ISSN: 2473-4901
v12 n6938

Building What the KUs Demand: A Framework for Translating CAE-CD Knowledge Units into Cybersecurity Instructional Materials

Aysun Karamustafaoglu
karamustafaoglua@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403 USA

Abstract

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) Cyber Defense (CD) designation, administered by the National Security Agency, organizes required learning outcomes (LOs) and topics into Knowledge Units (KUs). These KUs define important cybersecurity education requirements but do not provide ready-to-use instructional materials, and existing resources are not typically organized around the CAE-CD KU structure. This paper presents a repeatable KU-to-module development framework for translating CAE-CD requirements into structured, student-facing cybersecurity materials. The framework includes four phases: KU analysis and decomposition, content scope and module structure, content development, and expert review and revision. Applying the framework to the Cybersecurity Fundamentals (CSF) KU resulted in a proposed 10-module instructional structure and the development of Module 1 as a proof-of-concept prototype. A panel of twelve expert reviewers evaluated the prototype and supported its alignment, technical accuracy, clarity, and suitability for introductory learners while also identifying revisions to improve explanations and visual support. The framework offers CAE institutions a practical, modular approach for developing consistent, accessible, reusable, and KU-aligned cybersecurity instructional materials.

Keywords: Cybersecurity Education, Knowledge Units, CAE-CD, Cybersecurity Fundamentals, Instructional Design, Curriculum Alignment

ISSN: 2473-4901
v12 n6938

Building What the KUs Demand: A Framework for Translating CAE-CD Knowledge Units into Cybersecurity Instructional Materials

Aysun Karamustafaoglu, Geoff Stoker

1. INTRODUCTION

Higher education cybersecurity programs seeking designation through the NSA's National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, such as the Cyber Defense (CD) designation, must demonstrate curricular alignment with NCAE-C requirements. A key requirement for NCAE-CD designation is a validated Program of Study (PoS) (Application Process and Adjudication Rubric Cyber Defense Working Group, 2024). Validating a bachelor's PoS involves aligning 22 knowledge units (KU) with relevant courses within the PoS. "A Knowledge Unit (KU) is a thematic grouping that encompass [sic] multiple, related KU outcomes and learning topics." (Application Process and Adjudication Rubric Cyber Defense Working Group, 2024, p. 3). The KU criterion is described as the "cornerstone of the Cyber Defense (CD)'s Program of Study (PoS) validation" because it provides the scope and rigor for the PoS curriculum (Becker et al, 2024, p. 2). Three of the 22 required KUs are identified as foundational and are required for every level of the CAE-CD program, from associate through doctoral (Figure 1). These foundational KUs are: Cybersecurity Fundamentals (CSF), Cybersecurity Principles (CSP), and IT Systems Components (ISC). Because these foundational KUs are required, they are an important starting point for curriculum alignment and the development of instructional materials.

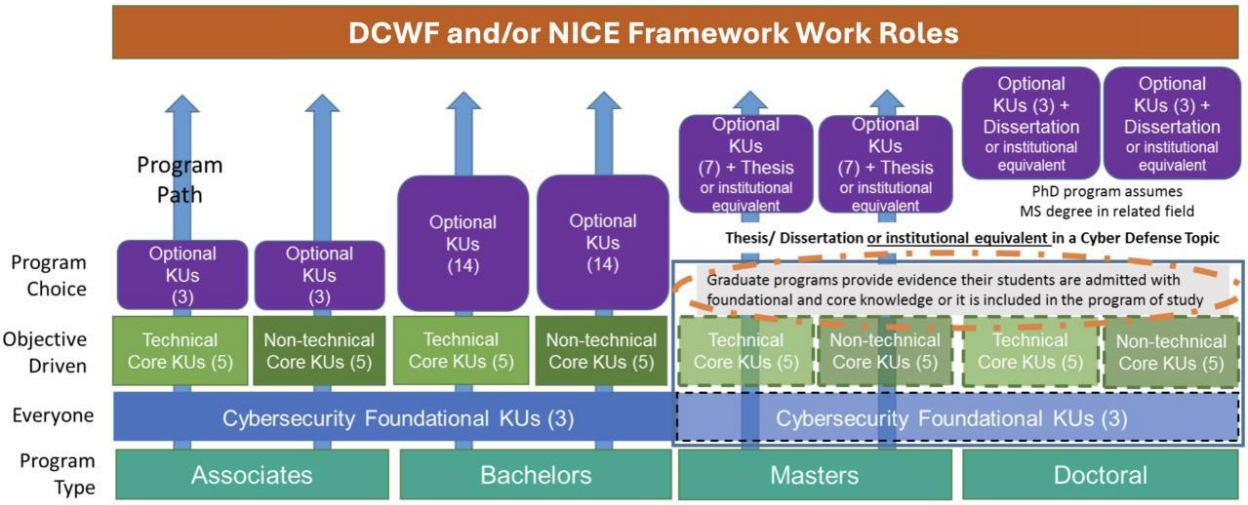

Figure 1. CAE-CD KU Alignment Requirements Overview (Becker et al, 2024, p. 2).

The NCAE-C guidance identifies what a KU-aligned course or set of courses must cover. However, it does not provide ready-to-use teaching materials. For each KU, a name, description, learning outcomes, topics, vocabulary, and related KUs are provided. Instructors need to decide how to organize the content, divide it into modules, choose examples, and design activities. This poses a practical instructional design challenge for CAE institutions. Faculty may be able to document KU alignment at the curriculum level, but they still need accessible, student-facing materials that translate KU requirements into teachable explanations, examples, activities, and assessments. Existing cybersecurity textbooks and open resources provide valuable coverage of cybersecurity topics, but they are rarely (if ever) organized around the KU structure. As a result, institutions may need to assemble, adapt, or supplement readings, activities, and assessments from multiple sources to support KU alignment.

This paper responds to the gap between official KU alignment requirements and accessible instructional materials by presenting a repeatable KU-to-module translation process. The purpose of this paper is to

describe and share a systematic process for developing educational resources directly from NCAE-C Program KUs. The framework begins with an analysis of the official KU, translates learning outcomes (LOs) and topics into a proposed instructional structure, develops instructional modules, and evaluates the resulting prototype through expert review. The paper demonstrates this process using a portion of the CSF KU as proof of concept. A module is created that focuses on selected CSF outcomes and topics. While the long-term goal is a learning resource aligned with all three foundational KUs, this paper presents a replicable framework for translating CAE-CD KU requirements into structured instructional modules and demonstrates it by developing a prototype module covering a portion of the CSF KU.

2. LITERATURE REVIEW

Research on cybersecurity curricula emphasizes the importance of establishing connections between LOs, instructional activities, assessments, and workforce expectations. Towhidi and Pridmore (2023), for example, used the backward design method to develop a cybersecurity course aligned with industry needs. Backward design begins by identifying targeted LOs, determining acceptable evidence of learning, and then planning instructional activities (Wiggins & McTighe, 1998). This approach is consistent with constructive alignment, which links intended LOs with teaching activities and assessment tasks (Biggs, 1996). Together, these models support a systematic course development process rather than organizing instruction as a collection of disconnected topics.

Curriculum mapping complements backward design and constructive alignment by making relationships among learning outcomes, instructional content, and assessment visible across a curriculum. Curriculum mapping can also support the identification of gaps, redundancies, and sequencing needs while helping programs maintain alignment between curricular requirements and instructional content (Arafeh, 2016; Joyner, 2016). These principles are particularly relevant when broad curricular requirements must be decomposed into smaller instructional units while maintaining traceability to required outcomes. Related instructional-design research also emphasizes formative evaluation during the development of instructional materials. Such evaluation may include expert review, learner testing, and revision to identify weaknesses and improve instructional materials before broader implementation (Weston, 1986). Beginner-level instruction also requires managing the complexity of unfamiliar material. Grouping related concepts into coherent units and sequencing foundational concepts before more advanced applications can help novice learners manage cognitive load (Sweller et al., 1998).

Outcome alignment is especially important in cybersecurity because curriculum frameworks often define broad expectations that must be translated into courses and learning activities. Current cybersecurity curricular guidance commonly organizes content through competencies, knowledge areas, and student LOs. For example, the Cyber2yr2020 guidance uses competencies and LOs to organize cybersecurity content for two-year programs (Association for Computing Machinery Committee for Computing Education in Community Colleges, 2020). Within the CAE-CD context, Miller et al. (2026) found that KUs vary substantially in curricular load and complexity. Their work suggests that KUs should not be treated as equivalent blocks and that LOs, topics, and Bloom's Taxonomy levels require more detailed examination during curriculum planning. These studies support careful outcome analysis and curriculum mapping, but they focus primarily on course or program structure rather than the development of complete student-facing instructional modules.

Cybersecurity education research also identifies a need for materials that can be shared and reused by other instructors. Švábenský et al. (2020) conducted a systematic review of 71 cybersecurity education papers and found that fewer than one-third provided supplementary materials that other educators could use. This finding suggests that cybersecurity education research frequently describes courses, exercises, and instructional approaches without always producing reusable teaching resources.

Open educational resources (OER) are teaching, learning, and research materials that are openly licensed to permit their free use, adaptation, and redistribution (Atkins et al., 2007). OER includes complete courses, modules, textbooks, videos, software, and other instructional resources that support teaching and learning. A central goal of the OER movement is to improve access to high-quality educational content while encouraging instructors to share, adapt, reuse, and remix materials to meet local instructional needs. Consistent with these goals, modular instructional resources can be reorganized and combined to support different courses and curricular needs. Cybersecurity-specific research similarly finds that faculty value the accessibility and adaptability of OER but still report barriers

ISSN: 2473-4901
v12 n6938

related to awareness, quality, selection, and integration (Stines, 2024). Modular resources may reduce some of this burden because individual instructional units can be reused, updated, and combined to meet different course needs.

Existing cybersecurity educational resources primarily address the question, "How can cybersecurity be taught?" In contrast, the CAE-CD KUs define "What must be taught." However, they provide little guidance on translating those requirements into reusable instructional modules while preserving alignment with official KU LOs and topics. This paper addresses that instructional translation problem by presenting and evaluating a KU-to-module development framework.

3. METHODOLOGY: THE KU-TO-MODULE DEVELOPMENT FRAMEWORK

This section describes the KU-to-module development framework used to translate CAE-CD KUs into instructional modules. The framework is intended to provide a systematic process that other institutions can adapt when developing KU-aligned educational materials. The framework consists of four phases: (1) KU analysis and decomposition, (2) content scope and module structure, (3) content development, and (4) expert review and revision (Figure 2).

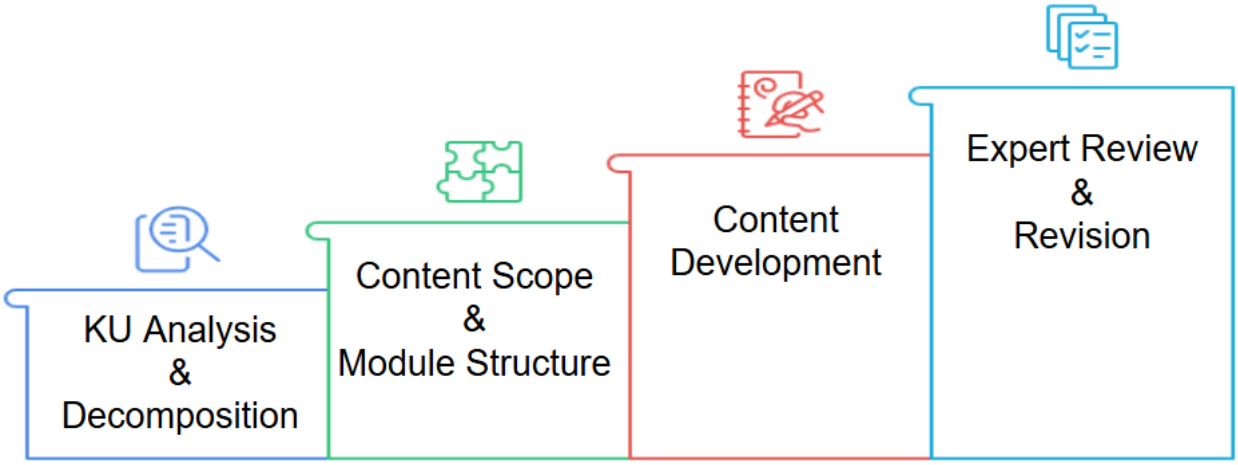

Figure 2: Four-Phase KU-to-Module Development Framework

3.1 Phase 1: KU Analysis and Decomposition

The first phase focuses on understanding the official KU before instructional design begins. The instructional team reviews the KU description, LOs, topics, vocabulary, and related KUs to identify the required scope and expected level of coverage. The LOs are examined through the lens of Bloom's Taxonomy. The team evaluates verbs such as define, describe, evaluate, apply, and discuss to determine the expected level of cognitive performance for each LO (Bloom et al., 1956; Krathwohl, 2002). This analysis helps guide whether instructional activities should focus on recall, explanation, analysis, or application. This phase establishes the instructional foundation for later design decisions.

3.2 Phase 2: Content Scope and Module Structure

Phase two translates KU requirements into a proposed instructional structure. Topics are expanded into instructional subtopics, related concepts are grouped together, and overlapping content is identified. Decisions are made about instructional sequencing and the depth at which concepts should be introduced or developed. During this phase, module planning remains traceable to the official KU LOs and topics.

Depth-control decisions are guided by the relationship between each topic and the module's assigned LOs, the cognitive level indicated by the LO action verbs (e.g., identify, describe, or apply), and prerequisite relationships among concepts (e.g., introducing authentication and authorization before examining more advanced access-control mechanisms). Topics that provide necessary background but are not the module's primary focus are introduced at a foundational level. Topics that directly support the module's assigned LOs are developed in greater depth through explanation, examples, and

application. Concepts previously introduced may also be reinforced in later modules when they support more advanced topics or applications. This approach allows related concepts to appear across modules without requiring the same level of instructional depth each time. Table 1 summarizes the depth-control heuristic used to distinguish among introductory, developed, and reinforced treatment of KU topics during module planning.

Depth Level	Decision Guideline	Typical Instructional Treatment
Introduce	Provides prerequisite or supporting knowledge but is not a primary focus of the module's assigned LOs	Basic definition, explanation, and example
Develop	Directly supports one or more LOs assigned to the module	Detailed explanation, examples, vocabulary support, knowledge checks, and application
Reinforce/Apply	Was introduced or developed previously and supports later concepts or applications	Scenarios, case studies, activities, or connections to new concepts

Table 1: Depth-Control Heuristic for Module Development.

Taken together, Phase 2 addresses five main questions:

- What content should be included?
- Which topics belong together?
- In what order should the modules be taught?
- How much depth should each topic receive?
- How can each module remain aligned with the official KU LOs and topics?

3.3 Phase 3: Content Development

The third phase develops instructional materials for each module. Content is organized around the selected LOs and topics while maintaining alignment with the official KU. Technical concepts are explained using clear language supported by authoritative definitions, examples, visualizations, vocabulary support, knowledge checks, case studies, and applied activities. Where appropriate, modules may also identify authoritative external resources and openly available learning materials, such as NIST guidance and glossaries, CISA educational resources, or relevant cybersecurity frameworks, that provide additional support for the KU topics being addressed. A consistent instructional structure is used across modules to support readability, comprehension, and consistent instruction.

3.4 Phase 4: Expert Review and Revision

Phase four evaluates the prototype module before classroom implementation. Expert reviewers evaluate the module for alignment, technical accuracy, clarity, organization, usability, and instructional readiness. Feedback is then used to revise the instructional materials before classroom use. This phase improves the prototype module and informs future use of the KU-to-module development framework.

4. RESULTS: APPLYING THE KU-TO-MODULE FRAMEWORK TO CSF

This section demonstrates the KU-to-module development framework by applying it to the CSF KU (Appendix A). The framework is used to analyze the CSF KU, organize its LOs and topics into a proposed instructional structure, develop Module 1 as a proof of concept, and evaluate the prototype through expert review.

Official KU → LO Analysis → Topic Expansion → Grouping → 10 Modules → Module Development → Expert Review → Revised Module

4.1 CSF KU Analysis and Decomposition Results

The first step in applying the framework was to analyze and decompose the official CSF KU. The analysis identified the KU description, 10 LOs, 25 topics, vocabulary, and related KUs. The team used each CSF KU component to guide a different part of the design process:

- ***KU description***: established the intended scope and level of coverage.

- ***Learning outcomes***: guided module goals, learning objectives, and assessment design.
- ***Topics***: guided module sections and subtopics.
- ***Vocabulary***: guided key-term selection and definitions.
- ***Related KUs***: helped identify connections and boundaries with other KUs.

The LOs were then interpreted using Bloom's Taxonomy to better understand the expected level of student performance. This translation helped distinguish outcomes that emphasized recall and explanation from those requiring application or evaluation. Table 2 provides selected examples of translations of the 10 CSF LOs.

CSF LOs	Instructional Translation
LO1: ***Define*** the fundamental principles of cybersecurity	Students should remember (be able to recall) basic ideas that guide cybersecurity, such as confidentiality, integrity, availability, authentication, authorization, accountability, non-repudiation, least privilege, defense-in-depth, and risk management.
LO3: ***Describe*** potential objectives of cyber attackers and their motivations	Students should understand (explain in their own words) that attackers usually have objectives, such as theft, disruption, denial of service, destruction, or espionage, and motivations such as money, revenge, ideology, fame, challenge, or state or corporate advantage.
LO4: ***Describe*** various types of cyber attacks	Students should recognize and be able to discuss major attack categories, including malware, network-based attacks, social engineering, credential attacks, web application attacks, and supply chain attacks.

Table 2: Example translation for a subset of CSF LOs

After translating the LOs, the instructional team grouped the 10 CSF LOs into four broader instructional categories (Table 3). The categories were used as instructional clusters, not strict boundaries. Some LOs naturally connect to more than one module.

Category	LOs	Main Idea
Foundations	1, 2	What cybersecurity is and what it tries to protect
Threats and Weaknesses	3, 4, 5	Who attacks, how they attack, and what weaknesses they use
Defense and Protection	6, 7, 8	How systems are protected and prepared
Response and Real World	9, 10	What to do after a compromise and how cybersecurity appears in current events

Table 3: CSF LOs grouped into four categories

This grouping created a simple instructional pathway:

Foundations → Threats and Weaknesses → Defense and Protection → Response and Real World

4.2 Proposed CSF Module Structure

In the second phase, the instructional team created a topic-expansion matrix. Each of the 25 CSF topics was expanded into possible subtopics, connected to related topics, and mapped to related LOs. This helped turn broad KU topic labels into more concrete instructional content. Table 4 provides an example of topic expansion for select CSF LOs.

ISSN: 2473-4901
v12 n6938

CSF Topic (T)	Example Subtopics	Related Topics	Related LOs
T2: Threats and Adversaries (threat actors, malware, natural phenomena, and human factors)	Threat actors, attacker motivations, attacker objectives, malware as a threat, natural threats, human factors, adversarial thinking	T6, T7, T14, T19, T24, T25 because attack frameworks, attack methods, malware, detection, current events, and awareness all depend on understanding threats and adversaries	LO3: this topic focuses on attacker objectives and motivations. LO4: threats and adversaries connect to types of attacks. LO10: threat actors and adversary behavior are often discussed through current cybersecurity events.
T3: Vulnerability Management	Vulnerability types, vulnerability scanning, patch management, prioritization, CVE, CVSS, exploitability, impact, remediation, mitigation	T4, T7, T17, T19, T23 because vulnerabilities connect to risk, attack methods, security mechanisms, detection, and best practices	LO5: is the primary fit because vulnerability management requires identifying vulnerability types and evaluating severity. LO6: protective mechanisms reduce vulnerability impact. LO7: tools such as scanners support vulnerability management. LO8: when students apply defense methods such as patching, remediation, or mitigation.
T10: Data Security (e.g., in transmission, at rest, in processing)	Data at rest, data in transit, data in processing, encryption, backups, classification, DLP, retention, secure disposal	T5, T9, T13, T17, T20, T21, T23 because data security connects to McCumber information states, cryptography, CIA, mechanisms, governance, legal/privacy issues, and best practices	LO1: data security is tied to the CIA and privacy. LO2: protecting data is a central cybersecurity goal. LO6: data security uses mechanisms such as encryption, access control, backups, and monitoring. LO7: tools support data protection. LO8: when students apply data protection methods. LO9: compromise response often involves protecting, restoring, or investigating data.
T14: Malware	Malware types, infection methods, detection, prevention, response, real-world examples	T2, T6, T7, T17, T19, T23 because malware connects to threat actors, attack frameworks, attack	LO3: fits when malware is connected to attacker objectives. LO4: fits because malware is a major

		methods, defense mechanisms, detection, and best practices	attack type. LO6: fits because students need to understand mechanisms that protect against malware. LO7: fits because malware defense involves tools such as antivirus, EDR, IDS, and monitoring. LO9: fits because malware incidents require response and recovery actions.

Table 4: Example Topic-Expansion Matrix including Related Topics and LOs

The team did not treat each CSF LO or topic as a separate module. That approach would have made the course feel like a checklist. The resulting sequence followed a beginner-friendly order:

Foundations → Threats → Attacks → Vulnerabilities/Risk → Access/Models → Cryptography/Data → Defense Tools → Secure Implementation → Governance/Ethics → Incident Response/Current Events

This order was selected because students first need to understand what cybersecurity protects. Then they can study who attacks systems and why. After that, they can learn how attacks occur, which weaknesses attackers exploit, and how risk affects security decisions. Once students understand threats and weaknesses, they are better prepared to study security models, access control, cryptography, data security, defense tools, secure implementation, governance, incident response, and current events.

The 10-module structure emerged from the outcome grouping, topic expansion, sequencing, overlap, and depth control analyses rather than from a predetermined module count. Fewer modules would combine too many unrelated concepts. A 25-module structure based directly on the topic list would be too fragmented. For an introductory audience, the 10-module structure reduced fragmentation while grouping related concepts into coherent instructional units and preserving alignment with the CSF KU. The resulting structure is shown in Table 5.

Module	Main CSF Topics	Related LOs
Module 1: Cybersecurity Foundations, Principles, and Goals	T1 Cybersecurity principles; T5 McCumber Cube; T13 CIA, access, authentication, authorization, non-repudiation, privacy; intro to T17 security mechanisms; intro to T23 best practices	LO1, LO2 intro LO6
Module 2: Threat Landscape, Adversaries, and Attack Motivations	T2 Threats and adversaries; intro to T24 current events; intro to T25 awareness	LO3 intro LO10
Module 3: Cyber Attacks, Malware, and Attack Frameworks	T6 Cyber Kill Chain, MITRE ATT&CK, ATLAS; T7 attack methods for vulnerability types; T14 malware; intro to T19 malicious activity detection/forms of attack	LO3, LO4 intro LO6, LO10
Module 4: Vulnerabilities, Severity, and Risk Management	T3 Vulnerability management; T4 basic risk management and assessment; connection to T7 attack methods; connection to T23 best practices	LO2, LO5 intro LO6
Module 5: Security Models, Identity, and Access Control	T11 security models; T12 access control models; T18 AAA and access control; deeper treatment of parts of T13;	LO1, LO2, LO6, LO7 intro LO8

	supporting T17 security mechanisms	
Module 6: Cryptography, PKI, and Data Security	T9 applications of cryptography and PKI; T10 data security; connection to T13 confidentiality, integrity, non-repudiation, privacy; supporting T17 mechanisms	LO1, LO2, LO6, LO7 intro LO8
Module 7: Security Mechanisms, Defense Tools, and Detection	T17 security mechanisms; T19 malicious activity detection/forms of attack; supporting T23 best practices; connections to T14 malware and T6 frameworks	LO6, LO7, LO8 intro LO9
Module 8: Security Life Cycle and Secure Implementation Basics	T8 security life cycle; T15 session management; T16 exception management; supporting T23 best practices; supporting T17 mechanisms	LO6, LO8 intro LO9
Module 9: Governance, Policy, Legal Issues, Ethics, and Awareness	T20 security governance, policies, controls, and countermeasures; T21 legal issues; T22 ethics; T25 cybersecurity awareness; supporting T23 best practices	LO2, LO6, LO9, LO10
Module 10: Incident Response, Continuity, and Current Events Case Studies	Deeper treatment of T20 disaster recovery, business continuity, and incident response; T24 current events; review of T19 detection; review of T23 best practices; review of T25 awareness	LO9, LO10 review LO3–LO8

Table 5. Proposed CSF Module structure.

The sequence generally progresses from foundational concepts toward more applied topics, although the modules are designed to remain adaptable to different course structures rather than function as a rigid prerequisite chain.

The grouping process also required depth-control decisions. Some CSF topics appear in more than one module because they support multiple learning goals. For example, applying the depth-control heuristic, security mechanisms (T17) are introduced in Module 1 to support foundational understanding but are developed in greater detail in Module 7, where security mechanisms and defense tools are a primary instructional focus. Cybersecurity best practices (T23) appear across several modules because they connect to many cybersecurity concepts. Security governance, policies, controls, and appropriate countermeasures (T20) appear in Module 9 for governance and in Module 10 for incident response, disaster recovery, and business continuity. Current events in cybersecurity (T24) can be introduced earlier but work best as a final application topic in Module 10.

This phase produced the proposed CSF module structure. It also helped the instructional team decide where concepts should be introduced, where they should be developed more deeply, and how the full CSF KU could be taught in a coherent sequence.

4.3 Development of CSF Module 1

After the proposed CSF module structure was completed, Module 1 was selected as the proof-of-concept module because it introduces the foundational concepts that support the remaining CSF modules. These concepts provide the knowledge students need before studying other topics.

Module 1 was developed using LO1, LO2, and LO6 and Topics T1, T5, T13, T17, and T23 as determined during the module planning process (Table 5). It directly addresses LO1 and LO2 and directly covers T1, T5, and T13 through cybersecurity principles, cybersecurity goals, the CIA Triad, the McCumber Cube, access, authentication, authorization, non-repudiation, and privacy. LO6 is introduced through examples of security mechanisms and best practices, including authentication, MFA, access control, encryption, audit logs, backups, privacy settings, and user awareness. Topics T17 and T23 are introduced in Module 1 but developed more fully in later modules.

The module followed a consistent instructional structure designed for introductory learners. Each major

concept included an opening explanation, the LOs and topics, authoritative definitions where appropriate, plain-language explanations, familiar examples, vocabulary, knowledge checks, and applied learning activities (Table 6). Adding additional real-world examples and strengthening scenario-based activities encourages students to explain their reasoning rather than simply memorize definitions. This structure was intended to maintain technical accuracy while improving readability and instructional consistency.

Design Choice	Purpose
Use official KU LOs and topics	Keep content aligned to the CSF KU
Use authoritative definitions where appropriate (e.g. NIST Glossary)	Maintain technical accuracy
Add plain-language explanations	Support introductory learners
Use analogies and familiar examples	Connect abstract cybersecurity concepts to familiar experiences
Use a consistent structure	Make the module easier to follow and teach
Use tables and figures	Make repeated information easier to compare and support visual learning
Include vocabulary review	Reinforce key terms and support learners with limited prior cybersecurity background
Add knowledge checks and case studies	Help learners practice and apply concepts
Design activities that require application, not just memorization	Encourage observation, reflection, and AI-resistant application

Table 6: Proposed instructional structure.

The completed prototype demonstrated how official KU LOs and topics could be translated into a complete student-facing instructional module. The module maintained traceability to the selected KU requirements while organizing the material into a logical instructional sequence suitable for introductory cybersecurity students.

4.4 Expert Review Results and Revisions

After CSF Module 1 was developed, it was evaluated by a panel of subject matter experts (N = 12) with experience in cybersecurity, information technology, computer science, and higher education. Reviewers were recruited using convenience sampling from faculty and staff accessible to the research team with relevant academic or professional experience in cybersecurity, information technology, computer science, higher education, or related fields. Potential reviewers were invited electronically to review the Module 1 prototype and complete an online evaluation survey. The survey was designed to evaluate four primary areas: (1) KU alignment, (2) technical accuracy, (3) clarity and accessibility, and (4) instructional design and usability.

The instructional team created a Qualtrics survey using a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree) to collect expert feedback on the module (Appendix B). The study received an exemption determination from the UNCW Institutional Review Board (IRB) before data collection (Study #H26-0961, Exemption Category 02, approved June 22, 2026). Table 7 reports representative items from each of the four evaluation areas to summarize the principal findings without reproducing the full survey; the complete survey instrument is provided in Appendix B.

Construct and Survey Metric	M	SD	Mdn
Curriculum Alignment & Scope			
Q9: Covers a subset of CSF KU LOs	4.58	0.90	5.0
Q11: Covers a subset of CSF KU topics	4.67	0.65	5.0
Q12: Covers all CSF KU LOs *Reverse-scored [RS]*	2.58	1.68	2.0
Q13: Covers all CSF KU topics *[RS]*	2.17	1.27	2.0
Technical Accuracy & Content Coverage			
Q14: Covers cybersecurity concepts with technical accuracy	4.67	0.49	5.0
Q15: Accurately covers the CIA Triad	4.75	0.87	5.0
Q18: Accurately covers authorization	4.92	0.29	5.0
Q19: Accurately covers privacy	4.92	0.29	5.0
Q21: Accurately covers the McCumber Cube	4.67	0.89	5.0
Pedagogical Design & Engagement			
Q24: Understandable for students with no prior tech background	4.67	0.65	5.0
Q25: Presents technical vocabulary in a clear way	4.92	0.29	5.0
Q31: Encourages students to only memorize definitions *[RS]*	2.17	0.94	2.0
Q33: Mini case study connects concepts to everyday technology	4.92	0.29	5.0
Q36: Applied activity encourages copy-paste of AI responses *[RS]*	2.25	0.97	2.0
Structural Layout & Course Adoption			
Q38: Uses a consistent, easy-to-follow structure	4.92	0.29	5.0
Q42: Appropriate for use with an introductory Cybersecurity class	4.83	0.39	5.0
Q43: Willing to use Module 1 as shared course material	4.42	0.79	5.0

Table 7: Expert Review Panel Quantitative Evaluations (N=12).

Reviewers evaluated the prototype positively. Reviewers agreed that Module 1 appropriately covered the selected subset of CSF LOs (M = 4.58, SD = 0.90) and topics (M = 4.67, SD = 0.65). Reverse-scored [RS] items asking whether Module 1 covered all CSF LOs (M = 2.58, SD = 1.68) and all CSF topics (M = 2.17, SD = 1.27) received low ratings, confirming that reviewers understood the module was intentionally limited to selected KU requirements.

Reviewers also rated the module highly for technical accuracy and instructional design. Technical vocabulary was presented clearly (M = 4.92, SD = 0.29), the module was understandable for students with no prior technical background (M = 4.67, SD = 0.65), and the instructional structure was easy to follow (M = 4.92, SD = 0.29). Reviewers also agreed that the module was appropriate for use in an introductory cybersecurity class (M = 4.83, SD = 0.39), and most indicated they would be willing to adopt the module as shared course material (M = 4.42, SD = 0.79).

The open-ended comments identified several opportunities for improvement. One recurring recommendation was to add more visualizations to support visual learners. Based on this feedback, additional figures were incorporated to illustrate concepts such as the CIA Triad and the McCumber Cube while maintaining an appropriate balance between visual content and page length.

Reviewers also suggested several improvements to increase technical clarity. For example, one reviewer noted that the online banking authentication scenario could lead students to believe that a valid digital certificate guarantees a website's trustworthiness. In response, the module was revised to clarify that a digital certificate verifies the domain's identity and supports encrypted communication, but it does not guarantee that the website itself is safe or free of malicious intent. Other reviewers' suggestions included clarifying technical terminology, expanding explanations of selected concepts, adding real-world examples, and strengthening scenario-based activities that encourage students to explain their reasoning rather than simply memorize definitions.

Overall, the expert review demonstrated that the prototype was suitable for introductory cybersecurity instruction and offered practical recommendations to improve the module's technical accuracy, clarity, and accessibility before classroom implementation.

5. CHALLENGES AND LESSONS LEARNED

Several challenges emerged during the KU-to-module development process. The CSF KU is broad, so it cannot be treated as a single chapter or module. KU decomposition was the most time-intensive part of the process. Several CSF topics also overlapped, so topic grouping required judgment. The instructional team had to decide which topics belonged together, which concepts should appear early, and which concepts should be developed more fully in later modules.

A major lesson was that KU-aligned materials need both a traceability process and student-friendly instructional design. Maintaining KU alignment while creating a logical learning flow was challenging. The module also had to balance technical accuracy with accessibility for beginner learners. Expert review helped identify places where examples, visuals, and explanations could be improved. Overall, the process created a useful design trail from KU requirements to module content and helped show how broad KU requirements can be translated into structured instructional materials.

6. DISCUSSION, LIMITATIONS, AND FUTURE WORK

This work shows that CAE-CD KU alignment requires more than listing topics in a course syllabus. The KUs define important LOs and topic areas, but instructors still need a practical way to translate those requirements into student-facing lessons, examples, activities, and assessments. The KU-to-module process provides one way to make that translation more systematic.

The framework may be useful for CAE institutions that need to develop or maintain KU-aligned instructional materials. A shared module structure can help reduce the course preparation burden, especially when multiple instructors teach the same course. It can also support more consistent coverage across sections while still allowing instructors to adapt examples, activities, and emphasis for their own students. An additional advantage of the proposed module structure is its flexibility. Because each module explicitly identifies the LOs and topics it addresses, instructors are not required to adopt the entire set of modules. Instead, they can select individual modules that align with the requirements of their own courses. This modular organization is a direct result of the KU-to-module framework, which breaks down official KU requirements into smaller, traceable instructional units that can be reused, updated, and integrated across instructional settings while maintaining alignment with those requirements. Over time, this process could also support the collaborative development of KU-aligned open educational resources for the CAE community across CAE institutions.

The modular design may also support broader use across NCAE-C educational pathways. Although this study focuses on the CAE-CD CSF KU, other curriculum-oriented NCAE-C designations, including CAE-CO and CyberAI, include foundational cybersecurity KUs that share many introductory concepts. CAE institutions could therefore adapt individual modules to support similar foundational requirements while preserving alignment with the LOs and topics of the applicable designation. For example, an introductory course that covers cybersecurity principles, the CIA Triad, access control, and cybersecurity best practices could adopt Module 1 without using the remaining modules. Similarly, a course emphasizing cyber threats, attacker motivations, and common attack methods could incorporate Module 2 independently. This modular approach allows instructional materials to be reused, reorganized, and adapted while maintaining alignment with the LOs of the target curriculum. Although this study demonstrates the framework using the CSF KU, it is based on common KU components shared across CAE-CD KUs. This suggests that the same process may be applied to additional KUs while preserving traceability to their LOs and topics.

The process also has implications for workforce alignment. KU-aligned educational resources can help make the pathway from course LOs to cybersecurity workforce expectations more transparent. When course modules clearly connect outcomes, topics, vocabulary, examples, and applied activities, students may better understand how introductory concepts relate to later coursework and cybersecurity roles. This can benefit students by making learning goals clearer and may also help programs communicate how their curriculum supports workforce preparation.

This study has several limitations. First, the process was demonstrated using a single prototype module rather than a complete set of CSF modules. Second, the expert review provided pre-implementation feedback but did not measure student LOs. Third, the work reflects one institutional context and may

require adaptation for other CAE programs.

Future work will also include classroom implementation of the revised prototype with introductory cybersecurity students. This evaluation can examine evidence of student learning, student perceptions of clarity and usability, and performance on assessments aligned with the targeted KU LOs and topics. In addition to classroom evaluation, the framework will be applied to the remaining foundational KUs, i.e., Cybersecurity Principles (CSP) and IT Systems Components (ISC). Completing all three foundational KUs will enable the development of a comprehensive KU-aligned introductory cybersecurity textbook that CAE institutions can adopt or adapt for their own programs. Long-term, this approach may support the collaborative development of KU-aligned open educational resources across CAE institutions. Future research may also explore the use of LLMs as a supplementary instructional review tool to support readability, consistency, and alignment before expert review. However, human subject matter experts should remain responsible for evaluating technical accuracy, pedagogical quality, and final approval.

7. CONCLUSION

The 2024 CAE-CD Knowledge Units define what cybersecurity programs should teach, but do not provide ready-to-use instructional materials. This paper presented a repeatable KU-to-module development framework for translating official KU requirements into structured instructional modules while maintaining alignment with the CAE-CD KUs.

The framework consists of four phases: KU analysis and decomposition, content scope and module structure, student-facing content development, and expert review and revision. Applying the framework to the CSF KU resulted in a proposed ten-module instructional structure and the development of Module 1 as a proof of concept. Expert review supported the module's alignment, technical accuracy, clarity, and suitability for introductory cybersecurity education, and provided recommendations to strengthen the prototype before classroom implementation.

This work contributes to a replicable development framework that other institutions can adapt when creating KU-aligned cybersecurity course materials. The framework provides a systematic approach for translating official KUs into teachable modules while preserving alignment with LOs and topics. As additional modules are developed and evaluated, this approach has the potential to support consistent, accessible, and reusable cybersecurity educational resources across CAE institutions.

8. REFERENCES

Application Process and Adjudication Rubric Cyber Defense Working Group. (2024, July). National Centers of Academic Excellence in Cybersecurity NCAE-C 2024 Designation Requirements and Application Process. 20240716_CAE2024_ CAE-CD_Designation_Requirements_Ver1.19. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

Arafeh, S. (2016). Curriculum mapping in higher education: A case study and proposed content scope and sequence mapping tool. Journal of Further and Higher Education, 40(5), 585–611. https://doi.org/10.1080/0309877X.2014.1000278

Association for Computing Machinery Committee for Computing Education in Community Colleges. (2020). Cyber2yr2020: Curricular guidance for associate-degree cybersecurity programs. ACM CCECC. https://ccecc.acm.org/files/publications/Cyber2yr2020.pdf

Atkins, D. E., Brown, J. S., & Hammond, A. L. (2007). A review of the open educational resources (OER) movement: Achievements, challenges, and new opportunities. https://oerderves.org/wp_content/uploads/2007/03/a_review_of_the_open_educational_resources_oer_movement_final.pdf

Becker, A., Blum, Z., Burgin, K. Carlin, A., Chu, B., Cranford-Wesley, D., Frank, S., Ghosh, T., Hamman, S., Joyce, R., Keller S., Kohnke, A., Levy, Y., Liu, X., Manikas, T., McBride, S., Mierzwa, S., Miller, S., Magaishi, M., … Zanella, G. (2024, December 9). National Centers of Academic Excellence in

Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) Knowledge Units (KUs). https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Biggs, J. Enhancing teaching through constructive alignment. High Educ 32, 347–364 (1996). https://doi.org/10.1007/BF00138871

Bloom, B.S. (Ed.), Engelhart, M.D., Furst, E.J., Hill,W.H., & Krathwohl, D.R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain. New York: David McKay.

Joyner, H. S. (2016). Curriculum mapping: A method to assess and refine undergraduate degree programs. Journal of Food Science Education, 15(3), 83-100. https://doi.org/10.1111/1541-4329.12086

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy: An Overview. Theory Into Practice, 41(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

Miller, K., Matthews, K., Clark, U.Y., Stoker, G., (2026). Excessive Equating: An Exploration of Knowledge Unit (KU) Curricular Load for CAE-CD Program Design and Evaluation. Cybersecurity Pedagogy and Practice Journal 5(1) pp 17-40. https://doi.org/10.62273/SYPT8785

Stines, A. (2024). Faculty perceptions of open educational resources in cyber curriculums. Issues in Information Systems, 25(2), 418–437. https://doi.org/10.48009/2_iis_2024_133

Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (pp. 2–8). Association for Computing Machinery. https://doi.org/10.1145/3328778.3366816

Sweller, J., van Merriënboer, J. J. G., & Paas, F. G. W. C. (1998). Cognitive architecture and instructional design. Educational Psychology Review, 10, 251–296. https://doi.org/10.1023/A%3A1022193728205

Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. Journal of Information Systems Education, 34(1), 70-83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html

Weston, C. B. (1986). Formative evaluation of instructional materials: An overview of approaches. Canadian Journal of Educational Communication, 15(1), 5–17. https://doi.org/10.21432/T22W3Q

Wiggins, G., & McTighe, J. (1998). What is backward design. Understanding by design, 1, 7-19. https://jaymctighe.com/wp-content/uploads/2024/10/What-is-Backward-Design.pdf

Appendix A - CSF KU

Foundational - Cybersecurity Fundamentals (CSF)
The intent of the Cybersecurity Fundamentals (CSF) Knowledge Unit is to provide students with a basic understanding of the fundamental concepts and vocabulary within the vast cybersecurity discipline. Students must be able to describe the current cybersecurity threat landscape, including the various motivations, objectives, and threats. This KU reinforces adversarial thinking and the need for cybersecurity. Students must also be able to describe the goals of cybersecurity, how risk management informs the approach to cybersecurity, and the principles and best practices of cybersecurity.

KU Learning Outcomes
To complete this KU, students will be able to:

1. Define the fundamental principles of cybersecurity.
2. Describe the goals of cybersecurity.
3. Describe potential objectives of cyber attackers and their motivations.
4. Describe various types of cyber attacks.
5. Describe various common vulnerability types and evaluate their severity.
6. Describe common mechanisms used to protect against cyber attacks.
7. Describe cyber defense tools, methods and components.
8. Apply cyber defense methods to prepare a system to repel attacks and provide system security.
9. Describe appropriate measures to be taken should a system compromise occur.
10. Discuss current events in cybersecurity.

Topics

1. Cybersecurity principles
2. Threats and Adversaries (threat actors, malware, natural phenomena, and human factors)
3. Vulnerability Management
4. Basic Risk Management and Assessment (Risk, Threats, Vulnerabilities, Risk Mitigation, Residual Risk, Risk Acceptance, Risk Transference, Risk Appetite)
5. The Cybersecurity/McCumber Cube (Confidentiality, Integrity, and Availability (CIA) Triad, Information States, Security Controls)
6. Cyber Kill Chain, MITRE ATT&CK, and ATLAS Frameworks
7. Attack methods for different vulnerability types`
8. Security Life-Cycle
9. Applications of Cryptography and PKI
10. Data Security (e.g., in transmission, at rest, in processing)
11. Security Models (e.g., Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
12. Access Control Models (e.g., MAC, DAC, RBAC, Lattice)
13. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
14. Malware
15. Session Management
16. Exception Management
17. Security Mechanisms (e.g., Identification/Authentication, Audit)
18. Authentication, authorization, and accounting (AAA) and access control
19. Malicious activity detection/forms of attack
20. Security Governance, Policies, Controls and Appropriate Countermeasures (include Disaster Recover, Business Continuity, and Incident Response Policies and concepts)
21. Key Legal issues associated with cybersecurity and privacy (HIPAA, HITECH, SOX, FERPA, GLBA, COPPA, FISMA, GDPR, court rulings on-going)
22. Ethics (e.g., ethics associated with cybersecurity profession)
23. Cybersecurity best practices
24. Current events in cybersecurity
25. Cybersecurity awareness

Vocabulary
Advanced Persistent Threat (APT); Cybersecurity Fundamentals; Threat Landscape; Adversarial Thinking; Risk Management; Cybersecurity Principles; Cyber Attacks; Vulnerabilities; Cyber Defense; Access Control; Confidentiality, Integrity, Availability (CIA); Security Models; Legal Issues in Cybersecurity

Related Knowledge Units:
Cybersecurity Principles (CSP); IT Systems Components (ISC); Policy, Legal, Ethics, and Compliance (PLE)

Most Related DCWF and/or NICE Framework Work Role(s)
Defensive Cybersecurity; Cybersecurity Policy and Planning; Cybersecurity Instruction; Infrastructure Support; Insider Threat Analysis

Appendix B – Survey

Expert Review of Module 1 of a CYBR 201 Reader/Textbook

Dear Participant, You are being asked to participate in a research study regarding a pre-implementation evaluation of Module 1: Cybersecurity Fundamental Concepts, Principles, and Goals. This module is designed as part of a shared set of structured course materials for UNCW's introductory cybersecurity course (CYBR 201 – Fundamentals of Cybersecurity), specifically aligned with the CAE-CD Cybersecurity Fundamentals (CSF) Knowledge Unit (KU). The research team conducting this study includes Dr. [redacted] and [redacted]. Neither researcher will benefit financially from this study. If you agree to participate in this research project, you will be asked to review a PDF file and fill out an electronic survey that should take approximately 20 minutes to complete. We will not link your name to any responses you give on the survey and will use a function to obfuscate your email address in any stored data, thereby pseudonymizing it. Also, we will not disclose to anyone how you responded. You may stop the electronic survey at any time and refuse to answer any question. You will not be treated differently or penalized in any way if you choose not to participate or if you choose to end the survey early. There will be no direct benefit or foreseeable risk to you if you choose to participate in this research project. If you choose to participate, it should be because you want to help with this study. If you have any questions now or later about this research project, please contact Dr. [redacted] at [redacted]. For questions about your rights as a research subject, please contact the [redacted] Institutional Review Board office at [redacted] or [redacted]. PARTICIPANT STATEMENT: By clicking on the arrow below, I agree to participate in the research project described above. I understand that my involvement in this project is voluntary, and I can stop at any time

Q1 First Name

_____

Q2 Last Name

_____

Q3 Academic Title
Assistant Professor (1) Assistant Professor of Practice (2) Associate Professor (3) Part-time Faculty (4) Professor (5) Student Mentor (6)
Other (7) _____

Q4 Unit
[redacted] Business Affairs (1) [redacted] Computer Science Department (2) [redacted] School (3)
Other (4) _____

Q5 Years of tech experience in any working role(s) focused on cybersecurity, information technology, computer science, or related fields.

_____

Q6 Years of experience teaching any subject.

_____

Q7 Have you taught [redacted]'s CYBR 201 Fundamentals of Cybersecurity?
No (1) Yes (2)

Q8 Have you taught students with no prior technical background?
No (1) Yes (2)

Q9 The next block of questions will help us evaluate the effectiveness of Module 1 of the textbook we are creating for use with CYBR 201 Fundamentals of Cybersecurity. The course and textbook are designed to cover several Knowledge Units (KU); however, Module 1 is only intended to cover a portion of one KU - Cybersecurity Fundamentals (CSF).

Module 1 covers a subset of the CSF KU learning outcomes.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q11 Module 1 covers a subset of the CSF KU topics.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q12 Module 1 covers all of the CSF KU learning outcomes.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q13 Module 1 covers all of the CSF KU topics.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q14 Module 1 covers cybersecurity concepts in a technically accurate manner.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q15 Module 1 accurately covers the CIA Triad.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q16 Module 1 accurately covers access.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q17 Module 1 accurately covers authentication.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q18 Module 1 accurately covers authorization.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q19 Module 1 accurately covers privacy.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q20 Module 1 accurately covers non-repudiation.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q21 Module 1 accurately covers the McCumber Cube.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q22 Module 1 accurately covers security mechanisms.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q23 Module 1 accurately covers cybersecurity best practices.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q24 Module 1 is understandable for students with no prior technical background.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q25 Module 1 presents technical vocabulary in a clear way.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q26 Module 1 provides examples that help make abstract cybersecurity concepts easier to understand.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q27 Module 1 follows a logical learning sequence.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q28 Module 1 structure supports consistent delivery by multiple instructors teaching the same course.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q29 Module 1 provides an appropriate balance among definitions, explanations, examples, knowledge checks, and applied activities.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q30 Module 1 encourages students to apply concepts.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q31 Module 1 encourages students to only memorize definitions.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q32 Module 1 mini case study helps students connect multiple concepts in a realistic scenario.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q33 Module 1 mini case study helps students connect cybersecurity concepts to technology they use in everyday life.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q34 Module 1 applied activity encourages personal reflection.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q35 Module 1 applied activity encourages concept application.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q36 Module 1 applied activity encourages copy-paste of AI responses.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q37 Module 1 uses a consistent structure across major concepts.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q38 Module 1 uses a consistent, easy-to-follow structure.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q39 Module 1 tables "When [concept] is compromised, common results include:" make content easier for students to understand.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q40 Module 1 tables "Common mechanisms and practices that support [concept] include:" make content easier for students to understand.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q41 Module 1 balanced use of paragraphs, bullet points, tables, images, etc. is appropriate.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q42 Module 1 is appropriate for use with CYBR 201 Fundamentals of Cybersecurity.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q43 I am willing to use Module 1 as shared course material in CYBR 201 Fundamentals of Cybersecurity.
Strongly disagree (1) Somewhat disagree (2) Neither agree nor disagree (3) Somewhat agree (4) Strongly agree (5)

Q44 What, if anything, would you change to improve Module 1 before classroom use?
_____

ISSN: 2473-4901
v12 n6938

Appendix C – First Two Pages of Module 1

Module 1: Cybersecurity Fundamental Concepts, Principles, and Goals

Learning Outcomes and Topics

This module supports the Cybersecurity Fundamentals (CSF) Knowledge Unit (KU).

This module aligns with the following CSF KU learning outcomes (LO) and topics (T):

- LO 1: Define the fundamental principles of cybersecurity.
- LO 2: Describe the goals of cybersecurity.
- LO 6: Describe common mechanisms used to protect against cyber attacks.

- T 1: Cybersecurity principles
- T 5: The Cybersecurity/McCumber Cube (Confidentiality, Integrity, and Availability (CIA) Triad, Information States, Security Controls)
- T 13: Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
- T 17: Security Mechanisms (e.g., Identification/Authentication, Audit)
- T 23: Cybersecurity best practices

Note: *Topics 17 and 23 are introduced here and further explained in later modules.*

Module Focus

The focus is on three big ideas:

- what cybersecurity protects,
- how the CIA Triad and McCumber Cube organize cybersecurity thinking,
- and how concepts such as access, authentication, authorization, non-repudiation, and privacy support everyday security decisions.

What is cybersecurity trying to protect, and how do cybersecurity professionals decide whether something is secure?

Every day, people around the world rely on digital systems to study, communicate, work, manage money, receive health care, stay connected, etc. Cybersecurity helps protect those digital systems and the information they contain so that they can be trusted. Think about a student's daily life: logging into a favorite app, submitting homework online, checking university email, using online banking, opening a patient portal, or scrolling through social media. What really keeps that information safe?

1. What Is Cybersecurity?

NIST defines **cybersecurity** as:

> "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Stated Simply: *safeguarding cyberspace activities and entities*

ISSN: 2473-4901
v12 n6938

What Is Protected	Example
Data / Information	Grades, passwords, bank information, medical records
Hardware / Devices	Phones, laptops, tablets, servers, routers
Software / Applications	Mobile apps, web apps, web browsers, operating systems, learning management systems
Accounts / Digital Identities	Student portal login, email account, social media account, cloud storage account
Networks	Campus Wi-Fi, home Wi-Fi, business networks
Services	Email delivery, online banking transactions, file storage and sharing, assignment submission, patient record access
People / Users	Students, employees, customers, patients

Knowledge Check: Think about one social media application you use. What needs protection in that system? Identify at least three things (e.g., account access). Briefly explain why each one needs protection.

2. The CIA Triad

In cybersecurity, the **CIA Triad** means **Confidentiality, Integrity, and Availability**. Together, these three goals form a foundational model for cybersecurity. They help answer three basic questions:

1. Are systems and information only accessed by people allowed to use and see them? (***Confidentiality***)
2. Are systems and information protected against unauthorized changes, including destruction? (***Integrity***)
3. Can authorized users access systems and information whenever they need them? (***Availability***)

For example, think about a social media account. **Confidentiality** protects private messages. **Integrity** protects the profile, posts, and settings from unauthorized changes. **Availability** means the account owner can log in and use the account when needed.

Understanding the CIA Triad is like learning the basic rules of the road before driving. Many other cybersecurity topics, such as defending against hackers, building secure applications, or recovering from attacks, connect back to the foundational CIA Triad.

Confidentiality

NIST defines **confidentiality** as:

> "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."

Stated Simply: only authorized people can see protected information

Think of confidentiality like: A private social media account accessible only to approved followers. The information is not meant for everyone; it is limited to those with permission.