviation infrastructure has emerged as a global priority, compelling stakeholders to invest heavily in advanced security measures. This imperative has driven the adoption and continuous advancement of technologies specifically designed to detect, analyze, and mitigate potential dangers at airport checkpoints, airside operations, and during flight. Traditional manual screening and observational methods, which rely heavily on human judgment, are increasingly inadequate in addressing modern threat vectors that are often concealed, fast-evolving, and

technologically sophisticated. As a result, aviation security frameworks have progressively shifted toward automated and intelligent systems that enhance detection accuracy, reduce human error, and improve overall operational efficiency (International Airport Review, 2024; Number Analytics, 2024).

Emerging technologies play a critical role in strengthening aviation security across multiple operational domains, particularly in passenger screening, baggage inspection, and access control. Advanced imaging systems, such as computed tomography (CT) scanners and backscatter X-ray technologies, provide high-resolution, three-dimensional images that allow security personnel to identify concealed weapons, explosives, and prohibited items with significantly greater precision than conventional two-dimensional X-ray systems. These technologies not only improve detection capability but also streamline screening processes by reducing the need for manual bag checks and passenger re-screening, thereby enhancing passenger experience without compromising safety (IDSTCH, 2025).

In parallel, artificial intelligence (AI) and machine learning technologies are transforming aviation security by



enabling real-time data analysis and predictive threat detection. AI-driven systems are increasingly deployed in baggage screening to automatically identify suspicious items and distinguish genuine threats from harmless objects, thereby minimizing false alarms and operational delays. Furthermore, machine learning algorithms support behavior analysis by identifying anomalous passenger movements or patterns that may indicate malicious intent. These intelligent systems continuously learn from new data, making them more adaptive to emerging threats and less reliant on static rule-based approaches (IATA, as cited in Number Analytics, 2024; International Airport Review, 2024). Biometric identification technologies, including facial recognition, fingerprint scanning, and iris recognition, are also reshaping passenger authentication processes. By enabling accurate and contactless identity verification, biometrics enhance security while reducing identity fraud, document forgery, and unauthorized access to restricted areas within aviation facilities (International Airport Review, 2024; Vertel Corporation, 2025).

Moreover, the emergence of unmanned aerial systems (UAS), cyber threats, and other unconventional risks has necessitated the development of specialized detection and mitigation technologies tailored to non-traditional threat environments. Unauthorized drones pose significant risks to airport operations, including collision hazards, airspace disruption, and potential use for surveillance or delivery of hazardous materials. To counter these risks, counter-UAS systems integrate radar, acoustic sensors, electro-optical systems, and radio-frequency detection technologies to identify, track, and neutralize rogue drones in proximity to sensitive aviation zones (Wang et al., 2020). Similarly, cybersecurity solutions are increasingly incorporated into aviation security architectures to protect critical systems from digital attacks that could compromise navigation, communication, or passenger data.

The growing complexity and interdependence of these technologies underscore the need for a holistic and coordinated action plan that aligns technological innovation with robust policies, continuous personnel training, and effective regulatory oversight. Without such integration, even the most advanced technologies may fail to deliver optimal security outcomes. Therefore, aviation security must adopt a proactive, layered, and adaptive approach that evolves in response to emerging threats while maintaining efficiency and passenger confidence.

This study examines the spectrum of current aviation security technologies, evaluates their effectiveness in detecting and mitigating threats, and proposes an actionable plan aimed at enhancing passenger safety through the strategic integration of advanced technological solutions.

Theoretical Framework

This study is anchored on Routine Activity Theory as the main theoretical lens, with Situational Crime Prevention Theory and the Technology Acceptance Model serving as supporting theories. Overall, these theories provide a comprehensive explanation of how the use of advanced technologies in aviation security contributes to effective threat detection and the enhancement of passenger safety.

Routine Activity Theory, as advanced by Cohen and Felson (1979), provides a foundational explanation for the occurrence and prevention of crime by emphasizing the interaction of three critical elements: a motivated offender, a suitable target, and the absence of a capable guardian. In aviation environments, this convergence is particularly pronounced due to the high concentration of passengers, valuable infrastructure, and the symbolic significance of airports and aircraft as targets of criminal and terrorist activity. Motivated offenders in this context may include terrorists, smugglers, or individuals seeking to exploit vulnerabilities in aviation systems. The absence or weakness of effective guardianship increases the likelihood of security breaches, making aviation facilities especially susceptible to threats. The deployment of advanced security technologies transforms the security landscape by introducing capable guardians that actively monitor, detect, and respond to potential threats. Technologies such as biometric identification systems, explosive detection equipment, advanced imaging scanners, and integrated surveillance networks enhance the visibility and predictability of guardianship, thereby discouraging potential offenders and interrupting threat execution. Through continuous monitoring and rapid threat identification, these technologies reduce opportunities for criminal acts, reinforcing the relevance of Routine Activity Theory in explaining how technological guardianship directly contributes to the prevention of aviation security threats and the protection of passengers.

Building upon this foundational theory, Situational Crime Prevention Theory offers a more operational perspective by focusing on the manipulation of environmental and situational conditions to reduce criminal opportunities (Clarke, 1995). Rather than addressing the underlying motivations of offenders, the theory emphasizes practical strategies that increase the effort required to commit a crime, heighten the risks associated with offending, reduce anticipated rewards, and remove situational excuses. In aviation security settings, technological interventions are designed explicitly to achieve these objectives. Advanced passenger and baggage screening systems increase the complexity and difficulty of concealing prohibited items, while access control technologies restrict unauthorized entry into secure areas of airports. Surveillance systems, including closed-circuit television and behavior detection technologies, elevate the perceived and actual risk of detection and apprehension. By systematically closing security gaps and hardening targets, these technologies make aviation facilities less attractive to offenders. Situational Crime Prevention Theory is therefore particularly useful to this study as it provides a practical and strategic framework for the formulation of an action plan that aligns technological deployment with specific preventive objectives aimed at reducing vulnerabilities and enhancing passenger safety.

Complementing the crime prevention perspective, the Technology Acceptance Model addresses the human and organizational factors that influence the effectiveness of security technologies. Davis (1989) posits that users' acceptance of technology is primarily determined by perceived usefulness and perceived ease of use, which shape attitudes and actual usage behavior. In aviation security, even the most advanced detection



technologies can fail to achieve their intended outcomes if they are poorly understood, inadequately operated, or resisted by users. Security personnel must be confident in the reliability and efficiency of technological systems to utilize them effectively, while passengers' perceptions of fairness, convenience, and intrusiveness influence their compliance with security procedures. Technologies that are intuitive, efficient, and minimally disruptive are more likely to gain acceptance, leading to consistent and effective application. The inclusion of the Technology Acceptance Model in this study highlights the importance of training, system design, and stakeholder engagement in ensuring that security technologies function optimally as preventive tools rather than merely as symbolic measures.

In synthesis, Routine Activity Theory offers the overarching explanation for how aviation security threats can be mitigated through enhanced technological guardianship, while Situational Crime Prevention Theory explains the specific mechanisms through which security technologies reduce opportunities for criminal activity. The Technology Acceptance Model complements these perspectives by emphasizing the critical role of human interaction, acceptance, and proper utilization in the successful implementation of security systems. Together, these theories provide a robust and integrated framework for analyzing the use of technologies in threat detection and for developing an evidence-based action plan aimed at strengthening aviation security and enhancing passenger safety.

Statement of the Problem

This study aimed to assess the use of technologies in the detection of threats on aviation security as the basis for an action plan towards enhancing passengers' safety.

Specifically, the study aimed to answer the following questions:

1. What is the level of efficiency of the use of technologies in the detection of threats in aviation security in terms of:

- 1.1 Use of sensor technology
- 1.2 Data analysis combination
- 1.3 Automated monitoring systems
- 1.4 Cybersecurity precautions
- 1.5 Passenger behavior analysis
- 1.6 Aviation regulatory adaptations

2. Is there a significant difference in the level of efficiency of the use of technologies in the detection of threats in aviation security in terms of the identified variables according to operational security stakeholders, technical and regulatory experts, and beneficiaries?

3. What is the degree of seriousness of the issues affecting the use of technologies in the detection of threats in aviation security in terms of:

- 2.1 False alarm rates
- 2.2 Privacy protection
- 2.3 Budget constraints
- 2.4 Technology integration
- 2.5 Technological reliability

2.6 Training requirements

4. Is there a significant difference in the degree of seriousness of the issues affecting the use of technologies in the detection of threats in aviation security in terms of the identified variables according to group?

5. What are the experiences of aviation security personnel with cybersecurity measures and analyzing passenger behavior during real threat detection?

6. How do regulatory requirements influence the efficiency of security technologies in airports?

7. What are the measures recommended to address the issues affecting the use of technologies in the detection of threats in aviation security?

8. What action plan towards enhancing passengers' safety can be formulated as an outcome of the study?

METHODOLOGY

This study employed a **mixed methods research approach using an Explanatory Sequential Mixed Methods Design**, which involves the collection and analysis of quantitative data followed by qualitative data to explain and elaborate on the quantitative findings (Creswell & Plano Clark, 2018). This design was appropriate because the study sought to determine the efficiency of aviation security technologies while also understanding the experiences, challenges, and contextual factors that influenced their implementation and effectiveness.

The **quantitative phase** measured the level of efficiency of aviation security technologies in terms of sensor technologies, automated monitoring systems, data analysis integration, cybersecurity precautions, passenger behavior analysis, and regulatory adaptations. Structured questionnaires were administered to operational security stakeholders, technical and regulatory experts, and beneficiaries to generate numerical data on technology efficiency, performance patterns, and significant differences among respondent groups. The quantitative results provided the baseline for identifying areas requiring further explanation.

The **qualitative phase** followed the quantitative analysis and explored the experiences, perceptions, and operational realities of aviation security personnel and other stakeholders. Interviews and focus group discussions were conducted to explain the quantitative findings, particularly regarding cybersecurity measures, passenger behavior analysis, regulatory influences, operational challenges, and strategies for improving threat detection. The qualitative findings provided contextual explanations for the observed quantitative results and helped clarify factors that contributed to the efficiency or limitations of specific technologies.

The integration of the quantitative and qualitative findings enabled the study to obtain a more comprehensive understanding of aviation security technology efficiency. The qualitative results were used to explain and contextualize the quantitative findings, thereby strengthening the interpretation and credibility of the results. Ultimately, the integrated findings served as the basis for developing an **evidence-based action plan** aimed at improving



the use of aviation security technologies, strengthening threat detection, and enhancing passenger safety.

Table 1. Respondents of the Study

Respondent	Population	Sample Size
Operational security stakeholders (Aviation security personnel and airport authorities)	420	201 (Raosoft)
Technical and regulatory experts (Technology experts, aviation regulatory bodies)	40	40 (Total enumeration)
Beneficiaries (Passengers)	Undetermined	128 (Convenience Sampling)
Total		369

The population of this study consists of three primary groups representing critical perspectives on aviation security and the use of technologies for threat detection: **(1) operational security stakeholders, (2) technical and regulatory experts, and (3) beneficiaries**. These groups were selected to provide comprehensive perspectives on the operational, technical, regulatory, and user dimensions of aviation security technologies. The inclusion of these three groups reflects the **multi-stakeholder nature of aviation security**, allowing the study to examine technology efficiency from complementary perspectives. The operational stakeholders provide practical and implementation-based insights, the technical and regulatory experts contribute specialized and compliance-related perspectives, and the beneficiaries provide user-centered experiences. Collectively, these perspectives support a more comprehensive assessment of aviation security technologies and provide relevant evidence for explaining the quantitative findings and developing an evidence-based action plan to enhance threat detection and passenger safety.

Further, this was conducted at Ninoy Aquino International Airport (NAIA) in Metro Manila and Mactan-Cebu International Airport (MCIA) in Cebu, Philippines. These airports were specifically chosen due to their strategic importance, passenger volume, and the complexity of aviation security operations.

A **researcher-developed survey questionnaire** based on related literature, aviation security frameworks, and relevant studies was used for the quantitative phase. It consisted of three parts: **(1) respondent profile, (2) efficiency of aviation security technologies in terms of sensor technology, data analysis combination, automated monitoring systems, cybersecurity precautions, passenger behavior analysis, and regulatory adaptations, and (3) seriousness of issues affecting technology use, including false alarms, privacy, budget, technology integration, reliability, and training. A four-point Likert scale** was used.

For the qualitative phase, a **semi-structured interview guide** was used to explore participants' experiences, challenges, regulatory influences, and recommended strategies related to aviation security technologies. Relevant aviation security **policies, regulations, guidelines, and international standards** were also reviewed to support and triangulate the findings.

Before data collection, the instruments underwent appropriate **validation**, and permission was obtained from the concerned authorities. Informed consent, confidentiality,

anonymity, and voluntary participation were observed throughout the study. The integrated findings from the **survey, interviews, and document analysis** served as the basis for developing the proposed action plan.

The quantitative data were analyzed using **SPSS Version 26. Frequency and percentage** were used to summarize the respondents' profiles, while the **median** was used to determine the level of technology efficiency and seriousness of issues due to the ordinal nature of the four-point Likert scale.

The **Kruskal-Wallis H test** was used to determine significant differences among the three respondent groups. When significant differences were found, the **Dunn-Bonferroni post hoc test** was applied to identify the specific groups that differed. All inferential tests were conducted at the **0.05 level of significance**.

The findings from the quantitative and qualitative phases, together with the document analysis, were integrated to provide the basis for the proposed action plan.

RESULTS AND DISCUSSIONS

Level of Efficiency of the Use of Technologies in the Detection of Threats in Aviation Security

Use of Sensor Technology. The overall median of 2.00 (Less Efficient) for the use of sensor technology in aviation security. Technical and Regulatory Experts rated all indicators Efficient (Median = 3.00), reflecting confidence in the capability of sensor technologies to detect threats, provide rapid alerts, operate reliably, provide adequate coverage, integrate multiple systems, and support maintenance. In contrast, Operational Security Stakeholders and Beneficiaries generally rated the indicators Less Efficient (Median = 2.00), indicating limitations in practical implementation, system integration, coverage, and real-world reliability.

The disparity among respondent groups suggests a gap between the technical capability of sensor technologies and their operational performance and user experience. The findings indicate the need to improve system integration and coverage, strengthen interoperability, provide adequate personnel training, and conduct regular system evaluation and maintenance. Greater coordination among technology developers, regulators, security personnel, and other stakeholders is also necessary to align technological capabilities with operational requirements.

Foreign literature supports the experts' higher ratings. Demir (2024) found that AI-enabled biometric systems can



improve threat detection and real-time decision-making, while Wang, Ismail, and Breckon (2019) demonstrated the effectiveness of 3D CT-based automated threat recognition in detecting concealed threats. However, other studies emphasize that the effectiveness of automated detection technologies depends on proper calibration, validation, and integration (Wang, Megherbi, & Breckon, 2020; Riz à Porta et al., 2022). Local sources likewise indicate that advanced airport technologies require human oversight, training, reliable data management, and effective system integration (DOTr & UltraPass, 2024; BOC Enhances Airport Security, 2026; Dela Peña et al., 2024). Thus, the literature supports the contrast between the experts' Efficient assessment and the Less Efficient ratings of operational stakeholders and beneficiaries.

The qualitative findings further explain the lower ratings. Operational Security Stakeholders reported instances in which sensor- or cybersecurity-generated alerts were later identified as false positives after verification. For example, OSS 1 reported that repeated booking modifications triggered an alert, but further checking showed that the passenger was a legitimate business traveler. Similarly, OSS 5 noted that an alert based on a passenger's travel profile was later determined to be a false positive. Other participants described cases involving VPN use, compromised systems used by travel agencies, and payment-processing errors, demonstrating that alerts alone were insufficient to establish the presence of a genuine threat.

The findings also show that multi-agency collaboration and human verification are essential to effective sensor-based threat detection. Participants emphasized coordination with airline personnel, intelligence officers, cybersecurity specialists, and law enforcement before clearing flagged passengers. These experiences explain the lower ratings for sensor accuracy, coverage, and integration and demonstrate that technology is most effective when supported by behavioral assessment, intelligence verification, and professional judgment.

Overall, the findings indicate that sensor technologies provide valuable early-warning and threat-detection capabilities, but their effectiveness is constrained by false positives, integration limitations, contextual factors, and the need for human verification. Therefore, maximizing their contribution to aviation security requires not only technological improvements but also interoperability, continuous training, system maintenance, and strengthened inter-agency coordination.

Data Analysis Combination. The overall findings indicate a median score of 2.00 (Less Efficient) for data analysis combination, although accuracy of predictive threat identification and data visualization effectiveness for decision-making received an overall median of 3.00 (Efficient). Technical and Regulatory Experts rated all indicators as Efficient, reflecting confidence in data integration, AI/ML, predictive analytics, real-time processing, interoperability, and visualization. In contrast, Operational Security Stakeholders and Beneficiaries generally rated these indicators as Less Efficient, indicating challenges in practical implementation and utilization.

The findings suggest a gap between the technical capabilities of data analysis technologies and their operational

application. The lower ratings highlight the need to strengthen data integration, interoperability, real-time processing, system reliability, personnel training, and user confidence. Conversely, the favorable ratings for predictive threat identification and data visualization demonstrate the value of analytics in improving situational awareness, decision-making, and proactive threat detection.

Foreign literature supports these findings. Studies indicate that AI and ML can improve threat detection accuracy and predictive capabilities but remain dependent on data quality, system integration, usability, and human-machine interaction (Pik, 2024; Wang et al., 2019; Xu et al., 2022). Interoperability challenges associated with legacy infrastructure, multiple platforms, and inconsistent data standards may also limit operational effectiveness (Akcaay & Breckon, 2020). Philippine studies similarly identify infrastructure limitations and fragmented system implementation as challenges to airport technology modernization (Tribune, 2022). These findings demonstrate that technological capability alone does not guarantee effective operational performance.

The qualitative findings further explain the lower assessments. Participants reported that cybersecurity alerts frequently required cross-checking with airline records, document verification, interviews, secondary screening, and coordination with cybersecurity and intelligence personnel before decisions could be made. Some alerts involving unusual booking modifications, VPN use, compromised systems, and unusual login locations were ultimately determined to be legitimate activities or technical issues. These experiences indicate that analytical systems can identify anomalies but may have difficulty distinguishing legitimate behavior from actual threats without contextual information and human verification.

Similarly, although participants acknowledged that systems could detect suspicious activities in real time, alerts often required additional investigation before operational action could be taken. This explains the lower assessment of real-time processing and demonstrates that rapid detection does not necessarily translate into immediate threat resolution.

In contrast, participants recognized the usefulness of predictive threat identification and data visualization in identifying suspicious patterns and supporting decision-making. However, the findings emphasize that these technologies function most effectively as decision-support tools rather than standalone threat detection mechanisms. Human judgment, professional objectivity, training, and multi-agency collaboration remain essential in validating technological outputs.

Overall, the findings show that data analysis technologies contribute significantly to aviation security through anomaly detection, predictive analysis, and improved situational awareness. However, their practical efficiency is constrained by data integration and interoperability issues, false positives, system limitations, and the need for human interpretation and coordination. Strengthening these areas is therefore essential to maximize the contribution of data analysis technologies to aviation security and threat detection.



Automated Monitoring Systems. The findings show an overall median of 2.00 (Less Efficient) for automated monitoring systems. Technical and Regulatory Experts rated all indicators Efficient (Median = 3.00), reflecting confidence in surveillance automation, automated threat detection, alert response, infrastructure integration, system reliability, and workload reduction. In contrast, Operational Security Stakeholders and Beneficiaries generally rated the indicators Less Efficient (Median = 2.00). Operational stakeholders recognized the efficiency of automated alerts and workload reduction but expressed concerns about surveillance coverage, threat detection accuracy, system integration, and reliability during continuous operation.

The findings indicate a gap between the technical capabilities of automated monitoring systems and their practical operational performance. While automation facilitates continuous surveillance, rapid alerts, and reduced manual workload, its effectiveness is limited by false positives, integration challenges, reliability concerns, and continued dependence on human verification. Improving detection algorithms, interoperability, system maintenance, redundancy, and personnel training may strengthen operational effectiveness and user confidence.

Foreign literature supports both perspectives. Demir (2024) and Arora, Rathore, and Gautam (2019) highlight the capacity of AI-driven systems to enhance continuous surveillance, threat detection, and real-time decision-making. However, Vukadinovic (2021) and Riz à Porta, Sterchi, and Schwaninger (2022) note that automated systems may generate false positives and require careful validation under real-world conditions. Local initiatives and studies likewise indicate that advanced airport technologies require human oversight, coordination, reliable infrastructure, and effective cybersecurity measures (DOT; BOC Enhances Airport Security, 2026; Dela Peña, 2025). These findings help explain the higher ratings of experts and the lower assessments of operational stakeholders and beneficiaries.

The qualitative findings further explain the Less Efficient ratings for surveillance automation, automated threat detection, infrastructure integration, and continuous reliability. Participants reported instances in which automated systems flagged unusual booking activities, login locations, reservation accounts, and electronic transactions that were later determined to involve legitimate activities, VPN use, compromised systems, or payment-processing errors. These experiences demonstrate that automated systems can effectively identify anomalies but may not always distinguish genuine threats from legitimate behavior.

In contrast, participants confirmed the value of automated systems as early-warning mechanisms. Automated monitoring was able to identify suspicious Wi-Fi access, reservation activity, phishing incidents, communication patterns, and failed authentication attempts, allowing security personnel to initiate timely investigation and response. Continuous automated monitoring also reduced the need for personnel to manually observe every digital activity, supporting the Efficient rating for workload reduction.

The qualitative findings further emphasized that automated alerts require human verification, professional judgment, and multi-agency coordination. Participants described the use of secondary screening, document verification, interviews, and coordination with cybersecurity teams, airline personnel, intelligence officers, and law enforcement agencies before making final security decisions. The themes on resolving discrepancies between automated alerts and passenger behavior, multi-agency collaboration, and maintaining professional objectivity reinforce the importance of human involvement.

Overall, automated monitoring systems provide valuable capabilities for continuous surveillance, rapid alert generation, and workload reduction, but their effectiveness is constrained by false positives, integration limitations, reliability concerns, and the need for human interpretation. Thus, automated monitoring technologies should function primarily as decision-support and early-warning mechanisms that complement rather than replace human expertise and professional judgment in aviation security operations.

Cybersecurity Precautions. The overall median score of 2.00 (Less Efficient) indicates that cybersecurity precautions were not perceived as fully effective by most respondents. Technical and Regulatory Experts consistently rated all indicators 3.00 (Efficient), reflecting confidence in network security controls, incident detection and response, data protection, cybersecurity awareness, backup and recovery, and compliance with standards. In contrast, Operational Security Stakeholders and Beneficiaries generally rated the indicators 2.00 (Less Efficient). Operational Security Stakeholders viewed passenger and operational data protection and compliance with cybersecurity standards as efficient, but rated network security controls, incident response, cybersecurity awareness and training, and backup and recovery as less efficient. Beneficiaries rated all indicators as less efficient.

The findings highlight the need to strengthen network security, incident response, staff preparedness, and operational resilience. Continuous monitoring, vulnerability management, advanced cybersecurity solutions, regular training, improved incident response procedures, and stronger backup and disaster recovery mechanisms are needed. Although data protection and regulatory compliance were viewed positively, the divergence between expert and end-user assessments suggests that established cybersecurity policies may not always translate into effective operational implementation or visible protection for users.

These findings are consistent with foreign and local literature. Zhao et al. (2020) and Hasan et al. (2023) noted that although AI-driven cybersecurity systems improve anomaly detection and predictive capabilities, implementation complexity, integration challenges, and operational readiness can limit their effectiveness. Pik (2024) emphasized that inadequate user awareness and training remain significant cybersecurity vulnerabilities, while Abuan et al. (2024) highlighted the importance of continuous capacity-building and staff preparedness in Philippine aviation. Hasan et al. (2023) further stressed the importance of robust backup and disaster recovery



systems for maintaining continuity in highly digitized aviation environments. Pik (2024) also emphasized the role of regulatory alignment with cybersecurity standards in protecting sensitive aviation information.

The qualitative findings further explain the quantitative results. Several participants described incidents involving compromised accounts, unauthorized access, and phishing that were successfully detected through cybersecurity measures. OSS 15 reported that an alert indicated possible unauthorized access to a passenger's account and, after coordination with the cyber unit, confirmed that "the account had indeed been compromised by a third party." Similarly, OSS 12 reported a suspected phishing incident in which the passenger was later determined to be "a victim rather than a suspect." These accounts demonstrate the value of cybersecurity measures in identifying threats and protecting passenger and operational information.

The qualitative findings also support the favorable assessment of Compliance with Cybersecurity Standards and Best Practices, which obtained an overall median of 3.00 (Efficient). Participants described consistently following established procedures when cybersecurity alerts conflicted with passenger behavior. OSS 10 reported that he "followed escalation procedures and coordinated with cybersecurity specialists before clearing the passenger," while OSS 15 stated that he "followed established security protocols, coordinated with the cyber unit, and waited for confirmation before allowing the passenger to proceed." These responses demonstrate that established cybersecurity protocols, escalation procedures, and inter-unit coordination are being applied in actual operations.

Overall, cybersecurity precautions provide important capabilities for detecting cyber threats, protecting sensitive information, and supporting secure aviation operations. However, their perceived effectiveness remains constrained by operational implementation gaps, human factors, incident response limitations, and concerns about system resilience. Strengthening staff capacity, cybersecurity monitoring, response mechanisms, backup systems, and communication with end users is therefore essential to improving both operational effectiveness and confidence in aviation cybersecurity measures.

Passenger Behavior Analysis. The overall median score of 2.00 (Less Efficient) indicates that technologies used in passenger behavior analysis were generally perceived as less efficient. Technical and Regulatory Experts rated all indicators 3.00 (Efficient), reflecting confidence in the effectiveness of technologies supporting threat detection and security operations. In contrast, Operational Security Stakeholders and Beneficiaries generally rated the indicators 2.00 (Less Efficient). Operational Security Stakeholders, however, rated incident detection and response capability and protection of passenger and operational data as 3.00 (Efficient), while Beneficiaries rated all indicators as less efficient.

The findings indicate a need to strengthen the operational effectiveness, reliability, usability, and transparency of technologies used in passenger behavior analysis. Although incident detection and response and data protection were viewed more favorably, continued system evaluation, modernization,

technological upgrades, and personnel training are necessary. The difference between expert assessments and stakeholder and beneficiary perceptions also suggests the need for greater stakeholder engagement and clearer demonstration of how these technologies support passenger security.

These findings are consistent with Hunt and Tamasi (2020), who emphasized that aviation security is strengthened when technological threat detection is integrated with human behavioral assessment and staff decision-making. Hunt (2021) similarly highlighted the importance of passenger behavior in interpreting security alerts and resolving inconsistencies between technological outputs and actual passenger conduct. These studies reinforce the view that automated and cybersecurity systems are most effective when complemented by human observation and professional judgment.

The qualitative findings further explain the quantitative results. Participants described situations in which passenger behavior was used to assess the credibility of cybersecurity alerts and determine appropriate responses. OSS 2 reported that although a passenger's account triggered an alert because of an unusual login location, there were "no signs of nervousness or suspicious behavior." The passenger was therefore subjected to secondary screening and document verification before being cleared. Similarly, OSS 10 explained that despite the discrepancy between the alert and the passenger's calm and cooperative behavior, he "followed escalation procedures and coordinated with cybersecurity specialists before clearing the passenger." These accounts demonstrate how behavioral assessment supports appropriate verification and threat-response decisions.

The qualitative findings also support the favorable assessment of Protection of Passenger and Operational Data, which obtained an overall median of 3.00 (Efficient). Behavioral observations helped distinguish legitimate passengers from potential cyber threats and prevented unnecessary action against innocent travelers. OSS 12 reported that a traveler associated with a possible phishing incident behaved normally and was later confirmed to be "a victim rather than a suspect." Likewise, OSS 15 described a passenger whose normal behavior contrasted with an alert indicating possible unauthorized account access; coordination with the cyber unit eventually confirmed that the account had been compromised by a third party.

Overall, passenger behavior analysis serves as an important human-centered complement to cybersecurity and automated threat-detection technologies. It enables security personnel to interpret alerts, validate potential threats, minimize false positives, and make informed decisions. The findings therefore support the efficient ratings for incident detection and response and data protection while emphasizing that technological systems should complement, rather than replace, human observation and professional judgment in aviation security operations.

Aviation Regulatory Adaptations. The overall median score of 2.00 (Less Efficient) indicates that aviation regulatory adaptations were generally perceived as less efficient in supporting technology-based threat detection. Technical and Regulatory Experts rated all indicators 3.00 (Efficient), reflecting



confidence in regulatory alignment, enforcement, clarity, responsiveness, flexibility, and stakeholder participation. In contrast, Beneficiaries rated all indicators 2.00 (Less Efficient). Operational Security Stakeholders provided mixed assessments, rating regulatory enforcement, guideline clarity, and stakeholder involvement as 3.00 (Efficient), but rating alignment with international standards, responsiveness to emerging regulations, and flexibility in addressing evolving threats as 2.00 (Less Efficient).

The findings highlight the need for more adaptive, responsive, and operationally relevant regulatory frameworks. Policies should keep pace with technological developments and emerging threats while maintaining alignment with international aviation security standards. Although enforcement and guideline clarity were viewed positively, continuous updating of regulations, clear communication, and stronger stakeholder participation are needed. The disparity between expert and beneficiary perceptions also suggests the importance of transparency and public communication to improve understanding and confidence in aviation security regulations.

These findings are supported by the International Civil Aviation Organization (ICAO, 2025), which emphasizes the importance of global standards and appropriate regulatory frameworks for integrating technologies such as AI, biometrics, and automated detection systems. Similarly, the International Air Transport Association (IATA, 2024) stresses the need for clear, enforceable, and adaptive regulations that can respond to emerging threats and be consistently applied in operational environments. These findings reinforce the observed gap between policy-level confidence among experts and implementation challenges perceived by operational stakeholders.

The qualitative findings further explain the quantitative results. Participants consistently demonstrated compliance with established procedures when responding to cybersecurity alerts. OSS 10 reported that despite a mismatch between the alert and passenger behavior, he “followed escalation procedures and coordinated with cybersecurity specialists before clearing the passenger.” Similarly, OSS 15 stated that he “followed established security protocols, coordinated with the cyber unit, and waited for official confirmation before allowing the passenger to proceed.” These responses demonstrate effective regulatory enforcement through adherence to prescribed procedures and escalation mechanisms.

The qualitative findings also support the favorable assessment of Clarity of Regulatory Guidelines, which obtained an overall median of 3.00 (Efficient). Participants demonstrated clear understanding of the procedures required when cybersecurity alerts and passenger behavior did not align. OSS 2 referred the passenger for secondary screening and document verification, while OSS 11 maintained professional objectivity, conducted the required security interview, and forwarded the case for technical review. The consistency of these practices indicates that established guidelines provide clear direction for managing potential threats and resolving alert-behavior discrepancies.

Overall, aviation regulatory adaptations provide an essential framework for guiding technology-supported security

operations. While enforcement and procedural clarity are strengths, the findings point to the need for more responsive regulations, stronger alignment with international standards, continuous policy updating, and greater stakeholder engagement. Ensuring that regulatory frameworks evolve alongside technology and emerging threats is essential for translating policy requirements into effective and consistent aviation security practices.

Significant Difference in the Level of Efficiency of the Use of Technologies in the Detection of Threats in Aviation Security According to Group

The findings indicate statistically significant differences in the perceived efficiency of technologies used in aviation threat detection across the three respondent groups—Operational Security Stakeholders, Technical and Regulatory Experts, and Beneficiaries. All six dimensions—Use of Sensor Technology, Data Analysis Combination, Automated Monitoring Systems, Cybersecurity Precautions, Passenger Behavior Analysis, and Aviation Regulatory Adaptations—obtained p-values of .001, which are below the 0.05 significance level. Thus, the null hypothesis was rejected for all dimensions. The high H-values, ranging from 299.139 to 304.135, further indicate substantial variation in the assessments of the three groups.

These differences suggest that respondents' expertise, experience, and exposure to aviation security technologies influence their perceptions of efficiency. Technical and Regulatory Experts tend to assess technologies based on technical capabilities, system performance, and regulatory compliance, whereas Operational Security Stakeholders and Beneficiaries are more likely to focus on usability, reliability, practical application, and observable outcomes. This pattern is consistent with Pik (2024), who noted that perceptions of technology effectiveness may vary according to users' technical knowledge, system familiarity, and functional responsibilities.

The significant differences in sensor technology and automated monitoring systems are consistent with Wang et al. (2019) and Wang et al. (2020), who emphasized that the effectiveness of advanced imaging, AI-supported screening, and automated surveillance may be affected by environmental conditions, system integration, and human interaction. Similarly, the differences in data analysis and cybersecurity precautions are consistent with Zhao et al. (2020) and Pik (2024), who identified implementation complexity, interpretability, and user trust as factors that may influence perceptions of technology effectiveness.

For passenger behavior analysis, the significant difference may be attributed to the complexity of interpreting human behavior alongside technology-generated information. Hasan et al. (2023) emphasized that behavioral monitoring is influenced by data quality, contextual interpretation, and ethical considerations. Meanwhile, differences in aviation regulatory adaptations suggest that although regulatory frameworks may be technically sound, their practical implementation and visibility may vary across stakeholder groups. This reinforces the



importance of translating policy requirements into consistent operational practices.

The findings have important implications for aviation security technology implementation. The divergence among respondent groups highlights the need for improved communication, continuous training, stakeholder education, and participatory implementation. Operational personnel and beneficiaries should be involved in the planning, implementation, and evaluation of security technologies to ensure that systems address actual operational needs and user concerns. Regular assessment of both technical performance and user experience is

also necessary to identify implementation gaps and strengthen stakeholder confidence.

Overall, the significant differences across all six dimensions demonstrate that the effectiveness of aviation security technologies is influenced not only by technical performance but also by user experience, operational context, familiarity, and stakeholder engagement. Bridging the perceptual gap among experts, operational stakeholders, and beneficiaries is essential to ensure that aviation security technologies are technically capable, operationally practical, and effectively accepted in real-world environments.

Table 2. Significant Difference in the Level of Efficiency of the Use of Technologies in the Detection of Threats in Aviation Security According to Group

Variable	H-value	p-value	Decision	Interpretation
Use of Sensor Technology	303.943	.001	Reject Ho	Significant
Data Analysis Combination	304.135	.001	Reject Ho	Significant
Automated Monitoring Systems	302.714	.001	Reject Ho	Significant
Cybersecurity Precautions	300.217	.001	Reject Ho	Significant
Passenger Behavior Analysis	299.139	.001	Reject Ho	Significant
Aviation Regulatory Adaptations	301.629	.001	Reject Ho	Significant

Degree of Seriousness of the Issues Affecting the Use of Technologies in the Detection of Threats in Aviation Security

This section presents the degree of seriousness of the issues affecting the use of technologies in the detection of threats in aviation security in terms of identified variables.

False Alarm Rates. The overall median score of 3.00 (Serious) indicates that false alarm rates are a significant issue affecting the use of technologies in aviation threat detection. Technical and Regulatory Experts rated all indicators 2.00 (Less Serious), suggesting greater confidence in the ability of existing technologies and procedures to manage false alarms. In contrast, Operational Security Stakeholders and Beneficiaries generally rated the indicators 3.00 (Serious). Operational Security Stakeholders identified false negatives, resource wastage, alarm fatigue, and the costs of investigating false alarms as serious concerns, while Beneficiaries rated most indicators as serious.

The findings highlight the operational consequences of false alarms and missed detections. False negatives are particularly concerning because undetected threats may directly compromise aviation security. Meanwhile, frequent false alarms can consume personnel and other resources, contribute to alarm fatigue, increase workload, and potentially reduce vigilance toward genuine threats. The financial costs associated with investigating false alarms further emphasize the need for more accurate and reliable detection technologies. Although operational delays and passenger inconvenience may be less consistently perceived as serious, repeated screening can still affect passenger flow and airport efficiency. Continuous improvement of detection algorithms, screening systems, and integrated analytics is therefore necessary to reduce both false positives and false negatives.

These findings are consistent with Vukadinovic (2021), who noted that AI-based X-ray and automated screening systems remain susceptible to false positives that can require additional

screening and disrupt airport operations. Similarly, Riz à Porta, Sterchi, and Schwaninger (2022) emphasized the importance of proper calibration and validation, noting that variations in automated system outputs may result in missed threats and unnecessary alarms, increasing workload and reducing operator efficiency. These studies reinforce the finding that false alarms remain an important operational limitation despite advances in automated threat detection.

The qualitative findings further explain the quantitative results. OSS 11 described an instance when equipment generated a false alarm, requiring additional screening despite the possibility of a technical problem. The participant noted that the incident affected passenger flow. This illustrates how inaccurate alerts can result in unnecessary security procedures and operational delays. Similarly, OSS 3 reported that during peak travel hours, multiple alerts were generated simultaneously, making it difficult to determine which required immediate attention while monitoring passenger behavior in a crowded environment. This demonstrates how excessive alerts can increase cognitive workload, strain available resources, and make prioritization of genuine threats more difficult.

Overall, the findings demonstrate that false alarm rates constitute a serious operational challenge in technology-supported aviation security. While technological systems enhance threat detection, excessive or inaccurate alerts may lead to unnecessary screening, resource wastage, alarm fatigue, passenger disruption, and increased costs. Strengthening system calibration, validation, accuracy, and integration, together with effective human oversight and alert prioritization, is essential to minimize false alarms while maintaining reliable detection of genuine threats.

Privacy Protection. The overall median score of 2.00 (Less Serious) indicates that privacy protection issues were generally perceived as less serious across all respondent groups.



However, notable differences emerged among the groups. Technical and Regulatory Experts consistently rated all indicators 2.00 (Less Serious), reflecting confidence in existing privacy safeguards, data protection mechanisms, and regulatory frameworks. Operational Security Stakeholders also generally rated privacy concerns as less serious, except for the ineffectiveness of data anonymization techniques and lack of transparency in data collection and storage, which they rated 3.00 (Serious). In contrast, Beneficiaries rated all indicators 3.00 (Serious), reflecting stronger concerns about unauthorized access, data anonymization, intrusive surveillance, regulatory compliance, transparency, and the ethical use of biometric information.

The findings highlight the importance of strengthening privacy safeguards, transparency, data anonymization, and ethical data management in aviation security. Concerns among beneficiaries regarding biometric and personal information indicate the need for clear data-handling policies, stronger privacy-preserving technologies, continuous compliance monitoring, and accessible communication regarding how passenger information is collected, stored, and used. The disparity between experts and beneficiaries also suggests the need for greater public education and transparency to strengthen trust and acceptance of security technologies.

These findings are supported by Dela Peña et al. (2024), who noted that biometric and automated identification technologies improve aviation security while raising concerns about data storage, unauthorized access, and privacy risks. Similarly, the European Commission (2022) emphasized that surveillance and biometric technologies should be accompanied by strong data protection, transparency, and ethical safeguards to protect passenger rights and maintain public trust. These studies reinforce the need to balance technological security capabilities with privacy protection.

The qualitative findings further explain the quantitative results. OSS 15 described a situation in which passenger behavior appeared inconsistent with the absence of a system alert, creating a challenge in deciding whether to conduct additional screening while respecting passenger rights. This illustrates the need to balance effective security intervention with the protection of privacy and individual dignity. Similarly, OSS 8 reported that an automated monitoring system identified unusual activity even though the passenger appeared normal. The participant emphasized the challenge of avoiding complacency while still treating the passenger respectfully, highlighting the importance of ethical and professional judgment when using surveillance technologies.

Overall, privacy protection is an important consideration in the implementation of aviation security technologies. Although security personnel and experts generally viewed privacy concerns as less serious, the stronger concerns expressed by beneficiaries demonstrate the need for transparent data practices, effective privacy safeguards, ethical use of biometric and surveillance technologies, and respect for passenger rights. Maintaining this balance is essential for strengthening both aviation security and public trust in technology-based security measures.

Budget Constraints. The overall median score of 2.50 (Less Serious) indicates that budget constraints were generally perceived as less serious across the respondent groups. However, perceptions varied considerably. Technical and Regulatory Experts rated all indicators 2.00 (Less Serious), suggesting that they viewed existing financial resources and funding mechanisms as generally adequate. Operational Security Stakeholders provided mixed assessments, identifying insufficient funding allocation, high procurement costs, and limited budgets for software and hardware upgrades as 3.00 (Serious), while rating maintenance costs, government funding dependence, and implementation delays as less serious. Beneficiaries rated all indicators 3.00 (Serious), reflecting stronger concerns regarding the financial challenges affecting aviation security technologies.

The findings indicate that financial limitations may affect the acquisition, modernization, maintenance, and sustainability of aviation security technologies. Insufficient funding and limited upgrade budgets may delay the adoption of advanced systems and reduce the capacity to respond to emerging threats. High procurement costs further highlight the need for cost-effective acquisition strategies, long-term financial planning, and prioritization of technologies with the greatest security benefits. Although dependence on government funding was generally viewed as less serious, diversified and sustainable funding mechanisms remain important. Greater transparency in funding priorities may also help strengthen public confidence in aviation security investments.

These findings are supported by Future Market Insights (2024), which noted that AI-driven screening, biometric authentication, and automated threat detection systems involve substantial procurement and implementation costs that may constrain adoption, particularly in resource-limited aviation systems. Similarly, Abuan et al. (2024) emphasized that Philippine airport security improvements may be constrained by limited resources for training, maintenance, and system upgrades, highlighting the importance of sustained financial support beyond the initial acquisition of technology. These findings reinforce the role of adequate and sustainable funding in maintaining effective aviation security technologies.

The qualitative findings further explain the quantitative results. OSS 13 identified insufficient training on new technologies as a challenge, noting that even when a system generates an alert, personnel may require additional assessment to understand its meaning. This suggests that limited investment in training and capacity development can affect personnel's ability to effectively utilize advanced security technologies. OSS 11 similarly described an equipment-related false alarm that required additional screening and affected passenger flow, illustrating how technology problems may generate additional operational demands and resource requirements.

Overall, the findings indicate that budget constraints can influence the effectiveness of aviation security technologies through limitations in training, system maintenance, upgrades, and operational efficiency. Although the overall assessment was Less Serious, the concerns expressed by Operational Security Stakeholders and Beneficiaries demonstrate that financial



limitations remain relevant to the sustainable implementation and modernization of threat detection technologies. Strategic resource allocation, continuous investment in personnel and technology, and sustainable funding mechanisms are therefore essential to maintaining effective aviation security operations.

Technology Integration. The overall median score of 2.50 (Less Serious) indicates that technology integration issues were generally perceived as less serious. However, perceptions varied across respondent groups. Technical and Regulatory Experts consistently rated all indicators 2.00 (Less Serious), suggesting that system incompatibility, integration complexity, interoperability limitations, redundancies, lack of standardization, and technical complexity are manageable within existing frameworks. In contrast, Operational Security Stakeholders and Beneficiaries generally rated most indicators 3.00 (Serious), particularly incompatibility between systems, difficulty integrating multi-vendor technologies, and data silos resulting from poorly integrated architectures. Both groups, however, rated limited interoperability, lack of standardization, and technical complexity as less serious.

The findings indicate that system compatibility and seamless integration remain important challenges in aviation security operations. Incompatibility between legacy and newly acquired systems and difficulties integrating multi-vendor technologies may result in fragmented workflows, data silos, duplicated efforts, and reduced situational awareness. These challenges highlight the need for standardized protocols, improved data-sharing mechanisms, interoperable systems, and user-friendly technologies. Greater involvement of operational personnel in system design, deployment, and evaluation is also necessary to ensure that technically feasible solutions address actual operational requirements.

The findings are consistent with Akcay and Breckon (2020), who identified interoperability challenges when advanced AI and sensor-based technologies are introduced into existing infrastructure. Similarly, Wang et al. (2020) noted that multi-vendor environments may create inconsistent data formats and integration difficulties, while Zhao et al. (2020) emphasized that fragmented systems can reduce situational awareness and delay security responses. Pik (2024) further highlighted the importance of standardization for scalability and interoperability, while Abuan et al. (2024) emphasized the need for continuous training and skilled personnel in managing complex security technologies.

The qualitative findings further explain the quantitative results. OSS 7 described the difficulty of simultaneously monitoring a cybersecurity alert and actual passenger movement, illustrating the challenge of coordinating technical systems with real-time operational activities. Similarly, OSS 4 identified information overload as a major challenge, noting that personnel receive alerts from different systems while simultaneously monitoring passengers face-to-face. These experiences demonstrate how fragmented information sources and multiple alert streams can complicate decision-making during potential security incidents.

Overall, technology integration issues are less serious at the aggregate level but remain operationally significant. The gap

between expert assessments and the experiences of operational stakeholders and beneficiaries suggests that integration should be evaluated not only from a technical perspective but also in terms of usability, interoperability, information flow, and operational demands. Developing standardized integration frameworks, strengthening interoperability, reducing information fragmentation, and providing appropriate personnel training are essential to ensuring that aviation security technologies operate as a cohesive and effective system rather than as isolated components.

Technological Reliability. The overall median of 2.00 (Less Serious) indicates that technological reliability issues are generally manageable when all respondent groups are considered. However, differences among groups reveal important operational concerns. Technical and Regulatory Experts consistently rated all indicators Less Serious (Median = 2.00), suggesting that they view aviation security technologies as generally stable and adequately supported through maintenance, backup systems, and vendor assistance. In contrast, Operational Security Stakeholders and Beneficiaries generally rated most indicators Serious (Median = 3.00), particularly system malfunctions, software glitches, hardware failures, environmental sensitivity, and inconsistent performance. Some indicators, such as prolonged downtime, backup system adequacy, and vendor support delays, were rated Less Serious, reflecting differences in operational experiences.

These findings suggest a gap between technical assessments and actual operational experiences. While experts perceive systems as reliable, operational users encounter occasional disruptions, particularly during high-traffic periods. This highlights the need to strengthen system resilience, scalability, calibration, environmental adaptability, and backup capacity. Regular testing of redundant systems, continuous maintenance, timely software updates, and stronger vendor support mechanisms are also necessary. Most importantly, continuous field validation and operational feedback should be incorporated to ensure that reliability assessments reflect actual performance under real-world conditions.

The findings are consistent with Vukadinovic (2021), who noted that AI-based and automated screening systems may experience errors, false alarms, and performance inconsistencies, particularly under demanding operational conditions. This supports the concerns of Operational Security Stakeholders and Beneficiaries regarding system malfunctions and inconsistent performance during high-traffic periods. Similarly, Riz à Porta, Sterchi, and Schwaninger (2022) emphasized that automated threat detection reliability depends on proper calibration, validation, and environmental conditions, with variations potentially reducing detection accuracy and requiring human verification. These findings reinforce the importance of maintaining reliable technology while preserving human oversight in aviation security operations.

The qualitative findings further support the quantitative results. OSS 11 reported that a false alarm required additional screening and disrupted passenger flow, illustrating how equipment inconsistencies can affect security operations. OSS 3



similarly explained that during peak travel hours, multiple simultaneous alerts made it difficult to determine which required immediate attention while monitoring passenger behavior in a crowded environment. These experiences demonstrate that even when technologies are generally reliable, occasional malfunctions, false alarms, and performance limitations can reduce operational efficiency.

Overall, technological reliability is perceived as Less Serious (Median = 2.00), but the concerns reported by operational stakeholders and beneficiaries indicate that reliability remains an important practical issue. Strengthening field testing, system resilience, environmental adaptability, redundancy, technical support, and human oversight is essential to ensure that aviation security technologies remain dependable during real-time and high-demand operations.

Training Requirements. The overall median of 3.00 (Serious) indicates that training-related issues are a significant challenge in the effective implementation of aviation security technologies. The results show a clear difference in perceptions among respondent groups. Technical and Regulatory Experts consistently rated all indicators Less Serious (Median = 2.00), suggesting that they consider existing training systems generally adequate. In contrast, Operational Security Stakeholders and Beneficiaries generally rated most indicators Serious (Median = 3.00), particularly insufficient training frequency, steep learning curves, shortage of qualified trainers, and difficulty keeping pace with technological changes. Some indicators, such as training costs and competency evaluation, were rated Less Serious by certain groups, reflecting differences in perceived impact.

These findings indicate that workforce readiness is essential to maximizing the benefits of advanced aviation security technologies. Insufficient and irregular training may limit personnel's ability to interpret system-generated alerts, operate new technologies, and respond appropriately during actual security incidents. The difficulty of adapting to rapid technological changes also highlights the need for continuous learning, user-friendly systems, qualified instructors, adequate training infrastructure, and standardized competency assessments. The divergence between expert and frontline perceptions further suggests that training adequacy may be viewed more positively at the technical or policy level than it is experienced in actual operations.

The findings are supported by Abuan et al. (2024), who emphasized that staff competence, training frequency, and exposure to modern security technologies influence the efficiency and consistency of airport security operations. Similarly, Demir (2024) highlighted the need for continuous training and human adaptation in AI-enabled and automated aviation security systems to ensure that personnel can correctly interpret system outputs and respond effectively. These studies reinforce the finding that technological advancement alone cannot ensure effective security operations when personnel lack sufficient knowledge, skills, and opportunities for continuous development.

The qualitative findings further support these results. OSS 13 reported that limited training on new technologies sometimes made system alerts difficult to interpret, requiring

additional assessment before appropriate action could be taken. OSS 14 emphasized the challenge of remaining objective under stressful conditions while interpreting technological information alongside passenger behavior. These experiences demonstrate that training must extend beyond basic system operation to include alert interpretation, decision-making, behavioral assessment, and performance under pressure.

Overall, training requirements are perceived as a Serious issue (Median = 3.00). Strengthening continuous and technology-focused training, developing qualified trainers, providing regular hands-on exercises, and implementing standardized competency assessments are essential to ensure that aviation security personnel can effectively and confidently use evolving technologies in real-world operations.

Significant Difference in the Degree of Seriousness of the Issues Affecting the Use of Technologies in the Detection of Threats in Aviation Security

The results indicate that all identified issues obtained *p*-values of .001, which are below the 0.05 level of significance. Thus, the null hypothesis is rejected for all variables, confirming statistically significant differences among the three respondent groups—Technical and Regulatory Experts, Operational Security Stakeholders, and Beneficiaries—in their perceptions of the seriousness of issues affecting the use of aviation security technologies. The *H*-values, ranging from 300.217 to 302.714, further indicate substantial variability in responses across groups.

These differences suggest that perceptions are influenced by respondents' roles, experiences, responsibilities, and exposure to aviation security operations. Technical and regulatory experts may assess issues based primarily on system design, technical feasibility, and regulatory compliance, whereas operational stakeholders and beneficiaries experience their practical effects more directly. The consistent differences across all variables therefore indicate a potential gap between technical or policy-level assessments and operational realities. This highlights the need for participatory decision-making that incorporates the perspectives of frontline personnel and technology users in system planning, evaluation, and improvement.

The significant differences in false alarm rates are consistent with Wang et al. (2019), who noted that false alarms can increase security personnel workload, reduce operational efficiency, and affect passenger experience. Experts may consider such issues technically manageable through algorithm refinement, while operational stakeholders and beneficiaries experience their immediate effects. Similarly, differences in privacy protection align with Pik (2024), who noted that technical and regulatory assessments may emphasize compliance, whereas end users are more concerned with transparency, consent, and potential misuse of personal information.

Differences in budget constraints also reflect concerns identified in the literature regarding the financial requirements of procuring, maintaining, and upgrading advanced security technologies. While experts may view funding as a strategic resource-allocation concern, operational personnel and



beneficiaries may experience its consequences through delayed upgrades or limited system availability. Technology integration and technological reliability likewise showed significant differences, consistent with Akcay and Breckon (2020), who emphasized interoperability and compatibility challenges that can affect system performance and operational continuity.

The significant difference in training requirements is further supported by Abuan et al. (2024) and Pik (2024), who emphasized the importance of continuous training and capacity building in maximizing the effectiveness of advanced aviation security technologies. Experts may perceive existing training frameworks as adequate, while operational personnel may

encounter practical gaps in training frequency, accessibility, and application.

Overall, the findings demonstrate that the seriousness of aviation security technology issues is not perceived uniformly across stakeholder groups. The consistent significant differences emphasize the importance of a multi-stakeholder and participatory approach to aviation security management. Integrating technical expertise with frontline experiences and user perspectives can help ensure that policies, technologies, training programs, and implementation strategies are technically sound, operationally practical, and responsive to actual aviation security needs.

Table 3. Significant Difference in the Degree of Seriousness of the Issues Affecting the Use of Technologies in the Detection of Threats in Aviation Security According to Group

Variable	H-value	p-value	Decision	Interpretation
False Alarm Rates	301.629	.001	Reject Ho	Significant
Privacy Protection	302.714	.001	Reject Ho	Significant
Budget Constraints	300.217	.001	Reject Ho	Significant
Technology Integration	300.217	.001	Reject Ho	Significant
Technological Reliability	302.714	.001	Reject Ho	Significant
Training Requirements	300.359	.001	Reject Ho	Significant

Experiences of Aviation Security Personnel with Cybersecurity Measures and Analyzing Passenger Behavior During Real Threat Detection

This section presents the experiences of 15 Operational Security Stakeholders (OSS) with cybersecurity measures and analyzing passenger behavior during real threat detection using thematic analysis by Braun and Clarke (2022).

Situation Where Cybersecurity Alerts and Observation of Passenger Behavior Did not Match. Discrepancies may arise when automated cybersecurity alerts do not correspond with the observed behavior of passengers. While cybersecurity systems detect digital anomalies such as suspicious login attempts, unusual booking patterns, or compromised accounts, security personnel simultaneously assess passenger behavior during screening. The qualitative findings show that personnel do not rely exclusively on either source. Instead, they use verification procedures, multi-agency coordination, and professional objectivity to resolve inconsistencies and ensure accurate threat assessment.

Theme 1: Resolving Discrepancies Through Verification Procedures. When cybersecurity alerts conflict with observed passenger behavior, security personnel employ systematic verification rather than relying solely on automated alerts or personal judgment. These measures include secondary screening, document verification, interviews, identity validation, and coordination with cybersecurity personnel.

OSS 1 stated, *"Instead of relying solely on the alert, I coordinated with our cybersecurity team and conducted additional document verification."* Similarly, OSS 3 explained that when digital alerts and observations did not match, the officer notified the operations center and conducted a more detailed interview. OSS 5 also reported coordinating with intelligence

officers and verifying the information before the alert was determined to be a false positive.

These findings indicate that verification procedures reduce false positives, minimize unnecessary passenger inconvenience, and promote balanced decision-making by combining technological intelligence with human observation. They also reinforce adherence to established protocols, strengthening operational and legal accountability.

Theme 2: Multi-Agency Collaboration as a Response to Alert-Behavior Inconsistencies. Resolving discrepancies often requires coordination with other agencies and airport stakeholders, including cybersecurity teams, airline representatives, law enforcement, intelligence units, and supervisors. OSS 6 reported requesting assistance from an airline representative after conducting additional questioning. OSS 7 referred a conflicting case to secondary inspection and coordinated with airport law enforcement, while OSS 9 cross-checked passenger information with airline records.

These experiences demonstrate that multi-agency collaboration provides additional layers of verification and institutional support. It strengthens communication, improves the accuracy of threat assessment, and provides personnel with access to technical, operational, and intelligence resources when individual observations or automated alerts are insufficient.

Theme 3: Maintaining Professional Objectivity Amid Conflicting Security Indicators. Conflicting technological and behavioral indicators require personnel to remain objective, avoid assumptions, and follow established procedures. OSS 11 emphasized maintaining professional objectivity, completing the required interview, and forwarding the case for technical review. OSS 12 similarly referred a case to the cyber response team after observing that a passenger behaved normally despite an automated alert. OSS 15 emphasized treating both the



cybersecurity alert and personal observations seriously, coordinating with the cyber unit, and awaiting confirmation before allowing the passenger to proceed.

Maintaining objectivity reduces the risk of bias and profiling while promoting fair, transparent, and evidence-based decisions. It also helps balance security requirements with passenger rights and strengthens confidence in both technological systems and professional judgment.

The findings are consistent with Pik (2024) and Wang et al. (2019), who emphasize the importance of human oversight when automated systems produce false positives or ambiguous outputs. Similarly, Zhao et al. (2020) and Hasan et al. (2023) highlight the value of integrated and collaborative response mechanisms in aviation cybersecurity. These studies support the finding that automated technologies should complement rather than replace human judgment, particularly when digital alerts and observed behavior do not correspond.

Overall, the findings demonstrate that aviation security personnel manage cybersecurity alert-behavior discrepancies through a multi-layered decision-making process. Verification procedures help establish the accuracy of alerts, multi-agency collaboration provides additional technical and operational support, and professional objectivity ensures that decisions remain fair and evidence-based. Together, these approaches enable personnel to integrate technological intelligence with human judgment while maintaining procedural integrity, passenger rights, and security effectiveness.

Challenges Faced When Using Both Technology and Personal Judgment During a Real Threat. In real-time aviation security operations, personnel rely on both technological systems and professional judgment to detect and assess potential threats. Screening scanners, surveillance systems, and cybersecurity tools provide automated alerts, while personnel use behavioral observation and experience to interpret and validate these signals. The findings reveal that these sources do not always produce consistent conclusions, creating challenges in decision-making, workload management, and behavioral interpretation.

Three themes emerged: (1) conflict between technological alerts and human judgment, (2) operational and cognitive overload, and (3) uncertainty in behavioral interpretation and emotional decision-making. Together, these themes highlight the need for integrated decision-support systems, appropriate training, and clear protocols that enable personnel to combine technological information with human judgment effectively.

Theme 1: Conflict Between Technological Alerts and Human Judgment in Decision-Making. Security personnel frequently encounter situations in which technological alerts do not correspond with observed passenger behavior. OSS 1 reported that a system flagged a passenger's bag as suspicious even though the passenger appeared calm, prompting secondary inspection. OSS 2 similarly noted that an alert involving an apparently ordinary passenger required compliance with procedure despite concerns about causing offense. OSS 8 emphasized the need to avoid complacency when automated systems detect unusual activity despite normal passenger behavior. OSS 11 also reported

that false alarms required additional screening and affected passenger flow, while OSS 12 described the difficulty of deciding how much weight to give system outputs versus professional experience.

These experiences demonstrate the need to balance security protocols, technological alerts, human judgment, and passenger rights. Overreliance on automated alerts may result in unnecessary screening and operational delays, while excessive reliance on personal judgment may overlook genuine threats. Thus, decision-support systems should integrate technological and behavioral indicators while allowing appropriate human oversight.

This finding is consistent with Pik (2024) and Wang et al. (2019), who emphasize that automated security systems may produce false or ambiguous alerts and therefore require human validation. The findings reinforce the importance of using technology as a decision-support mechanism rather than as a complete substitute for professional judgment.

Theme 2: Operational and Cognitive Overload in Real-Time Security Environments. Personnel also experience substantial cognitive and operational demands when managing multiple alerts, technologies, and passenger observations simultaneously. OSS 3 reported difficulty prioritizing multiple alerts while monitoring passengers, while OSS 4 described information overload from different systems during face-to-face passenger monitoring. OSS 7 similarly found it challenging to monitor a cybersecurity alert while observing passenger movement. OSS 9 emphasized the need to make rapid decisions with limited time for analysis, and OSS 13 noted that unfamiliarity with new technologies sometimes made system alerts difficult to interpret.

These experiences indicate that alert saturation, multitasking, time pressure, and limited familiarity with technology can increase cognitive burden and affect decision accuracy. Systems should therefore incorporate effective alert prioritization, simplified interfaces, and user-centered designs. Continuous training and workflow optimization are also necessary to reduce operator fatigue and improve situational awareness.

The findings are supported by Wang et al. (2020) and Zhao et al. (2020), who noted that large volumes of automated alerts can contribute to cognitive strain and operational inefficiency. Abuan et al. (2024) likewise emphasized the importance of training and workflow optimization in ensuring that increased automation improves rather than complicates aviation security operations.

Theme 3: Uncertainty in Behavioral Interpretation and Emotional Decision-Making. Another challenge involves interpreting passenger behavior when technological systems provide no clear indication of a threat. OSS 5 described the difficulty of responding to a nervous passenger without resorting to assumptions or profiling. OSS 6 noted that technology can detect objects or anomalies but cannot necessarily determine intent. OSS 10 highlighted the difficulty of distinguishing anxiety from genuinely suspicious behavior, while OSS 14 emphasized the need to remain objective under stress. OSS 15 similarly



described uncertainty when behavioral inconsistencies were observed without a corresponding system alert.

These findings demonstrate that behavioral cues are inherently difficult to interpret, particularly in high-stress situations. Anxiety, nervousness, or unusual behavior may not necessarily indicate malicious intent, while a calm demeanor does not guarantee the absence of risk. Personnel therefore require training in behavioral assessment, stress management, and bias awareness. Decision-making should also be supported by multiple sources of evidence rather than behavioral observation alone.

This finding aligns with Hasan et al. (2023) and Pik (2024), who emphasize the subjective nature of behavior-based threat detection and the importance of human oversight, validation, and ethical safeguards. The findings further highlight the need to balance legitimate security concerns with the avoidance of profiling and unfair treatment.

Overall, the findings demonstrate that effective real-time threat detection requires a balanced integration of technology and human judgment. Technological alerts provide valuable intelligence, but their interpretation requires trained personnel who can verify information, manage cognitive demands, and assess behavioral cues objectively. Strengthening decision-support systems, alert prioritization, continuous training, and clear operational protocols can improve decision accuracy while reducing unnecessary delays, passenger inconvenience, and the risk of biased assessments.

Influence of the Regulatory Requirements on the Efficiency of Security Technologies in Airports

Regulatory requirements play a critical role in shaping the efficiency, reliability, and adaptability of security technologies in airport environments. Regulations on international aviation security standards, data privacy, cybersecurity, certification, and system interoperability strengthen standardization, accountability, and system reliability, but may also cause operational delays, restrict rapid data access, slow procurement and upgrades, and create administrative burdens. The findings therefore reveal a dual impact of regulation, serving as both an enabler of secure operations and a constraint on flexibility and innovation.

Theme 1: Regulatory Frameworks Enhancing System Security and Standardization. Informants reported that regulatory frameworks strengthen aviation security by promoting standardized procedures, regular system testing, interoperability, and continuous improvement. TRE 1 noted that compliance with international standards ensured that screening systems were regularly updated and tested, while TRE 5 explained that interoperability requirements encouraged better coordination among departments. TRE 7 highlighted the role of regulatory audits in identifying system weaknesses, and TRE 9 emphasized that international regulations provide a framework for deploying automated threat-detection technologies.

However, informants also identified delays associated with approval and integration processes. Lengthy software approvals, months-long system integration processes, and

regulatory adaptation that does not keep pace with technological advancement may limit timely innovation. These findings indicate the need for adaptive regulatory pathways that preserve security standards while facilitating faster technology deployment.

This is consistent with ICAO (2025), which emphasizes that international standards promote consistency, system reliability, interoperability, and continuous security improvement. At the same time, the findings suggest that regulatory processes need to evolve alongside technological developments to prevent compliance requirements from unnecessarily delaying innovation.

Theme 2: Regulatory Constraints on Operational Flexibility and Innovation. Although regulations provide important safeguards, informants also described situations where compliance requirements limited operational flexibility. TRE 2 explained that data privacy regulations established clear procedures for handling passenger information but restricted rapid access during investigations because of additional authorization requirements. TRE 3 noted that cybersecurity compliance strengthened protection but strict procurement procedures delayed the replacement of outdated equipment. TRE 6 similarly reported that cybersecurity controls restricted external software installations, while TRE 8 noted that CCTV retention requirements could limit access to older footage for investigations.

These findings highlight the need to balance regulatory protection with operational responsiveness. Risk-based provisions and controlled exceptions for urgent situations may help security personnel respond more effectively without compromising privacy, cybersecurity, or accountability.

Theme 3: Compliance Requirements Creating Operational and Workforce Challenges. Compliance requirements may also create workforce and administrative pressures. TRE 4 explained that staff certification ensures qualified personnel operate security systems but may create scheduling difficulties during emergencies when certified personnel are limited. TRE 10 noted that regular vulnerability assessments strengthen cybersecurity but extensive documentation can delay urgent system upgrades. TRE 7 further observed that preparing for regulatory audits can divert resources from routine operational activities.

These findings suggest that compliance mechanisms should be supported by efficient resource allocation, digital compliance tools, streamlined documentation, and adequate staffing. Such measures can reduce administrative burdens while maintaining required security standards.

The findings are supported by IATA (2024), which recognizes that cybersecurity, data privacy, and procurement requirements are essential safeguards but may introduce procedural complexity and operational delays. This supports the experiences of informants regarding restricted data access and delayed equipment replacement.

Overall, the findings demonstrate that regulatory requirements have a dual role in aviation security technology management. They enhance standardization, accountability,



cybersecurity, and system reliability, but excessive procedural rigidity may reduce operational agility, delay modernization, and constrain innovation. The findings therefore support the adoption of adaptive governance, in which strong security oversight is maintained while regulatory processes are made more responsive, efficient, and flexible to meet evolving technological and operational demands.

Action Plan to Enhance Passengers' Safety

Below is an Action Plan toward Enhancing Passenger Safety, synthesized from the themes on challenges and themes on strategies/practices provided by the informants and the quantitative findings.

ACTION PLAN FOR ENHANCING PASSENGER SAFETY IN AVIATION SECURITY TECHNOLOGY USE

Themes	Proposed Actions/ Strategies	Key Activities	Responsible Units	Estimated Budget (PhP)	Expected Outcomes
1. Conflict Between Technological Alerts and Human Judgment in Decision-Making	Develop an integrated decision-support framework combining system alerts and behavioral assessment	1. Standardize protocols for resolving alert-behavior mismatches 2. Introduce AI-assisted decision dashboards that combine cyber and behavioral data 3. Implement dual-verification (system + human) checkpoints	Aviation Security Operations, Cybersecurity Unit, Regulatory Authority	1,500,00	Improved accuracy in threat detection; reduced false decisions; balanced reliance on technology and human judgment
2. Operational and Cognitive Overload in Real-Time Security Environments	Strengthen workflow optimization and alert prioritization systems	1. Introduce intelligent alert filtering and prioritization tools 2. Reduce system redundancies through platform integration 3. Design workload distribution protocols during peak hours	Airport Security Management, IT Systems Division	2,000,000	Reduced information overload; faster decision-making; improved operational efficiency during peak traffic
3. Uncertainty in Behavioral Interpretation and Emotional Decision-Making	Enhance behavioral analysis training and decision standardization	1. Conduct behavioral threat recognition workshops 2. Develop guidelines distinguishing anxiety vs threat behavior 3. Provide stress management and decision-making training	Training Division, Aviation Security Academy	1,500,000	Improved consistency in behavioral assessment; reduced subjective errors; enhanced officer confidence
4. System Integration and Interoperability Gaps	Implement a unified aviation security platform	1. Integrate surveillance, screening, cybersecurity, and analytics systems 2. Develop centralized command-and-control dashboard 3. Ensure real-time data sharing across agencies	Airport IT Department, Aviation Security Technology Office, Government Agencies	3,000,000	Faster threat identification; seamless coordination; reduced system fragmentation
5. System Maintenance, Cybersecurity Risks, and Technical Failures	Establish a preventive maintenance and cybersecurity resilience program	Regular system updates and vulnerability assessments Scheduled maintenance and performance testing Strengthened cyber monitoring and incident response systems	Cybersecurity Unit, Maintenance Engineering, IT Security Teams	2,000,000	Reduced system downtime; improved reliability; enhanced protection against cyber threats



6. Compliance Procedures Causing Delays in Decision-Making	Streamline regulatory compliance and emergency approval processes	1. Create fast-track approval for high-risk threat situations 2. Digitize compliance documentation and authorization processes 3. Define tiered compliance levels based on threat urgency	Aviation Regulatory Authority, Airport Management	2,000,000	Faster response time during emergencies; reduced procedural delays; maintained regulatory compliance
7. Training Gaps and Limited Technological Competency	Strengthen continuous training and simulation-based capacity building	1. Regular simulation drills using actual security systems 2. Mandatory refresher training for all security personnel 3. Continuous professional development programs	Training & Development Division, Airport Security Academy	1,500,000	Higher staff competency; improved system utilization; faster and more accurate responses
8. Communication Gaps and Lack of Real-Time Coordination	Develop a centralized communication and information-sharing system	1. Implement real-time inter-agency communication platform 2. Establish unified security command center 3. Standardize communication protocols across agencies	Airport Security Command Center, Government Security Agencies	3,000,000	Improved coordination; faster response time; reduced information delays
9. False Alarms and System Misclassification Issues	Enhance AI-based accuracy and intelligent filtering systems	1. Upgrade AI models for threat classification 2. Reduce false positives through machine learning calibration 3. Conduct periodic system validation testing	Cybersecurity Specialists, AI Developers, IT Department	1,500,000	Reduced false alarms; improved operational efficiency; minimized unnecessary screenings
10. Need for Balance Between Security and Passenger Convenience	Implement a passenger-centered security optimization approach	1. Introduce faster screening technologies 2. Optimize passenger flow management systems 3. Reduce unnecessary secondary screenings through better analytics	Airport Operations Management, Security Technology Division	2,500,000	Improved passenger experience; reduced delays; maintained high security standards

The estimated budget covers software acquisition and licensing, system integration, AI development, cybersecurity enhancements, training programs, communication infrastructure, maintenance, and operational implementation. Actual funding requirements should be determined through a detailed technical and financial feasibility assessment, procurement processes, and coordination with airport authorities and relevant government agencies.

Conclusions

With the findings derived from the study, the following are concluded:

The study concludes that aviation security technologies—covering sensor systems, data analytics, automated monitoring, cybersecurity measures, passenger behavior analysis, and regulatory frameworks—are generally perceived as less efficient in operational settings despite their technical advancement and favorable evaluation by experts. This indicates a persistent gap between technological capability and real-world application in airport security environments.



Significant differences in perceptions across technical and regulatory experts, operational security stakeholders, and beneficiaries further confirm that evaluations of system efficiency are strongly influenced by role, experience, and exposure to security operations. Experts tend to assess systems based on technical performance and design, while operational personnel and beneficiaries evaluate them based on usability, reliability, and observable effectiveness during actual implementation.

The study also found that certain issues, particularly false alarm rates and training requirements, are considered serious concerns that directly affect operational performance and personnel readiness. Meanwhile, issues such as privacy protection, budget constraints, technology integration, and technological reliability were generally perceived as less serious but remain important structural challenges that influence long-term system effectiveness.

Qualitative findings further revealed that aviation security operations rely heavily on the integration of technology and human judgment. Operational personnel frequently manage inconsistencies between system-generated alerts and observed passenger behavior through verification procedures, inter-agency collaboration, and adherence to established protocols. However, challenges such as alert-behavior conflicts, cognitive overload, and uncertainty in behavioral interpretation highlight the complexity of real-time decision-making in security environments.

Regulatory frameworks were found to play a dual role, supporting standardization and compliance while sometimes limiting operational flexibility and response speed. Despite this, clear regulatory guidelines and enforcement mechanisms remain essential in maintaining aviation security integrity.

Overall, the study concludes that effective aviation security cannot rely solely on technological advancement. Instead, it requires a balanced integration of advanced systems, well-trained personnel, responsive regulatory frameworks, and strong organizational coordination. Bridging the gap between technical design and operational experience is essential to achieving a more efficient, reliable, and user-centered aviation security system.

Recommendations

Based on the findings and the conclusions drawn, the following are hereby recommended:

1. Since the level of efficiency of the use of technologies in the detection of threats in aviation security was found to be less efficient in terms of sensor technology, data analysis combination, automated monitoring systems, cybersecurity precautions, passenger behavior analysis, and aviation regulatory adaptations, airport authorities, aviation security agencies, and government regulators should prioritize the modernization and integration of advanced security technologies. Investments should focus on enhancing sensor capabilities, implementing artificial intelligence (AI) and machine learning (ML)-based analytics, strengthening automated monitoring systems, improving cybersecurity infrastructure, refining passenger behavior analysis tools, and continuously updating regulatory policies to keep pace with emerging security threats. These initiatives will enhance the

overall efficiency and effectiveness of aviation security operations while ensuring passenger safety.

2. Considering the significant differences in the perceived efficiency of aviation security technologies among operational security stakeholders, technical and regulatory experts, and beneficiaries, aviation authorities should institutionalize stakeholder-centered planning, implementation, and evaluation mechanisms. Regular consultations, collaborative decision-making, and feedback systems should be established to ensure that technology adoption, operational procedures, and policy decisions are responsive to the needs and perspectives of all stakeholder groups. Such an inclusive approach will help bridge perception gaps and improve the acceptance and effectiveness of aviation security technologies.

3. Since false alarm rates and training requirements were identified as serious issues affecting the use of technologies in threat detection, airport management should prioritize the enhancement of AI-based threat detection systems to improve detection accuracy and reduce false positives. Continuous competency-based training programs, simulation exercises, and certification courses should likewise be institutionalized to strengthen personnel competency in operating advanced security technologies, interpreting automated alerts, and responding appropriately to evolving security threats. Although privacy protection, budget constraints, technology integration, and technological reliability were assessed as less serious, airport authorities should continue implementing preventive maintenance programs, strengthening cybersecurity measures, ensuring adequate budget allocation, and upgrading existing technologies to sustain long-term operational efficiency and system reliability.

4. Given the significant differences in the seriousness of issues affecting aviation security technologies among the different stakeholder groups, aviation authorities should adopt evidence-based and stakeholder-specific intervention strategies. Periodic needs assessments and performance evaluations should be conducted to identify the concerns of operational personnel, technical and regulatory experts, and airport beneficiaries. The results of these assessments should guide policy formulation, resource allocation, technology acquisition, and workforce development to ensure that interventions effectively address the unique needs of each stakeholder group.

5. Considering the experiences of aviation security personnel regarding cybersecurity measures and passenger behavior analysis during real threat detection, airport authorities should establish standardized decision-support frameworks that effectively integrate technological alerts with professional judgment. Human-in-the-loop verification procedures, behavioral threat assessment protocols, AI-assisted decision-support systems, and simulation-based exercises should be institutionalized to improve decision accuracy, reduce cognitive overload, and enhance the ability of security personnel to distinguish legitimate threats from false alarms. Furthermore, formal mechanisms for multi-agency coordination should be strengthened to facilitate timely information sharing,



collaborative verification, and unified responses during security incidents.

6. Since regulatory requirements were found to both strengthen aviation security and create operational challenges, aviation regulatory authorities should continuously review and update existing policies to achieve a balance between regulatory compliance and operational efficiency. Flexible and risk-based regulatory approaches, digitized compliance procedures, and expedited emergency approval mechanisms should be developed to minimize unnecessary delays while ensuring adherence to national and international aviation security standards. Such improvements will enable security personnel to respond more effectively to emerging threats without compromising legal and regulatory requirements.

6. Based on the measures identified by aviation security personnel to improve the use of technologies in threat detection, airport authorities should implement the proposed action plan focusing on system integration and interoperability, AI-enabled predictive analytics, cybersecurity enhancement, preventive system maintenance, continuous personnel training, organizational coordination, and centralized communication systems. Likewise, continuous monitoring and evaluation mechanisms should be institutionalized to regularly assess the effectiveness of aviation security technologies, measure stakeholder satisfaction, and identify areas for further improvement. The implementation of these recommendations is expected to enhance the efficiency of aviation security technologies, strengthen inter-agency collaboration, improve regulatory responsiveness, and ultimately contribute to safer, more secure, and more resilient airport operations.

7. The action plan proposed is recommended for adoption.

REFERENCES

1. Abdelaziz, A. B., et al. (2023). Photoplethysmography and AI-based authentication methods. *Electronics*, 12(1).
2. Abdelkhalid, H. J., Hashim, A. T., & Hasan, A. M. (2020). Segmentation approach for noisy iris images based on hybrid techniques. *Engineering Technology Journal*, 38(11A), 1684–1691.
3. Abuan, O. G., Corpuz, R. R. N., & Carmen, J. V. S. (2023). Safety risk management as related to airport passenger experience at Manila
4. International and Domestic Airports. *EPRA International Journal of Multidisciplinary Research (IJMR)*, 9(10). <https://doi.org/10.36713/epra14657>
5. ACI. (2023). Global role of advanced screening technologies in aviation security. *Airports Council International*.
6. Ahmed, S. (2025). Predictive analytics and behavior analysis in airport security. *International Journal of Social Science Research*.
7. AI-Generated False Positives or False Negatives in Threat Detection. (2025). *vixra Publication*.
8. AI-Powered Surveillance and Behavioral Analysis. (2025). *ReelMind Blog*. Millimeter wave scanner. (2025). In *Wikipedia*.
9. Akcay, S., & Breckon, T. (2020). Towards automatic threat detection: A survey of advances of deep learning within X-ray security imaging.
10. Automatic Dependent Surveillance–Broadcast. (2025). In *Wikipedia*.
11. American Society for Testing and Materials (ASTM). (2021). *Standards for advanced imaging technologies in airport security*. ASTM International.
12. Airport security and safety technologies (2024). *Journal of Transportation Security*.
13. Ardestani, A. (2025). Proactive aviation cybersecurity risk treatment through cognitive digital twins and AI-driven predictive analytics. *LinkedIn Publication*.
14. Arora, S., Rathore, A. S., & Gautam, S. (2019). Passenger screening using deep learning and artificial neural networks. *International Journal of Engineering and Management Research*, 9(3).
15. AVSEC Consulting. (2025). Threats: Challenges and responses. <https://avsecconsultinghk.com/blog/2025/2/9/threats-challenges-and-responses/>
16. Bureau of Customs. (2024). BOC enhances airport security with advanced scanners. <https://customs.gov.ph/boc-enhances-airport-security-with-advanced-scanners/>
17. Chen, Y., et al. (2023). Optimized intrusion detection systems for airport cybersecurity. *International Journal of AI Security*.
18. Civil Aviation Authority of the Philippines. (2025). Airport security program writing workshop report – compliance with ICAO Annex 17 and NCASP. CAAP. <https://www.caap.gov.ph/caap-successfully-concludes-second-airport-security-program-writing-workshop/>
19. Cybersecurity training and implementation issues in aviation technology adoption (2026). *Membrane Technology Journal*.
20. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends (2022). *MDPI Information*.
21. False alarm and reliability concerns in computational screening systems (2025). *National Academies Press*.
22. Demir, G. (2024). Artificial intelligence in aviation safety: Systematic review and biometric analysis. *Journal of Safety Research*. <https://doi.org/10.1007/s44196-024-00671-w>
23. Department of Transportation (DOTr) and UltraPass MOU for biometric airport systems. (2024, November 13). *Philippine News Agency*. <https://www.pna.gov.ph/index.php/articles/1237824>
24. Department of Transportation (DOTr) biometric passenger processing plans. (2024, February 14). *Philippine News Agency*. <https://www.pna.gov.ph/articles/1218854>
25. European Commission. (2022). Millimeter wave and backscatter X-ray technologies: Safety and privacy implications.
26. European Union Aviation Safety Agency (2022). *Artificial Intelligence Roadmap in Aviation*.
27. Future Market Insights. (2024). Airport security market strategic growth analysis: Biometric, CT, AI detection technologies.
28. Ghanbarzade, A., & Soleimani, H. (2025). GNSS/GPS spoofing and jamming identification using machine learning and deep learning. *arXiv*. <https://arxiv.org/abs/2501.02352>



29. Hasan, R., et al. (2023). Advanced persistent threat prediction using machine learning. *Cybersecurity Journal*.
30. Hassan, T., Khan, S. H., Akcay, S., Bennamoun, M., & Werghi, N. (2019). Cascaded structure tensor framework for robust identification of heavily occluded baggage items from multi-vendor X-ray scans. <https://arxiv.org/abs/1912.04251>
31. Heightened security alerts at Philippine airports after bomb threat. (2023, October 6). Philippine News Agency. <https://www.pna.gov.ph/articles/1211311>
32. Hunt, K. (2021). Technology adoption for airport security: Modeling public acceptance and threat perception. *Transportation Research Part A*.
33. Hunt, K., & Tamasi, S. (2020). Risk assessment techniques for civil aviation security. *Transportation Research Interdisciplinary Perspectives*.
34. IATA. (2024). IATA Annual Security Report 2024. International Air Transport Association.
35. ICAO. (2025). A42WP/561: Advanced technologies transforming aviation security. International Civil Aviation Organization.
36. IDSTCH. (2025). New airport security technology breakthroughs combating increasingly complex threat environment. <https://idstch.com/military/air/new-airport-security-technology-breakthroughs-combatting-increasingly-complex-threat-environment/>
37. Integrated automation and cybersecurity adaptations in aviation systems (2025). *International Journal of Social and Humanities Sciences Research*.
38. International Air Transport Association (2021). *Guidance on Data Management in Aviation Security*.
39. International Civil Aviation Organization (2023). *Aviation Security Manual (Doc 8973)*.
40. International Air Transport Association. (2023). What you need to know about aviation security. IATA. <https://www.iata.org/en/publications/newsletters/iata-knowledge-hub/what-you-need-to-know-about-aviation-security/>
41. International Air Transport Association. (2024). IATA Annual Security Report 2024. IATA. <https://www.iata.org/contentassets/b7736d5f28f34255ba1b366283f8f0d1/iater-2024-final-report.pdf>
42. International Airport Review. (2024). Innovating for today's airport security threats. <https://www.internationalairportreview.com/article/296310/innovating-for-todays-airport-security-threats/>
43. International Civil Aviation Organization (2022). *Cybersecurity Strategy*.
44. International Civil Aviation Organization. (2025). Coordinating the response to new and existing threats (ICAO Doc. 6605). ICAO. https://www.icao.int/sites/default/files/2025-02/6605_en.pdf
45. International Civil Aviation Organization. (2025). Cooperative Aviation Security Programme – Asia Pacific (CASPAP) Programme documents, Phase III extension. ICAO. [https://www.icao.int/sites/default/files/2025-08/caspap-documents/CASP-](https://www.icao.int/sites/default/files/2025-08/caspap-documents/CASP-AP-Programme-Extension-Phase-III-FINAL.pdf)
46. [AP-Programme-Extension-Phase-III-FINAL.pdf](https://www.icao.int/sites/default/files/2025-08/caspap-documents/CASP-AP-Programme-Extension-Phase-III-FINAL.pdf)
47. Kolte, R., et al. (2022). Generative adversarial networks for anomaly detection in X-ray security images. *Journal of Artificial Intelligence Research*.
48. Kühne, S. (2024). Searching for harmful intentions in airport security: Automated threat identification and traveller screening. *ESTS Journal*.
49. Liang, J., et al. (2018). Deep learning applications in 2D X-ray threat detection. *Computer Vision in Security*.
50. NAIA biometric egates and funding. (2025, June 11). Biometric Update. <https://www.biometricupdate.com/202506/philippines-sets-aside-millions-in-funding-for-biometric-airport-gates>
51. National Institute of Standards and Technology (2020). *Cybersecurity Framework*.
52. National Research Council. (1996). *Airline passenger security screening: New technologies and implementation issues*. National Academies Press. <https://doi.org/10.17226/5116>
53. Number Analytics. (2024). The future of aviation security screening. <https://www.numberanalytics.com/blog/future-of-aviation-security-screening>
54. Office for Transportation Security (OTS) has deployed enhanced screening and detection systems. (2025). Documentation of threat interceptions and screenings by OTS personnel. (Information retrieved from secondary sources detailing OTS operations).
55. Office for Transportation Security. (2024). OTS and ICAO CASPAP launch aviation security oversight, reporting and resolution software (ORR). OTS. <https://ots.gov.ph/news/ots-and-icao-casp-ap-launch-aviation-security-oversight-reporting-and-resolution-software/>
56. Omrani, P., et al. (2020). Machine learning for aviation incident prediction. *Decision Support Systems in Transport*.
57. Passenger Screening Limitations. (2024). Verdicraft Website.
58. Patel, S. (2018). Biometric identification technologies in airport security. *Security Technology Review*.
59. Peña, A. D. (2025). Cybersecurity in Philippine aviation: A multi-method evaluation of vulnerabilities and mitigation strategies through document analysis, case study, and risk modeling. *International Journal of Wireless and Microwave Technologies*, 15(6), 41–53. <https://doi.org/10.5815/ijwmt.2025.06.04>
60. Peña, A. C., Gutierrez, M., & Guinto, M. (2024). Balancing security and privacy: A study on biometric authentication implementation in airports and airlines. *International Journal of Advanced Research in Science, Communication and Technology*, 4(1). <https://doi.org/10.48175/IJARST-22659>
61. Petrescu, A. (2019). Facial recognition in passenger screening. *Journal of Biometrics and Security*.
62. Philippine National Police Aviation Security Group (PNPAVSEGROUP) operations. (2026). Grokipedia. https://grokipedia.com/page/philippine_national_police_aviation_security_group
63. https://grokipedia.com/page/philippine_national_police_aviation_security_group
64. Philippines' busiest airport bringing Amadeus biometric egates online. (2025, November 25). Biometric Update.
65. <https://www.biometricupdate.com/202511/philippines-busiest-airport-bringing-amadeus-biometric-e-gates-online>



66. Pik, E. (2024). Airport security: The impact of AI on safety, efficiency, and the passenger experience. *Journal of Transportation Security*, 17, 9.
67. Pik, E. (2024). Airport security: The impact of AI on safety, efficiency, and the passenger experience. *Journal of Transportation Security*, 17(1), 9. <https://doi.org/10.1007/s12198-024-00276-6>
68. Pratiwi, & Prayudhista (2023). AI training simulations for airport security personnel. *Simulation in Transportation Security*.
69. Prihodova, T., & Hub, M. (2020). Neural networks in fingerprint authentication. *International Biometric Journal. Toward automatic threat detection: Advances of deep learning within X-ray security imaging [Survey]*. (2022). *Pattern Recognition*.
70. Reducing False Alarms from Explosive Detection Systems. (2024). National Academies Press.
71. Riz à Porta, R., Sterchi, Y., & Schwaninger, A. (2022). How realistic is threat image projection for Xray baggage screening? *Sensors*, 22(6), 2220. <https://doi.org/10.3390/s22062220>
72. Sahic, S., & Cinac, J. (2022). Multi-agent systems for airport surveillance. *International Journal of Smart Systems*.
73. Sarkar, S., et al. (2016). Photoplethysmography applications in biometric systems. *Journal of Sensors*.
74. Transportation Security Administration (2022). *Advanced Technology Systems Overview*.
75. Transportation Security Administration (2021). *Behavior Detection Program*.
76. TSA. (2024). AI enhancements in baggage screening technologies. *Transportation Security Administration*.
77. Ukwandu, E. (2022). Cybersecurity challenges in aviation industry: A review. *Information*, 13(3), 146. <https://doi.org/10.3390/infetraction13.3.146>
78. Velayudhan, D., Ahmed, A., Alansari, M., et al. (2025). STING-BEE: Towards vision-language model for real-world X-ray baggage security inspection.
79. Vertel Corporation. (2025). *Evaluating the effectiveness of airport security technologies in preventing threats*.
80. <https://vertelcorp.com/vertel-insight/aviation/evaluating-the-effectiveness-of-airport-security-technologies-in-preventing-threats/>
81. Vukadinovic, D. (2021). *Xray baggage screening and artificial intelligence (AI)*. European Commission Publications.
82. Wang, Q., Megherbi, N., & Breckon, T. P. (2020). A reference architecture for plausible threat image projection within 3D X-ray computed tomography volumes.
83. Wang, Q., Ismail, K. N., & Breckon, T. P. (2019). An approach for adaptive automatic threat recognition within 3D computed tomography images for baggage security screening.
84. Wang, J., Liu, Y., & Song, H. (2020). Counter-Unmanned Aircraft System(s) (C-UAS): State of the art, challenges and future trends. <https://arxiv.org/abs/2008.12461>
85. Wei, L., & Cheng, H. (2022). Predictive risk analysis in airport operations using AI. *Transportation Analytics Journal*.
86. World Jurisprudence. (2023). Enhancing aviation security measures: A global perspective. <https://worldjurisprudence.com/aviation-security-measures>
87. Wowfare. (2024). Biometric technology in aviation: Enhancing airport security and passenger experience. *Wowfare*.
88. <https://wowfare.com/blog/biometric-technology-aviation/>
89. Xu, et al. (2022). Towards automatic threat detection: Advances of deep learning within X-ray security imaging. *Pattern Recognition*.
90. Zhao, X., et al. (2020). Passenger risk classification using neural networks and optimization methods. *Journal of Aviation Technology & Engineering*.
91. Ziegler, D., et al. (2021). Predictive analytics models in aviation safety. *Transportation Research Part C*.