ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

ANALYZING INSTITUTIONAL SECURITY MEASURES: IMPLEMENTATION, EFFECTIVENESS, AND CHALLENGES

Jaywel C. Mordido
Philippine College of Criminology

Article DOI: https://doi.org/10.36713/epra25270
DOI No: 10.36713/epra25270

ABSTRACT

This study examines institutional security measures with emphasis on their implementation, effectiveness, and challenges, utilizing an explanatory sequential research design. Security is a fundamental concern in institutional management as it ensures the protection of people, property, and information against potential risks. The research sought to determine the extent of implementation of security protocols, the level of their effectiveness, and the major challenges encountered in practice. Data were gathered through structured survey questionnaires administered to administrators, security personnel, and key stakeholders. The responses were analyzed using descriptive statistics to identify prevailing trends, measure the degree of effectiveness, and highlight recurring gaps in existing security practices.

Findings reveal that institutions generally maintain structured security frameworks; however, the level of implementation varies depending on resource availability, management priorities, and personnel capacity. Moderate to high effectiveness was observed in institutions that consistently followed established protocols, provided adequate training, and ensured proper coordination among units. Conversely, issues such as insufficient funding, outdated equipment, lack of specialized training, and weak monitoring systems were identified as persistent challenges that compromise security outcomes.

The study underscores the importance of continuous assessment, capacity-building, and the adoption of modern technologies to address emerging security threats. It further emphasizes the need for effective leadership, stakeholder participation, and adequate policy support to ensure sustainability. Overall, the research provides evidence-based recommendations to strengthen institutional security systems, enhance operational readiness, and promote a proactive culture of safety and resilience across organizations.

KEYWORDS: *Security, Security Measures, Implementation, Effectiveness,*

INTRODUCTION

Campus Security plays a critical role in keeping educational institutions' learning environments secure and comfortable. The main objective of campus security is to safeguard visitors, staff, instructors, and students. It includes several procedures and policies intended to stop and deal with different kinds of threats. These include emergency readiness, cyber security, and health and safety procedures in addition to physical security. The historical background of campus security shows how professional security officers with enhanced technology and specialized training have replaced traditional security guards.

Faculty members remain concerned about the welfare of their students. However, with their primary role as educators, faculty have faced unique challenges while engaging in issues about student high-risk drinking, most often trying to identify an appropriate role as they endeavor to address the problem. Likewise, senior staff from our project worked with key student affairs and student health offices, and campus and community efforts needed to be brought forward by the faculty and staff leadership team. In doing so, we intentionally modeled the type of collaboration we sought across campus and in the community.

Of course, an ongoing challenge that large universities continue to face is devising optimal ways to focus high-risk drinking at a level that addresses all students, regardless of their attitudes toward alcohol. Vehicles that help to disseminate university expectations invariably differ depending on each institution as well as the tools and resources that are available to students.

Security and safety are one of the basic needs as pointed out in Maslow's hierarchy of needs. This includes safety against accidents and injury which only show that people want control and order in their lives, so this need for safety and security contributes largely to behaviors.

Furthermore, it is innate to human beings to seek security and protection from dangers for them to survive and continue existing free from anything that may cause damage to their properties or may result in injury or death. In the ancient world, humans learned to unite themselves into clans, then into tribes,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

and later into bigger communities. As they organize themselves, their primary reason is the security of their life, their livelihoods, and security of their existence. Initially, humans were only worried about the natural causes of dangers such as earthquakes, typhoons, lightning, and attacks from animals. Later, other tribes became their enemies as other tribes and other groups of people competed for survival.

STATEMENT OF THE PROBLEM

1. What is the extent of implementation of the security measures at Siquijor State College in terms of the following;
    a. Physical Security,
    b. Personnel Security
    c. Information and Document Security
2. Is there a significant difference on the extent of Implementation of the Security Measures in terms of the identified variables according to the employees, students and Visitors?
3. What is the extent of effectiveness of the institutional security measures of the identified variables?
4. Is there a significant difference on the extent of effectiveness of the institutional security measures in terms of the identified variables according to the employees, students and Visitors?
5. What are the challenges encountered in the implementation of the institutional security measures at SSC?
6. Based on the findings, what security plan can be developed to enhance the institutional security measures at SSC?

METHODOLOGY

This study utilized an Explanatory Sequential Mixed-Methods Design, starting with quantitative surveys and followed by qualitative interviews and focus group discussions to evaluate the implementation and effectiveness of physical, personnel, and information security measures at Siquijor State College. A total of 669 respondents—students, employees, and visitors—participated in the survey, while nine key informants were interviewed to further explain findings and identify challenges. Conducted by the Campus Security Director, the research focused on campus security practices but was limited by restricted access to confidential information and limited generalizability. Data were analyzed using descriptive statistics, the Kruskal-Wallis H Test, and thematic analysis, ensuring ethical standards throughout the process. The findings will guide the development of a proposed security program for administrative review and potential implementation.

RESULT AND DISCUSSIONS

The overall findings show that the security measures at Siquijor State College are generally very much implemented, as reflected in the overall median rating of 4 across physical, personnel, and information/document security. Effective practices include the presence of secured gates, CCTV surveillance, security patrols, ID systems, and proper handling of sensitive records, which strengthen the institution's safety framework. However, some gaps were noted in protective lighting, perimeter reinforcements, personnel compliance with policies, and consistent document handling procedures, which were only rated as "implemented" by certain groups such as employees and visitors. These results suggest that while SSC has already established a solid foundation of campus security, there remains a need for continuous improvements through infrastructure upgrades, stricter enforcement of policies, and ongoing security awareness among stakeholders to ensure a more consistent and sustainable protection system.

The analysis of differences in perceptions among students, employees, and visitors on the extent of security measures implementation at Siquijor State College shows statistically significant variations across physical security, personnel security, and information/document security. For physical security, students (Mean Rank = 373, Median = 3.53) and visitors (Mean Rank = 366.6, Median = 3.60) rated the measures higher than employees (Mean Rank = 234.7, Median = 3.13), with a significant difference ($H = 65.6$, $p = 0.0001$). In personnel security, students (Mean Rank = 366.9, Median = 3.63) and visitors (Mean Rank = 373.3, Median = 3.75) also rated measures more favorably than employees (Mean Rank = 242.3, Median = 3.25), resulting in a significant difference ($H = 56.6$, $p = 0.0001$). In information and document security, students (Mean Rank = 378.4, Median = 3.64) and visitors (Mean Rank = 381.6, Median = 3.64) again assessed implementation more positively compared to employees (Mean Rank = 212.9, Median = 3.00), with the highest difference observed ($H = 97.3$, $p = 0.0001$). Overall, employees consistently rated security measures lower than students and visitors across all domains.

The overall findings on the extent of effectiveness of institutional security measures at Siquijor State College reveal that the school has very much effective (VME) security measures across the domains of physical security, personnel security, and information/document security, as reflected in the overall median of 4. For physical security, effectiveness is strongly demonstrated through the installation of gates, door-locking devices, CCTV surveillance, and consistent enforcement of protocols, though some employees rated aspects like barbed wire fencing, alarms, and parking lot surveillance only as moderately effective (ME), suggesting areas for improvement. In terms of personnel security, measures such as ID verification, campus patrols, visitor screening, and applicant evaluation were consistently rated as very effective. However, employees rated background checks, orientations, and job vacancy advertising only as moderately effective, indicating a need for stricter and more consistent enforcement of personnel-related policies. Meanwhile, information and document security was also perceived as very effective overall, particularly in policies on handling classified matters, security manuals, and controlled dissemination of

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

sensitive information. Yet, employees again rated most indicators only as moderately effective, highlighting perceived gaps in awareness, training, and document control.

The analysis of differences in the extent of effectiveness of institutional security measures at Siquijor State College across physical, personnel, and information/document security revealed statistically significant variations in perceptions among students, employees, and visitors, as all computed p-values were at 0.0001, leading to the rejection of the null hypothesis. For physical security, students and visitors had higher mean ranks and medians (348.4 and 362.9; Mdn = 3.73) compared to employees (287.6; Mdn = 3.60), suggesting that employees perceive physical measures like locks, gates, and surveillance systems as less effective. In terms of personnel security, both students (357.9; Mdn = 3.77) and visitors (359.4; Mdn = 3.77) again rated effectiveness higher than employees (270.7; Mdn = 3.62), indicating concerns among employees about the consistency of enforcement in ID systems, patrols, and background checks. Similarly, in information and document security, students (361; Mdn = 3.80) and visitors (379.7; Mdn = 3.80) expressed greater confidence in the safeguarding of sensitive records than employees (249.9; Mdn = 3.33), reflecting employees' closer awareness of gaps in document control, privacy practices, and compliance.

CHALLENGES ENCOUNTERED IN THE IMPLEMENTATION OF THE INSTITUTIONAL SECURITY MEASURES AT SSC.

Theme 1: Aging Infrastructures

Participant 2,3,5 and 7 reported that he structural challenge lies in the systemic neglect of facility maintenance and upgrades. Dilapidated doors, fragile windows, and deteriorating fences indicate not only a lack of resources but also a low prioritization of physical security in institutional planning. The absence of routine inspections and preventive maintenance programs creates persistent vulnerabilities. Over time, this neglect erodes both the functional reliability of infrastructure and the perceived safety of the campus community, making the environment more attractive to offenders.

Theme 2: Substandard Security Implementation

They also added that one problem is the Substandard Security Implementation. The root of this problem is the fragmented and underfunded integration of modern security systems. While CCTV and locks exist, their limited coverage and poor quality reveal the absence of a comprehensive strategy that aligns resources with actual security needs. This piecemeal implementation creates blind spots and an illusion of protection without real deterrence. Structurally, it reflects a reliance on outdated security models, where technology is deployed reactively rather than proactively, leaving the institution exposed to internal and external threats.

Mylonas and Roussos (2021) emphasized that most universities separate physical and cyber security measures, creating vulnerabilities. Locally, Pacapac (2022) revealed that Philippine HEIs adopted partial technologies during the pandemic but faced gaps in comprehensive surveillance. Gabata et al. (2024) also noted student concerns about low visibility of campus monitoring systems, reinforcing SSC's struggles.

Them 3. Need for technology

Further Participants 2, 3 4, and 8 stated that he structural issue underlying these experiences is the institutional gap in adopting modern, technology-based security systems. Outdated or low-resolution CCTVs create blind spots, while the lack of comprehensive coverage leaves key facilities vulnerable. Unlike private institutions that invest heavily in advanced systems such as biometric access control, SSC is hindered by financial limitations as a public school. Structurally, this reflects a resource disparity and systemic underinvestment in digital and surveillance technology, resulting in an over-reliance on human monitoring that cannot adequately cover the entire campus.

These concerns are consistent with Germann and Martinez (2023), who noted that many educational institutions have overlooked physical security upgrades while focusing on digital learning infrastructure post-pandemic. Mylonas and Roussos (2021) also stressed that a lack of integration between physical surveillance (e.g., CCTV) and broader security protocols weakens institutional resilience. Locally, Tejano (2023) found that Philippine HEIs in Koronadal City had only partial compliance in surveillance systems and recommended clearer SOPs and investments in updated CCTV coverage. Similarly, Laroya and Moyao (2024) reported that outdated equipment among state universities compromised the efficiency of school security guards, limiting their ability to respond to incidents.

The voices of the participants reveal that SSC's security framework is hampered by technological inadequacies, where outdated and insufficient surveillance tools undermine the broader goal of campus safety. This gap reflects not only financial and infrastructural limitations but also the growing disparity between public and private institutions in adopting modern security systems. Ultimately, this theme underscores the urgent need for investment in advanced, integrated surveillance technology as a cornerstone of institutional resilience.

Theme 4: Negative Security Culture

Participants pointed out non-compliance with security protocols. Participant 2 observed, *"It might be employees who are overly trusting, thus sometimes anybody can go in and out of the room." Participant 7 echoed, "People do not recognize signage and do not care about the messages they convey."*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

The deeper issue is the institutional culture of complacency and weak enforcement. Security protocols may exist, but they are undermined by non-compliance, lack of monitoring, and indifference among both employees and students. This signals a failure in fostering shared responsibility for safety and reflects weak leadership emphasis on discipline and accountability. Structurally, this creates an environment where even basic rules, like recognizing signage or restricting access, are disregarded, thereby normalizing lax security practices and exposing the institution to avoidable risks.

Harris (2021) asserted that digital and physical security efforts fail without user awareness and compliance. Locally, Rabacal et al. (2022) and Seva et al. (2024) confirmed that visible enforcement by guards and staff shapes safety behaviors among students. Mabanglo (2020) further observed that perceptions of security vary across stakeholders, affecting institutional compliance.

Theme 5: Indifference Towards Security Protocol

Same participants also describe a culture of complacency and selective compliance with existing security protocols. These accounts reveal a structural gap not in the absence of security measures, but in their consistent enforcement and acceptance by the community. Employees' excessive trust, disregard for signage, and failure to comply with ID protocols undermine the integrity of institutional security. Structurally, this reflects a weak security culture, where rules exist but are not fully internalized or respected. Such indifference erodes accountability and creates vulnerabilities, as even small acts of noncompliance accumulate into systemic risks.

This finding resonates with Rabacal et al. (2022) and Seva et al. (2024), who confirmed that student and employee adherence to safety protocols depends heavily on visible enforcement and cultural reinforcement by guards and faculty. Harris (2021) further argued that without consistent compliance, even the best-designed security frameworks are rendered ineffective. Locally, Mabanglo (2020) observed that security measures in Philippine colleges were implemented differently depending on stakeholder perceptions, resulting in uneven effectiveness.

The theme of indifference towards security protocols highlights that the success of institutional security lies not only in the presence of rules and guards but also in cultivating a culture of compliance and accountability. Without shared responsibility and active participation, even the most robust security systems become vulnerable to neglect and exploitation.

Theme 6: Shortage of Manpower

Textural Description: A lack of sufficient guards was a recurring concern. Participant 1 explained, "Participant 4 & 6 was quoted in saying, "In implementing the security measures inside the School Campus, there is a lack of security personnel". This was seconded by participant 1 when he said "I believe that we don't have enough security personnel ratio to the personnel of SSC". seconded by Participant 9 saying "kulang po ng security guard' (we don't have enough security guards Participant 4 also stressed that "the number of Security Personnel is not enough to fully secure all of them (visitors) when a threat occurs."

This problem stems from organizational underinvestment in human resources for security. The insufficient number of guards relative to the size of the campus and its population reduces patrol visibility and response time, weakening deterrence and monitoring. Structurally, the shortage reflects budgetary constraints and administrative priorities that do not allocate adequate funds for manpower. It also suggests the absence of workload analysis and staffing standards tailored to SSC's needs, leaving the institution reliant on an overstretched and potentially demoralized security workforce.

Fielder and Grant (2021) identified resource shortages as barriers to institutional security, especially in small colleges. Locally, Laroya and Moyao (2024) highlighted manpower shortages among guards, while Hernandez et al. (2025) found that staffing gaps hinder effective occupational safety policy implementation.

Theme 7: Inadvertent Disclosure

Participant 1 and 6 also described lapses in protecting sensitive records. The underlying structural issue is the lack of formalized data governance policies and staff training. Sensitive information, such as student grades and employee records, is mishandled due to insufficient awareness of privacy obligations and weak accountability mechanisms. Without institutionalized compliance frameworks (e.g., RA 10173), staff resort to informal practices that compromise confidentiality.

Structurally, this reflects gaps in leadership oversight, technological safeguards, and awareness-building, which leave SSC exposed to breaches of privacy and trust that could escalate into legal and reputational risks.

Corroboration: Koskosas and Ioannou (2020) stressed that universities with limited resources often struggle to adopt comprehensive cybersecurity frameworks. Brown and Clark (2021) further warned that breaches expose sensitive student data to risks of identity theft. Locally, Sancon (2023) found uneven compliance with RA 10173 (Data Privacy Act) among HEIs, while Flores (2024) identified training and leadership as crucial in bridging the gap between written policies and practice.

The findings reveal that SSC's challenges in implementing institutional security measures are interconnected, encompassing aging infrastructures, substandard technologies, negative security culture, manpower shortages, and weak information security practices. These challenges align with both global and local research showing that institutions often

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

struggle with fragmented, underfunded, and poorly integrated approaches to security. To address these gaps, SSC must adopt a holistic and proactive framework that merges physical and digital safeguards, strengthens manpower and training, and cultivates a culture of security compliance across all stakeholders.

Theme 8: Unprotected Network Facility

Participants 2 and 3 also stressed the vulnerability of SSC's digital infrastructure. These accounts reveal that SSC's network facility lacks sufficient safeguards for information governance and cyber resilience. The vulnerabilities stem not only from technical weaknesses but also from inadequate staff training in handling sensitive data and the absence of strict access controls. Structurally, this exposes the institution to threats of identity theft, cyber fraud, and reputational damage.

Koskosas and Ioannou (2020) highlighted that many educational institutions lack comprehensive cybersecurity frameworks due to limited resources. Similarly, Brown and Clark (2021) warned that breaches in student databases can result in identity theft. In the Philippine context, Sancon (2023) found that compliance with RA 10173 (Data Privacy Act) among universities is still uneven, while Flores (2024) stressed that leadership commitment and staff training are critical for protecting sensitive records.

Taken together, these themes show that SSC's institutional security challenges are multi-layered—ranging from physical infrastructure deficiencies, cultural indifference to protocols, vulnerable digital networks, and insufficient technology investments. The essence across all themes highlights a single truth: security cannot be effective when fragmented. Only through a holistic approach—updating infrastructure, fostering compliance, protecting digital assets, and modernizing technology—can the institution build a resilient and sustainable security framework.

CONCLUSIONS

The SSC community has a good understanding of the security procedures that are being implemented. However, while their assessment is commendable, there are special areas that need special attention to promote a well-rounded security culture.

Siquijor State College has established a strong foundation of campus security, with measures generally rated as "Very Much Implemented" across the three group of respondents. While effective practices such as CCTV systems, secured gates, and patrols are in place, gaps remain in lighting, perimeter reinforcements, personnel compliance, and document handling. Addressing these through continuous improvements will not only strengthen campus safety but also provide a practical contribution to criminology by demonstrating how effective security systems can deter crime, minimize risks, and promote a culture of safety within educational institutions.

In the perception of the 3 group of respondents, it is clearly demonstrated that while students and visitors generally view the security measures of Siquijor State College as well-implemented, employees consistently perceive them less favorably across all domains—physical, personnel, and information/document security. The significant differences in perceptions suggest that employees, being directly involved in day-to-day operations, may be more exposed to the practical gaps and challenges of institutional security compared to students and visitors who largely experience its outcomes. This disparity highlights the need for management to address the concerns of employees, as their perceptions may reflect operational shortcomings such as inconsistent enforcement of policies, inadequate facilities, or lack of support in security protocols. Bridging this gap is essential to ensure a more unified and accurate understanding of campus security effectiveness, thereby fostering a stronger culture of safety and accountability within the institution.

The findings affirm that Siquijor State College has established institutional security measures that are generally perceived as very much effective across the group of respondents, with an overall median rating of 4. The presence of strong physical security systems such as gates, CCTVs, and enforced entry protocols, as well as effective personnel and document security practices, reflects the college's commitment to ensuring a safe academic environment. However, the consistent trend of employees rating several measures only as moderately effective highlights operational gaps in enforcement, monitoring, and awareness. This discrepancy suggests that while systems are in place, their consistent application and communication to employees may be lacking. Therefore, strengthening training, capacity-building, and policy enforcement, while engaging employees more actively in the implementation process, is essential to bridge perception gaps and sustain a culture of security across all stakeholders.

The findings demonstrate that although institutional security measures at Siquijor State College are generally regarded as effective, there are significant perceptual gaps among stakeholder groups. Students and visitors consistently rated the effectiveness of physical, personnel, and information/document security measures higher, while employees provided lower evaluations across all domains. This difference indicates that employees, being more directly engaged in operational processes, are more attuned to practical shortcomings such as inconsistent enforcement, gaps in background checks, and vulnerabilities in document handling. The significant variations across groups suggest the need for SSC to prioritize employee perspectives in refining its security framework, as their insights can serve as a crucial basis for strengthening policies, practices, and infrastructure toward a more consistent and sustainable security system.

The challenges that are present are manifestations of the SSC administration's priority. They do not put a premium on

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

security considering that the identified challenges are the basic foundation of a strong and resilient campus security environment.

RECOMMENDATIONS

1. Based on the findings, it is recommended that SSC enhance Physical Security by improving underperforming features such as the barbed wire fencing, protective lighting, and window grills, while also expanding and maintaining CCTV coverage and the alarm system. Regular security patrols and emergency drills should be institutionalized to ensure preparedness and visibility. To address lower ratings from employees, the college should foster better communication, engage them in security planning, and raise awareness through training and a feedback mechanism. Strengthening the professionalism of security personnel and integrating physical security with broader campus safety strategies will further promote a safer and more secure learning environment for all stakeholders.
2. Siquijor State College can enhance its security by conducting regular security awareness seminars and training programs for employees, focusing on information and document security. Strengthening internal communication, reinforcing the implementation of policies, and ensuring active participation from all stakeholders, especially employees, will help bridge identified gaps. Additionally, periodic evaluations and updates of security protocols should be carried out to maintain a consistent, institution-wide standard of safety and preparedness.
3. Based on the findings, it is recommended that Siquijor State College enhance its existing security framework by addressing the operational gaps highlighted by employees' perceptions. Specifically, the institution should invest in continuous training and orientation programs to strengthen personnel awareness and compliance with established security protocols. Regular evaluation and upgrading of physical infrastructure, such as surveillance systems, perimeter reinforcements, and alarm devices, should also be prioritized to ensure they remain fully functional and reliable. In addition, stricter enforcement of personnel-related policies—particularly background checks, job screening, and employee orientation—must be implemented consistently across all units. Finally, fostering a participatory approach where employees, students, and visitors are equally engaged in the security process will help bridge perception gaps and promote a shared culture of vigilance and accountability.
4. It is recommended that Siquijor State College consider implementing the proposed security program to strengthen physical, personnel, and information/document security. The program is designed to address the challenges encountered in the implementation of existing security measures, ensuring a safer and more secure environment for students, employees, and visitors.

REFERENCES

Published Researches

1. *Anderson, R. (2020). Security Engineering: A guide to building dependable distributed System. IBSN: 978-1-119-64278-7 Retrieved from: https://www.wiley.com/en-es/search?filters[author]=Ross%20Anderson&pq=++*
2. *Bear, G.G. (2020). School Safety. Improving School Climate. https://doi.org/ 10.4324/9781351170482-9*
3. *Bongiovanni, I. (2019). The least secure places in the universe? A systematic Literature review on information security management in higher education. https://doi.org/10.1016/J.COSE.2019.07.003)*
5. *Cipres, M.C. (2022). Assessment of School Security Practices Implemented at Visayas State University Tolosa in the New Normal. International Journal of Innovative Science and Research Technology. ISSN No. 2456-2165.*
6. *Furnell, S. M. (2018). Cyber security risk assessment: Modelling and analysis approaches. Information Management & Computer Security, 26(1), 2-14. https://www.researchgate.net/publication/353436973_Information_Security_Risk_Assessment*
7. *Johnson AT. (2020). School Security? IEEE Pulse. 2020 Jan-Feb;11(1):25-26. doi: 10.1109/MPULS.2020.2972725. PMID: 32175849.*
8. *Szumiec, M. (2021). School security management – ethical, psychosocial, and institutional conditions. Scientific Journal of the Military University of Land Forces. DOI:10.5604/01.3001.0015.6175*
9. *National Center for Campus Public Safety. (2021). Best practices for campus security: Addressing emerging threats and strengthening institutional readiness. U.S. Department of Justice. https://www.nccpsafety.org/assets/files/library/Best_Practices_2021.pdf*
10. *UNESCO. (2022). Safe and inclusive learning environments: Global standards and practices. https://unesdoc.unesco.org/ark:/48223/pf0000381602*
11. *International Association of Campus Law Enforcement Administrators (IACLEA). (2023). Campus safety and security report 2023: Trends and challenges in post-secondary institutions. https://www.iaclea.org*
12. *Department of Education – Philippines. (2021). Guidelines on the implementation of school safety and security policies in higher education institutions. https://www.deped.gov.ph*
13. *Alvarez, R. (2020). Integrating Physical and Cybersecurity Measures in Philippine Institutions: Challenges and Opportunities. Philippine Journal of Security Studies, 14(2), 85-101.*
14. *Dela Cruz, M. (2022). Cybercrime Trends and National Security in the Philippines: An Analysis of Government Responses. Journal of Cybersecurity and Policy, 18(1), 122-140.*
15. *Garcia, J. (2021). Physical Security Challenges in Philippine Public Institutions: Case Studies and Solutions. Philippine Security Review, 23(4), 215-234.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

16. *Wang, M.-T., & Degol, J. L. (2020). School climate and its role in educational equity. Educational Psychologist, 55(3), 119–134. https://doi.org/10.1080/00461520.2020.1751676*
17. *Tan, J., & Lee, W. (2020). Cultural and Organizational Challenges in Implementing Security Policies: A Case Study of Public Institutions. International Journal of Organizational Security, 34(1), 55-70.*
18. *Lim, M., & Alvarado, A. (2022). Communication and Compliance in Institutional Security Policies in the Philippines: A Gap Analysis. Journal of Institutional Security, 8(1), 50-64.*
19. *Padilla, E., & Diaz, L. (2021). Cybersecurity and Legal Frameworks: Enforcement and Effectiveness in the Philippines. Philippine Cybersecurity Journal, 13(3), 185-200.*
20. *Santos, C. (2020). Employee Resistance to Security Policies in Philippine Educational Institutions: A Qualitative Study. Journal of Educational Security, 7(2), 34-50.*
21. *Santos, C., & Ramirez, J. (2023). A Comparative Study on the Effectiveness of Cybersecurity Policies in Philippine Institutions: Challenges and Solutions. Philippine Journal of Technology, 15(3), 145-163.*
22. *Koskosas, I., & Ioannou, L. (2020). Cybersecurity in higher education institutions: Challenges, threats, and solutions. Journal of Cybersecurity Education, Research and Practice, 4(1), 1-12.*
23. *Mylonas, A., & Roussos, G. (2021). The integration of physical and cybersecurity in public institutions: A comparative analysis. International Journal of Security and Networks, 16(2), 80-95. https://doi.org/10.1108/IJSN-08-2020-0123*
24. *Awan, H., & Boulton, G. (2022). The effectiveness of cybersecurity policies in educational institutions: A case study of the UK and US universities. Computers & Security, 110, 102372. https://doi.org/10.1016/j.cose.2021.102372*
25. *Germann, S., & Martinez, D. (2023). Physical security in educational institutions: Understanding the challenges in a post-pandemic era. Security Journal, 36(3), 347-365. https://doi.org/10.1057/s41284-020-00202-6*
26. *Fielder, A., & Grant, L. (2021). Barriers to effective implementation of cybersecurity frameworks in small and medium enterprises (SMEs): A global perspective. Journal of Information Security, 12(4), 278-289. https://doi.org/10.4236/jis.2021.124019*
27. *Cheng, D. (2021). Applicability of information governance for data privacy compliance in the Philippines. In DLSU Research Congress 2021 Proceedings. De La Salle University.*
28. *Cheng, D. (2024). A maturity model toolkit on information governance for Philippine universities to aid in implementing compliance to the Data Privacy Act of 2012 (RA 10173) [Doctoral thesis, Aberystwyth University].*
29. *Flores, M. L. (2024). IT security management challenges of state universities and colleges in the Zamboanga Peninsula. Cognizance Journal of Multidisciplinary Studies, 4(9), 1–10.*
30. *Gabata, J. S., Rarugal, J. M. J., & Torres, K. A. R (2024). Level of satisfaction on the security services of a state university: Basis for continuous improvement. In Proceedings of the 1st International Scholarly Research Congress (ISRC-2024). IIARI.*
31. *Hernandez, P. M. R., Yanilla, N. F., Obidos, F. A., Jr., Gundran, C. P. D., Flores, J. L. A., Co, H. U., Lintao, L. F. L., Samaniego, A. A., Tiro, D. C., Caoeng, G. J. B., & Navoa, I. L. B. (2025). Challenges and opportunities in the implementation of health and safety policies and programs in a state university in the Philippines. Acta Medica Philippina, 59(4), 14–25.*
32. *Lambo, V., & Rosacia, L. (2025). Study of security officers in selected colleges and universities in the Philippines. World Journal of Advanced Research and Reviews, 20(3), 452–459.*
33. *Laroya, A. R., & Moyao, W. G. (2024). A qualitative exploration of school security guards' experiences at Don Mariano Marcos Memorial State University. EPRA International Journal of Research & Development (IJRD), 9(12).*
34. *Misamis University. (2022). Level of preparedness of the school security personnel and their qualifications towards institutional security. [Unpublished study].*
35. *Pacapac, M. T. (2022). Security practices of higher education institutions in Ilocos Norte, Philippines in the upsurge of coronavirus. Jurnal Pendidikan Progresif, 12(2).*
36. *Sancon, R. J. A. Y. S. (2023). Data privacy best practices of a local higher educational institution: A model for governance. IOER International Multidisciplinary Research Journal, 5(3).*
37. *Seva, R. R., et al. (2024). Determinants of university students' safety behavior during the resumption of onsite classes in the Philippines. Safety Science, 172, 106324.*
38. *Tejano, A. C. (2023). Assessment on the campus security policies among higher education institutions (HEIs) in the City of Koronadal, South Cotabato. International Journal of Research Publications, 139(1), 116–136. https://doi.org/10.47119/IJRP10013911220235798*
39. *Gupta, S., Kumar, P., & Singh, R. (2024). Cybersecurity and Institutional Responses to Emerging Threats: A Global Perspective. Journal of Global Security, 18(3), 245-267.*
40. *Jain, A., & Shukla, S. (2022). Institutional Security Measures in an Evolving World: Challenges and Solutions. International Journal of Security Studies, 45(4), 320-336.*
41. *Lee, H., & Kim, Y. (2021). Assessing the Effectiveness of Cybersecurity Policies in Educational Institutions: A Global Comparative Study. Journal of Cybersecurity and Education, 10(2), 102-121.*
42. *Zhang, L., He, T., & Chen, X. (2023). Security in the Age of Remote Work: Lessons from the Pandemic. International Journal of Technology and Security, 25(1), 75-92.*
43. *Sani, A.I., Nunes, L.M., Azevedo, V., & Sousa, H.F. (2020). Campus Criminal Victimization among Higher Education Students: A Diagnosis of Local Security in Porto. Journal of Criminal Justice Education, 31, 250 - 266.*
44. *Aljanabi, S, & mahmood, R. (2021). The Role of Cubersecurity Awareness in Education Institutions. Cyber Security Journal, 10(2), 45-60*
45. *Anderson, J., & White, P. (2019). Phishing Scams in Schools: A Growing Concern. Journal of Educationa Technology 15)30, 112 – 128.*
46. *Andrews, M. (2022). Cybersecurity breaches in UK schools: Lesson Learned. European Journal of Cyber Studies, 17 (1), 89-104.*
47. *Brown, T. & Clarck, S. (2021) . Impact of data Breaches on student safety and Privacy. Journal Digital Education, 22 (4), 78-95.*
48. *Davis, R. (2022). Zero – Trust security in schools: The next big step. Cyber Security today, 18 (2), 44-59*
49. *Downey, P. (2020). Trust in Digital Learning; The Role of Cyber Securoty> Educational Techology Review, 12 (3), 30-48.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

50. *Everly, G.S n. Jr. (2018). A Clinical Applications of Crisis Theory, and Stress Response (3rd ed.): Springer.*
51. *Garcia, L. (2022). Enhancing personnel security in higher education institutions. Journal of Institutional Security, 5(2), 45-62.*
52. *Jones, A., & Brown, K. (2021). Risk management strategies for campus safety. Higher Education Security Review, 8(1), 12-28.*
53. *Jones, R., Smith, L., & Patel, M. (2021). Cyberbullying as a cybersecurity issue in schools. Digital Safety Review, 14(1), 88-103.*
54. *Kim, H. (2023). Protecting institutional data: A cybersecurity perspective. Information Security Journal, 12(3), 78-95.*
55. *Kumar, S., & Das, R. (2020). Ransomware attacks on educational institutions: Prevention strategies. Cybersecurity & Education, 19(3), 120-136.*
56. *Martinez, R. (2024). Measuring perceived safety and security in college environments. Campus Safety and Security Quarterly, 9(1), 22-39.*
57. *Myer, R. A. (2017). Crisis in Context theory: An Ecological Model. Journal of Counseling & Development, 84 (2), 163-172*
58. *Peak, K. J. (2016). Policing America: Challenges and best practices (8th ed.). Pearson.*
59. *Smith, C., & Johnson, B. (2022). Data privacy risks in educational institutions. Cybersecurity & Privacy Journal, 20(1), 33-50.*
60. *Smith, J. (2020). Defining institutional security: A conceptual framework. Journal of Security Studies, 15(4), 112-129.*
61. *White, K., & Taylor, P. (2020). Resistance to cybersecurity policies in schools: A behavioral analysis. Educational Technology Studies, 18(4), 125-141.*
62. *Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning.*
63. *Williams, T. (2020). Legal and ethical considerations in campus security. Journal of Legal Studies in Education, 10(2), 67-84.*
64. *Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5*