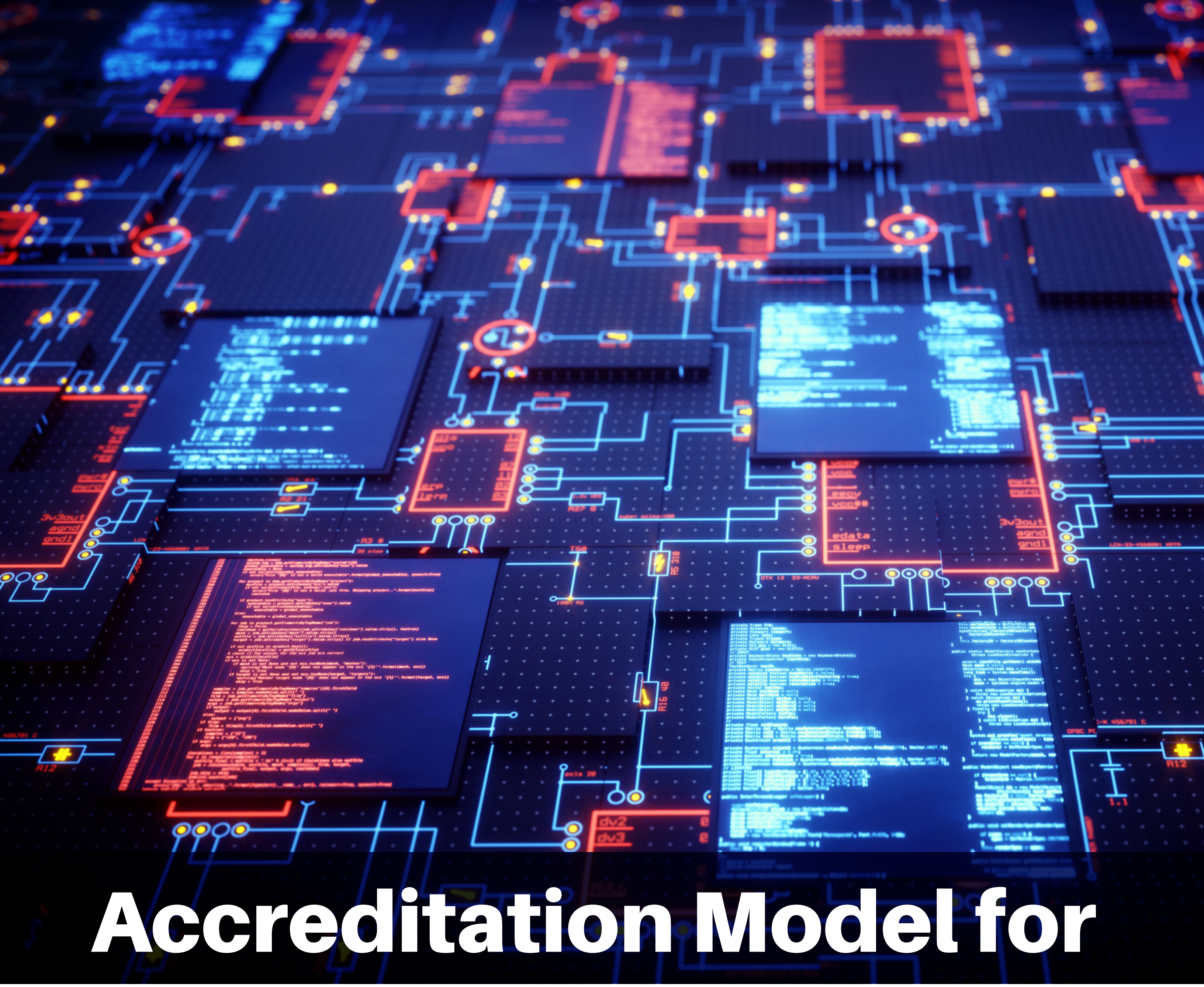


Accreditation Model for Cybersecurity Competency-Based Community Clinics

SEPTEMBER 2025

workcred
an affiliate of ANSI

Table of Contents

©2025, Workcred. All Rights Reserved.

Introduction

Given the high workforce demands for individuals with cybersecurity talent, quality programs must be developed to ensure course, certificate, and degree completion, is a valid indicator of the competence to perform related cybersecurity functions and roles. Recent data suggest that cybersecurity program completion has recently increased; however, this same report highlights a significant gap between enrollment in cybersecurity programs in the U.S. and completion of those programs. According to data from the National Student Clearinghouse, for associate degree programs in cybersecurity fall 2018 total enrollment was nearly 15,000 learners. However, by 2021 approximately 3,800 learners earned an associate degree, reflecting a completion rate of merely 25 percent.

Moreover, it is unknown how many of these graduates had developed the competence needed to become employed in a cybersecurity job after graduation. As reported by Knutson (2020), Sonya Miller, human resources director for IBM Security and Enterprise and Technology Security, provided a Congressional testimony which indicated “the U.S. education system is not producing candidates with relevant ‘soft skills’ or even the technical skills for jobs in the cybersecurity space except from a narrow swath of learners.”

Given the significant gap in enrollment and completion of cybersecurity programs, as well as the consistent demand for cybersecurity professionals with hands-on experience, there exists a need for more competency-based workplace learning aligned with cybersecurity practices where learners’ competencies are validated through appropriate assessments. The need for practice-forward learning is not new. In fact, the federal government has worked to identify what these practices may entail through the development of the NICE framework competency areas, which detail the competencies needed for managing and mitigating cybersecurity risks across various industries, as well as Cybersecurity Maturity Model Certification (CMMC) which provides guidance on how cybersecurity contractors can protect unclassified data.

Additionally, to address the need for more hands-on experience, there has been an increase in the development of various cybersecurity clinics across the nation. Programs such as the Consortium of Cybersecurity Clinics (supported by Google), a network of university-based cybersecurity clinics that work with local communities to provide cybersecurity services, as well as community-based clinics that operate outside of universities such as the Cyber Volunteer Resource Center. Yet, despite the work done to identify cybersecurity practices and provide hands-on experience through clinics, no framework exists to ensure that community-based clinics offers consistent, high-quality learning regardless of where learners choose to pursue their training. As such, this report summarizes findings from both the literature and the community to identify the elements that are needed for the development of an accreditation model for community-based cybersecurity clinics that provide learners with real-world, work-based learning opportunities.

Workcred, in partnerhsip with the National CyberWatch Center, developed this model to accredit cybersecurity community clinics against standards of learning outcomes and evidence-based cybersecurity and information system audit and assurance practices. The clinics the model is for are those operated by non-profit or for-profit organizations that are not a part of accredited institutions of higher education.

KEY TERMS

Cybersecurity community clinics: Clinics that are operated by non-profit or for-profit organizations that are not accredited institutions of higher education. They provide services and support to clients within the local community such as local government, non-profit organizations, or businesses within the area.

Competency: The integration of knowledge, skills, abilities, and judgment demonstrated through effective performance of tasks in context.

Mastery: Minimally acceptable proficiency and competency levels as defined by the clinic.

Must: These are mandatory requirements within the accreditation model.

May: These are recommendations within the accreditation model.

Literature Review and Data Collection Process

To collect information from the literature, the following criteria were established.

The inclusion criteria consisted of the following:

- ☑ Information was published within the last 10 years
- ☑ Information was virtually accessible
- ☑ Information was contained in peer-reviewed journal articles or evidence-based reports from government agencies, academic institutions, or professional bodies
- ☑ Studies addressed competency-based or cybersecurity education and training, including topics relating to resources, mastery of competencies, educational outcomes, assessment design, teaching learning interactions, and eligibility for competency-based education and training
- ☑ Studies involved learners in secondary and post-secondary education and training
- ☑ Studies related to experiential, applied, or work-based learning

Information was rejected if:

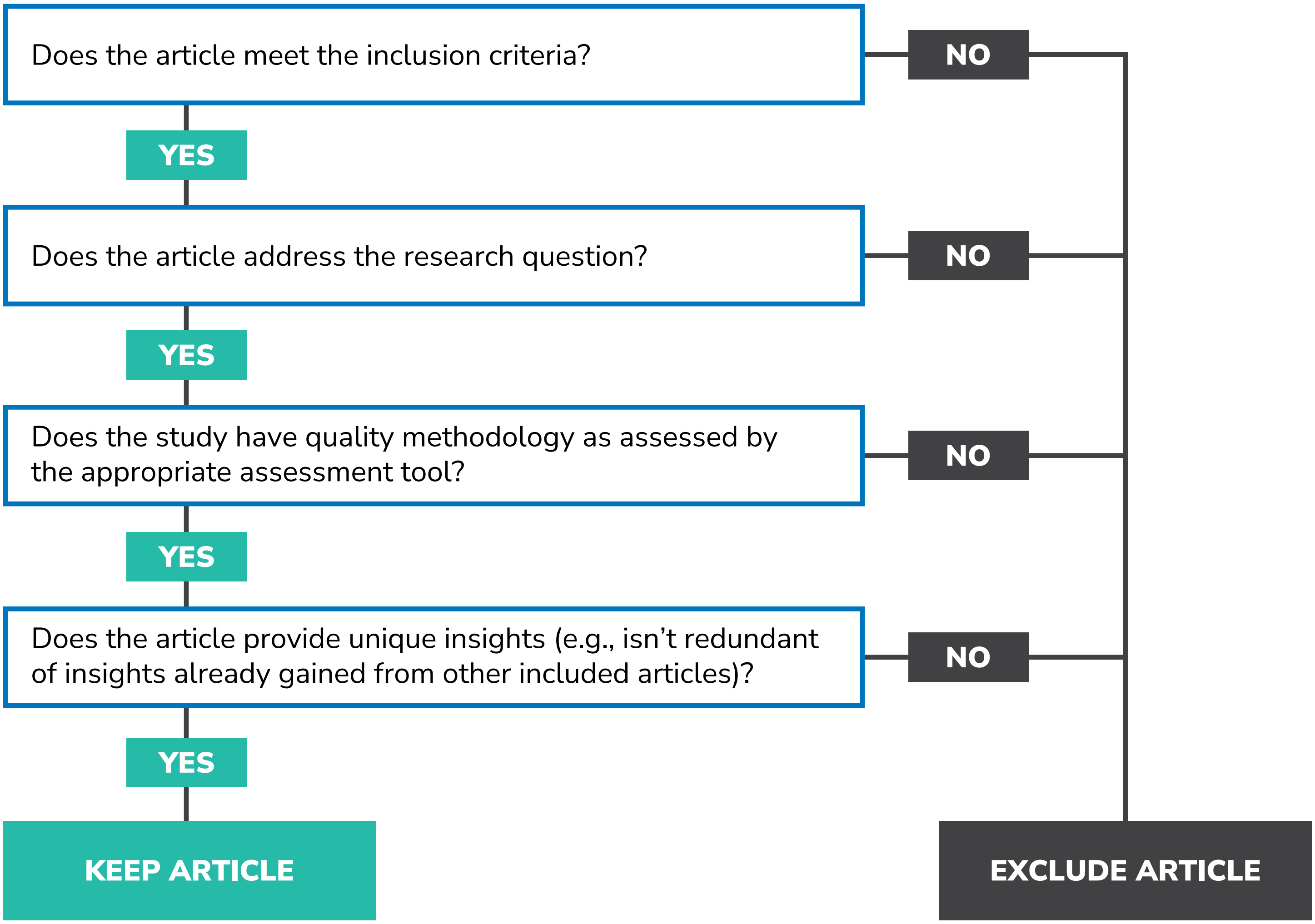
- ☒ It was not written in English
- ☒ It did not have sufficient data or methodological rigor
- ☒ It did not mention a clinical, experiential learning component, or performance-based assessment
- ☒ It was not fully accessible virtually

Relevance and contribution criteria:

- » Does it address themes regarding / related to the research question?
- » Does it provide unique insights or examples?
- » Does it provide sources, references, or evidence?
- » If applicable, is the methodology sample size explained and replicable?
- » If applicable, are limitations and biases explicitly addressed?

The decision process protocol for applying these inclusion and exclusion criteria is illustrated in Figure 1.

Figure 1. Literature review protocol for article selection


Does the article meet the inclusion criteria?
NO
YES
Does the article address the research question?
NO
YES
Does the study have quality methodology as assessed by the appropriate assessment tool?
NO
YES
Does the article provide unique insights (e.g., isn't redundant of insights already gained from other included articles)?
NO
YES
KEEP ARTICLE
EXCLUDE ARTICLE

During the initial screening process, the titles and abstracts of all the search results were reviewed to determine their relevance to the inclusion criteria as described above, resulting in 113 relevant sources. These 113 remaining sources were then given a deeper review to determine relevance and contribution against those criteria, leaving 44 sources to include for the structured abstract.

In addition to conducting this literature review, data were also derived from the cybersecurity community. Focus groups were held at four National CyberWatch Center regional summits (one held in the southwest, southeast, mid-atlantic, and mid-west) where stakeholders such as faculty, learners, and clinic leaders provided input and feedback on the development of this accreditation model through answering the questions that follow:[1]

- In hands-on experiences like clinics or internships, what do you think learners should walk away with that they might not get from a regular class?
- What do you think it means for a hands-on program to be successful for the learners, educators, and the community they serve?

[1] Author's note: the findings from these focus groups are explained beginning on page 7.

- What kind of lasting impact would you hope a program like this could have on learners, faculty, and the broader community?
- Where do you think learners (or you personally) tend to face the biggest challenges when applying what they have learned to real-world tasks or projects?
- How can you tell when someone is truly ready to step into real-world cybersecurity work after a hands-on program?
- What kinds of barriers (e.g., technical, personal, or organizational) can make it hard for learners to succeed in real-world projects?
- What strategies, resources, or types of support have you seen help overcome those barriers?
- What people, tools, or resources do you think are most important for creating high-quality hands-on learning experiences?
- What types of partnerships (inside or outside the educational institution) seem most valuable for programs like clinics or internships?
- What kinds of relationships between learners and mentors or faculty make these experiences most meaningful?
- In your experience, what makes mentorship especially effective in real-world, hands-on learning settings?
- How is mentoring or coaching in applied settings different from teaching in a traditional classroom?
- If you could make sure one thing is included when designing accreditation standards for programs like cybersecurity clinics, what would it be?

Reliability and Validity

For content validity purposes, a peer review panel was established to seek input from relevant stakeholder groups, including representatives from accreditation organizations, competency-based education experts, and adopters of current cybersecurity clinics.

A total of 21 candidates from one or more of these stakeholder groups were identified for the peer review panel, and email invitations were sent to gauge their interest in participating in the panel. Of the 21 candidates chosen, seven responded – three declined and four agreed to join the panel. Additional panelists were identified through referrals as well as networking at meetings and the regional cybersecurity summits, leading to three additional stakeholders for a total of seven stakeholders joining the review panel.

The panel ensured the data collected for the literature review was valid by doing the following:

- Reviewing and providing feedback on the literature review protocol
- Reviewing and providing feedback on the literature review outline
- Reviewing and providing feedback on the literature review
- Reviewing and providing feedback on the competency-based accreditation model

For additional reliability and validity purposes, after a review by the peer review panel, all work went under an internal examination where staff members conducted independent reviews of the content. While no rubric was used for this review, the continuous use of outside review provides evidence of reliability and validity.

Findings from the Four National CyberWatch Center Regional Summits

Establishing the Clinics

- Clinics should be intentionally integrated into the curriculum
- Clinics should have multiple entry points (i.e., meeting the needs for those who wish to start in high school, post-secondary education, and professionals already in the workforce)
- Clinics should be a reflection of their community (i.e., expecting learners to have a high level of prior knowledge when local training does not exist creates unrealistic barriers and is not a reflection of the community)

Outcomes of the Clinics

After completing a program in the clinic, learners should:

- Gain confidence
- Obtain experience in applying skills
- Develop professional communication skills
- Understand limitations and be able to ask for the appropriate level of support

Experience Types

Learners should gain experience through the following opportunities:

- Real-world projects
- Live simulations that can supplement real projects when clients are not readily available

Curriculum

Curriculum should include the following:

- Communication, adaptability, and critical reflection (e.g., being able to connect and communicate issues to a real business risk)
- Cybersecurity standards awareness
- Situational awareness

Assessments

Assessments should consist of the following:

- Structured reflection where learners are asked what, how, and why they did something
- Clear competency-based progression and planned observation checkpoints to track growth over time

Clinic Operations

- Clinics should have clear protocols for protecting client data and reducing liability
- Supervision of the learners in the clinics should be done by industry professionals who are certified and are current in the field
- Clinics should establish clear policies on liability and when law enforcement should be engaged
- Clinics should have long-term support models for their community partners (e.g., subscriptions, ongoing services)

Equity

- Clinics should address a variety of student backgrounds, recognizing some may not have prior exposure to technology and/or cybersecurity
- Mentorship and apprenticeships models should be included
- Clinics should include opportunities for upskilling current cybersecurity professionals, not just degree seekers

National Standards

- Shared tools and practices should be recommended by a national technology council
- Community-based voting should determine what tools to teach
- Clinics may benefit from participating in regional or national alliances to align tools, practices, and standards

Academic Credits and Financing

- Clinics could be linked to microcredentials or badging
- Clinics can work with education institutions to offer academic credit, non-degree credit, or clock-hour credit
- Clinics should consider offering learners stipends or paid internships
- Clinics should explore how federal work-study programs or Pell grants could support student participation

Elements of the Accreditation Model

To form the basis of the model, a deductive, thematic analysis was conducted to determine the elements needed, as portrayed below and described through each of the following sections.

- **Eligibility requirements for admission**
- **Competency framework**
- **Curriculum design**
- **Teaching-learning interactions**
- **Assessment design**
- **Educational outcomes**
- **Resources**

Eligibility Requirements for Admissions

Eligibility requirements for admissions play a key role in community-based cybersecurity clinics, and they define the minimum knowledge, skills, and abilities (KSA) applicants must demonstrate to be admitted into a cybersecurity clinic. It is a way to determine whether prospective learners meet the minimum entry standards set by the clinic. Eligibility requirements may also be used to inform placement for admitted learners.

Clinics must identify and document how the eligibility criteria for admissions have been validated.

Given the importance of eligibility requirements, clinics should have validated criteria tailored to the clinic's and community's needs. The validation methods are up to the clinic's discretion.

Examples of how the eligibility criteria can be validated include a local job task analysis, which can be used to determine local job competencies and ensure the clinics are providing services and opportunities that are of high impact to the local community, as well as competencies identified by certifications bodies, which can often be derived from test blueprints (Bendler & Felderer, 2023; Hernandez-de-Menendez et al., 2020; Henri et al., 2017; Lurie & Garrett, 2017; O'neil et al., 2014). The validation may also include an assessment of the resources available in the area to ensure the eligibility criteria are accessible to the population the clinic serves. For example, setting an eligibility requirement that demands a certain level of cyber skills when the community has minimal cybersecurity training opportunities creates unnecessary challenges for the learners. Once the eligibility criteria have been identified and validated, clinics should ensure the criteria are applied consistently through an application process that assesses the skills and knowledge of prospective learners.

Clinics must develop an application process that includes an assessment of eligibility requirements for admission.

Once eligibility criteria are set, clinics must assess applicants' prior knowledge to validate that applicants meet the eligibility requirements (Watkins et al., 2018), the criteria of which are determined by the clinic. The measurement of these competencies may inform the placement of the learners in the program (Gómez et al., 2017).

Measurement of competencies can be based on a combination of a job task analysis and the NICE framework (Brilingaitė et al., 2020), inclusive of both technical and non-technical skills. Hands-on demonstrations, interviews, and attainment of certifications (e.g., CompTIA Security+, Lean Six Sigma Green Belt, and other industry-recognized credentials) may also be used to validate knowledge of cybersecurity tools.

Validated assessments that have been tested for reliability and consistency may assess prior learning or performance through the means of high-fidelity simulations or in-field settings. For example, in the situation in which a field setting is used, learners are scored using a validated rubric by observers who have been trained on how to give the assessment, increasing interrater reliability (Brilingaitė et al., 2020). Here, learners can be assessed on multiple competencies with the level of their competency ranging from recall, proficient, competent, and mastery.

Clinics must establish and provide guidance to learners who are not admitted into a cybersecurity clinic. Information must be accessible without request.

In the case where applicants do not initially meet the minimum entry standards, entry results should be accompanied by recommended self-study or preparatory remediation programs designed to raise capability maturity to acceptable levels for entry. Moreover, eligibility guidance must be made readily accessible to learners without request, like on the clinic's website (Fjellström & Kristmansson, 2019; Gruppen et al., 2016; Hawkins et al., 2015; Rich et al., 2020; Sargeant et al., 2018). Providing applicants access to recommended self-study or preparatory programs provides opportunities for the applicants who have minimal gaps of knowledge to strengthen their competencies and reapply to the clinic.

Competency Framework

A competency framework necessitates that competencies must be created using a validated process (e.g., job task analysis, validation survey) to ensure it reflects current industry practices. Measuring learner progress using a structured model helps to identify the various stages of growth and validates that learners are developing the identified skills. This progression maturity approach includes four levels: knowledge recall (beginner), depth of understanding (proficient), skillful application (competent), and conditionalized expertise (mastery) (Tobey et al., 2018a; 2018b). This approach provides transparent evidence of student development.

Clinics must have a documented plan for learners achieving mastery, as defined by the clinic.

A documented roadmap towards achieving mastery should be developed by the clinics as a means of measuring learners' progress. The plan may be made accessible to the learners, so that there is transparency of clinic and learner expectations. The plan is also helpful in tracking areas of opportunities for learners and providing insight into opportunities for intervention in the event a learner does not meet the progress threshold. Having a plan allows for flexible learning and accurate tracking of the learners and supports individualized learning (Hawkins et. al., 2015).

Clinics must use a job task analyses and nationally recognized frameworks for alignment achieving mastery of competencies.[2]

By first mapping competencies to job task analyses, clinics ensure competencies reflect current and real-world responsibilities required in their community. Clinics must then align these competencies to nationally recognized frameworks such as CMMC and NICE to confirm consistency with broader workforce expectations. For example, a clinic focused on incident response may begin by identifying local job requirements for monitoring and responding to security threats, the align those competencies to the NICE framework protect and defend category and to CMMC practices in incident response and risk management. This dual alignment validates that learners are not only prepared to address local concerns but also meet industry-recognized standards for maturity and capability. While use of additional standardized documents such as test blueprints or the Cyber Security Body of Knowledge is not required, adoption can strengthen the rigor, consistency, and employer relevance of community cybersecurity clinics (Bendler & Felderer, 2023; Hernandez-de-Menendez et al., 2020; NICCS, 2025; O'Neil et al., 2014).

Cybersecurity clinics must include employability, management, and technical competencies.

Employability skills (e.g., communication, teamwork, adaptability, and problem-solving) are essential for functioning effectively in collaborative and high-pressure environments, like cybersecurity. Management competencies (e.g., project planning, risk assessment, and decision-making) help learners understand how to prioritize tasks and align technical efforts with organizational goals. Technical competencies (e.g., threat analysis, secure system configuration, and incident response) form the foundation of cybersecurity expertise. Clinics should intentionally design learning experiences and assessments that reflect this blend of competencies by requiring learners to complete team-based projects that simulate professional environments, delivering technical briefings, and documenting workflows using industry-standard tools. Research shows that in many cases, programs focusing more on technical skills often overlook the necessary employability and management skills needed to do the job (Bendler & Felderer, 2023; Chowdhury & Gkioulos, 2021; Hernandez-de-Menendez et al., 2020; Saharinen et al., 2020).

Curriculum Design

This construct necessitates that the curriculum design is congruent with competency-based and mastery learning models of instruction. It must be based on theoretical models that are accepted in learning science and/or in the workforce industry. These models can include mastery learning (Block, 1971; Bloom, 1968; Carroll, 1963), cognitive load (Moreno & Park, 2010), elaboration theory (Reigeluth, 1999), experiential learning (Kolb, 1984), readiness as the basis for aptitude (Corno et al., 2002), and how people learn (Bransford et al.,2000). Moreover, the curriculum design consists of a system of instruction, assessment, feedback, self-reflection, and ends with learners demonstrating that they have acquired the competencies as stated by the clinic.

[2] Author's note: examples of nationally recognized frameworks can include CMMC, NICE framework, and Cyber Security Body of Knowledge for alignment in achieving mastery of competencies.

Curriculum must be work-based, focused, and centered around real-world experiential learning with clients in the community.

Cybersecurity clinics must offer learners real-world, experiential learning opportunities with clients in the community. These experiential learning opportunities include engagements with local businesses, governments, and non-profit organizations. Clinics provide learners with authentic contexts to apply their skills such as, conducting risk assessments or supporting a cybersecurity audit. Community engagement also exposes learners to current industry tools, professional expectations, and collaborative problem-solving in environments that mirror actual workplace dynamics. By embedding community-based, experiential learning into the curriculum, clinics ensure that learners gain practical experience, build professional networks, and develop a deeper understanding of how their competencies translate into real-world impact (Assante et al., 2013; Brilingaitė et al., 2020; Bendler & Felderer, 2023; Chowdhury & Gkioulos, 2021; Hernandez-de-Menendez et al., 2020).

Community cybersecurity clinics must design a curriculum centered on practical, real-world cybersecurity tasks. Curricula based on real-world tasks will enable learners to acquire the KSAs that prepare them for a smoother transition into the workforce. While KSAs are essential components, competency requires their integrated application in practice. Previous studies have shown that although there are different methods for creating cybersecurity curricula, developing cybersecurity curricula that reflect real-world cybersecurity tasks requires significant time and resources to ensure alignment (Gómez et al., 2017; Brilingaitė et al., 2020; Chowdhury & Gkioulos, 2021; Boland et al., 2016).

Learning activities may include project-based opportunities.

Learning activities may include project-based opportunities with clients in the community. Additional project-based learning may involve simulated incidents and task management. Research has demonstrated that there are multiple types of learning models suited for cybersecurity education that allow learners to engage in experiential learning opportunities with community partners, covering topics such as security and privacy (Brilingaitė et al., 2020; Bendler & Felderer, 2023; Chowdhury & Gkioulos, 2021; Hernandez-de-Menendez et al., 2020).

Curriculum design must document how the curriculum enables the learner to move toward mastery of competency.

A well-structured curriculum should include a clear instructional sequence that demonstrates how each learning activity, assessment, and experience contributes to the mastery of competencies. This progression may begin with foundational concepts and technical skills, then advance through increasingly complex, applied tasks that reflect real-world cybersecurity challenges. Each stage of the curriculum should be intentionally aligned with specific competencies, supported by formative assessments and ongoing feedback to guide learner development. Documentation must show how these elements scaffold learning to ensure that, by the end of the clinic, learners have achieved the full range of KSAs required for competent, independent performance in their intended cybersecurity role (Mott et al., 2019; Bendler & Felderer, 2023; Ford & Meyer, 2015; Sargeant et al., 2018).

Clinics must provide documentation of job task analyses and the use of any nationally recognized frameworks.

To ensure transparency and alignment with workforce needs, clinics should maintain clear documentation of any job task analyses conducted, as well as the use of any standardized documents that inform curriculum design. This may include records of employer-informed analyses or references to established resources such as the NICE framework. Documenting these sources provides a clear foundation for the competencies being taught and assessed, demonstrating that the curriculum is grounded in validated, industry-relevant standards. It also supports accountability and helps external stakeholders understand how the clinic aligns training with real-world cybersecurity roles.

Clinics must document the process to determine the frequency of job task analyses in collaboration with subject-matter experts.

Staying aligned with the evolving demands of the cybersecurity workforce requires clinics to maintain a documented process for determining the frequency of job task analyses. This process should be developed in collaboration with subject-matter experts, who provide insight into emerging technologies, industry practices, and regulatory changes. Together, they can identify when updates are needed and establish a regular review cycle to ensure curriculum content remains accurate and relevant. By clearly outlining how and when job task analyses are conducted, clinics demonstrate their commitment to delivering training that reflects real-world expectations and prepares learners for the current job market.

Teaching-Learning Interactions

This construct uses accepted theoretical models to produce a measurable progression to proficiency, competency, and mastery as defined in Tobey et al. (2018a; 2018b). Examples of acceptable instructional models that allow for aligning instruction with the readiness level of the student are problem-based learning, social learning theory, constructivist learning, project-based learning, and student-centered learning.

Clinics must have active learner-centered teaching strategies based on adult learning theory.

Examples of learner-centered teaching strategies include mentorship and coaching, peer learning and collaboration, project-based learning, problem-based learning, and approaches grounded in social learning theory, to ensure meaningful engagement and skill development among learners. These strategies place learners at the center of the educational process, allowing them to apply knowledge in real-world contexts, collaborate with others, and build confidence through hands-on experiences. Such approaches are particularly well-suited for the dynamic and applied nature of cybersecurity, where problem-solving and critical thinking are essential. Prior research has consistently shown that active, learner-centered teaching methods are vital to effective curriculum implementation and learner success, supporting both cognitive and professional growth (Ford & Meyer, 2015; Brilingaitė et al., 2020; Gruppen et al., 2016; Boland et al., 2016). By embedding these strategies into their instructional design, community clinics can foster more inclusive, effective, and sustainable learning environments in the cybersecurity field.

Clinical facilitators must document how they guide learners in applying real-world contexts.

Clinical facilitators play a critical role in helping learners connect theory to practice and should document how they guide this application within real-world contexts. This may include outlining instructional techniques such as scenario-based discussions, debriefs following simulations, guided reflection, or integration of current cybersecurity case studies (Chowdhury & Gkioulos, 2021; Mott et al., 2019; Bendler & Felderer, 2023; Daniel et al., 2020; Quew-Jones & Rowe, 2022). Documentation should describe how facilitators prompt learners to analyze complex situations, apply technical and decision-making skills, and reflect on outcomes in relation to professional standards. By capturing these instructional practices, clinics demonstrate intentionality in bridging classroom learning with authentic workplace demands, reinforcing both relevance and competency development.

Clinics must document how they identify and provide intervention to learners who are not progressing according to the curriculum design.

Clinics must document their strategy for identifying and providing interventions to learners who are not progressing according to the curriculum design. This process may involve assigning additional practice exercises, providing individualized coaching, or facilitating peer support. The learner's performance may be reassessed after the intervention to determine whether further progress has been made. By documenting each phase of this process, the clinic ensures that support is intentional, consistent, and aligned with the goal of helping every learner achieve competency.

Assessment Design

This construct is one of most important of all the model elements because it is focused on diagnosing the source of errors to improve learning, and to deliver instruction to the student at a pace that optimizes engagement (Csikszentmihalyi, 1990). This construct validates that there is continuous improvement of the student's readiness to learn and demonstrate proficiency, competency, or mastery. The assessment construct includes formative assessment, summative assessment, and authentic assessment, which includes some contextualization of the competencies in different environments and applied to current practice. Formative assessments should be offered iteratively throughout the learning process, allowing learners to demonstrate their understanding, receive targeted feedback, and retake assessments after dedicated learning opportunities to showcase their progress towards mastery. While the summative assessments are offered to assess eligibility into the program as well as assessed at the end of the program as a means of tracking progress.

Clinics must use a validated assessment tool to assess competencies prior to enrollment and at completion of the clinic.

This validated assessment tool should be competency-based and aligned with the clinic's defined learning outcomes and may include practical simulations, structured performance tasks, or scenario-based evaluations that mirror real-world cybersecurity challenges. For example, learners might be required to respond to a simulated cybersecurity incident, demonstrate secure system configuration, or present findings from a vulnerability assessment to a panel of instructors or industry partners. The tool must be validated on the specific student populations and be tested for reliability and fairness, ensuring it accurately reflects mastery of both technical and employability competencies and assessors must be calibrated using inter-rater reliability. Using a validated end-of-program assessment ensures consistency in evaluating outcomes, supports student credentialing, and reinforces the clinic's credibility with employers and external stakeholders. Together, these practices help ensure that assessments are fair, accurate, and reflective of best practices in cybersecurity education and workforce preparation (Almuhaideb & Saeed, 2021; Cruz et al., 2020; Cunningham et al., 2016; Lockyer et al., 2017; O'Neil et al., 2014).

Competency-based assessments must be based on job task analyses.[3]

All competency-based assessments must be validated based on job task analyses. Assessment may also be aligned to standardized documents such as NICE framework or certification test blueprints. These sources provide a standardized approach that ensures alignment with the KSAs required for roles across the cybersecurity workforce. By grounding assessments in the job task analyses and other standardized documents, instructors can ensure that learners are evaluated against industry-relevant benchmarks, promoting consistency and transferability of skills. This approach not only supports learner readiness for real-world roles but also strengthens the overall credibility of the training program. Additionally, the use of job task analyses in assessment design is supported by prior research, which emphasizes their relevance and effectiveness in guiding cybersecurity education and workforce development (Saharinen et al., 2020; Bendler & Felderer, 2023; Henri et al., 2017; Chowdhury & Gkioulos, 2021). For instance, a clinic preparing learners for a cybersecurity defense analyst role might assess skills in threat detection, incident response, and log analysis. Using the job task analyses and other standardized documents as the foundation for assessments helps maintain consistency, relevance, and credibility, while also supporting transparency for learners, employers, and stakeholders regarding the competencies being developed and measured.

Clinics must use competency-based formative assessments throughout the clinical experience on an ongoing, systematic basis.

Monitoring learner performance involves collecting and analyzing data across multiple points in the clinical experience, including formative assessments, practical exercises, peer collaboration, and instructor observations. Learners must receive regular, actionable feedback on their performance. The feedback must be aligned with defined competencies to ensure clarity in expectations and support meaningful improvement. Regular review cycles, combined with facilitator feedback, help identify learners who may need additional support and allow for timely instructional interventions. Examples of a structured performance tracking system may include a digital portfolio or competency dashboard that documents learner's strengths, areas for improvement, and completion of required benchmarks. This structured approach not only supports skill development but also mirrors professional environments where feedback is tied to real-world outcomes. The importance of such practices is well-documented in both educational standards and research literature (ASTM-E3416; Chimea et al., 2020; Rich et al., 2020; Lockyer et al., 2017; Sargeant et al., 2018), highlighting feedback as a critical component of effective learning and performance evaluation. Moreover, by systematically monitoring performance, clinics can uphold high standards, maintain instructional quality, and ensure equitable learning outcomes for all participants.

[3] Author's note: Competency-based assessments may also be aligned to standardized documents such as the NICE framework.

Educational Outcomes

This construct is foundational to the program, tracking educational outcomes such as student retention, program completion, and the development of competent cybersecurity professionals. Clinics will need to identify a management system to track outcomes that anonymizes and protects student identity. In addition, the management system will need to permit assessor review to determine if conclusions are congruent with data acquired and the effectiveness of actions taken. Post-graduation outcomes will also need to be included in the management system to track areas such as employment, time to employment, employer satisfaction with competencies, and student satisfaction with job and wage information.

Clinics must track internal outcomes to share with clinical facilitators.[4]

Tracking outcomes enables clinical facilitators to monitor individual and cohort-level development, identify areas needing support or adjustment, and make data-informed instructional decisions. Internal outcomes may include skill progression, formative assessment, practical lab performance, participation in team-based exercises, and final capstone evaluations (Gómez et al., 2017; Henri et al., 2017; Boland et al., 2016). Facilitators should have timely access to this data through secure platforms or shared documentation systems to guide feedback, tailor mentoring, and uphold consistent evaluation standards. Transparent outcome tracking supports continuous improvement of the community clinic model and reinforces accountability in the learning process.

Clinics must also track external outcomes.[5]

Collecting and analyzing external data helps clinics align their offerings with workforce demands, maintain relevance in a rapidly evolving field, and demonstrate value to stakeholders. Methods may include alumni follow-up surveys, employer feedback forms, and partnerships that facilitate job placement or internship opportunities (Henrich, 2016; Saharinen et al., 2020; Gómez et al., 2017). Tracking external outcomes supports continuous quality improvement and strengthens the clinic’s credibility with learners, the community, and the cybersecurity industry.

Resources

This construct includes requirements for both human and non-human resources. Human resources include documentation of qualifications and the minimally acceptable ratios for program faculty (e.g., instructional, clinical, and learning advisor) to facilitate competency development. Non-human resources include instructional materials, proper learning spaces and equipment as well as financial support to create the necessary teaching environment needed in a competency-based program.

[4] Author’s note: Internal outcomes may be learner skill progression, learner satisfaction of the program, and completion rates of the program.

[5] Author’s note: External outcomes may be employment rates, community partner satisfaction, and recognition of competencies by employers.

Clinics must have financial resources to design and implement the program.

To deliver high-quality cybersecurity training, clinics must have financial resources to implement and sustain clinical education (Daniel et al., 2020b). The clinic's funding portfolio may consist of a variety of elements including, but not limited to, federal or state grants. Clinics may also follow a subscription model, whereby clinics may offer a monthly or yearly subscription for their services.

Clinics must have facilities and equipment conducive to implementing curriculum design and assessment.

Clinics must have the technologies available to support cybersecurity clinical education and assessment. Facilities may include access to secure, isolated cybersecurity environments allowing for virtual simulations, sandboxes, adaptive learning tools. This may also mean access to tools and platforms aligned with industry standards. (Brilingaitė et al., 2020; Dunagan & Larson, 2021; Chowdhury & Gkioulos, 2021; Hernandez-de-Menendez et al., 2020).

Clinics must have sufficient personnel available with the necessary competence to perform necessary functions.

Instructors in cybersecurity clinics must possess demonstrated expertise in the field, either through holding industry-recognized certifications or substantial professional experience. This foundation ensures that they can provide accurate, current, and relevant instruction aligned with the demands of the cybersecurity workforce. Beyond technical knowledge, instructors play a critical role as mentors, guiding learners through complex concepts, and helping them apply skills in real-world contexts. Prior research underscores the importance of mentorship in promoting learner success, particularly in technical and rapidly evolving fields like cybersecurity (Chowdhury & Gkioulos, 2021; Mott et al., 2019; Bendler & Felderer, 2023; Daniel et al., 2020b; Quew-Jones & Rowe, 2022). Effective instructors draw on their own experiences to contextualize learning, model problem-solving strategies, and support learners in building both competence and confidence. Their dual role as subject-matter experts and mentors is essential to fostering meaningful engagement and long-term success in cybersecurity education.

Clinics must provide training for staff who do not meet the established job description criteria.[6]

Training for clinical education staff who do not meet established job descriptions should address gaps in teaching methodologies and learner assessment. Training should validate that clinical education staff have the necessary competence to perform their role after receiving the training.

Clinics must establish formal community partnerships.

Clinics must establish partnerships with local community clients through formal, signed contracts. A foundational element of these clinics is that they provide opportunities for learners to gain experiential learning. This learning can only occur if clinics remain engaged with clients that provide learning opportunities for learners (Daniel et al., 2020b). As such, clinics must develop formal agreements with them that may outline responsibility, data security, and learning outcomes. Clinics may also choose to establish agreements with educational institutions.

[6] Author's *note: staff competence must include not only technical expertise, but also the ability to teach and assess learners effectively.*

It is of note that if a clinic collaborates with an education institution and meets the necessary criteria, it may be eligible to receive Workforce Pell funding or funding for learners who qualify for federal work study. These opportunities are not available to a clinic independently; therefore, clinics can seek to establish relationships with their local colleges or universities to gather additional information (American Association of Community Colleges, 2025).

Clinics must have policies and procedures for addressing confidentiality and security that are compliant with NIST 800-171.

To mitigate risk and protect all parties involved at the clinic, clinics must implement policies and procedures that ensure confidentiality and security, including student records as well as the information derived from the clinics (Daniel et al. 2020b). As part of that policy, clinics must demonstrate compliance with NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* as the baseline standard for safeguarding unclassified data.

Clinics must have policies and procedures for addressing liability.

To further protect clinics, learners, faculty, and clients and community partners, clinics must establish clear policies and procedures that outline liability responsibilities, including a definition of who is accountable for potential risks that arise from clinic activities. Policies must include supervision requirements, ensuring learners are appropriately guided by qualified professionals to minimize risk. Furthermore, clinics must obtain and maintain liability insurance that covers clinical activities, supervision, and student engagement with clients to safeguard against finical and legal risks associated with clinical operations (Daniel et al., 2020b).

Clinics must document the responsibilities and qualifications of clinic personnel.

Clinics must maintain clear and up-to-date documentation of clinic personnel roles, responsibilities, and qualifications. Having this documentation promotes transparency and accountability and may serve administrative and quality assurance purposes (ASTM-E3416).

Clinics must have a legally enforceable agreement covering outsourced work.

Clinics must establish legally enforceable agreements with each external body to address confidentiality, security, conflict of interest, and liability, providing protection to all parties involved (ASTM-E3416).

Recommendations

Further Feedback Needed

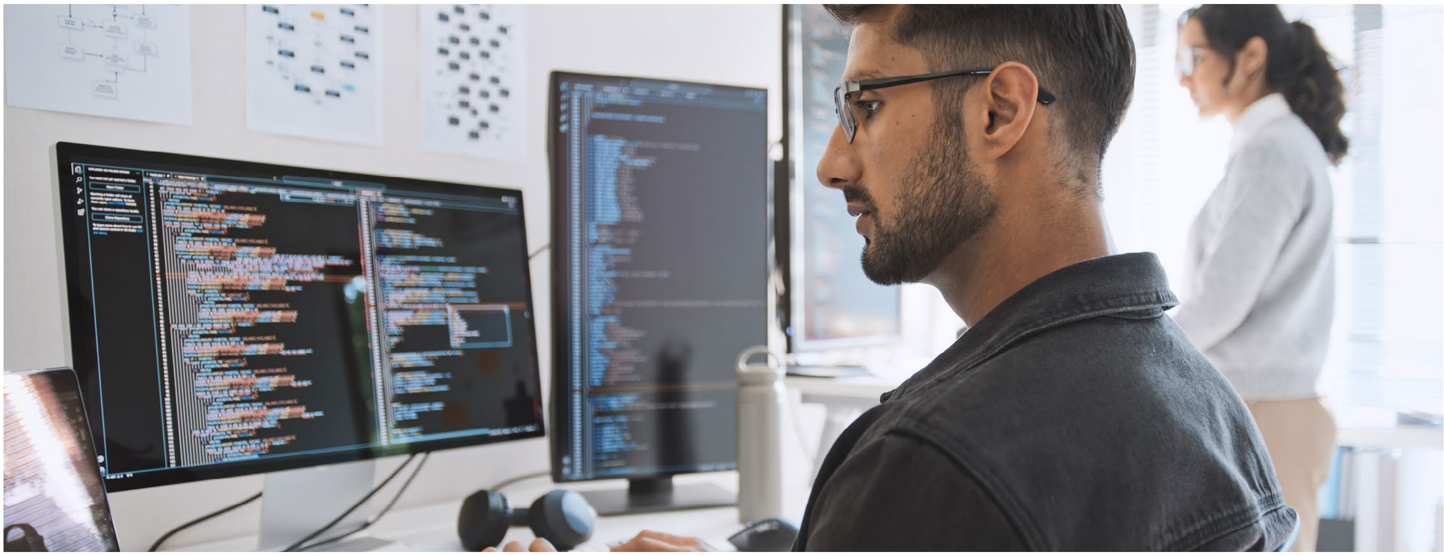
The accreditation model was drafted from information gathered through regional cybersecurity summits, review of existing literature, and insights from peer review panelists, and it remains a work in progress that would benefit from additional feedback from the broader cybersecurity community. Further engagement will create opportunities for this model to receive insights from a variety of perspectives across various sectors, thus strengthening the model's relevance and credibility as well as shared alignment. Dedicated efforts should be made to make this accreditation model accessible through various channels for feedback. Examples of this could include sending a survey to various conference participants, collaborating with organizations such as the National Science Foundation or ISACA, conducting listening tours in person or virtually, and inviting the community to share their insights in other ways.

Development of a Community Task Force

The formation of a community task force, including key industry partners, would help identify the tools or certifications that are of priority for clinics and require industry partners to be involved. Future efforts must prioritize active community engagement to gather diverse perspectives and ensure the proposed solutions meet real-world needs.

Piloting

There is a need to pilot this accreditation model directly within various clinical sites to identify potential operational challenges and clarify job roles and responsibilities in practice. Furthermore, these pilot programs will be instrumental in clarifying specific job roles and responsibilities within the accreditation model, ensuring that all stakeholders understand their contributions and expectations, and refine the model in a real-world environment.



Conclusion

The gap between cybersecurity workforce needs and the preparedness of graduates highlights the urgency for building a structured, competency-based experiential learning opportunity. Cybersecurity clinics can be instrumental in bringing this gap. However, without consistent standards, the quality and outcomes of these clinics pose a risk of failing to hit the mark, potentially resulting in little changes within the industry.

This accreditation model provides a foundation for validating that learners are prepared with the technical, managerial, and employability skills required for workforce readiness. By grounding requirements in job task analyses and aligning them with nationally recognized frameworks such as NIST, NICE, and CMMC, the model offers both local relevance and national consistency.

Moving forward, the refinement, piloting, and scaling of this model necessitates strong engagement from educators, industry partners, policymakers, and the community at large. With continued collaboration, this model can help create a pipeline of practice-ready cyber professionals.

Acknowledgements

This report was produced with the support of NSF Grant #2054753, awarded to Prince George's Community College for the National CyberWatch Resource Center project.

Findings and recommendations expressed in this report are those of Workcred and do not necessarily reflect the views of the National Science Foundation.

Appendix

Summary Matrix of Accreditation Model Components

Component	Summary of Component Details	References
Eligibility Requirements for Admissions	Clinics must identify and document how the eligibility criteria for admissions have been validated. Clinics must develop an application process that includes an assessment of eligibility requirements for admission. Clinics must establish and provide guidance to learners who are not admitted into a cybersecurity clinic. Information must be accessible without request.	Bendler & Felderer (2023); Henri et al. (2017); Lurie & Garrett (2017); Gómez et al. (2017); Hawkins et al. (2015); Gruppen et al. (2016); Fjellström & Kristmansson (2019); Rich et al. (2020); Sargeant et al. (2018)
Competency Framework	Clinics must have a documented plan for learners achieving mastery, as defined by the clinic. Clinics must use a job task analyses and nationally recognized frameworks for alignment achieving mastery of competencies. Clinics must include employability, management, and technical competencies.	Block (1971); Bloom (1968); Carroll (1963); Kolb (1984); Bransford, Brown & Cocking (2000); Reigeluth (1999); Sweller et al. (1998); Mott et al. (2019); Bendler & Felderer (2023); Gómez et al. (2017); Chowdhury & Gkioulos (2021); Brilingaitė et al. (2020)
Curriculum Design	Curriculum must be work-based, focused, and centered around real-world experiential learning with clients in the community. Learning activities may include project-based opportunities. Curriculum design must document how the curriculum enables the learner to move toward mastery competency. Clinics must provide documentation of job task analyses and the use of any nationally recognized frameworks. Clinics must document the process to determine the frequency of job task analyses in collaboration with subject-matter experts.	Block (1971); Bloom (1968); Carroll (1963); Kolb (1984); Bransford, Brown & Cocking (2000); Reigeluth (1999); Sweller et al. (1998); Mott et al. (2019); Bendler & Felderer (2023); Gómez et al. (2017); Chowdhury & Gkioulos (2021); Brilingaitė et al. (2020)
Teaching-Learning Interactions	Clinics must have active learner-centered teaching strategies based on adult learning theory. Clinical facilitators must document how they guide learners in applying real-world contexts. Clinics must document how they identify and provide intervention to learners who are not progressing according to the curriculum design.	Ford & Meyer (2015); Brilingaitė et al. (2020); Gruppen et al. (2016); Boland et al. (2016); Chowdhury & Gkioulos (2021); Mott et al. (2019); Bendler & Felderer (2023); Daniel et al. (2020); Quew-Jones & Rowe (2022)

Component	Summary of Component Details	References
Assessment Design	Clinics must use a validated assessment tool to assess competencies prior to enrollment and at completion of the clinic. Competency-based assessments must be based on job task analyses. Clinics must use competency-based formative assessments throughout the clinical experience on an ongoing, systematic basis.	Almuhaideb & Saeed (2021); Cunningham et al. (2016); Cruz et al. (2020); Lockyer et al. (2017); Rich et al. (2020); Sargeant et al. (2018); Saharinen et al. (2020); Brilingaitė et al. (2020); Henri et al. (2017); ASTM-E3416
Educational Outcomes	Clinics must track internal outcomes to share with clinical facilitators. Clinics must track external outcomes.	Gómez et al. (2017); Henri et al. (2017); Boland et al. (2016); Henrich (2016); Saharinen et al. (2020)
Resources	Clinics must have financial resources to design and implement the program. Clinics must have facilities and equipment conducive to implementing curriculum design and assessment. Clinics must have sufficient personnel available with the necessary competence to perform necessary functions. Clinics must provide training for staff who do not meet the established job description criteria. Clinics must establish formal community partnerships. Clinics must have policies and procedures for addressing confidentiality and security that are compliant with NIST 800-171. Clinics must have policies and procedures for addressing liability. Clinics must document the responsibilities and qualifications of clinic personnel. Clinics must have a legally enforceable agreement covering outsourced work.	Daniel et al. (2020b); Brilingaitė et al. (2020); Dunagan & Larson (2021); Chowdhury & Gkioulos (2021); Mott et al. (2019); Quew-Jones & Rowe (2022); Henrich (2016); ASTM-E3416

References

Almuhaideb, A., & Saeed, S. (2021). A Process-Based Approach to ABET Accreditation: A Case Study of a Cybersecurity and Digital Forensics Program. *Journal of Information Systems Education*, 32(2), 119–133. **https://aisel.aisnet.org/jise/vol32/iss2/5**

American Association of Community Colleges. (2025). *AACC budget reconciliation summary*. Retrieved from **https://www.aacc.nche.edu/2025/07/10/aacc-budget-reconciliation-summary/**

Assante, M. J., Tobey, D. H., & Vanderhorst, D. (2013). Mission critical role project report: A competency analysis of cybersecurity work. Pacific Northwest National Laboratory.

ASTM International. (2019). ASTM E3416-19: Standard Practice for Competency-based Workplace Learning Programs West Conshohocken, PA: ASTM International. **https://store.astm.org/e3416-23.html**

Bendler, D., & Felderer, M. (2023). Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM Transactions on Computing Education*, 23(2), 1–33. **https://doi.org/10.1145/3573205**

Block, J. H. (1971). Mastery learning: Theory and practice. New York, NY: Holt, Rinehart & Winston.

Bloom, B. S. (1968). Learning for mastery. Evaluation Comment, 1(2), 1–12. Los Angeles: UCLA, Center for the Study of Evaluation.

Bok, H. G. J., de Jong, L. H., O'Neill, T., Maxey, C., & Hecker, K. G. (2018). Validity evidence for programmatic assessment in competency-based education. *Perspectives on Medical Education*, 7(6), 362–372. **https://doi.org/10.1007/s40037-018-0481-2**

Boland, D. H., Scott, M. A., Kim, H., White, T., & Adams, E. (2016). Interprofessional immersion: Use of interprofessional education collaborative competencies in side-by-side training of family medicine, pharmacy, nursing, and counselling psychology trainees. *Journal of Interprofessional Care*, 30(6), 739–746. **https://doi.org/10.1080/13561820.2016.1227963**

Bransford, J. D., Brown, A. L., & Cocking, R. R. (2000). How people learn (Vol. 11). Washington, DC: National academy press.

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, 88, 101607. **https://doi.org/10.1016/j.cose.2019.101607**

Carroll, J. B. (1963). A model of school learning. Teachers College Record, 64(8), 723–733. **https://doi.org/10.1177/016146816306400801**

Chimea, T. L., Kanji, Z., & Schmitz, S. (2020). Assessment of clinical competence in competency-based education. Canadian Journal of Dental Hygiene, 54(2), 83–91. **https://pubmed.ncbi.nlm.nih.gov/33240368/**

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information & Computer Security*, 29(5), 697–723. **https://doi.org/10.1108/ICS-07-2020-0121**

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, 113, 102551. **https://doi.org/10.1016/j.cose.2021.102551**

Corno, L., Cronbach, L. J., Kupermintz, H., Lohman, D. F., Mandinach, E. B., Porteus, A. W., & Talbert, J. E. (2002). Remaking the concept of aptitude: Extending the legacy of Richard E. Snow. Lawrence Erlbaum Associates Publishers.

Cruz, M. L., Saunders-Smits, G. N., & Groen, P. (2020). Evaluation of competency methods in engineering education: a systematic review. *European Journal of Engineering Education*, 45(5), 729–757. **https://doi.org/10.1080/03043797.2019.1671810**

Csikszentmihalyi, M. (1990). Flow: *The psychology of optimal experience*. New York, NY: Harper & Row.

Cunningham, J., Key, E., & Capron, R. (2016). An evaluation of competency-based education programs: A study of the development process of competency-Based programs. *The Journal of Competency-Based Education,* 1(3), 130–139. **https://doi.org/10.1002/cbe2.1025**

Daniel, E. I., Oshodi, O. S., Arif, M., Henjewele, C., & Haywood, K. (2020a). Strategies for improving construction craftspeople apprenticeship training programme: Evidence from the UK. *Journal of Cleaner Production*, 266, 122135. **https://doi.org/10.1016/j.jclepro.2020.122135**

Daniel, E. I., Oshodi, O. S., Gyoh, L., & Chinyio, E. (2020b). Apprenticeship for craftspeople in the construction industry: a state-of-the-art review. *Education + Training,* 62(2), 159–183. **https://doi.org/10.1108/ET-02-2019-0041**

Dunagan, L., & Larson, D. A. (2021). Alignment of Competency-Based Learning and Assessment to Adaptive Instructional Systems. In R. A. Sottilare & J. Schwarz (Eds.), *Adaptive Instructional Systems. Design and Evaluation* (pp. 537–549). Springer International Publishing. **https://doi.org/10.1007/978-3-030-77857-6_38**

Fjellström, M., & Kristmansson, P. (2019). Constituting an apprenticeship curriculum. *Journal of Curriculum Studies,* 51(4), 567–581. **https://doi.org/10.1080/00220272.2019.1616115**

Ford, R., & Meyer, R. (2015). Competency-based Education 101. *Procedia Manufacturing*, 3, 1473–1480. **https://doi.org/10.1016/j.promfg.2015.07.325**

Gómez, M., Aranda, E., & Santos, J. (2017). A competency model for higher education: an assessment based on placements. *Studies in Higher Education*, 42(12), 2195–2215. **https://doi.org/10.1080/03075079.2016.1138937**

Gruppen, L. D., Burkhardt, J. C., Fitzgerald, J. T., Funnell, M., Haftel, H. M., Lypson, M. L., Mullan, P. B., Santen, S. A., Sheets, K. J., Stalburg, C. M., & Vasquez, J. A. (2016). Competency-based education: programme design and challenges to implementation. *Medical Education,* 50(5), 532–539. **https://doi.org/10.1111/medu.12977**

Hawkins, R. E., Welcher, C. M., Holmboe, E. S., Kirk, L. M., Norcini, J. J., Simons, K. B., & Skochelak, S. E. (2015). Implementation of competency-based medical education: are we addressing the concerns and challenges? *Medical Education*, 49(11), 1086–1102. **https://doi.org/10.1111/medu.12831**

Henri, M., Johnson, M. D., & Nepal, B. (2017). A Review of Competency-Based Learning: Tools, Assessments, and Recommendations. *Journal of Engineering Education*, 106(4), 607–638. **https://doi.org/10.1002/jee.20180**

Henrich, J. (2016). Competency-based education: The employers' perspective of higher education. *The Journal of Competency-Based Education*, 1(3), 122–129. **https://doi.org/10.1002/cbe2.1023**

Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C. A., & McGovern, M. (2020). Competencies for Industry 4.0. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, 14(4), 1511–1524. **https://doi.org/10.1007/s12008-020-00716-2**

Knutson, T. (2020, February 11). Cybersecurity jobs going begging as college computer science grads lack skills/experience, says House leader. Forbes. **https://www.forbes.com/sites/tedknutson/2020/02/11/cybersecurity-jobs-going-begging-as-college-computer-science-grads-lack-skillsexperience-says-house-leader/**

Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Englewood Cliffs, NJ: Prentice Hall.

Lockyer, J., Carraccio, C., Chan, M.-K., Hart, D., Smee, S., Touchie, C., Holmboe, E. S., Frank, J. R., & on behalf of the ICBME Collaborators. (2017). Core principles of assessment in competency-based medical education. *Medical Teacher*, 39(6), 609–616. **https://doi.org/10.1080/0142159X.2017.1315082**

Lurie, H., & Garrett, R. (2017). Deconstructing competency-based education: An assessment of institutional activity, goals, and challenges in higher education. *The Journal of Competency-Based Education*, 2(3), e01047. **https://doi.org/10.1002/cbe2.1047**

Moreno, R., & Park, B. (2010). Cognitive load theory: Historical development and relation to other theories. In J. L. Plass, R. **https://doi.org/10.1017/CBO9780511844744.003**

Moreno, & R. Brünken (Eds.), Cognitive load theory (pp. 9–28). New York, NY: Cambridge University Press. **https://doi.org/10.1017/CBO9780511844744**

Mott, J. H., Hubbard, S. M., Lu, C.-T., Sobieralski, J. B., Gao, Y., Nolan, M. S., & Kotla, B. (2019). Competency-Based Education: A Framework for Aviation Management Programs. *The Collegiate Aviation Review International,* 37(1). **https://doi.org/10.22488/okstate.19.100211**

National Initiative for Cybersecurity Careers and Studies (NICCS). (2025). *NICE Framework*. Cybersecurity & Infrastructure Security Agency. **https://niccs.cisa.gov/tools/nice-framework**

O'Neil L., T.J. Conway, D.H. Tobey, F.L. Greitzer, A.C. Dalton, and P.K. Pusey. 2014. *Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals.* Richland, WA: Pacific Northwest National Laboratory. **https://www.pnnl.gov/publications/secure-power-systems-professional-phase-iii-final-report-recruiting-selecting-and**

Quew-Jones, R. J., & Rowe, L. (2022). Enhancing the degree apprenticeship curriculum through work-based manager and mentor intervention. *Journal of Work-Applied Management,* 14(2), 242–256. **https://doi.org/10.1108/JWAM-03-2022-0015**

Radunović, V., & Rüfenacht, D. (2016). Cybersecurity Competence Building Trends: Research report Commissioned by the Federal Department of Foreign Affairs of Switzerland. *DiploFoundation.*

Reigeluth, C. M. (1999). Instructional-design theories and models: A new paradigm of instructional theory (Vol. II). Mahwah, NJ: Lawrence Erlbaum Associates.

Rich, J. V., Fostaty Young, S., Donnelly, C., Hall, A. K., Dagnone, J. D., Weersink, K., Caudle, J., Van Melle, E., & Klinger, D. A. (2020). Competency-based education calls for programmatic assessment: But what does this look like in practice? *Journal of Evaluation in Clinical Practice,* 26(4), 1087–1095. **https://doi.org/10.1111/jep.13328**

Saharinen, K., Backlund, J., & Nevala, J. (2020). Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. *2020 12th International Conference on Education Technology and Computers,* 172–176. **https://doi.org/10.1145/3436756.3437041**

Sargeant, J., Wong, B. M., & Campbell, C. M. (2018). CPD of the future: a partnership between quality improvement and competency-based education. *Medical Education,* 52(1), 125–135. **https://doi.org/10.1111/medu.13407**

Tobey, D. H., Gandhi, R. A., Watkins, A. B., & O'Brien, C. W. (2018a). Competency is Not a Three Letter Word A Glossary Supporting Competency-based Instructional Design in Cybersecurity. Cybersecurity Skills Journal: Practice and Research, 20, 32-38.

Tobey, D. H., Watkins, A. B., & O'Brien, C. W. (2018b). Applying competency-based learning methodologies to cybersecurity education and training: Creating a job-ready cybersecurity workforce.