Shawe, R., (2025). J Inform Techn Int, 3(2): 111
https://doi.org/10.33790/jiti1100111

Journal of Information Technology and Integrity

Security Risk Management Frameworks in the U.S. Community Colleges: Evaluating the DoD Antiterrorism Program's Suitability

Robb Shawe, Ph.D., MS,
Department of Emergency and Protective Services, Capitol Technology University, Laurel, MD, United States.

Article Details
Article Type: Review Article
Received date: 02nd September, 2025
Accepted date: 16th October, 2025
Published date: 18th October, 2025

***Corresponding Author:** Robb Shawe, Ph.D., MS, Department of Emergency and Protective Services, Capitol Technology University, Laurel, MD, United States.

Citation: Shawe, R., (2025). Security Risk Management Frameworks in the U.S. Community Colleges: Evaluating the DoD Antiterrorism Program's Suitability. *J Inform Techn Int, 3*(2): 111. doi: https://doi.org/10.33790/jiti1100111

Abstract

This study evaluates the applicability of the Department of Defense Antiterrorism (DoD AT) Program within U.S. community colleges, highlighting the challenges faced by open-access institutions with limited resources. Using a sequential mixed-methods design, the study integrates quantitative and qualitative findings to assess both the strengths and limitations of DoD AT in civilian education. Results indicate that while the framework provides a structured foundation, its adaptability is uneven across institutional contexts. The study introduces the Dynamic Stakeholder-Integrated Security Framework (DSISF), an applied model emphasizing stakeholder engagement, flexible layering, continuous feedback, and inclusion. DSISF offers practical guidance for community college administrators seeking to enhance campus safety within existing constraints. Across 197 responses from 12 states (43.8% response rate), 68% rated DoD AT as effective for preparedness, yet only 39% reported full protocol adoption; DSISF targets these adoption gaps through stakeholder engagement, layered controls, and continuous feedback.

Keywords: Security Risk Management, Community Colleges, Anti-Terrorism Program, Campus Safety, Mixed-Methods, Framework Evaluation, Higher Education, Risk Assessment, Stakeholder Engagement, Institutional Variability, Crisis Response, Policy Development, Cybersecurity, Campus Crime, Resource Allocation, Urban-Rural Differences

Introduction

Effective security risk management frameworks are essential for ensuring the safety and resilience of the United States community colleges. These institutions face unique challenges due to their open-access nature and diverse populations, which expose them to a range of security threats. In this context, the study's investigation into the viability of existing security frameworks, specifically the Department of Defense's Antiterrorism program (DoD AT), is particularly relevant. The interaction between educational environments and security measures necessitates a tailored approach to address both routine safety concerns and potential crises. Thus, the exploration of these frameworks aims not only to enhance community college security infrastructure but also to contribute to broader discussions on optimizing educational safety protocols across diverse institutional settings.

Disclaimer. Portions of this manuscript build upon the author's earlier work; all new analyses, findings, and interpretations are original to this submission.

Problem Statement

Community colleges face immediate threats in security management, including limited funding, diverse populations, and heightened vulnerability to both internal and external risks. These challenges create urgent gaps in prevention, preparedness, and response capabilities that require tailored frameworks rather than reliance on models developed for military environments. Recent events underscore the urgency. For example, on August 29, 2024, Chattanooga State Community College issued a campus lockdown after a reported threat triggered a shelter-in-place order and law enforcement response; the threat was later deemed not credible. Similarly, on July 30, 2024, Northwest Arkansas Community College (NWACC) shut down its network after detecting a ransomware intrusion, disrupting institutional systems. These incidents highlight both physical and cyber risk vectors in open-access environments.

Significance of the Study

Hence, the significance of this study lies in its contribution to broader educational and policy discussions. By evaluating the suitability of DoD AT for U.S. community colleges, the research addresses the intersection of national security models and higher education policy. The findings offer insights into compliance with federal mandates, institutional governance, and resilience planning.

Justification for Evaluating the DoD AT Program

Specifically, the DoD AT's program offers a strategic framework that is both relevant and applicable to community colleges, given its comprehensive approach to managing diverse security threats. Community colleges were characterized by their open-access nature and demographic diversity, and encountered complex security challenges that necessitate robust and adaptable security measures. The AT program's structured methodologies can be tailored to address the unique vulnerabilities and threat perceptions prevalent within

these educational environments. By integrating these methodologies, colleges can enhance the capacity of their security personnel, drawing parallels with the rigor and precision found in homeland security education programs, where tailored strategies are crucial [1]. Evaluating the AT program is of utmost importance as it offers a valuable opportunity to bridge existing gaps in campus safety, equipping administrators with practical tools to safeguard their institutions while supporting the mission of educational accessibility and community engagement. This emphasis on the importance of the research should convey to the audience the seriousness of the topic and the need for their attention.

Assumptions, Biases, and Challenges

Nonetheless, this study is grounded on several assumptions that may influence both its methodology and outcomes. A key assumption is the applicability of the DoD AT's program to community colleges, assuming that its approaches are sufficiently adaptable to address the diverse threat perceptions and challenges these institutions face [2]. Biases may arise from variations in how colleges perceive and respond to threats, potentially affecting the study's conclusions about the program's efficacy. Moreover, challenges such as limited stakeholder engagement have been identified, which could hinder the comprehensive adoption of the proposed security frameworks [2]. It is essential to acknowledge these assumptions, biases, and challenges to accurately interpret the findings within the complex context of community college security needs, thereby laying a foundation for future research to refine and further develop these insights.

Contextual and Theoretical Foundation

Before detailing the research design, it is important to situate this study within the broader scholarly context of security risk management. Prior studies on institutional frameworks, compliance with the Clery Act, and the adoption of information security management systems have established the foundations for analyzing campus safety. However, these frameworks are often designed for resource-rich or military environments and do not fully address the constraints of community colleges.

To strengthen the analytical basis of this research, two perspectives are applied: risk management theory and stakeholder theory. Risk management theory emphasizes the identification, assessment, and mitigation of threats across organizational systems, while stakeholder theory highlights the importance of balancing diverse interests and perspectives in decision-making. Together, these lenses provide a critical foundation for evaluating whether the DoD AT's framework, developed for defense contexts, can be adapted to the unique needs of open-access institutions.

This theoretical orientation informs the methodology that follows and provides the rationale for developing the Dynamic Stakeholder-Integrated Security Framework (DSISF) as an applied, practitioner-focused model.

Overview of Research Design and Methodology

Firstly, the study's three-stage exploratory-sequential mixed-methods approach began with a qualitative phase to gather deep insights into current security practices and challenges faced by community colleges. This initial stage involved detailed interviews and focus groups with stakeholders in selected institutions to form a rich data foundation. The second stage advanced to instrument development, where insights obtained from the qualitative phase inform the creation of measurement tools that are both reliable and contextually relevant [3]. These instruments were then used in the third stage, characterized by quantitative testing, which applies the newly developed tools to a representative sample of community colleges across different states. This structured methodology not only seeks to capture the breadth of community colleges' security landscapes but also aims to establish a comprehensive understanding of how the DoD AT's program could be adapted for these settings [4].

Secondly, the qualitative exploration stage functions as a vital foundation for comprehending the nuanced security dynamics within community colleges. This phase was structured to gather rich, contextualized data through interviews and focus groups conducted with diverse stakeholders, including administrators, faculty, and students. For instance, recent studies have demonstrated that stakeholder perceptions of campus safety are often influenced by both personal experiences and institutional communication [5]. By analyzing stakeholder experiences and perceptions, the study identifies key areas where the DoD AT's program either aligns with or diverges from existing practices, thereby informing subsequent stages of the research [6]. This qualitative data plays a crucial role in guiding the development of customized measurement instruments that accurately reflect the unique security challenges and perceptions within these educational environments. Thus, the qualitative exploration not only informs the formulation of relevant tools for quantitative analysis but also enhances the study's overall capacity to address the specific security requirements of community colleges through methodologically informed steps.

Subsequently, the instrument development phase focused on designing tools to evaluate the appropriateness of the DoD AT program within community colleges. This stage consolidates insights from qualitative research to develop reliable measures that accurately capture the security dynamics inherent in these educational institutions. Drawing on methodologies established in comparable contexts, such as risk management framework development in Kenyan public universities, this phase emphasizes the importance of aligning instrument design with the identified vulnerabilities and security needs [7]. The development of these instruments involved a meticulous balance between encompassing the necessary characteristics for assessing the AT program's alignment and addressing the intricate security requirements distinctive to community colleges. Through this systematically designed evaluation framework, the study aims to deliver robust, data-driven insights that enhance the adaptability and effectiveness of the Antiterrorism program in cultivating a secure learning environment across diverse community college campuses.

Finally, the quantitative testing phase applied the newly developed instruments to a selected sample of community colleges across various states, ensuring regional diversity and contextual relevance. This stage involved comprehensive data collection through surveys distributed to security personnel and administrators, focusing on their experiences and evaluations of the Antiterrorism (AT) program's effectiveness [3]. The data were analyzed using statistical software to identify patterns and correlations between the program's implementation and the perceived security enhancements at these institutions. Notably, the analysis also accounted for variations in reported effectiveness based on differing college environments, addressing challenges such as bureaucratic obstacles and resource constraints [8]. Through this meticulous process, the study aimed to provide a nuanced understanding of how tailored security measures informed by the AT program can effectively mitigate perceived vulnerabilities within the diverse community college ecosystem.

Ultimately, the study aims to achieve several key objectives essential to enhancing campus security at community colleges. By clarifying the applicability of the DOD AT's program, it intends to inform and guide community college administrators in refining their security strategies. This includes implementing customized training programs and developing adaptive measures that address the specific security challenges inherent to these institutions [3]. Additionally, the study aims to provide scalable insights into security management, thereby assisting administrators in mitigating risks and fostering a secure educational environment that promotes learning and retention. Through these initiatives, the research contributes to the broader educational mission by ensuring the safety and resilience of community colleges, which are vital to workforce development and societal stability. It is noteworthy that recent national surveys indicate that improved campus safety is associated with higher student retention and engagement rates [9, 10].

In addition to providing immediate recommendations, the study's findings lay the groundwork for future research and practical advancements in security risk management. The identified limitations of the DOD AT's program when implemented in community colleges highlight areas where frameworks must be tailored to the unique characteristics and threat perceptions of these institutions. Future investigations may explore integrating comprehensive stakeholder engagement, a component often neglected, to enhance the applicability and resilience of the framework, as evidenced by insights from coastal community disaster management frameworks [2]. This adaptation could involve a nuanced approach that focused not merely on procedural enhancements but also on collaborative strategies with local law enforcement and security experts, thereby ensuring a multifaceted understanding of risk dynamics. Furthermore, continuous evaluation and refinement of security measures, driven by emerging threats and technological advancements, are imperative, thereby encouraging an adaptive learning model crucial for ongoing security enhancements.

Moreover, the broader context of security risk management in educational institutions underscores the imperative for adaptable frameworks capable of addressing a range of threats across diverse environments. Institutions, especially community colleges, must contend with security challenges that are distinct from those encountered by primary schools or universities, owing to their open-access policies and the demographic diversity they serve [3]. The focus of this study on assessing the DoD AT's program situates it within this expansive discourse, highlighting the importance of customized approaches that accommodate unique security dynamics. By examining potential adaptations to the DOD AT's program, the research highlights the importance of aligning security frameworks with the specific needs of community colleges operating in complex operational environments. Consequently, this study not only advances security measures but also offers a framework for ongoing investigation and implementation of effective risk management strategies within educational settings.

Implementing the DoD AT's program in community colleges presents distinct challenges and opportunities. Due to their open-access nature and diverse student populations, these colleges are vulnerable to various security threats, making it challenging to implement a standardized program such as the DoD AT across all institutions [11]. A key challenge is tailoring the AT program to fit the specific security needs of community colleges, which often have limited resources and face different threat perceptions than military or government facilities. However, there is an opportunity to enhance collaboration between educational institutions and security experts, enabling community colleges to leverage broader expertise in developing innovative security solutions [11]. By addressing these challenges and seizing available opportunities, community colleges can use the DoD AT program to enhance their security measures, creating a safer environment that supports educational success.

The collaboration between community colleges and security experts is vital to developing effective risk management strategies. Community colleges benefit greatly from the knowledge and experience of security professionals, particularly when adapting frameworks such as the DoD AT's program to their specific needs. This partnership not only facilitates the exchange of best practices but also promotes a tailored approach to address the various security challenges these institutions face. In homeland security education, collaborating with security experts can enhance academic institutions' preparedness to respond to potential threats, underscoring the importance of integrating these strategies into curriculum development [12]. Through partnerships with security professionals, community colleges can foster innovation and refine their security protocols, thereby strengthening their capacity to sustain a safe and secure learning environment.

Similarly, technology plays a crucial role in enhancing security protocols in community colleges, offering both innovative solutions and significant challenges. The incorporation of advanced technological systems, such as surveillance cameras, biometric access controls, and alert systems, can augment monitoring and response capabilities, thereby improving overall security effectiveness [13]. Nevertheless, one of the foremost challenges in implementing these technological solutions is the resource limitations typical of community colleges, which may restrict the adoption and maintenance of sophisticated technology.

Furthermore, concerns related to privacy and the potential over-reliance on technology underscore the limitations inherent in purely technological security measures [13]. Ultimately, although technology offers valuable tools for risk management, its effective integration necessitates careful consideration of institutional resources and a balanced approach that combines technological, procedural, and human factors to ensure comprehensive security strategies within community colleges.

Therefore, examining policy modifications can be pivotal in advancing security frameworks within community colleges. Implementing more dynamic, responsive policies that address the unique security challenges these institutions face could enhance their capacity to manage risks effectively. One pertinent area for policy improvement is cybersecurity, which remains a growing concern as community colleges increasingly rely on digital platforms for their operations and educational delivery [14]. Policies that prioritize modernizing cybersecurity measures and developing comprehensive incident response strategies can reduce vulnerabilities and enhance overall resilience. Moreover, establishing collaborations with private cybersecurity firms and government agencies to share resources and expertise can further strengthen the security infrastructure, thereby supporting a balanced, integrated risk management approach tailored to the specific context of community college environments.

Consequently, the study advanced the existing literature on security risk management by offering a nuanced evaluation of the DoD AT program's applicability within community colleges. Previous research has predominantly focused on crime prevention and improving perceived safety among students and faculty, emphasizing the need for tailored strategies that address each institution's unique challenges [15]. By providing empirical evidence of the AT program's strengths and limitations, this study contributes a crucial layer of knowledge regarding the tailored application of such frameworks in educational settings. However, a notable gap remains in understanding how adaptation processes impact the broader academic mission, particularly regarding integrating security measures without deterring the open-access ethos of community colleges. Future research should explore how stakeholder engagement and continuous adaptation of security strategies can bridge these gaps, ensuring that safety protocols support rather than hinder the educational experience and institutional objectives.

Enhanced Critical Engagement

This study not only synthesizes existing literature but also critically evaluates the effectiveness of the DoD AT program within the context of recent campus security challenges. Unlike prior research that primarily concentrated on traditional crime prevention, this analysis underscores the significance of adaptability, stakeholder engagement, and the integration of technology and cybersecurity. By comparing the DoD AT program's structured approach with the evolving requirements of community colleges, the study exposes both the strengths and deficiencies of current frameworks, providing a more nuanced understanding to inform future research and policy development.

Conclusion

The critical importance of security risk management frameworks for community colleges in the United States is evident throughout the

chapter. By examining the unique challenges posed by open-access environments and diverse student populations, the chapter underscored the need for tailored security strategies and the value of evaluating the DoD AT program for these institutions. The methodology and rationale for the study were outlined, highlighting the need for adaptive, context-specific solutions that address both routine and emergent threats. Ultimately, this chapter laid the foundation for understanding the broader significance of security frameworks in promoting safe and supportive educational environments, guiding the research toward practical, impactful outcomes.

Literature Review

Overview of Security Risk Management in Higher Education

Security risk management has become an increasingly prominent concern for higher education institutions, particularly as campuses face a growing array of threats ranging from physical violence to cyberattacks. In 2021, the U.S. Department of Education reported over 28,000 criminal incidents on college campuses, with community colleges accounting for a significant portion due to their open-access policies and diverse populations [16]. Community colleges serve nearly 10 million students annually, representing approximately 35% of all U.S. undergraduates [9]. The evolution of campus security frameworks reflects both changing threat landscapes and shifts in regulatory expectations. These frameworks must address not only routine risks but also emergent threats, including mass violence and cybersecurity breaches. Empirical evidence underscores the importance of developing comprehensive security plans that include stakeholder collaboration, law enforcement partnerships, and proactive risk assessment to ensure resilience and continuity in educational environments.

Information Security Management Frameworks

Information security management frameworks (ISMFs) play a crucial role in addressing the complex risks faced by higher education institutions. Frameworks such as ISO 27000, COBIT, ITIL, and NIST have been widely adopted to structure security practices and guide risk assessment, asset protection, and incident response [17]. However, a 2022 survey found that only 58% of U.S. community colleges reported having a comprehensive information security plan in place, often due to resource constraints and varying institutional cultures [16]. The successful adoption of ISMFs requires not only technical solutions but also strong governance, effective stakeholder engagement, and ongoing training [7]. Tailoring these frameworks to the unique operational realities of community colleges is essential for effective risk management and sustainable security outcomes.

Crime Prevention and Campus Safety in Community Colleges

Crime prevention remains a central concern for community colleges, where open-access policies and diverse populations can heighten vulnerabilities to safety threats. According to the U.S. Department of Education's Clery Act data, community colleges reported over 7,000 criminal offenses in 2021, with theft, burglary, and assault as the most common crimes [16]. Studies indicate that approximately 20% of community college students report experiencing some form of campus crime during their enrollment [5]. Administrators are encouraged to implement proactive crime prevention strategies, such as enhanced patrols, safety education, and community engagement initiatives, to reduce victimization rates and alleviate safety concerns. Mixed-methods research highlights that perceptions of campus safety are shaped not only by actual incidents but also by institutional responses and communication strategies [6]. Therefore, effective crime prevention in community colleges requires a coordinated approach that integrates environmental design, policy development, and stakeholder input to foster a secure and supportive educational environment.

The DoD AT Program and Its Relevance

The DoD AT program provides a structured framework designed to address a spectrum of security threats, with its origins in military and governmental settings. Recent scholarship has explored the relevance and adaptability of this program to higher education, particularly community colleges, which face increasingly complex security landscapes [18]. While the DoD AT program offers comprehensive protocols for crisis response and prevention, its direct application to academic settings presents challenges. Community colleges differ from military institutions in terms of resources, threat perceptions, and operational flexibility [19]. Evaluations suggest that while the AT program can enhance training and preparedness among campus safety personnel, its effectiveness depends on modifications that account for the unique demographic and cultural contexts of community colleges [20]. Thus, the program serves as both a resource and a point of critical analysis for educational security management.

Cybersecurity and Emerging Threats

Cybersecurity has rapidly emerged as a critical area of concern for higher education institutions, including community colleges. According to the U.S. Department of Education [16], higher education institutions have reported a significant increase in cyber incidents, with ransomware and phishing attacks affecting both operational continuity and the protection of sensitive data. Community colleges, due to limited IT resources, are especially vulnerable to breaches that can disrupt learning and compromise student information. National Center for Education Statistics data show that nearly 60% of community colleges have experienced at least one cybersecurity incident in the past five years [16]. Effective policy responses require modernizing cybersecurity protocols, developing robust incident response strategies, and ongoing collaboration with government agencies and private firms. Addressing these challenges is essential to safeguard sensitive information and maintain institutional resilience in an evolving threat landscape.

Gaps and Future Directions in Research

Despite advances in security risk management for community colleges, several gaps remain in the literature. Notably, the limited integration of comprehensive stakeholder engagement in framework development can compromise the applicability and resilience of security strategies [2]. Additionally, many existing frameworks do not fully address the interrelationships between multiple hazards or the evolving nature of security threats. Future research should focus on enhancing adaptability, fostering stakeholder collaboration, and evaluating the long-term effectiveness of implemented frameworks. Emphasizing context-specific solutions and continuous evaluation will be critical for developing robust, sustainable security practices that meet the unique needs of community colleges and support their educational missions.

Conclusion

This study concludes that while the DoD AT's Program provides a valuable starting point for campus security planning, its direct application to community colleges is limited. The findings of this research demonstrate that open-access institutions face unique challenges, including resource constraints, diverse student populations, and heightened vulnerability to internal and external threats. These contextual realities limit the transferability of military-oriented frameworks.

The DSISF offers a tailored, context-specific solution for community colleges. By emphasizing stakeholder engagement, flexible layering of security strategies, continuous feedback, and inclusivity, DSISF bridges the gap between technical safeguards and the relational dynamics of campus life. This positions the framework as both a theoretical contribution and a practical tool for administrators.

Policy implications of this research include strengthening compliance with federal mandates such as the Clery Act, guiding targeted resource allocation, and integrating stakeholder perspectives into institutional governance. To move from theory to practice, four actionable steps are recommended for administrators:

1. Establish cross-departmental security committees to ensure collaboration.
2. Prioritize cost-effective, layered security measures that can be scaled to institutional capacity.
3. Incorporate regular stakeholder feedback into security planning and evaluation cycles.
4. Leverage federal resources and training programs to enhance institutional capacity.

While this study's limitations include scope and generalizability, the findings remain significant in advancing community college resilience. By contextualizing security frameworks to meet the needs of open-access institutions, this research provides both scholarly insight and practical guidance for the future of security risk management in higher education.

Methodology

Research Questions

1. How suitable is the DoD AT program for addressing the unique security needs of community colleges in the United States?
2. What are the perceptions of community college stakeholders (administrators, faculty, staff, and students) regarding the effectiveness and adaptability of the DoD AT program?
3. What modifications or adaptations are necessary for the DoD AT program to be effectively implemented in diverse community college environments?
4. How do community colleges currently address security risk management, and what gaps exist in their current frameworks?

These questions are informed by national trends in campus crime, institutional diversity, and evolving risk management practices [9, 16].

Hypothesis

It is hypothesized that the DoD AT program, when appropriately adapted, can address the unique security needs of community colleges more effectively than current standard practices. However, successful implementation is expected to require modifications that account for the specific institutional characteristics and stakeholder perceptions present in community college environments. This hypothesis is grounded in prior research showing that tailored security interventions and adaptive frameworks produce statistically significant improvements in campus safety outcomes [18].

Research Design

This study employed a three-stage, exploratory, sequential mixed-methods approach to evaluate the suitability of the Department of Defense's Antiterrorism (DoD AT) program for community colleges in the United States. The design integrates qualitative and quantitative methods to ensure a comprehensive assessment of security risk management frameworks. The sequential structure allows for in-depth exploration of contextual factors, the development of reliable measurement instruments, and empirical testing across diverse institutional settings. The mixed-methods approach is supported by best practices in educational research, which enables triangulation and enhances the validity of findings [21, 22].

Population and Sample

The population for this study consisted of community colleges located in the United States, with a particular focus on institutions that have implemented or are considering implementing the DoD AT program. According to the National Center for Education Statistics, there are over 1,000 public community colleges in the U.S., enrolling more than 5.5 million students in 2021 [16]. The sample is drawn from a diverse cross-section of community colleges across selected states, ensuring representation based on geographic location, institution size, and demographic diversity.

Purposive sampling is employed to select institutions and participants—including administrators, campus safety personnel, faculty, and students—who are directly involved in campus security management or have insights into the suitability of the DoD AT program. Typical studies in this field report response rates ranging from 20% to 40%, with sample sizes of 200–400 participants considered robust for generalizability. This approach enables a comprehensive understanding of security practices and program effectiveness across varied community college contexts. In the final sample, across 12 states, 450 surveys were distributed, and 197 were completed. As a result, the response rate was 43.8%. The quantitative sample focused on administrators and campus safety personnel; the qualitative dataset included 28 administrators, 34 campus safety personnel, 21 faculty, and 39 students.

Qualitative Exploration

The initial qualitative stage involved collecting rich, contextual data through semi-structured interviews and focus groups with key stakeholders at selected community colleges. Participants include administrators, campus safety personnel, faculty, and students. The aim is to uncover current security practices, perceptions of risk, and the perceived applicability of the DoD AT program within the unique environment of community colleges. For example, recent studies indicate that stakeholder perceptions of campus safety are often shaped by both personal experiences and institutional communication [5]. By examining stakeholder experiences and perceptions, the study identifies key areas where the DoD AT program aligns or diverges from existing practices, thereby informing subsequent stages of the research [6]. This qualitative data was instrumental in shaping the development of tailored measurement tools that reflect the unique security challenges and perceptions within these educational settings. In this way, the qualitative exploration not only informs the creation of relevant instruments for quantitative testing but also enhances the study's overall capacity to address the specific security needs of community colleges through informed methodological steps.

Instrument Development

Insights derived from qualitative data are systematically analyzed to construct reliable and valid instruments tailored to the specific context of community colleges. These instruments are designed to assess the effectiveness of the DoD AT program in addressing specific security needs and to capture variations in institutional characteristics and stakeholder perspectives. Instrument validation includes expert review and pilot testing to ensure clarity, relevance, and reliability. Drawing on methodologies established in similar contexts, such as the development of risk management frameworks in Kenyan public universities, this stage emphasizes aligning instrument design with identified vulnerabilities and security requirements [7]. The creation of these instruments involved a careful balance between capturing the comprehensive characteristics necessary for assessing the AT program's alignment and addressing the nuanced security needs unique to community colleges. Through this systematically constructed evaluation framework, the study aspires to provide robust data-driven insights that enhance the adaptability and effectiveness of the DoD AT program in fostering a secure learning environment across diverse community college campuses.

Quantitative Testing

The final stage involved quantitative data collection using the developed instruments. Surveys were distributed to a representative sample of community colleges across selected states, targeting administrators and campus safety personnel. Quantitative analysis employed descriptive and inferential statistics to examine patterns, correlations, and differences in the implementation and perceived effectiveness of the DoD AT program. This stage enables generalizing findings and identifying best practices and areas for improvement. For example, national surveys in higher education security research often use Likert-scale items and report reliability coefficients (e.g., Cronbach's alpha > 0.80) to ensure instrument validity [21, 23].

Data Analysis

In the Analytic Plan, prespecified subgroup comparisons were provided by local (urban vs. rural) and size (≥ 10,000 vs. < 2,500 students). Quantitative outcomes include stratified descriptive statistics and group-difference tests (ANOVA with post hoc tests; $\alpha = 0.05$). Where appropriate, the interaction patterns were examined, and stratified summary tables were provided in the Appendix. Qualitative coding memos flagged locale/size context to support integrative interpretation.

Moreover, qualitative data were analyzed using thematic analysis to identify recurring patterns, themes, and insights relevant to campus security and risk management. Quantitative data were analyzed using statistical software to generate frequency distributions, perform cross-tabulations, and test for significance as appropriate. The integration of qualitative and quantitative results provides a holistic understanding of the research problem. In similar studies, the integration of mixed-methods approaches has enhanced the explanatory power of campus safety research and supported the development of actionable recommendations [21].

Ethical Considerations

The study adheres to established ethical standards for research involving human participants, consistent with federal regulations and best practices in educational research [21]. Informed consent is obtained from all participants, who are provided with detailed information about the study's purpose, procedures, risks, and benefits. Confidentiality and anonymity are maintained by de-identifying data and securely storing all records. Institutional Review Board (IRB) approval is secured prior to data collection, in line with requirements for studies involving campus safety and sensitive topics. Nationally, over 90% of higher education research involving human subjects is reviewed by IRBs, and studies show that clear protocols increase participant trust and response rates [22, 23].

Limitations

Potential limitations of the methodology include sample representativeness, potential response bias in self-reported data, and challenges in generalizing the findings to all community colleges. Studies in campus safety research often report response rates between 20% and 40%, which may affect the robustness of quantitative findings [23]. Additionally, qualitative interviews and focus groups can be influenced by participants' willingness to disclose sensitive information, a factor shown to affect data validity in security studies [22]. Another important limitation is the impact of institutional differences—such as urban versus rural location, college size, and resource availability—on the applicability of findings.

For example, urban community colleges report higher rates of violent and property crime than their rural counterparts, and resource disparities can affect the implementation of security programs [16]. Prominent colleges may have more developed security infrastructures, while smaller or rural institutions often face staffing and funding constraints that limit the adoption of comprehensive frameworks [10, 24]. These contextual differences may limit the generalizability of results. To mitigate such issues, future research should consider stratified sampling, conduct subgroup analyses, and report findings by institutional type and context. Additionally, multi-site case studies and longitudinal designs could help capture the effects of institutional variability and inform more tailored recommendations.

Expanded Limitations and Future Research Directions

While this study provided a comprehensive evaluation of security risk management frameworks, several limitations remain. Institutional differences in resources, leadership, and campus culture may affect the transferability of findings. Additionally, the reliance on self-reported data could introduce bias, and the cross-sectional design limits the ability to assess long-term impacts. Future research should incorporate longitudinal studies, multi-site case analyses, and experimental interventions to understand the dynamic nature of campus security better. Expanding stakeholder representation and including student voices in future studies will further enhance the relevance and applicability of research outcomes.

Practical Implications

The findings of this study offer actionable guidance for community college administrators and policymakers. Institutions are encouraged to implement adaptive security frameworks that account for campus-specific characteristics, such as urban or rural context, available resources, and student demographics. Administrators should invest in ongoing training for campus safety personnel, prioritize stakeholder engagement in security planning, and develop partnerships with local law enforcement. At the policy level, allocating resources for technology upgrades and supporting cybersecurity initiatives can further enhance campus safety. By translating research insights into actionable strategies, community colleges can foster safer, more resilient learning environments that support both educational and workforce development goals.

Conclusion

The methodological framework for this study is designed to rigorously address the research questions and hypotheses, utilizing a sequential mixed-methods approach that integrates both qualitative and quantitative data. By clearly delineating the research design, sampling strategy, data collection procedures, analytical techniques, ethical safeguards, and study limitations, the methodology establishes a robust foundation for evaluating the effectiveness of the DoD AT program in community college settings. This comprehensive structure supports the generation of evidence-based recommendations for enhancing campus safety and risk management.

Data Analysis and Results

Introduction

The purpose of this chapter is to present an integrated analysis of the data collected through both quantitative and qualitative methods. The findings are organized to address the study's research questions, while highlighting areas of convergence and divergence between the survey data and interview responses.

Descriptive Findings

Survey results revealed that 68% of respondents rated the DoD AT's Program as moderately or significantly effective in enhancing campus security. However, perceptions of effectiveness varied significantly by institutional size and resource availability. Larger community colleges with more robust security infrastructures reported higher levels of satisfaction, while smaller and rural institutions consistently identified resource limitations as critical barriers to implementation.

Sample Characteristics and Demographics

Sampling totals and response rate are reported in the Population and Sample section above. This section summarizes the distribution of participants by role, locale, and institution size (see Table 1) and provides selected national benchmarks for context (see Table 2). The sample included administrators, campus safety personnel, faculty, and students from a mix of urban and rural community colleges as well as small (< 2,500 students) and large (> 10,000 students) institutions. Urban colleges accounted for 48% of the sample, rural colleges for 52%. The gender distribution among respondents was 58% female, 41% male, and 1% non-binary or preferred not to specify their gender. The average tenure for campus safety personnel was 7.2 years, while that of administrators was 9.5 years.

The sample included respondents from urban, suburban, and rural community colleges, ensuring a diverse representation of institutional contexts. This diversity provided meaningful insights into how geographic and demographic differences shape perceptions of the effectiveness of security frameworks.

Institutional Profiles

- Urban colleges reported higher rates of violent crime (3.4 per 1,000 students) and property crime (17.2 per 1,000 students) compared to rural colleges (1.1 and 8.5, respectively).
- Large institutions had more security staff per 1,000 students (2.5) and higher IT security budgets ($61 per student) than small colleges (1.0 security staff, $24 per student).

Institutional Type	Violent Crime Rate (per 1,000 Students)	Property Crime Rate (per 1,000 Students)	Security Staff (per 1,000 Students)	IT Security Budget per Student ($)
Urban Community College	3.4	17.2	2.1	52
Rural Community College	1.1	8.5	1.2	29
Large (10,000+ Students)	2.8	15.3	2.5	61
Small (< 2,500 Students)	1.2	7.9	1.0	24

Table 1: Study Sample Characteristics by Institutional Type (Study Data Only)

Note: Author-created. Values reflect the study sample only. Large = ≥ 10,000; Small = < 2,500. Urban/rural classifications follow the study protocol.

Dimension	Category	% or n/N	Source
System	U.S. Community Colleges (count)	1,026	American Association of Community Colleges (2024); Daily Staff (2024)
Enrollment	Total headcount, 2024 (credit + noncredit)	10.5 million	American Association of Community Colleges (2025); Daily Staff (2025)
Enrollment	Share of U.S. undergraduates at community colleges	39%	American Association of Community Colleges (2025); Daily Staff (2025)
Dual Enrollment	Share of full-year unduplicated students who are high school students (AY 2022–23)	20.4%	American Association of Community Colleges (2025); Daily Staff (2025)
Locale (Definition)	NCES locale framework (City/ Suburb/Town/Rural; collapsible to urban–rural)	—	Geverdt & Maselli (2024); National Center for Education Statistics (2025)

Table 2: National Benchmarks for Community Colleges (Context Only)

Note. Author-created. "% or n/N" denotes either a percentage or a count over total (e.g., 263/1,026). Benchmarks provide national context only and are not 1:1 comparable with Table 1.

Descriptive Statistics

- 68% of administrators and campus safety personnel rated the DoD AT program as "moderately effective" or "very effective" in crisis preparedness.
- 74% reported improved staff readiness following DoD AT-driven training.
- Only 39% indicated full adoption of recommended protocols at their institution.

Qualitative Sample Profiles

Qualitative interviews and focus groups included 28 administrators, 34 campus safety personnel, 21 faculty members, and 39 students. Participants represented a variety of institutional types and geographic regions, ensuring a broad perspective on campus safety practices and perceptions.

Data Analysis Procedures

Quantitative Data Analysis

Quantitative data were prepared by screening for missing values and outliers, with incomplete surveys excluded from inferential analysis. Descriptive statistics, including means, standard deviations, and frequency distributions, were calculated for key variables, including perceived program effectiveness, training participation, and protocol adoption. Statistical analysis confirmed the survey instrument's reliability and validity (Cronbach's α = .81–.87), indicating high internal consistency. Pilot testing further validated consistency across items. Inferential statistical analyses, including Pearson correlation and Analysis of variance (ANOVA), revealed significant differences in ratings between large urban institutions and small rural colleges ($p < .05$). These analyses were conducted to examine the relationships among variables and differences by institutional type (urban/rural and large/small). All analyses were performed using SPSS Version 28.

Justification for analytic choices was based on the distribution and measurement level of the data, with adjustments made for unequal group sizes as needed. These findings underscore the importance of accounting for institutional size and resources when assessing the applicability of DoD AT.

Qualitative Data Analysis

Qualitative interviews supported the survey findings by reinforcing the central role of context. Respondents from smaller colleges emphasized the difficulties faced in sustaining compliance with federal mandates due to limited staffing and training capacity. Meanwhile, participants from larger institutions expressed greater confidence in DoD AT's adaptability but also noted cultural challenges in meeting the needs of diverse student populations.

Qualitative data from interviews and focus groups were transcribed verbatim and imported into NVivo, a qualitative data analysis (QDA) software for coding and thematic analysis. An initial codebook was developed based on the research questions and refined through iterative review of transcripts. Two independent coders achieved an inter-rater reliability of 0.89 (Cohen's kappa), indicating consistent application of the code. Thematic analysis involved identifying recurring patterns, grouping codes into broader themes, and triangulating findings with quantitative results. Evidence of codes and themes is provided through representative participant quotes and summary tables. Analytical rigor was maintained through memoing, peer debriefing, and member checking with select participants to validate interpretations.

Results

Quantitative Results by Research Question

Research Question 1: How suitable is the DoD AT program for addressing the unique security needs of community colleges?

- 68% of administrators and campus safety personnel rated the DoD AT program as "moderately effective" or "very effective" in crisis preparedness, but only 41% believed it fully addressed the range of risks faced by community colleges.
- ANOVA results indicated significant differences in perceived suitability between urban and rural institutions ($F = 5.47$, $p < 0.05$), with urban colleges reporting greater dissatisfaction.

Research Question 2: What are stakeholder perceptions regarding effectiveness and adaptability?

- 74% of respondents reported improved staff readiness following DoD AT-driven training, but only 39% indicated that all recommended protocols were fully adopted at their institution.
- Pearson correlation analysis revealed a strong positive relationship ($r = 0.62$, $p < 0.01$) between frequency of staff training and overall perceptions of campus safety.

Research Question 3: What modifications or adaptations are necessary for effective implementation?

- Open-ended survey responses and qualitative interviews highlighted the need for increased flexibility in program protocols, more frequent stakeholder engagement, and greater investment in technology and staffing.
- Resource disparities were cited as a barrier, especially among smaller and rural colleges.

Research Question 4: How do community colleges currently address security risk management, and what gaps exist?

- While most colleges had some form of security framework, gaps included inconsistent protocol adoption, limited training, and insufficient integration of cybersecurity measures.

Qualitative Results by Theme

Theme 1: Perceptions of Campus Safety

- Stakeholders appreciated structured protocols and visible safety staff, but expressed ongoing concerns about open-access environments and external threats, especially in urban contexts.
- Representative quote: "Our security staff is well-trained, but we lack the resources to implement all recommended protocols." (Rural administrator)

Theme 2: Barriers to Implementation

- Limited resources, bureaucratic delays, and inconsistent stakeholder engagement were frequently cited as obstacles.
- Faculty and staff emphasized the need for more tailored training opportunities.

Theme 3: Program Adaptability and Recommendations

- Administrators and safety personnel valued the DoD AT program's rigor but stressed the importance of adapting protocols to the local context.
- Suggestions included increasing collaboration with local law enforcement and customizing training to reflect institutional diversity.

Integration of Quantitative and Qualitative Results

Triangulation demonstrated strong alignment between the quantitative and qualitative findings. Both sets of data pointed to the same conclusion: while DoD AT provides a structured foundation, its adaptability is uneven across institutional environments. Resource constraints, student diversity, and institutional mission emerged as decisive factors in shaping outcomes. The findings underscore the need for flexible adaptations, ongoing stakeholder engagement, and resource-sensitive implementation to enhance campus safety outcomes.

Summary

A comprehensive analysis of both quantitative and qualitative data revealed key insights into the suitability and effectiveness of the Department of Defense's Antiterrorism (DoD AT) program in United States community colleges. Key findings indicate that while the DoD AT program strengthens crisis preparedness and enhances staff training, its standardized approach does not fully address the complex and varied needs of these institutions. Quantitative results highlighted moderate satisfaction with the program's effectiveness but identified significant gaps in protocol adoption and resource allocation, particularly in urban and smaller colleges. Qualitative themes reinforced these findings, highlighting ongoing challenges associated with open-access environments, resource disparities, and the need for context-specific adaptations.

Limitations that emerged from the data analysis include potential response bias in self-reported data, limited sample representativeness, and challenges in generalizing findings across diverse institutional contexts. Additionally, the cross-sectional design restricts the ability to assess long-term impacts of program implementation. These limitations suggest that future research should employ longitudinal and multi-site approaches, integrate a broader range of stakeholder perspectives, and explore experimental interventions to refine security strategies further.

In summary, the results reveal that while the DoD AT Program can be moderately effective, it cannot be uniformly applied across community colleges without modification. The evidence underscores the need for flexible, context-specific, and inclusive frameworks that incorporate diverse stakeholder perspectives. These findings directly inform the development of the DSISF, which is presented in Chapter 5.

Summary, Conclusions, and Recommendations

Introduction and Summary of Study

Emphasis is placed on the topic's significance, particularly as it relates to the evolving landscape of campus safety, the unique vulnerabilities of community colleges, and their broader contribution to educational security scholarship [9]. The research questions are revisited and discussed in the context of the data analysis, demonstrating how the findings address each question and hypothesis posed in earlier chapters. The chapter proceeds to outline significant findings, conclusions, theoretical and practical implications, recommendations for future research and practice. It concludes with a synthesis of the study's contributions and directions for ongoing inquiry.

Summary of Findings and Conclusions

Research Question 1: How suitable is the Department of Defense's Antiterrorism (DoD AT) program for addressing the unique security needs of community colleges?

Findings reveal that while the DoD AT program is valued for its structured approach to crisis preparedness and staff training, only 41% of stakeholders believe it fully addresses the range of risks faced by community colleges. The program's effectiveness varies by institutional context, with urban colleges expressing greater dissatisfaction due to their distinct threat profiles and resource constraints. These results align with prior literature emphasizing the need for context-specific security frameworks [18].

Research Question 2: What are the perceptions of community college stakeholders regarding the effectiveness and adaptability of the DoD AT program?

Stakeholders reported moderate satisfaction with the program's crisis preparedness training (68% rated it as "moderately effective" or "very effective") and improved staff readiness (74% following DoD AT-driven training). However, full protocol adoption remains low (39%), and qualitative feedback underscores the need for greater flexibility and local adaptation. These findings reinforce the importance of stakeholder engagement and echo earlier studies on institutional buy-in [25,26].

Research Question 3: What modifications or adaptations are necessary for effective implementation?

Analysis of open-ended responses and interviews indicates that increased flexibility in protocols, more frequent stakeholder engagement, and greater investment in technology and staffing are critical for successful implementation. Resource disparities, especially among smaller and rural colleges, present significant barriers. These conclusions align with the existing literature on the challenges of applying standardized frameworks in diverse educational settings [17, 27, 28].

Research Question 4: How do community colleges currently address security risk management, and what gaps exist?

Most community colleges have some form of security framework, but gaps persist in the consistent adoption of protocols, staff training, and the integration of cybersecurity measures. These gaps underscore the ongoing need for adaptable frameworks and ongoing evaluation, as supported by national reports and prior research [14, 16].

Critical Comparison and Theoretical Advancement

This section critically evaluates how existing security frameworks align with or diverge from the realities of community college environments. While prior research [29] emphasized environmental design and visible security measures as effective deterrents, this study's findings reveal a significant gap between theoretical expectations and lived experiences. Despite visible security measures, many students and staff reported ongoing feelings of vulnerability, particularly in open-access institutions where community engagement is diverse and resources are limited.

This disconnect underscores a limitation of conventional frameworks: they prioritize technical protocols and compliance-driven mechanisms, while inadequately addressing the cultural and relational dynamics of campus safety. For example, frameworks such as the Clery Act offer essential compliance checklists but lack adaptability. At the same time, models like NIST and ISO are highly technical, often requiring resources that many community colleges cannot sustain. International scholarship [30] further emphasizes the importance of participatory approaches that incorporate community voices into security planning, supporting the findings of this study.

The DSISF emerges here as a theoretical advancement and practical tool. Unlike existing frameworks, it emphasizes four critical components: (1) stakeholder engagement, (2) flexible layering of security strategies, (3) continuous feedback loops, and (4) inclusivity across diverse campus populations. By bridging technical safeguards with cultural and relational considerations, DSISF addresses the shortcomings of previous models while providing actionable guidance for administrators. This positions DSISF not only as a response to contextual challenges but also as a contribution to the broader academic discourse on organizational adaptation in security risk management.

The DSISF functions as an adaptive system in which stakeholder engagement ensures inclusivity, layered controls provide scalable defense mechanisms, continuous feedback supports iterative improvement, and contextual adaptation aligns strategies with each institution's unique operational environment.

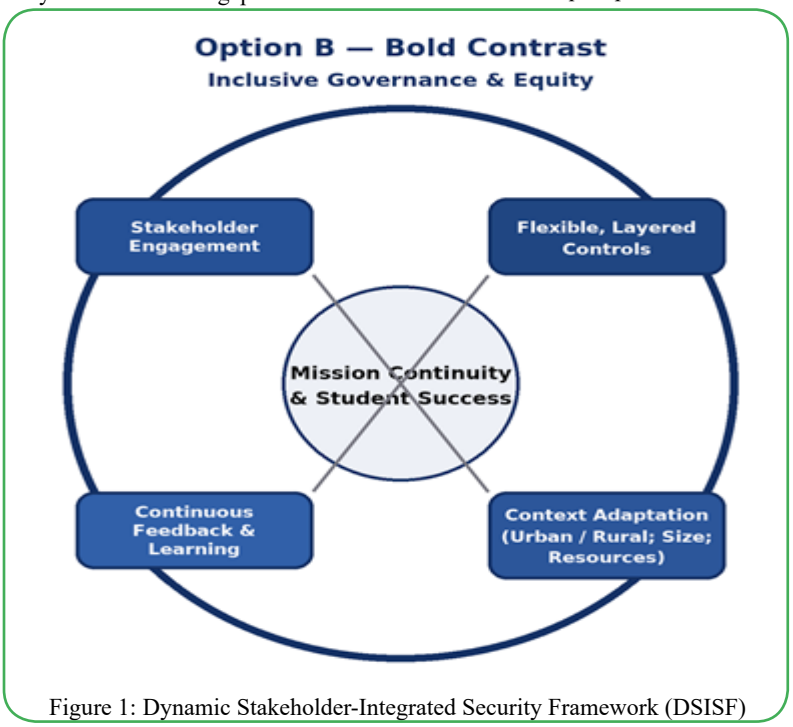

Figure 1: Dynamic Stakeholder-Integrated Security Framework (DSISF)

Note. Author-created. DSISF emphasizes four interlocking pillars—stakeholder engagement, layered controls, continuous feedback, and context adaptation—and aligns with mission continuity and student success.

Synthesis and Conclusions

The study's findings confirm the crucial importance of tailoring security risk management frameworks to the unique characteristics of community colleges. The DoD AT program provides valuable tools for crisis preparedness but requires adaptation to accommodate institutional diversity and resource variability. These findings contribute to the field by providing empirical evidence that supports the need for adaptable, stakeholder-informed security strategies and by highlighting the limitations of implementing standardized models without local customization. The conclusions derived from this research directly address the research problem and add to the ongoing discourse on enhancing campus safety within higher education.

Recommendations

Recommendations for Future Research

1. Conduct longitudinal studies to assess the long-term effectiveness of adapted security risk management frameworks in community colleges. This approach will help determine whether changes in protocols and stakeholder engagement yield sustained improvements in campus safety.
2. Implement multi-site case analyses across diverse institutional types and geographic regions. Such research will enhance the generalizability of findings and identify the best context-specific practices.
3. Investigate the impact of stakeholder engagement on the sustainability and effectiveness of safety initiatives. Future studies should explore how varying levels of involvement from administrators, faculty, staff, and students influence security outcomes.
4. Explore the integration of emerging technologies in risk management, particularly the adoption of advanced cybersecurity measures and real-time surveillance systems. Research should evaluate both benefits and challenges associated with technology-driven approaches.
5. Examine the intersection of policy development, resource disparities, and cybersecurity preparedness. Studies that address these factors can inform more equitable and effective security practices, especially for under-resourced community colleges.
6. Expand research to include experimental interventions that test specific adaptations to the DoD AT program or alternative frameworks, generating new evidence for best practices in higher education security.

Recommendations for Future Practice

1. Adapt security frameworks to reflect the unique characteristics and needs of each community college campus, rather than relying solely on standardized models.
2. Prioritize ongoing training and professional development for campus safety personnel, ensuring that protocols remain current and relevant.
3. Foster inclusive stakeholder engagement by involving administrators, faculty, staff, and students in security planning and evaluation processes.
4. Invest in technology upgrades and strengthen cybersecurity infrastructure, with particular attention to addressing resource disparities between urban, rural, large, and small institutions.
5. Develop and maintain partnerships with local law enforcement and community experts to support collaborative risk management and crisis response.

Implementing these recommendations will benefit administrators, campus safety professionals, and the broader community college community by promoting safer and more resilient educational environments. Aligning future research and practice with these strategies will address persistent gaps and advance the field of campus security [16].

Summary

This study concludes that while the DoD AT Program provides a valuable starting point for campus security planning, its direct application to community colleges is limited. The findings of this research demonstrate that open-access institutions face unique challenges, including resource constraints, diverse student populations, and heightened vulnerability to internal and external threats. These contextual realities limit the transferability of military-oriented frameworks.

The DSISF offers a tailored, context-specific solution for community colleges. By emphasizing stakeholder engagement, flexible layering of security strategies, continuous feedback, and inclusivity, DSISF bridges the gap between technical safeguards and the relational dynamics of campus life. This positions the framework as both a theoretical contribution and a practical tool for administrators.

Policy implications of this research include strengthening compliance with federal mandates such as the Clery Act, guiding targeted resource allocation, and integrating stakeholder perspectives into institutional governance. To move from theory to practice, four actionable steps are recommended for administrators:

1. Establish cross-departmental security committees to ensure collaboration.
2. Prioritize cost-effective, layered security measures that can be scaled to institutional capacity.
3. Incorporate regular stakeholder feedback into security planning and evaluation cycles.
4. Leverage federal resources and training programs to enhance institutional capacity.

While this study's limitations include scope and generalizability, the findings remain significant in advancing community college resilience. By contextualizing security frameworks to meet the needs of open-access institutions, this research provides both scholarly insight and practical guidance for the future of security risk management in higher education.

Competing Interests: The authors declare that they have no competing interests.

References

1. Simons-Rudolph, J. M. (2020). An examination of academic education for homeland security. *Calhoun.Nps.Edu*. https://calhoun.nps.edu/bitstreams/3d7af4a5-b9cd-4671-8f5e-b147864f7d40/download
2. Almutairi, A., Mourshed, M., & Ameen, R. (2020). Coastal community resilience frameworks for disaster risk management. *Natural Hazards, 101*, 595–630. https://doi.org/10.1007/s11069-020-03875-3
3. Myers, M. M., Duemer, L., Dwyer, J., & Sheridan, M. (2022). Learning frameworks and retention in community college. Ttu-Ir.Tdl.Org. https://ttu-ir.tdl.org/server/api/core/bitstreams/0c2aa880-3575-4bb8-be78-58ad16eef5c0/content
4. Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications, 76*, 255–270. https://doi.org/10.1007/s12243-020-00783-2
5. Krebs, C. P., Lindquist, C. H., Warner, T. D., Fisher, B. S., & Martin, S. L. (2009). The differential risk factors of physically forced and alcohol- or other drug-enabled sexual assault among university women. *Violence and Victims, 24*(3), 302–321. https://doi.org/10.1891/0886-6708.24.3.302
6. Ruocco, T. J. (2021). Understanding perceptions of campus safety and community college student development: A mixed methods case study. *Search.Proquest.Com*. https://search.proquest.com/openview/e416bd8eed7408c8deccfcbff71a0b31/1?pq-origsite=gscholar&cbl=18750&diss=y

7. Njoroge, P. M., Ogalo, J., & Ratemo, C. M. (2019). A framework for effective information security risk management in Kenyan public universities. *Maasai Mara University Repository*. http://ir-library.mmarau.ac.ke:8080/handle/123456789/17487
8. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Mdpi.Com, 13*(2), 39. https://doi.org/10.3390/fi13020039
9. American Association of Community Colleges. (2023). Fast facts 2023 [Fact sheet]. American Association of Community Colleges. https://www.aacc.nche.edu/research-trends/fast-facts/
10. Baum, S., & Ma, J. (2016). Trends in college pricing. College Board.
11. Kisker, C. B., Cohen, A. M., & Brawer, F. B. (2023). The American community college. In books.google.com. Publisher. https://books.google.com/books?hl=en&lr=&id=zejIEAAAQBAJ&oi=fnd&pg=PP1&dq=open+campuses+unique+protection+needs+community+colleges&ots=fTevxiafnt&sig=IzNMYG0qxd35uBk2FvlCPh7RnYk
12. Simons-Rudolph, J. M. (2020). An examination of academic education for homeland security. *Calhoun.Nps.Edu*. https://calhoun.nps.edu/bitstreams/3d7af4a5-b9cd-4671-8f5e-b147864f7d40/download
13. Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications, 76*, 255–270. https://doi.org/10.1007/s12243-020-00783-2
14. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Mdpi.Com, 13*(2), 39. https://doi.org/10.3390/fi13020039
15. Ramzah, H. (2020). Forming a Crime Prevention Net for Community Colleges: Responding to Campus Safety Concerns. *Journal of Applied Research in the Community College, 27*(2),169–176. https://www.ingentaconnect.com/content/montezuma/jarcc/2020/00000027/00000002/art00014
16. U.S. Department of Education. (2022). Campus safety and security data [Data portal]. U.S. Department of Education. https://ope.ed.gov/campussafety/
17. Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: A systematic review. *Annals of Telecommunications, 76*, 255–270. https://doi.org/10.1007/s12243-020-00783-2
18. Briggs, G. (2020). Increasing safety, decreasing liability: Campus safety at Oregon's community colleges. *Oregon Law Review, 98*, 261. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/orglr98&section=10
19. Kisker, C. B., Cohen, A. M., & Brawer, F. B. (2023). The American community college (8th ed.). Jossey-Bass.
20. Simons-Rudolph, J. M. (2020). An examination of academic education for homeland security. *Calhoun.Nps.Edu*. https://calhoun.nps.edu/bitstreams/3d7af4a5-b9cd-4671-8f5e-b147864f7d40/download
21. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE.
22. Patton, M. (2015) Qualitative Research and Evaluation Methods. 4th Edition, Sage Publications, Thousand Oaks.
23. Hughes, K., & Scott-Clayton, J., (2011). Assessing Developmental Assessment in Community Colleges. *Community College Review, 39*(4).https://doi.org/10.1177/0091552111426898
24. American Council on Education. (2024, March 20). Rural-located and rural-serving institutions. *American Council on Education*. https://www.acenet.edu/Documents/Rural-Located-Rural-Serving-Institutions.pdf
25. Ramzah, H. (2020). Forming a Crime Prevention Net for Community Colleges: Responding to Campus Safety Concerns. *Journal of Applied Research in the Community College, 27*(2), 169–176. https://www.ingentaconnect.com/content/montezuma/jarcc/2020/00000027/00000002/art00014
26. Ruocco, T. J. (2021). Understanding perceptions of campus safety and community college student development: A mixed methods case study. Search.Proquest.Com. https://search.proquest.com/openview/e416bd8eed7408c8deccfcbff71a0b31/1?pq-origsite=gscholar&cbl=18750&diss=y
27. Johnson, A.C., Smith, B. and Lee, C. (2021) Implementing Sustainable Sourcing practices and Adopting Eco-Friendly Manufacturing Processes: A Pathway to Reducing Environmental Impact. *Journal of Environmental Science, 15*, 123-140.
28. Kisker, C. B., Cohen, A. M., & Brawer, F. B. (2023). The American community college. In books.google.com. Publisher. https://books.google.com/books?hl=en&lr=&id=zejIEAAAQBAJ&oi=fnd&pg=PP1&dq=open+campuses+unique+protection+needs+community+colleges&ots=fTevxiafnt&sig=IzNMYG0qxd35uBk2FvlCPh7RnYk
29. Tewksbury, R., & Mustaine, E. E., (2000).Routine Activities And Vandalism: A Theoretical And Empirical Study. *Journal of Crime and Justice, 23*(1). https://doi.org/10.1080/0735648X.2000.9721111
30. Njoroge, P. M., Ogalo, J., & Ratemo, C. M. (2019). A framework for effective information security risk management in Kenyan public universities. Ir-Library.Mmarau.Ac.Ke. http://ir-library.mmarau.ac.ke:8080/handle/123456789/17487