Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 12| 2025

Research Article **Received:** 05-11-2025| **Accepted:** 30-11-2025 | **Published:** 13-12-2025

Cybersecurity Curriculum Alignment with Industry Needs: A Literature Review of Educational Models Integrating Labs, Certifications, and Research

***Kenneth Nnadi* [1], *and Jochebed Akoto Opoku* [2]**

[1] *University of Oregon, USA*

[2]*Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana*

Abstract: This literature review examines how cybersecurity curricula align with industry needs through integrated models combining hands-on labs, certifications, and research experiences. Current programs often emphasize theory, leaving graduates underprepared for practical roles. The review combines evidence from many educational concepts, including course-centric, program-wide, industry-cooperative, certification-first, and research-led courses, with growing hybrid approaches. It investigates how these models relate to frameworks such as the National Initiative for Cybersecurity Education (NICE) and the National Institute of Standards and Technology (NIST), and assesses their impact on student outcomes, like skill acquisition, certification attainment, and employment. The findings emphasize the benefits of modular labs, organized certification pathways, and research engagement, while also identifying problems such as resource restrictions, rapid technology change, and the possibility of fragmented learning. This review offers promising methods for incorporating these components into a cohesive curriculum and emphasizes the importance of constant alignment with changing workforce competencies.

Keywords: Cybersecurity Education, Certifications, Competency Frameworks, Industry Alignment.

INTRODUCTION

Cybersecurity is increasingly at the core of economic stability, critical infrastructure protection, and national security. Nonetheless, organizations across all industries complain that they are unable to recruit enough personnel with the necessary mix of technical, analytical, and soft abilities to safeguard their systems. Employers routinely complain that many fresh graduates lack practical experience with real-world systems. They are frequently unfamiliar with standard professional qualifications and struggle to engage with or comprehend practical cybersecurity research (Burton, 2025). Recent curriculum studies support these concerns. They demonstrate that many university curricula continue to place a strong emphasis on theory or limited technical areas. Alignment with industry frameworks such as Information Systems 2020 Curriculum Guidelines (IS2020), Centers of Academic Excellence in Cyber Defense (CAE-CD,) and the NICE Workforce Framework is patchy. In this setting, the topic of how cybersecurity curricula may better reflect market demands has become critical. It is now a major worry for institutions, accreditors, and companies alike (Erickson & Kim, 2021).

At the same time, there is growing recognition that successful cybersecurity education cannot be limited to lectures and static exercises alone. Practice-oriented teaching is now regarded as crucial. This includes labs, simulations, and capture-the-flag exercises. These approaches assist students in developing operational abilities that meet workplace standards. Burton recently released a modular framework for cybersecurity lab design that demonstrates this clearly. It discovers that well-structured, hands-on laboratories matched with competence frameworks can lead to measurable improvements in learner performance and engagement. Program-level research in business schools and computing departments points in the same direction. Courses that clearly link learning outcomes, lab activities, and evaluation to established standards and occupational duties are better suited to preparing graduates for specific job functions. However, much of the literature continues to regard hands-on labs, industry certifications, and research exposure as distinct design options. They are rarely provided as part of a cohesive teaching program (Burton, 2025).

Recent studies on cybersecurity curriculum design are beginning to explicitly address the workforce shortfall and skills gap. Towhidi and Pridmore (2023), for example, implemented a backward course design strategy in a business school context. They linked a cybersecurity course to both the NIST Cybersecurity Framework and the NICE. The new course included theory, laboratories, and a vendor certification path based on interviews with industry people. Yang *et al.,* (2019) researched cybersecurity bachelor's programs at Association to Advance Collegiate Schools of Business (AACSB)-accredited business

***Corresponding Author:** Kenneth Nnadi

DOI- https://doi.org/10.5281/zenodo.17923740

institutions. They used the survey results to create a curricular model based on IS2020 and CAE-CD standards. The analysis revealed both areas of convergence and disparities in basic course offerings among universities. Together, these efforts indicate a definite move towards explicit curriculum conformity with industrial norms. However, they also highlight persistent issues such as limited space in degree programs, fast technological change, and the need to reconcile fundamental principles with job-ready abilities.

Parallel work on lab-based cybersecurity teaching demonstrates the clear benefits of modular, scalable labs. These labs support realistic attack-and-defense scenarios, leverage virtualization, and have built-in assessment capabilities. Burton's framework is an example. It demonstrates how a lab environment based on experiential learning theory can improve exam results and learner adaptability (Burton, 2025). At the same time, the framework remains flexible, allowing labs to be updated as threats and tools evolve. Certifications demonstrate competency to businesses and encourage students. They do, however, advise that curricula should not be reduced to mere exam preparation sessions. Yang *et al.*, (2019) demonstrate that structured cybersecurity research experiences, such as Research Experiences for Undergraduates (REU) sites, help students enhance their research abilities, confidence, and enthusiasm in further study. These benefits are especially significant for underrepresented populations. Despite these advancements, there is still a lack of systematic synthesis of how labs, certifications, and research experiences can be integrated into a unified teaching model. We also lack explicit mappings between such integrated models and the competency frameworks that businesses actually utilize.

Given this context, the primary goal of this review is to synthesize current evidence on how cybersecurity curricula connect with industry objectives by incorporating three pillars: labs, certifications, and research. The review intends to expand beyond isolated case studies, such as single-course lab designs or one-time certification arrangements. Instead, it seeks patterns in educational models that incorporate these components across programs and institutions. A secondary goal is to investigate how these integrated models relate to competency frameworks. Examples include the NICE Framework, the NIST Cybersecurity Framework, CAE-CD knowledge units, and other curriculum-design standards. A third goal is to determine what is known about the efficacy of these models. This covers the impact on student learning, employability, and advancement to advanced or research positions.

These objectives lead to four guiding research questions.

RQ1: What kinds of educational models in literature explicitly integrate hands-on labs, industry certifications, and research experiences within cybersecurity curricula?

RQ2: To what extent, and in what ways, do these models map to established industry competency frameworks, such as NICE and other national or sector-specific standards?

RQ3: What empirical evidence is reported about the effectiveness of these models on student outcomes? This includes knowledge gains, practical skills, certification attainment, job placement, and engagement with research.

RQ4: What gaps, challenges, and best practices do studies identify for the design, implementation, and continuous improvement of such integrated curricula?

By structuring the review around these questions, the paper provides a clear picture of where the field currently stands and where further work is most needed.

CONCEPTUAL FRAMEWORKS AND BACKGROUND

Competency frameworks used by industry

Industry competency frameworks provide a common language for explaining cybersecurity tasks and expectations for practitioners. The most influential example is the NICE Cybersecurity Workforce Framework. It identifies job classifications, specialist areas, work positions, and their associated duties, as well as knowledge, skills, and abilities. NICE is intended to serve as a reference structure rather than a curriculum in and of itself. Employers, professional bodies, and educational institutions utilize it to define roles and connect training and education with workforce requirements (Newhouse *et al.*, 2017). In parallel, higher education academics have begun to view these frameworks as design tools. Towhidi and Pridmore (2023) suggest a backward course design strategy for aligning cybersecurity courses with the NIST Cybersecurity Framework and NICE standards. They conduct interviews with industry

Publisher: SARC Publisher

specialists to determine course learning objectives, assessment evidence, and content.

These frameworks are neither exhaustive nor static. They must be updated as new technologies and dangerous environments arise, and they may require adaptation for particular national, sectoral, or institutional contexts. However, they do give a practical foundation for alignment. In a review of cybersecurity activities and curricula, Ismail *et al.*, (2024) observe that many educational programs continue to struggle to connect course content, lab activities, and assessment directly to explicit competency models, which can limit transparency and make it difficult to demonstrate that graduates meet industry expectations.

Role of certifications in education

Professional credentials exist in an ambiguous region between academia and industry. On the one hand, they provide standardized indicators of knowledge and talent, which employers recognize and frequently expect. There is concern that if curricula are too tightly aligned with certification objectives, learning may be reduced to exam preparation. This can undermine foundational thinking and jeopardize academic independence. It's also vital to differentiate between vendor-neutral and vendor-specific certifications. Vendor-neutral certifications, such as CompTIA Security+, emphasize broad ideas and cross-platform capabilities. Vendor-specific certifications, such as those offered by AWS, Cisco, and Microsoft, focus on specific technologies and ecosystems.

Tran *et al.*, (2023) offer a "three-legged stool" approach to cybersecurity education. Curriculum material, hands-on skills, and certifications are all complementary in this concept, rather than substitutes. Their survey of Atlanta-area IT organizations reveals that many employers either require or strongly prefer candidates with credentials for entry-level positions.

They conclude that including a combination of vendor-neutral and vendor-specific certifications in programs can accelerate students' workplace preparation. This works best when labs and projects are designed to simultaneously improve conceptual knowledge and exam preparedness. James & Callen (2018) discovered comparable perspectives using interview-based case studies with cybersecurity educators and professionals. Participants generally agree that certifications, when combined with real-world experience, help graduates increase their knowledge, skills, and employability. They also advise against "paper certs" that indicate memorization rather than true skill.

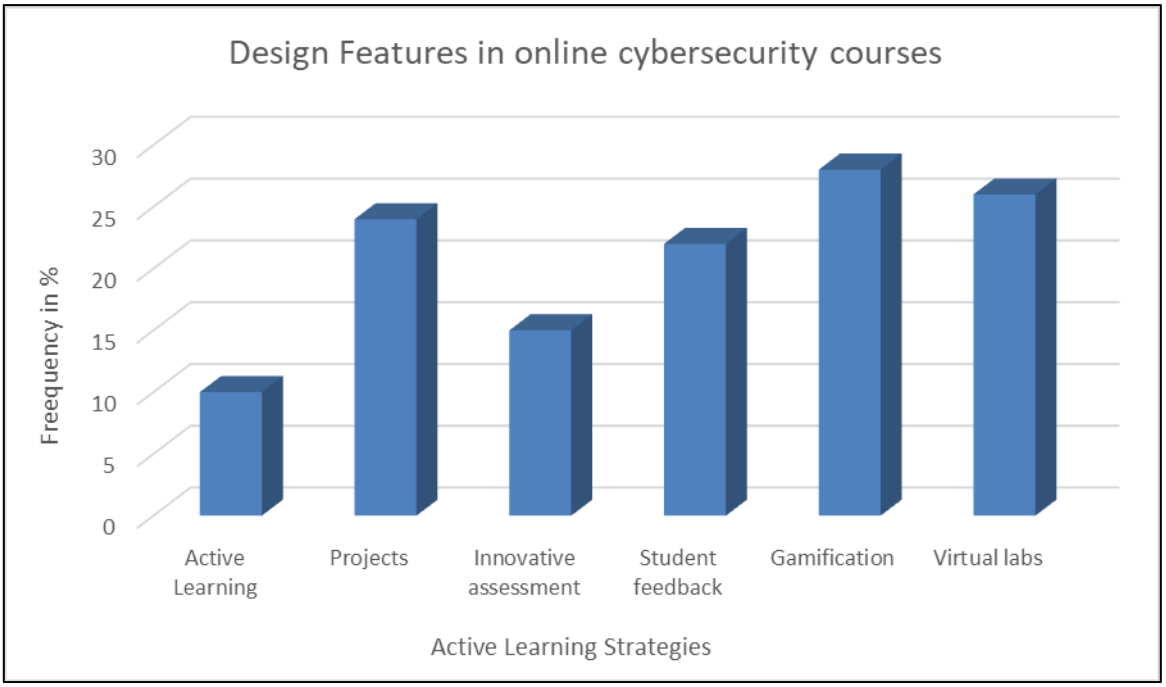

Figure 1. **Frequency of active learning strategies in cybersecurity education.**

Figure 1 illustrates the relative emphasis on different active learning strategies reported in recent cybersecurity education studies. Virtual labs and gamification appear most frequently, followed by projects and student feedback, indicating a strong trend towards experiential and interactive

Publisher: SARC Publisher

teaching approaches (Source: Adapted from Ismail *et al.,* 2024).

Typology of educational models

A great way to examine how cybersecurity curricula adapt to industry needs is to categorize programs depending on how they integrate laboratories, certificates, and research. This typology is not rigorous or exhaustive, but it does assist in organizing the large range of techniques seen in literature and in actual programs. Some institutions primarily follow one model. Others combine features from several. Surveys of cybersecurity courses reveal that most programs include hands-on labs and frequently refer to workforce frameworks. However, they differ greatly in how these features are incorporated and linked to certifications and research activities. The five fundamental concepts described here are course-centric, program-wide, industry-cooperative, certification-first, and research-driven. These are followed by a brief discussion of hybrid and developing concepts, such as micro-credentials and virtual ranges (Ismail *et al.,* 2024).

Model A - Course-centric integration

In the course-centric model, integration of labs, certification preparation, and research happens mainly at the level of a single course or a small cluster of courses. A typical example is an upper level "Introduction to Cybersecurity" or "Network Defense" course that uses backward design to align learning outcomes with selected industry frameworks, embeds structured labs, and offers optional pathways toward a certification. The strengths of this model are flexibility and relatively low implementation cost. Departments can pilot a modernized cybersecurity experience inside one course without rewriting the whole degree. It also works well in programs where cybersecurity is a concentration rather than the main major, such as information systems or computer science degrees with one or two security electives. Because the integration is local, instructors can react quickly to new threats, tools, or certification objectives and update their labs and exam coverage. The main weakness is fragmentation: students may get rich, aligned experience in one course but see little reinforcement elsewhere, which can limit long-term skill development and employability impact (Petersen *et al.*, 2020).

Model B - Program-wide alignment

In the program-wide alignment concept, an entire degree (for example, a BSc in Cybersecurity) is purposefully linked to industry competency frameworks like the NICE Workforce. Multiple lab-intensive courses serve as a scaffold, allowing students to continually practice critical skills such as network protection, secure coding, incident response, and digital forensics at increasingly complicated levels (Catal *et al.,* 2023). Certifications are integrated into the curriculum pathway rather than being tied to a single course, such as Network+ in year one, Security+ or Cisco Certified Network Associate (CCNA) Cyber Ops in year two, and an advanced certification option related to a final-year practicum. The model is completed with an obligatory capstone or thesis, which is frequently based on an applied research or design problem linked with industry-defined requirements (Petersen *et al.,* 2020).

Evidence demonstrates that an integrated, outcome-based curriculum can increase the coherence and transparency of graduates' knowledge and skills. Program-level mapping also enables schools to demonstrate workforce coverage and explain their offerings to accrediting bodies and employer councils (Ismail *et al.,* 2024). However, the methodology necessitates extensive governance: curriculum committees must routinely check mappings against updated framework versions, coordinate assessment across several modules, and keep lab infrastructure, software, and teaching personnel up to date with best practices (Zafar *et al.,* 2024).

There is also a risk of "checklist alignment," in which the program appears well-mapped on paper, but students nonetheless receive disconnected instruction if teachers do not coordinate or if assessment is based on recall rather than authentic performance. Because several certifications are intertwined throughout the degree, students may experience stress or financial hardship if exam vouchers are not funded or workloads are not well managed (James & Callen, 2018).

Model C - Industry-cooperative model

The industry-cooperative model is based on strong connections with employers. Here, labs, certificates, and research are part of a larger work-integrated learning (WIL) ecosystem. This includes co-op placements, internships, industry-led laboratories, collaborative capstone supervision, and sometimes shared facilities like a cyber range. The fundamental strength of this model is its authenticity. Students learn in real-world settings, develop professional networks, and frequently convert assignments into jobs. Employers profit from a stream of talent and can

Publisher: SARC Publisher

tailor programs to meet current demands. It is strongly reliant on local industry's capability and willingness to host students, which might limit access for colleges in less crowded areas. The quality of learning differs between placements if monitoring and assessment are not uniform. There is also a risk of over-specialization: students may be taught narrowly in a certain company's technology stack or processes, which may not translate effectively if they shift industries or vendors (Zafar *et al.*, 2024).

Model D - Certification-first model

In the certification-first model, the curriculum is designed primarily around one or more industry certifications. Course outcomes, lecture topics, and lab activities closely follow published exam objectives, and success is often measured by pass rates on external exams. Tran *et al.*, (2023) describe a three-legged "stool" of cybersecurity education in which curriculum content, hands-on skills, and certifications are equal pillars, and provide survey evidence from employers that certifications are widely used in hiring decisions and salary setting.

The clear strength of this model is signaling power. Certifications provide recognizable, sometimes standardized credentials that employers understand and often demand, especially for entry-level roles in operations, support, and compliance. For students seeking fast access to the job market, a certification-focused pathway can feel efficient and concrete. Over-focusing on test objectives can crowd out deeper conceptual understanding and critical thinking, especially if instructors "teach to the exam" rather than integrate examinations into a broader educational design. Vendor-specific certifications can introduce dependence on technologies and leave gaps in areas such as policy, human factors, or emerging threats not yet covered in exam blueprints. Finally, because certifications require ongoing renewal, graduates may face recurring costs to maintain their credentials unless employers provide support (Erickson & Kim, 2021; Tran *et al.*, 2023).

Model E - Research-led advanced track

The research-led advanced-track model is most often seen in master's and doctoral programs or in honors tracks within undergraduate degrees. Here, labs are tightly coupled with ongoing research projects, and students spend significant time on independent or team-based research that addresses open problems in cybersecurity. In such tracks, certification preparation is typically optional; the emphasis is on scientific method, experimentation, and dissemination rather than on external exams. Industry needs to enter through problem choice and co-supervision: organizations propose topics, share data or infrastructure, and sometimes co-author outputs.

The key strength of this model is its ability to develop higher-order competencies that industry frameworks list but that undergraduate curricula often struggle to deliver at scale: research literacy, problem formulation, innovation, and leadership in complex projects. Graduates from research-intensive tracks are attractive not only for doctoral programs but also for roles in security R&D, advanced consulting, or roles that demand continuous learning and adaptation. At the same time, this model has limitations as a primary workforce strategy. It usually reaches fewer students because it requires small cohorts, close supervision, and access to research infrastructure. Without careful design, research-led tracks can also drift away from day-to-day operational concerns, leaving students very strong in theory but less practiced in routine security operations or standard tools. Some studies of REU implementations point to the importance of balancing advanced topics with structured mentoring and explicit professional skills training so that students can bridge from research back into industry roles (Yang *et al.*, 2019).

Hybrid and emerging models

In practice, many universities are using hybrid models that combine characteristics from earlier types while introducing new aspects such as micro-credentials, stacking certificates, and online or cloud-hosted labs. Micro-credentials in cybersecurity are increasingly being used to certify specific skill sets, and they can often be combined with bigger certificates or degrees. Some suppliers expressly link micro-credentials to frameworks such as Skills Framework for the Information Age (SFIA) or national cybersecurity standards, presenting them as adaptable building blocks for lifelong learning and skill building. In a hybrid university approach, a student may finish a standard degree that adheres to a program-wide alignment pattern while simultaneously obtaining various micro-credentials related to contemporary tools, techniques, or specialty domains such as cloud security or industrial control systems.

Another key rising trend is the utilization of remote labs and cyber ranges, which can be given entirely online or in hybrid formats. Research on

Publisher: SARC Publisher

virtual laboratories in cybersecurity education indicates that well-designed online labs can enable effective practice, particularly when physical access to equipment is limited or when students are geographically scattered (Haron *et al.*, 2024; Otoum *et al.*, 2025). Virtual ranges can be integrated into course-centric, program-wide, or industry-cooperative models, and they are especially well-suited to micro-credential approaches since they allow for short, intensive practice focused on certain competencies. Hybrid models also alternate between emphases over time: a first year that appears course-centric, a middle phase that follows certification-first design for entry-level credentials, and a final year with research-led capstones and co-op placements. These hybrid and emergent models strive to strike a balance between responsiveness and coherence. They can respond more quickly to changing threats and technologies than inflexible, fully planned programs, and they provide many entry and departure points for learners at various career levels. However, they also raise additional concerns about fragmentation, recognition, and quality assurance. When students accumulate a large number of little credentials and experiences, employers and sometimes even students themselves may struggle to comprehend how all of the parts fit together to form a coherent capability profile. Surveys of curriculum activities stress the importance of integrated frameworks and advise against patchwork learning routes that lack depth in fundamental topics (Ismail *et al.*, 2024).

Table 1**. Summary of Typology of Educational Models.**

Model	Core idea	Example sources
Course-centric (A)	Integration of labs, frameworks, and optional certification inside one or a few courses, often as an "intro to cybersecurity" or "network defense" course.	Towhidi & Pridmore (2023); Burton (2025)
Program-wide alignment (B)	Entire degree mapped to frameworks (NICE, CyBOK, etc.), with multiple lab-based courses, sequenced certifications, and a capstone or thesis.	Newhouse *et al.*, (2017); Ismail *et al.*, (2024)
Industry-cooperative (C)	Deep links with employers: co-op, internships, industry-led labs, joint supervision, sometimes shared cyber ranges.	Zafar *et al.*, (2024); other WIL/co-op studies
Certification-first (D)	Curriculum built mainly around one or more certifications; labs and assessments closely follow exam objectives.	Tran *et al.*, (2023); Erickson & Kim (2021)
Research-led advanced track (E)	Labs and projects tied to ongoing research; strong focus on inquiry, REU projects, theses, and advanced topics.	Yang *et al.*, (2019); Samanthula (2021)
Hybrid/emerging	A mix of the above, often with micro-credentials and virtual/online labs or ranges.	Ahmed *et al.*, (2020); Haron *et al.*, (2024); Otoum *et al.*, (2025)

Labs: types and technologies

Labs are the core mechanism that turn abstract cybersecurity concepts into usable skills. They give students a safe place to misconfigure, attack, defend, and break things before they do this in real systems. This section organizes the main types of labs, the supporting technologies, how they are designed and assessed, the challenges institutions face, and what the evidence says about their impact on learning, confidence, and employability.

Lab taxonomy

Cybersecurity education now uses a broad mix of lab formats. Traditional physical labs are still important in areas that require direct interaction with hardware, networks, or industrial systems. These labs host dedicated servers, switches, firewalls, programmable logic controllers, and other equipment, often in an isolated network. They are especially valuable for teaching topics such as network monitoring, industrial control system (ICS) security, and hardware attacks, where students must see or manipulate physical devices. Burton's modular framework stresses that such labs can be organized as reusable building blocks aligned to specific competencies, rather than as ad hoc machine rooms (Burton, 2025).

Virtual labs are now common in both face-to-face and online courses. They rely on virtual machines and cloud-hosted environments, allowing students to work from any location. Son *et al.*, (2012) early work on a virtual cybersecurity lab showed that virtualization can provide flexible, cost-effective

Publisher: SARC Publisher

hands-on practice while protecting institutional infrastructure. Contemporary examples include university "virtual cyber security labs" where students request virtual machines on demand and keep them across a semester. Remote labs extend this idea further by giving students controlled access to shared lab environments via the internet (Kebande, 2024).

Simulation and emulation labs overlap with ranges and virtual labs but focus more on modeling particular systems or attacks. For example, emulated industrial networks or Internet of Things (IoT) ecosystems let students test policies or defenses without touching real infrastructure (Robles-Gómez *et al.*, 2020). In parallel, IoT and embedded security labs use microcontrollers, sensors, smart devices, and small robots to explore firmware security, wireless security, and physical attacks. These labs respond to growth in IoT deployments and the need for graduates who can understand both software and hardware aspects of security. Platform-based designs, such as Vaish's web-based cybersecurity platform, aim to support both education and research across many lab types in a single environment (Vaish *et al.*, 2024).

In practice, many programs combine several lab types. Introductory courses might rely on simple VMs and guided labs. Later courses move into cyber ranges and specialized IoT or Information and Computer Science (ICS) labs. The taxonomy is therefore best seen as a spectrum of environments rather than separate boxes.

Technologies and platforms.

Underneath these lab types is a layer of enabling technologies. Virtualization is the baseline. Hypervisors allow multiple isolated operating systems to run on the same hardware, each with its own configuration and vulnerabilities. Virtualization makes it easy to snapshot, reset, and distribute lab environments, which lowers risk and maintenance effort. Early studies in virtual computer laboratories show that virtualization supports flexible, repeatable practice and can improve experiential learning when combined with good instructional design (Kebande, 2024).

Containerization builds on this by packaging applications and their dependencies into lightweight containers. For cybersecurity labs, containers are useful for quickly deploying vulnerable applications, specific tool chains, or microservices that students can attack and defend. Container orchestrators can spin up entire scenarios with multiple interacting services and then tear them down when a lab ends. Sandboxing tools add another safety layer by restricting what a process or application can do on the host system, which reduces the risk that malware or misconfigurations in a lab will escape into production networks. Managed cyber range platforms combine virtualization, containerization, orchestration, and scenario authoring tools into integrated products. Some are commercial, some open-source or institutional. They support features such as automated scenario deployment, scoring, real-time monitoring, and built-in assessment dashboards. These technological choices shape what is possible pedagogically. A simple virtualization setup might support basic exercises but struggle with large classes or complex simulations. A full cyber range can deliver realistic, multi-step incidents but requires more investment and staff expertise (Robles-Gómez *et al.*, 2020).

Challenges and mitigation

Despite their benefits, cybersecurity labs bring significant challenges. Cost is a major issue. Physical labs require specialized hardware, secure networks, and dedicated facilities. Cyber ranges and remote labs require servers, storage, licenses, and bandwidth. Even virtualization-based labs can be expensive once scaled to hundreds of students. Studies of remote labs underscore the importance of efficient resource management and scheduling to minimize infrastructure overhead. Shared or cloud-based platforms, institutional consortia, and open-source tools are common mitigation strategies (Vaish *et al.*, 2024).

Maintenance is another concern. Operating systems, tools, and vulnerabilities change rapidly. Lab images can become outdated within a semester. Burton's framework emphasizes modularity and version control for lab units as one way to manage this churn: small, self-contained lab modules can be updated and reused more easily than monolithic course images. Automation scripts and configuration management tools also help institutions rebuild environments quickly and consistently (Burton, 2025).

Scalability and security are tightly linked. When many students run malware, exploits, or aggressive scans, there is a risk that activity leaks onto production networks or the public internet. Proper network isolation, sandboxing, and strict access controls are essential. Remote lab studies stress the importance of role-based access, strong

Publisher: SARC Publisher

authentication, and logging for both security and academic integrity. Institutions also need clear policies specifying permissible tools and targets, along with explicit definitions of misconduct. For example, policies may prohibit activities such as scanning networks beyond the designated lab environment, deploying unauthorized exploits, or attempting privilege escalation on institutional systems.(Catal *et al.,* 2023).

Instructor expertise is another bottleneck. Effective lab-based teaching requires not only technical skill but also pedagogy: designing good exercises, scaffolding, and assessments. Reviews of online cybersecurity teaching note that instructors often struggle to balance workload, lab complexity, and timely feedback when classes are large. Professional development, team-teaching (pairing pedagogical and technical specialists), and sharing lab resources across institutions can help (Haron *et al.,* 2024).

Academic integrity and cheating are ongoing issues, especially in remote and Capture The Flag (CTF)-style environments. Students can share solutions, flags, or scripts. Some studies respond by designing labs where process and reflection matter as much as final answers, using unique per-student configurations, or integrating oral defenses and live demonstrations into assessment. CTF research also suggests using structured frameworks to measure learning outcomes rather than relying only on whether a challenge was solved.

Certifications: role, selection, and integration strategies

Certifications sit at the boundary between higher education and the labor market. For cybersecurity students, they are often the most visible "signal" that connects what they learned in class to what hiring managers ask for in job postings. For curriculum designers, certifications can act as a moving benchmark for what the industry expects, but they can also pull programs toward narrow exam preparation if they are not handled carefully. This section outlines types and roles of certifications, ways they are integrated into curricula, the main benefits and risks, the evidence and debates in the literature, and policy and equity questions that arise when certifications become de facto entry tickets to cybersecurity work.

Types and roles of certifications in curricula

Most curricula that engage with certifications work with three broad clusters: entry-level vendor-neutral certifications, vendor-specific certifications, and advanced professional certifications. Entry-level vendor-neutral certifications (for example, CompTIA Security+ or ISC2 Certified in Cybersecurity) aim to test foundational security principles, basic network and host security, risk concepts, and introductory governance. These credentials are widely used in government and defense contexts; job-ad analyses show high demand for Security+ in entry-level postings, alongside business-oriented certifications such as Information Technology Infrastructure Library (ITIL) and Project Management Professional (PMP) (Knapp *et al.,* 2017). In curricula, these certifications usually mark the point at which students are expected to demonstrate basic operational readiness, often after one or two core security courses (Erickson & Kim, 2021).

Vendor-specific certifications, such as Cisco's CCNA Security, Microsoft and Amazon Web Services (AWS) security credentials, or cloud-provider associate and specialty certifications, focus on specific platforms and toolchains. They tend to require more detailed configuration and troubleshooting skills for a particular ecosystem. Studies that review industry-standard certifications and governing bodies note that these vendor-specific credentials cover overlapping bodies of knowledge but map to different technology stacks, which forces programs to decide how far they want to embed particular vendors in their teaching. In curricula, vendor-specific certifications often appear in advanced electives or in co-op and industry-oriented pathways where local employers have clear preferences (Samanthula, B.K., 2021).

Advanced professional certifications, such as CISSP (Certified Information System Security Professional), CISM (Certified Information Security Manager), or specialized GIAC (Global Information Assurance Certification) certifications, cover broad domains like security management, architecture, incident response, or digital forensics at a more senior level. James and Callen's (2018) study "Cybersecurity Certifications Matter" reports that practitioners and managers see these certifications as indicators of experience, responsibility, and commitment, not just technical recall. These certifications are rarely the primary focus of undergraduate curricula, but they influence curriculum content and are often used as reference points when defining learning outcomes for graduate programs or executive education. Knapp and colleagues argue that professional certifications can provide valuable

Publisher: SARC Publisher

guidance to keep cybersecurity curricula current because certification bodies are under strong pressure to update domains in line with evolving threats and technologies (Knapp *et al.,* 2017).

Across all three clusters, the role of certifications in curricula is to provide externally validated targets for knowledge and skills, to help students signal their readiness to employers, and to give programs a practical check on whether content remains aligned with industry expectations. The literature also warns that this role should remain supportive rather than dominant.

Integration approaches

There are several recurring patterns in how curricula integrate certifications. One common pattern is to build exam-aligned modules into existing courses. In this model, one or more modules in a core cybersecurity course are mapped directly to specific exam objectives, and labs are designed to practice those objectives. Mukherjee's case study on integrating industry certifications into a foundations course, for example, aligns course topics and labs with Security+ domains while still covering broader concepts.

Another pattern is to offer stand-alone electives focused on certification preparation. These may be one-semester courses titled "Security+ Prep" or "Cloud Security Certification Lab," where lecture and lab time follow the exam blueprint closely, and students are expected to attempt the exam soon after. This approach keeps most of the curriculum concept-driven while concentrating certification pressure in a single course (Mukherjee *et al.,* 2024).

A third pattern treats certifications as credit-bearing components. Some institutions grant academic credit when students pass recognized certifications, either as prior learning credit or as part of structured pathways. Tran and colleagues (2023) describe a three-tiered model in which foundational courses map to entry-level certifications, upper-division courses support intermediate and vendor-specific certifications, and capstone or graduate courses align with advanced certifications. In their model, certification content is woven through the program rather than attached at the edges. There are also employer-sponsored certification pathways. In these arrangements, industry partners commit to co-funding training and exam vouchers and may co-design modules around specific credentials (Tran *et al.,* 2023).

Pros and cons

The main argument for integrating certifications is that they are recognized and valued in the labor market. Tran *et al.,* (2023) summarize survey data in which 67% of IT (Information Technology) executives reported requiring cybersecurity certifications as an entry requirement, and 80% of IT professionals said certifications were useful for their careers. Marquardson and Elnoshokaty's (2020) analysis of 11,938 entry-level cybersecurity job postings found that 29% explicitly required at least one certification, in addition to 60% requiring a degree. Other industry studies suggest that candidates with technology certifications are more likely to be hired than similarly qualified candidates without them. This aligns with James and Callen's (2018) practitioner interviews, where certifications are reported to add credibility, support advancement, and help employers filter candidates.

Beyond hiring, certifications can support curriculum maintenance. Because certification bodies update their domains and exam objectives frequently, mapping courses to these domains can help programs notice when their coverage of areas like cloud security, threat intelligence, or privacy has fallen behind. Knapp *et al.,* (2017) argue that professional certifications offer "valuable guidance" for maintaining a cybersecurity curriculum's currency, though they caution that they should be one input among others, not the sole driver.

On the downside, certification-driven design can narrow learning. Exam blueprints tend to emphasize specific technologies, frameworks, and lists of controls, which can encourage memorization and "teaching to the test" at the expense of conceptual depth, critical thinking, and research skills. Tran *et al.,* (2023) report faculty concerns that focusing too heavily on certifications risks producing "paper certs" that signal short-term recall but not durable competence

There is also a risk of misalignment between academic outcomes and exam objectives. Certifications may underemphasize ethics, social and organizational dimensions, and emerging areas not yet codified in exam outlines. Finally, the time and cost of preparation can displace other valuable activities like research projects or interdisciplinary electives, especially in compressed programs.

Publisher: SARC Publisher

Mapping curricula to industry needs: frameworks and evidence

Curriculum alignment work in cybersecurity usually starts from a simple question: "If our graduates take a specific job, what exactly should they know and be able to do?" Industry and policy bodies answer this using workforce and knowledge frameworks such as NICE, ECSF (European Cybersecurity Skills Framework), CyBOK (Cyber Security Body of Knowledge), and CSEC2017(Cybersecurity Education Curriculum). Universities then try to map course outcomes to these frameworks and see where they are strong, weak, or misaligned with demand (Chouliaras *et al.,* 2021). This section primarily outlines a practical approach to curriculum mapping and briefly touches on supporting evidence from recent studies.

Method for mapping (recommended approach)

The basic mapping process described in the literature follows a few common steps. Newhouse *et al.,* (2017) explain that the NICE Framework defines work roles, tasks, and knowledge, skills, and abilities (KSAs) and is meant to guide curriculum and training design. Ngambeki *et al.,* (2021) report a case where a whole computing program was mapped to NICE: they first listed all courses in the program, then collected for each course its topics, learning outcomes, and main assessments, and finally linked these elements to NICE categories, specialty areas, and selected KSAs. The result was a coverage matrix with courses on one axis and NICE elements on the other, showing which parts of the framework were addressed, how often, and at what depth.

Ramezanian and Niemi take a more detailed approach. They map all 630 knowledge descriptions from NICE to the knowledge areas and units in the CSEC2017 curriculum, compute weights for each area based on importance to work roles and then identify where the curriculum is dense or thin relative to those weights. This work suggests that mapping can go beyond a simple checklist: it can be used to prioritize knowledge areas and design roadmaps for students targeting specific job categories (Ramezanian & Niemi, 2024).

A practical mapping method can be implemented as follows. First, one or more reference frameworks (such as NICE together with CyBOK or ECSF) are selected, and their versions are fixed for the duration of the mapping exercise (Marquardson & Elnoshokaty, 2020). Next, an inventory of courses is built, with clearly stated learning outcomes and main activities such as labs, projects, certifications, and research tasks. A two-way mapping is then performed: for each course, the relevant framework areas and KSAs it supports are tagged, and for each framework competence, the courses that address it and the corresponding Bloom level are identified. For example, Towhidi and Pridmore (2023) combine the revised Bloom's taxonomy with NICE KSAs to ensure that learning outcomes reach higher cognitive levels rather than stopping at simple recall. This information is then organized into a coverage matrix, which is examined for uncovered competencies, overloaded areas, and weak progression. Finally, the mapping is validated with industry partners or alumni to confirm that it reflects real-world roles and expectations rather than only aligning with formal documents.

Integration models evaluation: effectiveness, metrics, and evidence

The previous sections described different ways curricula integrate labs, certifications, and research. This section looks at how these integration models are evaluated in the literature. It outlines common outcomes and metrics, summarizes comparative findings about which approaches seem most effective, and highlights methodological limits that affect how strongly we can interpret the evidence.

Outcomes and metrics used in the literature

Studies of cybersecurity education use a mix of quantitative and qualitative indicators. At the simplest level, many papers report on student satisfaction, perceived learning, or self-efficacy using pre- and post-course surveys. For example, research on virtual labs and cyber ranges often measures changes in students' confidence in performing security tasks and their attitudes toward cybersecurity careers. CTF studies use performance on challenges plus self-reported gains in knowledge and motivation (Son *et al.,* 2012).

Job placement rates, time to first job, and job role alignment are all examples of employment-related measures. Erickson & Kim's 2021 study, for example, employs the NICE Framework to compare graduates' projected positions with the ones they actually hold, assessing how effectively a school prepared them for those tasks. Employer satisfaction is occasionally measured using surveys or focus groups, but these are often small and local. In their study of collaborative paths between academia and business, Zafar *et al.,* (2024) collect

Publisher: SARC Publisher

qualitative feedback from industry partners on the perceived readiness and strengths of graduates from programs that emphasize work-integrated learning and joint projects.

Competency assessments are utilized in some lab and range investigations. Researchers create cyber range scenarios that correspond to various abilities and then assess student performance using flags captured, services maintained, or configuration states obtained. According to NIST's cyber range guide, such performance metrics may be more accurate predictors of job preparation than written assessments. Supervisors in work-integrated learning studies evaluate students based on technical independence, communication, professionalism, and alignment with workplace norms. McKenzie *et al.*, (2025) case study on IT work-integrated learning employs extensive rubrics to assess progress during and following placements.

Exam and certification pass rates are another popular statistic, particularly in certification-first or certification-integrated programs. Tran *et al.*, (2023) track security and other certification outcomes for students who follow an integrated, three-tier curriculum, using pass rates and employer survey data to demonstrate that their strategy increases workforce preparation. Some programs see obtaining a specific certification as a capstone achievement.

Lastly, some research investigates bigger concepts like self-efficacy and strength. Rumsa *et al.*, (2025) research on strengths-based cybersecurity education finds that matching learning activities with students' perceived strengths increases self-efficacy, engagement, and early career results. Mukherjee *et al.*, (2024) conduct strategic evaluations that categorize results as knowledge acquisition, practical skills, critical thinking, and alignment with framework-derived learning objectives.

Comparative findings across models and methodological limitations

Evidence from the literature suggests that program-wide alignment and industry-cooperative models generally yield stronger outcomes in job placement and employer satisfaction. At the same time, hybrid approaches appear most adaptable for addressing rapid technological change and diverse learner needs (Zafar *et al.*, 2024). Certification-first models often improve short-term employability but risk narrowing conceptual depth, and research-led tracks excel at fostering higher-order skills such as innovation and problem-solving, though they typically reach smaller cohorts (Tran *et al.*, 2023). Despite these insights, methodological limitations constrain the strength of these conclusions. Most studies rely on self-reported data or local case studies, with few longitudinal analyses tracking career progression. Comparative evaluations across models are rare, and sample sizes are often small, making generalization difficult. Additionally, the absence of standardized performance metrics and the dominance of descriptive rather than experimental designs mean that claims about effectiveness should be interpreted cautiously (Mukherjee *et al.*, 2024). These limitations underscore the need for coordinated, multi-institutional research efforts to determine which integration strategies most effectively support long-term workforce readiness and learning outcomes.

CONCLUSION

This review underscores the urgent need for cybersecurity curricula to evolve beyond theory-driven models and embrace integrated approaches that combine hands-on labs, certifications, and research experiences. Evidence from the literature demonstrates that modular, experiential labs significantly enhance practical skills and adaptability, while structured certification pathways provide industry-recognized signals of competence. Although less common on a large scale, research participation promotes higher-order thinking and innovation, equipping graduates for advanced employment and lifelong learning. Among the educational models analyzed, which include course-centric, program-wide, industry-cooperative, certification-first, and research-led tracks, hybrid designs appear to be the most promising for closing the skills gap. They provide greater flexibility and can better respond to technological change. However, difficulties remain, such as limited resources, fragmented learning, and the possibility of overemphasis on exam preparation. Effective integration requires intentional mapping to frameworks like NICE and NIST Cybersecurity Framework, ongoing curriculum revision, and collaboration with industry partners. Finally, the findings call for coherent, outcome-based designs that combine basic knowledge with job-ready competencies, ensuring that graduates can meet changing employment demands and contribute meaningfully to cybersecurity resilience.

Publisher: SARC Publisher

REFERENCES

1. Ahmed, A., Lundqvist, K., Watterson, C., & Baghaei, N. "Teaching cyber-security for distance learners: A reflective study." *2020 IEEE Frontiers in Education Conference (FIE)* (2020): 1–7.
2. Burton, S. L. "A modular framework for cybersecurity laboratory design in higher education." *Laboratories* 2.4 (2025): 21.
3. Catal, C., Ozcan, A., Donmez, E., & Kasif, A. "Analysis of cyber security knowledge gaps based on cyber cybersecurity body of knowledge." *Education and Information Technologies* 28.2 (2023): 1809–1831.
4. Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. "Cyber ranges and testbeds for education, training, and research." *Applied Sciences* 11.4 (2021): 1809.
5. Erickson, M., & Kim, P. "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning." *Issues in Information Systems* 22.4 (2021).
6. Haron, N. S., Batrisyia, N. I., Taib, S. M., & Abdul Rahman, A. S. "Enhancing online delivery of practical labs for cyber security course using virtual laboratories." *Journal of Electrical Systems* 20.4s (2024): 885–887.
7. Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. "Cybersecurity activities for education and curriculum design: A survey." *Computers in Human Behavior Reports* 16 (2024): 100501.
8. James, J. E., & Callen, J. "Cybersecurity certifications matter." *Issues in Information Systems* 19.3 (2018).
9. Kebande, V. R. "The impact of virtual laboratories on active learning and engagement in cybersecurity distance education." *arXiv* 2404.04952 (2024).
10. Knapp, K. J., Maurer, C., & Plachkinova, M. "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance." *Journal of Information Systems Education* 28.2 (2017): 101–114.
11. Marquardson, J., & Elnoshokaty, A. "Skills, certifications, or degrees: What companies demand for entry-level cybersecurity jobs." *Information Systems Education Journal* 18.1 (2020): 22–28.
12. McKenzie, S., Bangay, S., & Young, K. "A case study analysis of the criteria used for authentic evaluation of information technology students' progress on workplace-based work-integrated learning." *International Journal of Work-Integrated Learning* 26.3 (2025): 459–476.
13. Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. "Strategic approaches to cybersecurity learning: A study of educational models and outcomes." *Information* 15.2 (2024): 117.
14. Newhouse, W., Keith, S., Scribner, B., & Witte, G. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." *NIST Special Publication 800-181* (2017).
15. Ngambeki, I. B., Rogers, M., Bates, S. J., & Piper, M. C. "Curricular improvement through course mapping: An application of the NICE framework." *2021 ASEE Virtual Annual Conference* (2021).
16. Otoum, N., Al Maqousi, A., Alauthman, M., & Almomani, A. "Remote labs in cybersecurity education: Analyzing software requirements and challenges." *International Journal of Cloud Applications and Computing* 15.1 (2025): 1–27.
17. Petersen, R., Santos, D., Smith, M., & Witte, G. "Workforce framework for cybersecurity (NICE framework)." *NIST Special Publication 800-181 Rev. 1* (2020).
18. Ramezanian, S., & Niemi, V. "Cybersecurity education in universities: A comprehensive guide to curriculum development." *IEEE Access* 12 (2024): 61741–61766.
19. Robles-Gómez, A., Tobarra, L., Pastor-Vargas, R., Hernández, R., & Cano, J. "Emulating and evaluating virtual remote laboratories for cybersecurity." *Sensors* 20.11 (2020): 3011.
20. Rumsa, S., Afsharnejad, B., Lee, E. A. L., Bölte, S., Tan, T., & Girdler, S. "Strengths-based cybersecurity education and training program for autistic adolescents: A feasibility study." *Neurodiversity* 3 (2025): 27546330251370656.
21. Samanthula, B. K. "REU SITE: Enhancing undergraduate research experiences in cybersecurity and privacy-enhanced technologies." *NSF Directorate for Computer and Information Science and Engineering* 20.2050548 (2021): 50548.
22. Son, J., Irrechukwu, C., & Fitzgibbons, P. "Virtual lab for online cyber security education." *Communications of the IIMA* 12.4 (2012): 5.

Publisher: SARC Publisher

23. Towhidi, G., & Pridmore, J. "Aligning cybersecurity in higher education with industry needs." *Journal of Information Systems Education* 34.1 (2023): 70–83.
24. Tran, B., Benson, K. C., & Jonassen, L. "Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce." *Journal of Cybersecurity Education, Research and Practice* 2023.2 (2023).
25. Vaish, A., Kumar, R., Bobek, S., & Sternad, S. "Development of cyber security platform for experiential learning." *Journal of Cybersecurity Education, Research and Practice* 2024.1 (2024).
26. Yang, D., Xu, D., Yeh, J. H., & Fan, Y. "Undergraduate research experience in cybersecurity for underrepresented students and students with limited research opportunities." *Journal of STEM Education* 19.5 (2019).
27. Zafar, H., Hollingsworth, C. L., Bandyopadhyay, T., & Randolph, A. B. "Collaborative pathways to cybersecurity excellence: Insights from industry and academia in the southeastern US." *Journal of Cybersecurity Education, Research and Practice* 2024.1 (2024).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Nnadi, K. and Opoku, J. A. " Cybersecurity Curriculum Alignment with Industry Needs: A Literature Review of Educational Models Integrating Labs, Certifications, and Research." *Sarcouncil Journal of Engineering and Computer Sciences* 4.12 (2025): pp 64-76.

Publisher: SARC Publisher