Feasibility Study on Bachelor of Science in Industrial Security Management (BSISM)

Jake S. Lupos

Independent Researcher

DOI: https://doi.org/10.47772/IJRISS.2026.101000457

Received: 23 October 2026; Accepted: 28 October 2026; Published: 05 November 2026

ABSTACT

The Philippine security profession continues to confront a pronounced professionalization deficit, as most security practitioners enter the workforce through brief pre-licensing briefings rather than structured academic preparation, leaving critical infrastructure, private enterprises, and communities vulnerable to evolving threats such as terrorism, cybercrime, industrial sabotage, and natural disasters. In response to this gap, CICOSAT Colleges Inc. has conceptualized the Bachelor of Science in Industrial Security Management as a four-year undergraduate program intended to formalize the education of Filipino security practitioners and align local practice with international standards of competence.

This study undertakes a comprehensive feasibility assessment of that proposed program, systematically examining its market viability, curricular conformity with Commission on Higher Education Memorandum Order No. 06, Series of 2018, operational readiness of institutional resources, and projected financial sustainability over a five-year implementation horizon.

Anchored on established multidimensional evaluation frameworks previously applied to comparable Philippine higher education offerings, the inquiry adopts a mixed-methods descriptive research design integrating stakeholder surveys, focus group discussions with community leaders and prospective students, comparative analysis of analogous BSISM offerings, and expert consultations with industry partners and regulatory bodies.

The investigation is organized around four central research dimensions: the strength of market demand within the institution's catchment area, compliance of the proposed curriculum with CHED standards and industry-recognized competency benchmarks, the adequacy of CICOSAT's faculty credentials, laboratory facilities, and instructional infrastructure, and the financial viability of the program under realistic enrollment projections. By producing rigorous evidence-based conclusions across these dimensions, the study aims to equip institutional leaders, regulators, and industry stakeholders with actionable recommendations that will guide decisions regarding program approval, modification, or implementation, and ultimately contribute to the elevation of the Philippine security profession and the development of a formally educated workforce capable of addressing contemporary security challenges.

INTRODUCTION

The Philippines faces an increasingly complex security environment shaped by persistent terrorism threats, the proliferation of cybercrime targeting both private firms and public institutions, incidents of industrial sabotage, and the recurring devastation of natural and man-made disasters that demand reliable protection of lives, assets, and critical infrastructure. Within this landscape, the demand for a competent and responsive security workforce has become more urgent than ever,yet security work in the country continues to be widely perceived as a low-skill vocation rather than as a specialized profession grounded in rigorous academic preparation.

The prevailing reality is that many security personnel operate with only basic pre-licensing briefings and informal in-service guidance, leaving them inadequately prepared to apply standardized procedures, maintain situational response readiness, or integrate contemporary surveillance and detection technologies into their daily routines.

This professionalization gap not only undermines the operational effectiveness of private security agencies but also leaves Philippine industries exposed to vulnerabilities that a more formally educated workforce could meaningfully address, reinforcing the call to align local security practice with international standards and the evolving expectations of a modernizing economy.

Against this backdrop, CICOSAT Colleges Inc. has conceptualized the Bachelor of Science in Industrial Security Management as a four-year undergraduate program intended to formalize the education of Filipino security practitioners and to elevate the broader security profession through structured academic grounding.

The present study undertakes a rigorous feasibility assessment of that proposed program to determine its operational, technical, and economic viability within collaborative enterprise environments and to establish whether the framework possesses the structural coherence and market relevance necessary to contribute meaningfully to closing the country's professionalization deficit.

The inquiry extends beyond the simple question of program launchability, probing the curriculum's alignment with Commission on Higher Education Memorandum Order No. 06, Series of 2018, its congruence with industry-recognized competency benchmarks, the adequacy of institutional resources at CICOSAT to deliver quality instruction, the readiness of partner industries to absorb program graduates, and the degree of stakeholder demand among prospective students within the institution's catchment area.

The assessment is designed to produce evidence-based conclusions that institutional leaders, regulators, and industry partners can use in deciding whether to support, modify, or proceed with the program offering.

To operationalize this feasibility assessment, the study is anchored on a set of explicit research questions and objectives that draw from established frameworks in Philippine higher education program evaluation, particularly the market-viability model previously applied to BSISM offerings in state-funded colleges (Patalinghug & Patalinghug, 2021) and the multidimensional technical and operational criteria adopted in evaluating comparable program offerings at Philippine higher education institutions (Kirab et al., 2025; Maroma et al., 2024).

Within this analytical structure, the study seeks to determine the strength of market demand for BSISM graduates in the institution's catchment area, to verify that the proposed curriculum complies with CHED standards and related regulatory issuances, to confirm the operational readiness of CICOSAT in terms of faculty credentials, laboratory resources, and instructional infrastructure, and to assess the program's projected financial sustainability across a five-year implementation horizon.

LITERATURE REVIEW

The evolution of pedagogical assessment within technical and vocational education has increasingly relied on digital-first diagnostic tools, which prioritize data-driven insights to monitor learner trajectories. However, these generalized monitoring systems often struggle to encapsulate the unique demands of security-focused curricula, where proficiency is not solely dictated by theoretical retention but by the ability to execute high-stakes operational tasks, and this highlights a significant oversight in how institutions track the readiness of security professionals.

Furthermore, moving toward a formalized degree, such as the Bachelor of Science in Industrial Security Management, represents a critical pivot from informal vocational guidance to a rigorous, academic-based approach, necessitating that feasibility assessments look beyond enrollment metrics toward the alignment between institutional instructional outputs and the actual competencies demanded by modern industrial security environments. Recent scholarship reinforces the feasibility of such programs, emphasizing that institutional viability is best evaluated through integrated assessments of market demand, operational readiness, and financial sustainability (Kirab et al., 2025; Patalinghug & Patalinghug, 2021).

Evidence from comparable programs in the Philippines suggests that a well-structured security curriculum, when designed in alignment with both CHED standards and evolving industry benchmarks, successfully

addresses critical gaps in professionalized workforce development (Maroma et al., 2024; Testa, 2025). Specifically, the literature highlights that bridging the gap between theoretical training and operational security requirements necessitates a holistic approach to program design, incorporating everything from physical threat assessment protocols to proactive digital risk mitigation strategies (Montalban & LEGASPI, 2022; Roberts & Greene, 2010).

By addressing the documented shortage of formally educated security personnel and integrating education 4.0 principles to navigate modern cyber-physical risks, the proposed BSISM program aligns with broader research trends calling for more resilient, standards-compliant, and practice-based pedagogical frameworks (Abrahams et al., 2024; Cadiz et al., 2024; Yang et al., 2023).

METHODOLOGY

Research Design

This study adopted a sequential explanatory mixed-methods research design to systematically evaluate the feasibility of the proposed BSISM program. In the initial quantitative phase, descriptive surveys were administered to prospective students to empirically gauge market demand and student interest within the institution's catchment area.

Subsequently, the qualitative phase involved focus group discussions with key stakeholders to rigorously evaluate institutional instructional infrastructure, faculty qualifications, and projected sustainability. Through the triangulation of these quantitative and qualitative data sources, the study produced a robust, evidence-based assessment that clarified the program’s structural coherence and institutional viability, ensuring that all findings were directly reflective of the institution's capacity and the surrounding community's needs.

Locale of the Study

The study is conducted across two group of respondents to ensure a comprehensive assessment of the proposed program's feasibility. Market demand is empirically gauged through surveys administered to both Grade 12 students and their parents at La Union High School, San Fernando City to ensure that there is a robust representation of the stakeholder’s perspective.

Sources of data

The research utilized a combination of primary and secondary data, encompassing structured survey questionnaires, semi-structured interviews with key industry partners, and comprehensive institutional documentary analysis.

Primary data includes the responses in the questionnaire made by grade 12 students and there parents/guardian. on the other hand, secondary data were taken from the printed copies of institutional enrollment projections, CHED curricular compliance reports, and existing facility inventory logs, which serve to validate the operational and fiscal benchmarks of the proposed program.

Furthermore, secondary data also include the printed materials of CHED memoranda, RA 5487, and RA 7722.

Respondents

A total of 162 individuals were purposively drawn into this investigation to provide well-rounded perspectives on the proposed program's viability. The sample comprised 87 graduating senior high school learners alongside 45 parents or guardians sourced from La Union High School, whose input was central to understanding prospective enrollment behavior and community-level acceptance of the degree.

Moreover, to complete the institutional lens, 30 members of the CICOSAT Colleges community (including academic personnel and key administrative officers) were likewise tapped to share insights on faculty preparedness, available learning resources, and the college's overall capacity to absorb a new offering.

Layering these viewpoints through both survey instruments and interview protocols allowed the researchers to construct a feasibility picture grounded not only in external demand signals but also in the internal realities of program delivery, ensuring that recommendations emerged from a balanced reading of stakeholder concerns.

Research Instrument

The study utilized a researcher-developed survey instrument that underwent pilot-testing to ensure internal consistency and validity before full-scale administration. Three distinct versions of the questionnaire were developed, tailored respectively to students, parents, and school administrators and faculty. The structure of these instruments comprised four sections: the first part gathered personal profile information, while the second and third parts consisted of closed-ended questions examining factors and challenges encountered when choosing a college course, as well as the specific reasons driving that decision. To capture more nuanced data, the fourth and final part included open-ended questions, allowing respondents to provide detailed, qualitative feedback.

Complementing these instruments, survey questionnaires were distributed to all Grade 12 senior high school students at La Union High School as well as their parents or guardians, ensuring a comprehensive assessment of prospective market interest.

Concurrently, data were systematically gathered from CICOSAT Colleges administrators and faculty members through semi-structured interviews and focus group discussions, which facilitated a rigorous evaluation of the institution's existing instructional infrastructure, faculty qualifications, and overall capacity to support the proposed BSISM program.

Treatment of Data

The collected information was handled through a unified set of statistical, thematic, and documentary review procedures that corresponded directly with the sequential explanatory mixed-methods framework guiding the entire investigation.

In the quantitative strand, numerical responses drawn from the structured survey instruments were summarized using frequency distributions, percentage shares, and weighted averages, with all Likert-type items measured on a four-point response format to avoid any neutral midpoint and to push respondents toward a definite positive or negative position; the verbal anchors accompanying the scale were set at 3.51–4.00 for Strongly Agree or Very High, 2.51–3.50 for Agree or High, 1.51–2.50 for Disagree or Low, and 1.00–1.50 for Strongly Disagree or Very Low.

The same descriptive tools were likewise applied to characterize the demographic profile of the respondents, to sort out preferred course options, motivating considerations, and perceived obstacles to enrollment, and to compare the responses coming from the Grade 12 learners with those contributed by their parents or guardians at La Union High School.

Meanwhile, the qualitative strand relied on a structured thematic reading of the focus group discussions and semi-structured interviews conducted with CICOSAT Colleges administrators and faculty, in which recurring assertions and observable patterns were carefully coded and assembled into coherent categories that captured institutional readiness and program sustainability.

Running alongside these efforts, a documentary review of CICOSAT's secondary records (including enrollment projections, CHED compliance submissions, facility inventories, the relevant CHED memoranda, and the texts of RA 5487 and RA 7722) was carried out to confirm regulatory conformity, clarify existing operational capacity, and surface background details on faculty credentials and available infrastructure.

Taken together, these complementary procedures enabled the researchers to cross-check the numerical findings against the lived perspectives of stakeholders and against the documentary record, producing a layered and methodologically sound appraisal of the BSISM program's market viability, instructional feasibility, and long-term sustainability.

RESULTS AND DISCUSSION

Legal basis of the Course BSISM

Republic Act No. 7722 establishes the fundamental mandate for higher education institutions to align academic programs with national, regional, and local development priorities (Olipas et al., 2022).

Furthermore, the implementation of the BSISM program directly addresses the critical demand for robust cybersecurity frameworks in response to the escalating landscape of digital threats facing Philippine higher education institutions (Bondoc & Malawit, 2020).

Such alignment necessitates the integration of established international standards with domestic regulatory mandates to ensure that institutional security architectures remain both compliant and resilient against evolving vulnerabilities (Ramos & Esponilla, 2022; Yang et al., 2023).

RA 5487 , known as the Private Security Agency Law, serves as the primary regulatory framework governing the practice of security professions in the Philippines, providing the necessary legal foundation for the licensure and professionalization of those who are interest to be part of the security profession.

CMO No.06, series of 2018 "Policies, Standards and Guidelines for the Bachelor of Science in Industrial Security Management (BSISM) Program. Under this CMO, Provides a rigorous framework for integrating professional competencies with industry-specific security protocols, effectively bridging the gap between theoretical academic training and the practical governance requirements mandated for secure organizational operations (Roberts & Greene, 2010).

Need for the Course

The rapid emergence of security threats necessitates a curriculum that bridges these technical gaps, ensuring that students acquire the specialized proficiency required to navigate modern industrial risks (Almajed et al., 2017). Furthermore, the introduction of a specialized Bachelor of Science in Industrial Security Management aligns with industry-standard frameworks that emphasize proactive threat mitigation and risk management strategies (Ani et al., 2024; Nowrozy & Jam, 2024).

Furthermore, it can be noted that there is growing interest among the prospective students in pursuing formalized credentials that emphasize both physical security operations and digital asset protection, reflecting a broader shift toward multidisciplinary risk management expertise (Abelgos et al., 2025).

This heightened demand for specialized expertise underscores the urgency of integrating academic programs that directly address contemporary security challenges and align with professional standards (Hemawati, 2025).

In the Philippines, there are limited higher education institutions currently offering comprehensive curricula specialized in industrial security management, creating a significant gap in the development of a professionalized security workforce (Aquino, 2025). This removes the opportunity for those who are seeking formal educational development related to security. This systemic deficiency hampers the capacity of local industries to deploy personnel equipped with standardized threat assessment methodologies and crisis response protocols (Testa, 2025).

It is for this reason that the CICOSAT Colleges Inc. want to propose a comprehensive Bachelor of Science in Industrial Security Management to address the critical shortage of certified professionals capable of implementing standardized security protocols.

By developing a specialized academic framework, the institution intends to align its instructional strategies with current industry requirements for physical security management and proactive risk hazard analysis (Montalban & LEGASPI, 2022). This curriculum design will incorporate Education 4.0 principles, ensuring that students engage with automated and virtualized learning environments essential for navigating the cyber-

physical systems prevalent across modern industrial sectors (Cadiz et al., 2024). This approach is further bolstered by the necessity of addressing the existing cybersecurity talent shortage, which remains a critical vulnerability across higher education and industrial sectors (Abrahams et al., 2024).

Sustainability

To ensure long-term viability, the program will conduct rigorous financial and operational analyses, evaluating resource allocation and infrastructure requirements against local market demand (Maroma et al., 2024). This evaluation includes assessing the availability of qualified faculty and the necessary technical resources to maintain high pedagogical standards in alignment with industry-standard security frameworks (Patalinghug & Patalinghug, 2021).

Additionally, the institution will prioritize the integration of a robust cybersecurity framework to protect critical academic data and research repositories, mirroring strategies adopted by other Philippine higher education institutions to mitigate emerging digital vulnerabilities.

Table 1 shows that the projected revenue exhibits a consistent upward trend from Academic Year 2026–2027 through 2030–2031, providing strong empirical evidence for the program's financial sustainability. This steady growth in tuition and institutional fees directly enables the continuous upgrading of laboratory facilities and the recruitment of qualified faculty, both of which are critical for maintaining the program's high pedagogical standards in alignment with industry-standard security frameworks (Patalinghug & Patalinghug, 2021).

By successfully reconciling these positive financial forecasts with the robust community interest, the institution establishes a resilient operational model that secures the necessary resources for long-term viability and academic success (Maroma et al., 2024).

Table 1. Income Based on Tuition and Other School Fees for BSISM for over Five Years (In pesos)

Income from Tuition and Other School Fees	**Proposed Fees per Semester per Student (AY 2026–2027)**	**AY 2026–2027 (25 Students)**	**AY 2027–2028 (28 Students)**	**AY 2028–2029 (30 Students)**	**AY 2029–2030 (33 Students)**	**AY 2030–2031 (37 Students)**
TUITION						
Tuition per Unit	₱365.72	₱18,286.00	₱20,480.32	₱21,943.20	₱24,137.52	₱27,063.28
Average of 24 Units per Semester	₱8,777.28	₱438,864.00	₱491,527.68	₱526,636.80	₱579,300.48	₱649,518.72
OTHER SCHOOL FEES						
Registration	₱418.26	₱20,913.00	₱23,422.56	₱25,095.60	₱27,605.16	₱30,951.24
Student Services	₱1,316.51	₱65,825.50	₱73,724.56	₱78,990.60	₱86,889.66	₱97,421.74
Auxiliary Services	₱971.98	₱48,599.00	₱54,430.88	₱58,318.80	₱64,150.68	₱71,926.52
Library	₱611.29	₱30,564.50	₱34,232.24	₱36,677.40	₱40,345.14	₱45,235.46
Student Development Fee	₱547.32	₱27,366.00	₱30,649.92	₱32,839.20	₱36,123.12	₱40,501.68
Insurance	₱40.22	₱2,011.00	₱2,252.32	₱2,413.20	₱2,654.52	₱2,976.28
Total Other School Fees	**₱3,905.58**	**₱195,279.00**	**₱218,712.48**	**₱234,334.80**	**₱257,768.28**	**₱289,012.92**
Grand Total	**₱12,682.86**	**₱634,143.00**	**₱710,240.16**	**₱760,971.60**	**₱837,068.76**	**₱938,531.64**
Computer Fee	₱1,206.49	₱60,324.50	₱67,563.44	₱72,389.40	₱79,628.34	₱89,280.26
Grand Total with Laboratory	**₱13,889.35**	**₱694,467.50**	**₱777,803.60**	**₱833,361.00**	**₱916,697.10**	**₱1,027,811.90**

Table 2: Increase of Student Population by 10% per Year

Academic Year	Projected Student Population (10% Increase)	Rounded Student Population
Year 1	25	25
Year 2	27.5	28
Year 3	30.25	30
Year 4	33.275	33
Year 5	36.6025	37

Note: The projected student population is based on a **10% annual increase** from the first-year enrollment of **25 students**. Since student counts must be whole numbers, the projected figures are rounded to the nearest whole number. Thus, **27.5 is rounded to 28**, **30.25 to 30**, **33.275 to 33**, and **36.6025 to 37**.

This growth trajectory underscores the program's scalability, aligning with the necessity of closing the persistent labor-market gap for skilled security professionals (AlDaajeh et al., 2022). Furthermore, this expansion strategy acknowledges the necessity of balancing student-to-faculty ratios to maintain instructional quality while addressing the increasing demand for specialized cybersecurity and industrial threat management expertise (Ramos, 2025).

Table 3: Income and Expenses for BSISM Over Five Years (In Philippine Pesos)

Particulars	Year 1 (AY 2026–2027)	Year 2 (AY 2027–2028)	Year 3 (AY 2028–2029)	Year 4 (AY 2029–2030)	Year 5 (AY 2030–2031)
Income (Tuition and Other School Fees)	₱694,467.50	₱777,803.60	₱833,361.00	₱916,697.10	₱1,027,811.90
Expenses for Salaries and Benefits of Teaching and Non-Teaching Staff	₱486,127.25	₱544,462.52	₱583,352.70	₱641,687.97	₱719,468.33
Expenses for Maintenance and School Development	₱138,893.50	₱155,560.72	₱166,672.20	₱183,339.42	₱205,562.38
Total Expenses	**₱625,020.75**	**₱700,023.24**	**₱750,024.90**	**₱825,027.39**	**₱925,030.71**
Net Income	**₱69,446.75**	**₱77,780.36**	**₱83,336.10**	**₱91,669.71**	

Table 3 present the Income and Expenses for BSISM Over Five Years shows that the program maintains a positive net financial position across the projected period, demonstrating the fiscal robustness required to support academic infrastructure and faculty development (Kirab et al., 2025). it can be notes from this table that the program achieves consistent annual profitability, providing a financial buffer that mitigates risks associated with fluctuating enrollment or unforeseen operational costs (Holdener & Shown, 2024).

Furthermore, it can be seen from the table that Expenses for Salaries and Benefits of Teaching and Non-Teaching Staff represent the primary operational cost, reflecting a commitment to competitive compensation that is essential for attracting and retaining qualified cybersecurity faculty (Betiz, 2026). This investment in human capital is vital, as the lack of standardized pedagogical approaches in cybersecurity currently contributes to inconsistent graduate competencies and workforce shortages (Basta et al., 2026).

However, the approach remains sensitive to market volatility, necessitating ongoing budget sensitivity analyses to manage inherent uncertainties in enrollment and overhead costs (Zott & Amit, 2009). To enhance the resilience of the BSISM model, future iterations should incorporate a rigorous break-even analysis to ensure that programs maintain profitability even if initial enrollment targets are not met (Florea et al., 2021; Shrivastava & Mohammed, 2017).

Marketability

The marketability of the BSISM program is intrinsically linked to the growing industry demand for specialized cybersecurity talent, which correlates with the documented expansion of academic program offerings in response to identified workforce gaps (Mero et al., 2025). This alignment with industry requirements positions the curriculum as a primary solution to the nation's critical shortage of security specialists, incident analysts, and IT auditors (Quweider et al., 2024).

READINIESS OF THE COLLEGE

Note: the BSISM is under the CCJ and is a distinct and separate college. Moreover, it is headed by a full-time Dean with Doctorate degree in Criminology.

This table presents the qualifications for the administrator. It can be seen that the appointed administrator meets the mandated academic and professional requirements established by the Commission on Higher Education, ensuring competent leadership for the program (Omorog, 2020). This complies with the qualification set be the CHED Memo Number 06, series of 2018, such institutional compliance strengthens the college's overall operational readiness, mirroring the strategic planning standards required to mitigate potential risks like faculty shortages or enrollment fluctuations (Cuyos & Castino, 2025).

TABLE 4. Qualifications for the Administrator

Qualification	Justification	Remarks
Holder of Doctoral degree in Criminology or other allied courses such as Psychology, Sociology, and Doctor of Laws; Holder of any of the undergraduate programs under the Criminal Justice Education	The Dean has a Doctorate Degree in Criminology and is a license criminologist	Complied
With credentials duly authenticated by the Commission;	The credentials of the dean of CCJE is duly authenticated by the commission.	Complied
Must have at least five (5) years teaching experience; Must have at least three (3) years administrative/supervisory experience	The dean has more than five (5) years of teaching experience with more than three (3) years of administrative experience.	Complied

This structural integration facilitates a multidisciplinary approach to curriculum development by merging criminal justice expertise with essential industrial security protocols. Such interdisciplinary synergy is critical for bridging the gap between theoretical criminology and the pragmatic demands of modern cybersecurity, ensuring that graduates possess the transferable skills necessary to navigate rapidly evolving industry threats (Blažič, 2021).

Furthermore, to ensure sustained relevance, the program should establish formal academic networks and public-private partnerships, which are essential for sharing situational awareness regarding emerging cyber-threat landscapes.

Table 5. Program Head

Qualification	Justification	Remarks
Holder of at least M.S. in Criminology Holder of graduate of B.S. Criminology; A registered Criminologist with valid PRC ID;	The Program Head is a licensed criminologist and holds a Master's degree in Criminal Justice.	Complied

Must have at least three (3) years teaching experience;Must have at least one (1) year administrative/supervisory experience; and	The program head has more than three (3) years of teaching experience and supervisory works.	Complied
Must be an active member of the accredited professional association.	The program head is an active member of PCAP.	Complied

Table 5 illustrates the institutional capacity and leadership preparedness essential to addressing the systemic management challenges often faced by higher education institutions, such as inadequate administrative support and infrastructure deficiencies (Flores, 2024). By integrating these leadership standards into the departmental structure, the institution establishes a robust framework for accountability and operational transparency (Díaz, 2024).

It further highlight institution's adherence to the stringent administrative and academic standards outlined in the curriculum requirements, which serves as a critical indicator of operational readiness. By ensuring the program head holds the necessary graduate degree, professional licensure, and substantial supervisory experience, the college fulfills the mandate for high-quality leadership essential for program success (Omorog, 2020). Furthermore, this strict compliance with regulatory benchmarks mitigates risks associated with administrative gaps and supports the long-term sustainability of the BSISM program, thereby bolstering its overall feasibility (Cuyos & Castino, 2025; Flores, 2024).

The administrative qualification demonstrate that the program fulfills the stringent institutional requirements mandated by CHED (CHED Memo no. 06, serries of 2018), serving as a critical indicator of operational readiness and providing a foundational framework for mitigating risks associated with management gaps (Cuyos & Castino, 2025; Omorog, 2020).

This established alignment with regulatory standards not only validates the program's current leadership capacity but also confirms its structural resilience, which is essential as the institution moves toward refining its comprehensive quality assurance mechanisms to better harmonize internal operations with evolving industry-specific benchmarks (Flores, 2024).

Faculty

Faculty for Professional Courses shall comply with any of the qualifications as follows: In accordance with Commission on Higher Education standards, faculty members must possess at least a Master's degree in Criminology or related fields, alongside a valid professional license, to ensure the delivery of high-quality instruction. This academic requirement is fundamental to fostering a cohesive faculty development strategy, which is critical for aligning instruction with the rigorous performance standards expected in professional licensure environments (Buan & Moyao, 2026).

Table 6 shows that the institutional faculty profile exceeds the minimum regulatory requirements, demonstrating a strong alignment between academic credentials and professional practitioner experience (Habiatan, 2019). This synthesis of academic rigor and field-based expertise is instrumental in fostering high levels of educator readiness, ensuring that the department not only satisfies mandatory regulatory benchmarks but also provides students with a learning environment deeply anchored in both theoretical depth and practical industry application (Buan & Moyao, 2026).

Furthermore, the high concentration of full-time faculty members, which exceeds the required 50% threshold, provides the necessary institutional stability and continuity to facilitate sustained mentorship and consistent academic monitoring factors that are critical for driving high-quality instruction and preparing students for the rigorous requirements of professional licensure (Buan & Moyao, 2026).

Despite these strengths, the institution must remain vigilant in mitigating potential instructional inconsistencies, as the reliance on part-time practitioners—who may face external professional demands—can occasionally disrupt classroom continuity and student progress (Albina et al., 2021).

Table 6. Faculty Qualification

Qualifications	Justification	Remarks
Holder of at least a master's degree in allied programs such as but not limited to: Industrial Security, Criminology and or Criminal Justice, Master in National Security Administration, Master in Public Safety Administration	There are 9 faculty members who are license criminologist with allied training and experiences in the field of security and one (1) who is Juris Doctor..	Complied
Must have at least one (1) year teaching experience		
Holder of graduate of S.S. Industrial Security Management, Criminology or related degree;	All of the 8 faculty members are with Masters in Criminal Justice.	
must have been a practitioner for at least three (3) years of experience in their respective fields of specialization;	All 9 faculty members have more than three years experience in there area of specialization.	Complied
Faculty members to teach the Law courses offered under this program shall be at least holders of a bachelor's degree in Law and preferably members of the Philippine Bar.	The faculty members to teach the law course offered has a bachelor's degree in law.	Complied
At least 50% of the professional courses offered under this must be taught by full-time faculty members.	70 % of the professional course offered is will be taught by full=time faculty members	Complied

Demand for the Course

Table 7. What are your main interest?

	Students		Parents	
	f	%	f	%
1. arts	22	19.84%	13	16%
2. business	16	17.46%	15	18%
3. science	25	29.37%	13	16%
4. sports	10	10.32%	17	20%
5. technology	16	16.67%	15	18%
6. others	7	6.35%	10	12%
TOTAL	96		83	

Table 7 present the main interest of the respondents, it illustrates that science emerged as the predominant field of interest among the surveyed population with 29.37%, followed closely by arts with 19.84% and business with 17.46%. This result implies that a substantial portion of the prospective student body prioritizes analytical and creative disciplines, which should inform the curriculum design for the proposed Bachelor of Science in Industrial Security Management.

Furthermore, according to Mapatac, (2026) the integration of specialized security curricula may bridge the current gap between foundational analytical competencies and the specialized professional standards demanded by contemporary industrial environments. Additionally, qualitative feedback indicates that respondents value content that mirrors real-world professional scenarios, highlighting a preference for curriculum relevance over purely theoretical models. Such alignment necessitates the incorporation of practical, discipline-specific modules that directly address the multifaceted hazards inherent in modern security management (Mekheimer, 2025).

Parents on the other hand show a distinct preference for sports-oriented career paths at 20%, reflecting a divergent set of expectations compared to the academic priorities emphasized by the students. This divergence

underscores the need for institutional stakeholders to reconcile these disparate expectations through targeted communication strategies that emphasize the long-term career stability inherent in the industrial security profession (Miller, 2023).

Bridging these perceptions requires a strategic focus on career development pathways that highlight how security management aligns with professional stability, much like the traditional careers favored by families (Lalith et al., 2022). This strategic alignment is particularly critical given that students often prioritize fields associated with higher pay, job security, and modern technological utility when evaluating their prospective educational paths (Awais et al., 2026).

Career Growth

Table 8. Which of the following course do you prefer in college?

Table 8 shows that the majority of respondents exhibit a strong inclination toward specialized professional programs, with 36% of students and 33% of parents favoring BS in Criminology, followed by BS in Industrial Security Management at 30% and 23% respectively, mirroring broader trends where job market prospects and long-term security heavily influence post-secondary educational trajectories (Kirab et al., 2025; Patalinghug & Patalinghug, 2021). This robust stakeholder interest validates the program's alignment with local career aspirations, effectively countering potential stagnation in enrollment while addressing the regional need for qualified security professionals (Kirab et al., 2025).

Table 8.

Course	**Students**		**Parents**	
	f	**%**	**f**	**%**
BS in Criminology	31	36%	27	33%
BS in Industrial Security Management	26	30%	19	23%
BS in Forensic Science	16	18%	17	21%
other course	14	16%	18	22%
Total	87		81	100%

This interest appears to be driven by a pragmatic recognition of evolving labor market trends, where students strategically align their educational choices with sectors perceived to offer greater stability and professional growth (Hasan & Akter, 2023).

Moreover, institutional efforts to bolster this interest should focus on bridging current competency gaps in areas such as marksmanship, technical report writing, and advanced communication skills (Jimmy & Ayeo-eo, 2024).

Such pedagogical adjustments would not only align the program with industry standards but also mitigate the risks associated with program-strand mismatch, ensuring students are adequately prepared for the demands of the workforce (S. et al., 2025; Tagsip, 2025).

Furthermore, integrating industry-aligned experiential learning and mentorship opportunities can address the complexities students face when transitioning from senior high school to specialized degree programs, (Navarra & Reyes, 2026). As these transitions often involve navigating significant structural and financial challenges that necessitate proactive institutional support (Tagsip, 2025).

Furthermore, fostering strong partnerships with relevant professional organizations and governmental agencies is essential to enhance the program’s relevance and ensure that graduates meet the rigorous standards expected by employers (Nayoyos-Refugia, 2024). By formalizing these collaborative frameworks, the institution can effectively navigate the intersection of student passion and industry-driven career prospects (Nobis, 2025). Ultimately, the successful implementation of this program requires an evidence-based approach that

acknowledges the socio-economic backgrounds and diverse career aspirations of students as critical variables in their persistence.

Table 9. Which of the following course do you prefer in college?

Course	Students		Parents	
	f	%	f	%
BS in Criminology	31	36%	27	33%
BS in Industrial Security Management	26	30%	19	23%
BS in Forensic Science	16	18%	17	21%
other course	14	16%	18	22%
Total	87		81	100%

Table 9 shows that a significant portion of prospective students and their parents perceive the Bachelor of Science in Industrial Security Management as a highly viable career path, with 30% of students expressing a clear preference for the program. This strong stakeholder interest validates the program's alignment with local career aspirations and serves as a proactive measure against regional educational stagnation (Kirab et al., 2025).

Furthermore, the empirical findings indicate that successfully integrating industry-driven components into the BSISM curriculum will be pivotal for converting expressed stakeholder interest into sustained enrollment and graduate employability.

The 30% student preference rate captured in the survey, coupled with the 23% parental endorsement of the program, demonstrates that BSISM resonates meaningfully with both prospective learners and the households shaping their educational decisions, effectively positioning the offering as a credible response to the under representation of locally relevant security degrees and the broader national deficit in industrial security professionals (Kirab et al., 2025; Patalinghug & Patalinghug, 2021).

In addition, this alignment between stakeholder interest and labor-market demand mirrors patterns observed across the wider cyber-security education landscape, where curricula anchored in industry competencies, professional certifications, and experiential learning have proven decisive in strengthening marketability and producing workforce-ready graduates (Knapp et al., 2017).

Moreover, embedding structured partnerships with private security agencies, government regulators, and certifying bodies within BSISM would further reinforce its value proposition by exposing students to operational environments, applied risk-management scenarios, and recognized credentials that amplify the marketability signal already evident in the survey (P. et al., 2025; Quweider et al., 2024).

Such integration ensures that the program remains responsive to evolving employer expectations while assuring that graduates possess both the theoretical grounding and the practical competencies required by security-sensitive industries (Mero et al., 2025; P. et al., 2025). Ultimately, the long-term marketability of BSISM depends not solely on communicating its alignment with workforce priorities but also on continuously refining its industry-driven components to sustain relevance amid shifts in the threat landscape, regulatory regime, and competency standards facing the security sector (Patalinghug & Patalinghug, 2021).

CONCLUSION

The feasibility study underscores the imperative for offering the Bachelor of Science in Industrial Security Management as a strategic intervention to bridge the regional gap between educational offerings and professional labor demands. The strong, documented interest from prospective students and stakeholders validates the program's necessity, positioning it as an essential response to the national deficit of skilled security professionals.

Its long-term sustainability is anchored in the continuous integration of industry-aligned competencies and the formalization of experiential learning partnerships, which collectively ensure that the curriculum remains adaptive to evolving threat landscapes and regulatory requirements.

Furthermore, by grounding the program in practical, skill-focused training and professional certification pathways, the BSISM is uniquely positioned to enhance graduate marketability, ensuring that students are not only technically proficient but also immediately workforce-ready upon completion.

Moving forward, subsequent evaluative phases should focus on longitudinal assessments of graduate performance within the field and the refinement of curriculum frameworks through recurring stakeholder feedback loops. These efforts will further substantiate the program's role in promoting regional socioeconomic stability, demonstrating the broader efficacy of specialized academic initiatives in directly addressing localized labor market saturation and professional skill deficits.

REFERENCES

1. E. M. H., & -, M. P. M. (2025). Academic Program Audit: A Quality Assurance Mechanism for Higher Education Programs in the University of Baguio. *International Journal For Multidisciplinary Research*, *7*(1). https://doi.org/10.36948/ijfmr.2025.v07i01.36565
2. Abelgos, A. H., Maroma, D. P., & Maroma, A. N. (2025). Integrating Technological Advancements to Improve Pedagogical Quality in Drafting Technology. *International Journal of Multidisciplinary Applied Business and Education Research*, *6*(10), 5232–5249. https://doi.org/10.11594/ijmaber.06.10.30
3. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699
4. Albina, A. C., Balasabas, J. Y., Laquinon, B. J. I., Pampilo, M. H., & Caballero, L. J. (2021). Factors and Challenges Influencing the Criminologist Licensure Examination Performance through the Non-passers' Lens. *European Journal of Educational Research*, 365–380. https://doi.org/10.12973/eu-jer.11.1.365
5. AlDaajeh, S. H., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *IRIS*, *119*, 102754–102754. https://doi.org/10.1016/j.cose.2022.102754
6. Almajed, A., Al-Kathiri, F., Al-Ajmi, S. E., & Alhamlan, S. (2017). 21st Century Professional Skill Training Programs for Faculty Members—A Comparative Study between Virginia Tec University, American University & King Saud University. *Higher Education Studies*, *7*(3), 122–122. https://doi.org/10.5539/hes.v7n3p122
7. Ani, N., Millah, S., & Sunarya, P. A. (2024). Optimizing Online Business Security with Blockchain Technology. *Startupreneur Business Digital (SABDA Journal)*, *3*(1), 67–80. https://doi.org/10.33050/sabda.v3i1.488
8. Aquino, J. M. (2025). Best practices of high performing higher education institutions in the Philippines towards the development of harmonized quality-assured instructional leadership framework. *Frontiers in Education*, *10*. https://doi.org/10.3389/feduc.2025.1663289
9. Basta, S., Alkadi, I., & Basta, R. M. (2026). Proposed Standards for Cybersecurity Curricula in Higher Education. *International Journal of Innovative Science and Research Technology (IJISRT)*, 1481–1481. https://doi.org/10.38124/ijisrt/26mar896
10. Betiz, J. (2026). Offering Bachelor of Science in Information Systems (BSIS) in Bicol College, Daraga, Albay: A Feasibility Study. *International Journal of Research and Scientific Innovation*, *13*(1), 1719–1727. https://doi.org/10.51244/ijrsi.2026.13010150
11. Blažič, B. J. (2021). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

12. Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, *2*(3), 16–21. https://doi.org/10.30574/gjeta.2020.2.3.0013
13. Buan, E. A. U. of B., & Moyao, W. G. (2026). *Enhancing Licensure Examination Outcomes: Best Practices among Top-Performing Criminology Schools in Region III, Philippines*. https://european-science.com/eojnss/article/view/6931
14. Cadiz, Ma. C. D., Manuel, L. A. F., Reyes, M. M., Natividad, L., & Ibarra, F. P. (2024). TECHNOLOGY INTEGRATION IN PHILIPPINE HIGHER EDUCATION: A CONTENT-BASED BIBLIOMETRIC ANALYSIS. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi|JIITUJ|*, *8*(1), 35–47. https://doi.org/10.22437/jiituj.v8i1.31807
15. Cuyos, M. M., & Castino, J. M. P. (2025). Feasibility Study on the Offering of Bachelor of Science in Business Administration Major in Human Resource Management (BSBA-HRM) Program at Cronasia Foundation College, Inc. *International Journal of Research and Innovation in Social Science*, 3736–3762. https://doi.org/10.47772/ijriss.2025.903sedu0270
16. Díaz, A. O. (2024). ASSESSMENT OF SENIOR HIGH SCHOOL PROGRAM DELIVERY TOWARDS QUALITY ASSURANCE: EVIDENCE FROM THE PHILIPPINES. *Education Sustainability & Society*, *7*(2), 74–83. https://doi.org/10.26480/ess.02.2024.74.83
17. Florea, N. V., Paschia, L., Coman, D. M., Ionescu, C. A., Coman, M. D., Ene, C. M., & Nicolau, N. L. G. (2021). BIDIRECTIONAL APPROACH FOR UNIVERSITY MANAGEMENT: IMPROVED RELATIONSHIP WITH STUDENTS AND EDUCATIONAL COSTS MANAGEMENT. *Journal of Business Economics and Management*, *22*(5), 1209–1230. https://doi.org/10.3846/jbem.2021.14687
18. Flores, M. L. (2024). IT Security Management Challenges of State Universities and Colleges. *Cognizance Journal of Multidisciplinary Studies*, *4*(9), 18–37. https://doi.org/10.47760/cognizance.2024.v04i09.003
19. Habiatan, E. N. (2019). Bachelor of science in criminology program: Extent of compliance on the policies and standards prescribed by the commission on higher education. *International Journal of Advanced Research in Management and Social Sciences*, *8*(10), 113–135. https://www.indianjournals.com/ijor.aspx?target=ijor:ijarmss&volume=8&issue=10&article=005
20. Hemawati, H. (2025). Integrating Technology to Enhance Teaching and Learning: A Mixed-Methods study. *International Journal of Scientific Research in Science and Technology*, *12*(5), 274–278. https://doi.org/10.32628/ijsrst25125131
21. Holdener, E., & Shown, D. (2024). Building Software Engineering Capacity through a University Open Source Program Office. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2406.08679
22. Kirab, F. D., Macabinta, J. G., & Castino, J. M. P. (2025). Proposing a Bachelor of Science in Industrial Security Management (BSISM) at SKSU Palimbang: Addressing Enrollment and Employment Challenges in Sultan Kudarat. *International Journal of Research and Innovation in Social Science*, 2276–2281. https://doi.org/10.47772/ijriss.2024.8120190
23. Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of the Association for Information Systems*, *28*(2), 101–114. https://aisel.aisnet.org/jise/vol28/iss2/4
24. Maroma, A. N., Galita, W. M., & Maroma, D. P. (2024). A Feasibility Study on the Offering DITM Doctor of Industrial Technology Management (DITM) at the Graduate School Bulacan State University-Main Campus. *International Journal of Multidisciplinary Applied Business and Education Research*, *5*(11), 4788–4799. https://doi.org/10.11594/ijmaber.05.11.37
25. Mero, P., Pepsin, A., & Kreider, C. (2025). Assessing the Maturity of Cybersecurity Education in Virginia and the Impact of State Level Investment. In *ArXiv.org*. https://doi.org/10.48550/arxiv.2502.18456
26. Montalban, L. J. T., & LEGASPI, N. M. (2022). ILOILO SCIENCE AND TECHNOLOGY UNIVERSITY SECURITY MANAGEMENT CAPABILITY: BASIS FOR FORMULATING SECURITY MANAGEMENT ACTION PLAN. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.6942422
27. Nowrozy, R., & Jam, D. (2024). Embracing the Generative AI Revolution: Advancing Tertiary Education in Cybersecurity with GPT. In *arXiv (Cornell University)*. Cornell University.

https://doi.org/10.48550/arxiv.2403.11402

28. Olipas, C. N. P., Luciano, R. G., Sison, R. B., Padre, J. M., Collado, M. C., & Pula, R. L. (2022). A Convergent-Parallel Analysis on the Technical Assistance Provided by Information Technology Faculty Extensionists: Basis for Training and Extension Activities Plan. *Path of Science*, *8*(11), 4007–4015. https://doi.org/10.22178/pos.87-6
29. Omorog, C. D. (2020). IDAE framework: A guide for establishing industry-driven academic programs. *International Journal of Evaluation and Research in Education (IJERE)*, *9*(2), 461–461. https://doi.org/10.11591/ijere.v9i2.20341
30. P., M., John Paul, I., T., Marlon, & D., C., Joel. (2025). Cybersecurity skills in new graduates: a Philippine perspective. In *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2512.14778
31. Patalinghug, M. E., & Patalinghug, H. F. (2021). Market Needs Assessment for Bachelor of Science in Industrial Security Management in a State-Funded College. *Jurnal Pendidikan Progresif*, *11*(3), 602–609. https://doi.org/10.23960/jpp.v11.i3.202111
32. Quweider, M., Khan, F., Zhang, L., & Lei, H. (2024). *Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century*. https://doi.org/10.18260/1-2--41292
33. Ramos, M. C. (2025). Gearing Up for Cyberwarfare: A Feasibility Study for a Bachelor of Science in Cybersecurity Program. *Asia Pacific Journal of Management and Sustainable Development*, *13*(1), 80–91. https://doi.org/10.70979/bbme2966
34. Ramos, N. M. D., & Esponilla, F. D. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation and Research in Education (IJERE)*, *11*(3), 1198–1198. https://doi.org/10.11591/ijere.v11i3.22863
35. Roberts, D., & Greene, L. (2010). The theatre of high-fidelity simulation education. *Nurse Education Today*, *31*(7), 694–698. https://doi.org/10.1016/j.nedt.2010.06.003
36. Shrivastava, U., & Mohammed, T. (2017). A Cybersecurity Executive DBA? *Journal of Information Technology Education Discussion Cases*, *6*, 9–9. https://doi.org/10.28945/3925
37. Testa, E. (2025). Level of Compliance and Challenges Encountered in Criminology Program Implementation: Basis for Quality Enhancement Measures. *International Journal of Innovative Science and Research Technology (IJISRT)*, 1643–1643. https://doi.org/10.38124/ijisrt/25nov1024
38. Yang, Y., Song, Z., & Monreal, R. N. (2023). DESIGN OF THE NETWORK SECURITY ARCHITECTURE FOR SMART CAMPUS IN THE PHILIPPINES. *Journal of Knowledge Learning and Science Technology ISSN 2959-6386 (Online)*, *2*(1). https://doi.org/10.60087/mrb0hh55
39. Zott, C., & Amit, R. (2009). Business Model Design: An Activity System Perspective. *Long Range Planning*, *43*, 216–226. https://doi.org/10.1016/j.lrp.2009.07.004