CCECC

Committee for Computing Education in Community Colleges

Cybersecurity Curricular Guidance

for Associate-Degree Programs

January 2020

Cybersecurity Curricular Guidance for Associate-Degree Programs

Cyber2yr2020

30 January 2020

Association for Computing Machinery (ACM)
Committee for Computing Education in Community Colleges (CCECC)

ISBN: 978-1-4503-7555-9
DOI: 10.1145/3381686
Web link: http://dx.doi.org/10.1145/3381686

Sponsoring Society

This report was made possible with financial support
from the Association for Computing Machinery (ACM)

The Cyber2yr2020 Final Report has been endorsed by
Association for Computing Machinery (ACM)
ACM Committee for Computing Education in Community Colleges (CCECC)

Printed in the United States

Cyber2yr2020 Task Group

Cara Tang*+ | Portland Community College, Portland, OR

Cindy Tucker* | Bluegrass Community and Technical College, Lexington, KY

Christian Servin* | El Paso Community College, El Paso, TX

Markus Geissler* | Cosumnes River College, Sacramento, CA

Melissa Stange* | Lord Fairfax Community College, Middletown, VA

Nancy Jones | Coastline Community College, Garden Grove, CA

James Kolasa | Bluegrass Community and Technical College, Lexington, KY

Amelia Phillips | Highline College, Des Moines, WA

Lambros Piskopos | Wilbur Wright College, Chicago, IL

Pam Schmelz | Ivy Tech Community College, Columbus, IN

* Steering Committee
+ Task Group Chair

Table of Contents

Acknowledgements

The task group would like to thank our advisory group for their valuable support and feedback throughout the project:

Antonio Bologna, Rapid 7, Austin, TX
Elizabeth K. Hawthorne, Union County College, Cranford, NJ
Sepi Hejazi Moghadam, Google, Mountain View, CA
Phil Helsel, Microsoft, Redmond, WA
Sidd Kaza, Towson University, Towson, MD
Bill Newhouse, NICE (National Initiative for Cybersecurity Education), Gaithersburg, MD
Casey O'Brien, National CyberWatch Center, Largo, MD
Allen Parrish, Mississippi State University, MS
John Sands, Moraine Valley Community College, Palos Hills, IL
Brian Ventura, SANS Instructor, Portland, OR
Berk Veral, Microsoft Cybersecurity Solutions Group, Redmond, WA

The task force would like the thank the following reviewers for their valuable feedback on the StrawDog and IronDog draft versions:

Alvin Brewer, Lord Fairfax Community College, VA
Virginia Carneiro de Paula, Ph.D., Palm Beach State College, Lake Worth, FL
Henry Coffman, Lord Fairfax Community College, Middletown VA
John Cook, Herkimer College, Herkimer, NY
Crystal Dye, Southwest Virginia Community College, Richlands, VA
Elizabeth K. Hawthorne, Union County College, Cranford, NJ, Vice-Chair ACM Education Board
Suvineetha Herath, Carl Sandburg College, Galesburg, IL
John Impagliazzo, Hofstra University, Hempstead, NY
Karl Linderoth, Bay College, Escanaba, MI
Michael McKeever, Santa Rosa Junior College, Petaluma, CA
Diana Merkel, Germanna Community College, Fredericksburg, VA
Jacob Miller, Pennsylvania College of Technology, Williamsport, PA
Sepi Hejazi Moghadam, Google, CA
Margaret, Montgomery College, MD
Trang D. Nguyen, Prince George's Community College, Largo, MD
Tim Preuss, Minnesota State Community and Technical College, Moorhead, MN
Daniel Sehnal, Rappahannock Community College (RCC), Glenns Campus, Saluda, VA
Tony Vargas, El Paso Community College, El Paso, TX
Berk Veral, Microsoft Cybersecurity Solutions Group, Redmond, WA
James Walden, Northern Kentucky University, Highland Heights, KY

Introduction

Overview of the Curricular Development Process

In early 2018 the Association for Computing Machinery (ACM) endorsed their first curricular volume for Cybersecurity designed for four-year institutions, Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [15], referred to as CSEC2017 (cybered.acm.org). The ACM Committee for Computing Education in Community Colleges (CCECC) formed a task force in early 2018 to create similar cybersecurity curriculum guidance for two-year programs. The content of these guidelines, known as Cyber2yr2020, is based on CSEC2017, and considers other inputs including the CAE-CD 2Y 2019 knowledge units [18] (requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense) and the NICE Cybersecurity Workforce Framework [16].

The ten-member Cyber2yr2020 task force is made up of community college educators with varying expertise in cybersecurity from community and technical colleges across the United States. The task force met online from April 2018 through December 2019, with an in-person meeting during the 3CS conference in August 2018. In addition to the focused work and contributions of these ten educators, input into the first draft, known as StrawDog, was incorporated from the face-to-face breakout groups at a pre-NICE event in November 2018. The StrawDog draft was released in February 2019, and presented publicly to the community for review and comment during the period February 25 - April 17, 2019. This period began with a special session presentation and discussion at the SIGCSE Symposium 2019, and included dissemination through a variety of venues, newsletters, and mailing lists. Feedback was collected via notes during feedback sessions, emails received, as well as through a survey. Those providing input represent both two-year and four-year educators as well as industry professionals.

The feedback on the StrawDog draft was reviewed by the task group and was very valuable in informing the next draft, known as IronDog. IronDog went through a similar period of public review and comment July 5 - August 15, 2019, including dissemination through a variety of channels and presentation at the 3CS conference in July 2019. Based on reviewer feedback, significant changes have been made to the early drafts of Cyber2yr2020 and the final guidelines have been improved immensely.

How to Use These Guidelines

The competencies and learning outcomes itemized in the Cybersecurity Curricular Framework section of this document can be used but are not limited to the following.

Conducting program reviews to update and create curriculum

For example, the cybersecurity learning outcomes can be used by colleges to conduct periodic program reviews with the intent of validating existing cybersecurity courses, certificates, and degrees, as well as to create new cybersecurity curriculum. These guidelines can assist in the creation of both career and transfer curriculum, as well as certificate credentials. Two program examples correlated to the competencies presented in this guidance are given in Appendix D. Program examples make it easy for colleges to compare and develop new courses, certificates and degree programs in cybersecurity. The full collection of program examples from across the nation is available at ccecc.acm.org/guidance/cybersecurity. If you are interested in submitting a program example, visit ccecc.acm.org/correlations for instructions, and contact the CCECC with any questions at ccecc.acm.org/contact.

Facilitating program and course articulation

Two-year cybersecurity programs may utilize these guidelines in articulation conversations with four-year transfer partners whose programs use CSEC2017. For example, the cybersecurity competencies and learning outcomes were used by ABET to develop criteria for two-year cybersecurity programs. ABET's program-specific criteria for cybersecurity at the baccalaureate level (four-year programs), found at www.abet.org/accreditation/accreditation-criteria, were guided by CSEC2017 [1]. The CCECC will map those criteria to the Cyber2yr2020 competencies and learning outcomes at which time you can view the ABET mapping and others at ccecc.acm.org/guidance/cybersecurity.

Complying with government-sponsored frameworks

For example, the ACM CCECC cybersecurity competencies align to the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [16] as shown in Appendix A, as well as to the Centers of Academic Excellence – Cyber Defense (CAE-CD) Two-Year Knowledge Units [18] as shown in Appendix B. The competencies and learning outcomes in this document align with 100% of the outcomes and topics in the Foundational Core and Technical Core CAE KUs. Additional mappings are also available, and the full collection can be found at ccecc.acm.org/guidance/cybersecurity.

Interacting with local advisory boards

For example, cybersecurity program advisory boards may review the Cyber2yr2020 competencies and learning outcomes with local needs in mind. Advisory boards often make recommendations for strengthening a local program of study, and the Cyber2yr2020 competencies provide a framework for discussion of cybersecurity competencies, courses, certificates, and degrees.

Two-Year/Community College Environment

According to the American Association of Community Colleges, over 40% of all undergraduates in the United States are enrolled in two-year colleges, and more than half of undergraduates from some demographic groups attend community and technical colleges [2]. “Community colleges are centers of educational opportunity. They are an American invention that put publicly funded higher education at close-to-home facilities, beginning nearly 100 years ago with Joliet Junior College (in Joliet, Illinois). Since then, they have been inclusive institutions that welcome all who desire to learn, regardless of wealth, heritage, or previous academic experience. The process of making higher education available to the maximum number of people continues to evolve...” [3].

The community college environment is uniquely positioned, resulting from the threefold mission of these institutions to provide a learning environment for:

- transfer into baccalaureate programs;
- entrance into the local workforce; and
- lifelong learning for personal and professional enrichment.

In addition, many two-year colleges are drivers of local economic development, providing workforce development and skills training, as well as offering noncredit programs ranging from English as a second language to skills retraining to community enrichment programs and cultural activities.

Two-year colleges serve high school graduates proceeding directly into college, workers needing to upgrade skill sets or master new ones in order to re-enter the workforce, immigrants seeking to become integrated into the local culture and master a new language, individuals leaving the workplace to engage college-level coursework for the first time, returning students with college degrees who have decided to pursue an alternative career path, and many individuals in need of ongoing training and skill updating. This diversity is addressed in numerous ways, including targeted career counseling, remediation of basic skills, specialized course offerings, individualized instruction and attention, flexible scheduling and delivery methodologies, and a strong emphasis on retention and successful completion. Furthermore, because two-year colleges have less restrictive entrance requirements, faculty must be prepared to instruct students exhibiting a broad range of academic preparations, aptitudes, and learning styles. The mission of two-year college faculty is to focus their full-time attention on effective pedagogy for educating a diverse student population, as well as remaining current in their discipline and in the scholarship of teaching and learning, and fostering student success.

Two-year, community or technical colleges, as well as certain four-year colleges, award associate degrees to students completing between 60 and 66 higher education semester credits in a specific program of study. It is often the case that an associate-degree requires

approximately half the college credit of a bachelor's degree. Associate-degree programs are complete, whether designed specifically to enable graduates to transfer into the upper division of a baccalaureate program or to gain entry into the workforce. Additionally, these institutions also offer certificate programs, intended to be fulfilled in less time than a complete degree program; such programs are often designed for targeted student audiences and focused on specific content.

At the earliest opportunity, faculty and academic advisors must help each student determine which type of program best serves the student's educational and career goals. Such considerations include the distinctions between certificate, career and transfer programs, the academic requirements of each, and the associated employment options.

Career and Transfer Programs

Typically, associate-degree computing programs fall into two categories: those designed to prepare graduates for immediate entry into career paths, usually an Associate of Applied Science (A.A.S), and those designed for transfer into baccalaureate degree programs, usually an Associate of Science (A.S.) or Associate of Arts (A.A.) or in some cases with no degree awarded.

Colleges should make students aware at the onset of their studies of the distinctions between career and transfer programs, the academic requirements of each, and the resultant employment options.

Career-oriented associate-degree programs provide students with the specific knowledge, skills, and abilities necessary to proceed directly into employment in a targeted work environment. The program of study may include professional development coursework as well as courses that emphasize communication skills, mathematical reasoning, and other general education requirements. In addition, many students will augment their formal studies with technical industry certifications to enhance their immediate employability.

It is important to note that a career-oriented associate degree program is not intended to facilitate transfer into a baccalaureate program, but rather to provide entry into a career that requires specialized post-secondary skills and an advanced level of expertise and education. Nevertheless, many students graduating from career-oriented programs subsequently elect to further their education at the baccalaureate level.

Transfer-oriented degree programs provide the academic foundation and pathway to continue a program of study at a four-year college or university. Articulation is a key consideration in associate-degree programs which are designed as transfer curricula. Articulation of courses and programs between academic institutions is a process that facilitates transfer by students from one institution to another. The goal is to enable students to transfer in as seamless a manner as possible. Efficient and effective articulation requires an accurate assessment of courses and

programs as well as meaningful communication and cooperation among institutions. Both students and faculty have responsibilities and obligations for successful articulation. Ultimately, students are best served when educational institutions establish well-defined articulation agreements that actively promote transfer.

Diversity in the Computing Profession

Across the globe, there is a high demand for computing and cybersecurity professionals and a significant shortfall in job vacancies in many locations. The growth of new and emerging roles in computing, technology, and engineering fields exceeds the rate that underrepresented groups enter these fields. Academic research continues to bear light on the pressing need to increase the diversity of students pursuing computing degrees and the numerous benefits of doing so. To help fulfill the increasing shortage of cybersecurity professionals, computing faculty should increase efforts to effectively recruit and retain a wider range of students and build and provide effective support structures so that all students can successfully graduate.

Ethics and Professionalism

Ethical reasoning and professional conduct are important concepts in the overall curricula for computing disciplines, including cybersecurity, and must be integrated throughout the programs of study. This ethical and professional context should be established at the onset and should appear routinely in discussions and learning activities throughout the curriculum. Updated in 2018, the ACM Code of Ethics notes that “Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good” [4]. The Code goes on to provide an excellent framework for conduct that should be fostered beginning early in students’ experiences (www.acm.org/code-of-ethics).

As computing technologies become ubiquitous in society, ethical behavior and adherence to codes of conduct for computing professionals are imperative; therefore, careful consideration of legal, ethical, and societal issues involving computing, the Internet and databases are essential to the education of computing professionals. Students who realize the potential uses and abuses of technology will, as citizens, be able to contribute to public policy debate from a knowledgeable perspective on issues such as property rights and privacy concerns that affect everyone.

Computer systems have a substantial social impact in nearly every setting including applications such as healthcare, finance, transportation, defense, government, education, and communications. Engaging students in the consideration of the ethical aspects involved in decisions about technology and computing systems enables them to make more judicious choices. It is crucial that students pursuing careers in cybersecurity or computing more generally be made aware of and properly equipped to handle the complexities of professional judgments -

as computing professionals, graduates must follow codes of conduct and take responsibility for their actions and be accountable for the systems that they develop, support, and protect.

Cybersecurity, in particular, is a discipline in which ethics play a critical role, and ethics should be incorporated throughout a cybersecurity curriculum. Cybersecurity codes of ethics offer dictates such as “Promote generally accepted information security current best practices and standards” found in the ISSA (Information Systems Security Association) Code of Ethics [14] and “Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks” found in the EC-Council Code of Ethics [12].

Employability Skills

The need for students to attain various employability skills, which are often referred to as “soft skills” and typically include communication skills and teamwork, continues to be emphasized by employers of graduates and industry advisory boards. Instructors are therefore encouraged to model professional behavior and to challenge their students by having them practice and apply various employability skills, such as presentations, team member interactions, and role-play scenarios.

Mathematics Requirements

Mathematics provides a language for working with ideas relevant to computing, specific tools for analysis and verification, and a theoretical framework for understanding important concepts. For these reasons, mathematics content must be initiated early in the student’s academic career, reinforced frequently, and integrated into the student’s course of study. Curriculum content, pre- and co-requisite structures, and learning activities and laboratory assignments must be designed to reflect and support this framework. Many students enter two-year colleges with insufficient mathematics preparation for a computing program. Such students must devote additional semesters to achieve the mathematical maturity and problem-solving skills required to be successful in computing coursework.

A variety of mathematics and logic courses and embedded content may be appropriate for undergraduate cybersecurity majors. This may include discrete mathematics, statistics, probability, and linear algebra, among others. Transfer programs may have more extensive mathematics requirements to align with four-year partner programs. This curricular guidance does not include specific student learning outcomes for mathematics but supports the inclusion of sufficient mathematics to meet the cybersecurity outcomes for a given program.

The Cybersecurity Discipline

Cybersecurity has only recently emerged as an identifiable discipline, and cybersecurity degree programs are still relatively young. CSEC2017 defines cybersecurity as: “A computing-based discipline involving technology, people, information, and processes to enable assured

operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management."

The growth of Cybersecurity is evidenced by a number of surveys, articles, and studies. A survey by Nationwide Mutual Insurance Company found that 58% of business owners with up to 299 employees had been victims of a cyber-attack [17]. With growing cyber threats in both the private and public sectors, continuous curriculum development is critical because the nature of the threats continuously evolves, thus increasing the knowledge and skill set needed by the cybersecurity workforce. The cybersecurity workforce is currently experiencing a shortage across the nation. The Cyberseek project by the National Initiative for Cybersecurity Education (NICE), CompTIA, and Burning Glass estimates that there are 997,058 workers employed in cybersecurity-related positions, and 504,316 online job listings for cybersecurity-related positions as of November 2019, with the number of openings continuing to grow [10]. Cybersecurity Ventures predicts there will be approximately 3.5 million unfilled cybersecurity jobs by 2021 [9]. The U.S. Bureau of Labor Statistics predicts that jobs for information security analysts will grow by 32% between 2018 and 2028 [19].

Many computing skills in the cybersecurity discipline overlap with concepts in computational thinking, such as decomposition, pattern recognition / data representation, generalization / abstraction, and algorithms. Computational thinking is being incorporated into computing curriculum at all levels, precisely to solve computing problems using different levels of abstraction [11].

In addition to being an important discipline in its own right, cybersecurity is becoming an increasingly important element of all computing programs. Curriculum content in creating and maintaining secure computing environments is a critical component in associate-degree computing programs. Almost every career path open to a computing student encompasses some aspect of security. System administrators and engineers must be able to properly design, configure, and maintain a secure system; programmers and application developers must know how to design and build secure, fault-tolerant software systems from the bottom up; web specialists must be capable of assessing risks and determining how best to reduce the potential impact of breached systems; user support technicians must be knowledgeable in security concerns surrounding desktop computing; and project managers must be able to calculate the cost/benefit tradeoffs involved with implementing secure systems.

It is the responsibility of faculty to ensure that students are well prepared for the cybersecurity challenges they will inevitably encounter in their careers as computing professionals. ACM CCECC curricular guidelines for associate-degree Computer Science [5] and Information Technology [6] programs have cybersecurity infused throughout the content. Likewise, it is vitally important that students understand the need to remain current in a fast-paced field.

Cybersecurity Curricular Framework

These guidelines for associate-degree cybersecurity programs maintain the CSEC2017 division into eight knowledge areas (KAs), with each knowledge area having a number of knowledge units. The terms “domain” and “subdomain” are preferred to “knowledge area” and “knowledge unit” respectively since our focus is on competencies and outcomes, which go beyond knowledge to also include skills and dispositions in context. To maintain consistency with CSEC2017 and allow easy comparison of sections of the curricular framework, the KA structure and terms used in organizing CSEC2017 are maintained in this document, though the content focuses on competencies and outcomes as discussed below.

The following table delineates the eight knowledge areas/domains and their definitions, paraphrased from CSEC2017:

Knowledge Area	**Definition**
Data Security	Focuses on the protection of data at rest, during processing, and in transit. This knowledge area may require the application of mathematical and analytical algorithms.
Software Security	Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited. The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.
Component Security	Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems. The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

Connection Security	Focuses on the security of the connections between components including both physical and logical connections. It is critical that every cybersecurity professional has a basic knowledge of digital communications and networking. Connections are how components interact. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.
System Security	Focuses on the security aspects of systems that are composed of components and connections, and use software. Understanding the security of a system requires viewing it not only as a set of components and connections but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems.
Human Security	Focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity. Humans have the responsibility to ensure the confidentiality, integrity, and availability (CIA) of their organizational and personal computer systems.
Organizational Security	Focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. Organizations have the responsibility to meet the needs of many constituencies and those needs must inform risk management, security governance, business continuity, and security program management.
Societal Security	Focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse. Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across global society is serious and growing. Laws, ethics, and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

Several pervasive themes, referred to as cross-cutting concepts in CSEC2017, are woven throughout the knowledge areas, including

- **Confidentiality**, rules that limit access to system data and information to authorized persons;
- **Integrity**, assurance that the data and information are accurate and trustworthy;
- **Availability**, the data, information, and system are accessible;
- **Risk**, the potential for gain or loss;
- **Adversarial thinking**, a thinking process that considers the potential actions of the opposing force working against the desired result; and
- **Systems thinking**, a thinking process that considers the interplay between social and technical constraints to enable assured operations.

These pervasive themes can be found in all eight knowledge areas. They help students explore connections among the knowledge areas and reinforce the security mindset conveyed throughout each knowledge area.

Within each knowledge area, these associate-degree guidelines are divided into Essential and Supplemental portions. This recognizes the fact that there can be a variety of flavors of associate-degree cybersecurity programs. The content in Essential is content that would be expected to appear in all associate-degree cybersecurity programs at the suggested Bloom's level or higher. The content in Supplemental is content that is likely to appear in some flavor of an associate-degree cybersecurity program, but not in other flavors of an associate-degree cybersecurity program.

The heart of this curricular framework is a small set of competencies for each knowledge area/domain, along with a variety of student learning outcomes organized by knowledge unit/subdomain within each knowledge area. The competencies follow the definition presented in *Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines* [13]: "Competency integrates knowledge, skills, and dispositions and is context-situated." Knowledge ("know-that") refers to "mastery of core concepts and content knowledge." Skills ("know-how") are "qualities that people develop and learn over time with practice and through interactions with others." Dispositions ("know-why" and "know-yourself") include "attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems." Context is the setting in which competencies manifest, the "authentic situations related to problems/issues and aspects of work" [13].

The student learning outcomes represent more detailed outcomes than the competencies and may be seen as course or lesson learning outcomes. Learning outcomes emphasize what students *can do* over merely what students *know*. Both competencies and learning outcomes are expressed using action verbs from Bloom's Revised Taxonomy. The Bloom's level - Remembering, Understanding, Applying, Analyzing, Evaluating, or Creating - represents the

depth of cognition for a given competency or learning outcome. See Appendix E for the table of Bloom's verbs used in these guidelines.

In this document, the content is presented by knowledge area/domain, with competencies representing the cross-cutting concepts that span knowledge areas presented first. Each knowledge area has a "card" giving the definition (from CSEC2017), essential competencies, supplemental competencies, and list of knowledge units/subdomains. After the knowledge area card, the more detailed learning outcomes are presented, organized by knowledge unit within the knowledge area and marked as essential or supplemental. The Bloom's level of each competency and learning outcome is indicated after it in italics.

Cross-Cutting Concepts

Definition

The pervasive themes of confidentiality, integrity, availability, risk, adversarial thinking, and system thinking that help students explore the connections among the eight knowledge areas and reinforce the importance of a security mindset throughout all knowledge areas.

Essential Competencies

- [CC-1] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*
- [CC-2] Assess and respond appropriately to various risks which can affect the expected operation of information systems. *Evaluating*
- [CC-3] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. *Applying*
- [CC-4] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. *Applying*
- [CC-5] Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. *Understanding*

Data | Software | Component | Connection | System | Human | Organizational | Societal

Data Security

Definition

Focuses on the protection of data at rest, during processing, and in transit.

This knowledge area requires the application of mathematical and analytical algorithms to fully implement.

Essential Competencies

- [DAT-E1] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. *Applying*
- [DAT-E2] Discuss forensically sound collection and acquisition of digital evidence. *Understanding*
- [DAT-E3] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents. *Applying*
- [DAT-E4] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks. *Applying*
- [DAT-E5] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. *Understanding*

Supplemental Competencies

- [DAT-S1] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. *Applying*
- [DAT-S2] Outline complex technical concepts to technical and non-technical audiences as they relate to data security. *Analyzing*

Knowledge Units

Cryptography
Digital Forensics
Data Integrity and Authentication
Access Control
Secure Communication Protocols
Cryptanalysis
Data Privacy
Information Storage Security

Data | Software | Component | Connection | System | Human | Organizational | Societal

Data Security Learning Outcomes

Cryptography

Essential Learning Outcomes

[DAT-LO-E01] Analyze which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation. *Analyzing*

[DAT-LO-E02] Apply symmetric and asymmetric algorithms as appropriate for a given scenario. *Applying*

[DAT-LO-E03] Investigate hash functions for checking integrity and protecting authentication data. *Applying*

[DAT-LO-E04] Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, and Enigma machine simulator, to encrypt and decrypt data. *Applying*

Supplemental Learning Outcomes

[DAT-LO-S01] Compare the benefits and drawbacks of applying cryptography in hardware vs software. *Analyzing*

[DAT-LO-S02] Demonstrate the importance of mathematical theory in the application of cryptography. *Understanding*

[DAT-LO-S03] Deduce minimum key strength for symmetric algorithms to be effective. *Analyzing*

[DAT-LO-S04] Contrast trust models in PKI, such as hierarchical, distributed, bridge,and web of trust. *Analyzing*

[DAT-LO-S05] Explain how symmetric and asymmetric encryption are used in tandem to secure electronic communications and transactions, such as cryptocurrencies and other crypto assets. *Understanding*

[DAT-LO-S06] Apply symmetric and asymmetric cryptography, such as DES, Twofish, AES, RSA, ECC, and DSA for a given scenario. *Applying*

Digital Forensics

Essential Learning Outcomes

[DAT-LO-E05] Discuss the concept, need, and value of digital forensics. *Understanding*

[DAT-LO-E06] Describe components of a digital investigation, sources of digital evidence, limitations of forensics, and ethical considerations. *Understanding*

[DAT-LO-E07] Discuss key rules, laws, policies, and procedures that impact digital forensics. *Understanding*

[DAT-LO-E08] Explain how to preserve the chain of custody for digital evidence. *Understanding*

[DAT-LO-E09] Perform fundamental incident response functions including detecting, responding, and recovering from security incidents. *Applying*

Supplemental Learning Outcomes

[DAT-LO-S07] Demonstrate the benefits of digital forensic readiness and planning. *Understanding*

[DAT-LO-S08] Examine legal issues, authorities, and processes related to digital evidence. *Analyzing*

[DAT-LO-S09] Describe the role and ethical responsibilities of a forensic examiner. *Understanding*

[DAT-LO-S10] Outline a variety of digital forensic tools (open source vs. closed source) and their limits. *Analyzing*

[DAT-LO-S11] Describe digital forensics investigative procedures, such as identification of evidence, collection and preservation of evidence, timelines, reporting, chain of custody, and authentication of evidence. *Understanding*

[DAT-LO-S12] Carry out forensically sound acquiring and handling of digital evidence following chain of custody best practices. *Applying*

[DAT-LO-S13] Analyze digital evidence from non-PC devices, such as smartphones, tablets, GPS, game consoles, Smart TVs, and IoT devices. *Analyzing*

[DAT-LO-S14] Apply documentation techniques and reporting of findings using industry standard and technically accurate terminology and format. *Applying*

[DAT-LO-S15] Outline complex technical concepts and processes so that they are easily understood by non-technical audiences. *Analyzing*

[DAT-LO-S16] Carry out verification and validation of evidence during forensic acquisition, preservation, and analysis, including the use of hashes. *Applying*

[DAT-LO-S17] Summarize the best practices in collecting and isolating mobile devices when part of digital evidence. *Understanding*

Data Integrity and Authentication

Essential Learning Outcomes

[DAT-LO-E10] Contrast the concepts and techniques to achieve data integrity, authentication, authorization, and access control. *Analyzing*

[DAT-LO-E11] Summarize the benefits and challenges of multifactor authentication. *Understanding*

[DAT-LO-E12] Execute one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools. *Applying*

[DAT-LO-E13] Apply basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers. *Applying*

Supplemental Learning Outcomes

[DAT-LO-S18] Implement multifactor authentication using tools and techniques, such as cryptographic tokens, cryptographic devices, biometric authentication, one-time passwords, and knowledge-based authentication. *Applying*

[DAT-LO-S19] Illustrate the use of cryptography to provide data integrity, such as message authentication codes, digital signatures, authenticated encryption, and hash trees. *Applying*

Access Control

Essential Learning Outcomes

[DAT-LO-E14] Describe access control best practices, such as separation of duties, job rotation, and clean desk policy. *Understanding*

[DAT-LO-E15] Discuss physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction. *Understanding*

[DAT-LO-E16] Implement data access control to manage identities, credentials, privileges, and related access. *Applying*

[DAT-LO-E17] Differentiate among the different types of identities, such as federated identities. *Understanding*

[DAT-LO-E18] Differentiate access control models, including role-based, rule-based, and attribute-based. *Understanding*

Supplemental Learning Outcomes

[DAT-LO-S20] Investigate access control models, such as role-based, rule-based, and attribute-based. *Applying*

[DAT-LO-S21] Illustrate the fundamental value and benefits of security architectures used to protect information in computer systems. *Applying*

Secure Communication Protocols

Essential Learning Outcomes

[DAT-LO-E19] Explain end-to-end data security. *Understanding*

[DAT-LO-E20] Illustrate important application and transport layer protocols, such as HTTP, HTTPS, SSH, SSL/TLS, IPsec and VPN technologies. *Applying*

Supplemental Learning Outcomes

[DAT-LO-S22] Explain security threats and mitigations to data at the data link layer. *Understanding*

[DAT-LO-S23] Illustrate attacks and countermeasures on TLS, such as downgrade attacks, certificate forgery, implications of stolen root certificates, and certificate transparency. *Applying*

[DAT-LO-S24] Explain security threats and mitigations to data at the data link layer. *Understanding*

[DAT-LO-S25] Investigate privacy preserving protocols, such as Mixnet, Tor, Off-the-record message, and Signal. *Applying*

Cryptanalysis

Essential Learning Outcomes

[DAT-LO-E21] Classify various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force. *Understanding*

Supplemental Learning Outcomes

[DAT-LO-S26] Contrast different well-known cryptanalysis attacks. *Analyzing*

[DAT-LO-S27] Demonstrate timing attacks and their effects on well-known algorithms such as RSA, ElGamal, and the Digital Signature Algorithm. *Understanding*

[DAT-LO-S28] Describe how meet-in-the-middle attacks affect the privacy aspect of data. *Understanding*

[DAT-LO-S29] Categorize in terms of complexity different techniques for attacks against public key ciphers, such as Pollard's p-1 and rho methods, quadratic sieve, and number field sieve. *Analyzing*

Data Privacy

Essential Learning Outcomes

[DAT-LO-E22] Examine various ways that privacy can be jeopardized by using contemporary technology, including social media. *Analyzing*

Information Storage Security

Essential Learning Outcomes

[DAT-LO-E23] Discuss storage device encryption implemented at the hardware and software levels. *Understanding*

[DAT-LO-E24] Contrast techniques for data erasure and their limitations in implementation. *Analyzing*

Software Security

Definition

Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

Essential Competencies

- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

Supplemental Competencies

- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

Knowledge Units

Fundamental Principles
Design
Implementation
Analysis and Testing
Deployment and Maintenance
Documentation
Ethics

Data | **Software** | Component | Connection | System | Human | Organizational | Societal

Software Security Learning Outcomes

Fundamental Principles

Essential Learning Outcomes

[SOF-LO-E01] Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. *Applying*

[SOF-LO-E02] Execute access decisions and permissions based on explicit need. *Applying*

[SOF-LO-E03] Diagram a simple secure application design. *Applying*

[SOF-LO-E04] Explain software security controls in an open design. *Understanding*

[SOF-LO-E05] Modify the levels of abstraction in a given piece of software to provide single layer abstraction whenever possible. *Applying*

[SOF-LO-E06] Implement software as a system of secure co-operating components. *Applying*

[SOF-LO-E07] Explain session management and its role in securing web-based applications and services. *Understanding*

Supplemental Learning Outcomes

[SOF-LO-S01] Test authorization and access control for a given class. *Applying*

[SOF-LO-S02] Develop software for a specific process among multiple secure modules. *Applying*

[SOF-LO-S03] Illustrate isolation through a virtual machine or sandbox. *Applying*

[SOF-LO-S04] Write software specifications that include security specifications infused in the design and implementation specifications. *Applying*

[SOF-LO-S05] Diagram a software design that is adjustable to environmental changes. *Applying*

[SOF-LO-S06] Decompose a software design to reduce the common mechanism among system components. *Analyzing*

[SOF-LO-S07] Investigate an object's access authorization following the principle of complete mediation. *Applying*

[SOF-LO-S08] Test authorization and access control for a given class. *Applying*

[SOF-LO-S09] Develop software for a specific process among multiple secure modules. *Applying*

[SOF-LO-S10] Illustrate isolation through a virtual machine or sandbox. *Applying*

[SOF-LO-S11] Write software specifications that include security specifications infused in the design and implementation specifications. *Applying*

[SOF-LO-S12] Diagram a software design that is adjustable to environmental changes. *Applying*

[SOF-LO-S13] Decompose a software design to reduce the common mechanism among system components. *Analyzing*

[SOF-LO-S14] Investigate an object's access authorization following the principle of complete mediation. *Applying*

Design

Essential Learning Outcomes

[SOF-LO-E08] Explain security requirements in software design for a given scenario. *Understanding*

[SOF-LO-E09] Examine the waterfall and agile development models' relationship to software security. *Analyzing*

[SOF-LO-E10] Describe what makes a programming language type-safe. *Understanding*

Supplemental Learning Outcomes

[SOF-LO-S15] Explain the relationship between software security requirements and a business' mission. *Understanding*

[SOF-LO-S16] Translate software security requirements into written formal, informal, and testing specifications. *Understanding*

Implementation

Essential Learning Outcomes

[SOF-LO-E11] Discuss significant implementation issues in a secure software life cycle. *Understanding*

[SOF-LO-E12] Write secure code which implements input validation and prevents buffer overflow, integer range violations, and input type violations. *Applying*

[SOF-LO-E13] Apply appropriate restrictions to process privileges. *Applying*

[SOF-LO-E14] Implement appropriate error and exception handling and user notification. *Applying*

[SOF-LO-E15] Develop a secure application or script using defensive programming techniques. *Creating*

Supplemental Learning Outcomes

[SOF-LO-S17] Use an API to detect errors and implement security policy. *Applying*

[SOF-LO-S18] Implement process and resource checking. *Applying*

[SOF-LO-S19] Use cryptographic randomness appropriately for a given scenario. *Applying*

[SOF-LO-S20] Implement process isolation. *Applying*

Analysis and Testing

Essential Learning Outcomes

[SOF-LO-E16] Carry out security-related testing procedures, for a given piece of software. *Applying*

[SOF-LO-E17] Explain the difference between static and dynamic software analysis and testing. *Understanding*

Supplemental Learning Outcomes

[SOF-LO-S21] Distinguish different methods of static and dynamic analysis. *Analyzing*

[SOF-LO-S22] Test software components as they are integrated. *Evaluating*
[SOF-LO-S23] Test software as a whole while incorporating unit testing and software testing. *Evaluating*
[SOF-LO-S24] Test the security of a given piece of software, including granting access one OSI model layer at a time while reducing access points. *Evaluating*

Deployment and Maintenance

Essential Learning Outcomes

[SOF-LO-E18] Perform software installation, configuration, maintenance, and patching tasks in a secure manner. *Applying*
[SOF-LO-E19] Explain potential security implications for software decommissioning and retiring. *Understanding*

Supplemental Learning Outcomes

[SOF-LO-S25] Summarize software development and operations. *Understanding*

Documentation

Essential Learning Outcomes

[SOF-LO-E20] Write appropriate security notations within software documentation. *Applying*
[SOF-LO-E21] Use available documentation to resolve security-related issues throughout the software life cycle. *Applying*

Supplemental Learning Outcomes

[SOF-LO-S26] Write documentation for software installation and configuration. *Applying*
[SOF-LO-S27] Write user documentation emphasizing user security dangers. *Applying*

Ethics

Essential Learning Outcomes

[SOF-LO-E22] Explain various ethical aspects related to software development, including vulnerability disclosure. *Understanding*

Supplemental Learning Outcomes

[SOF-LO-S28] Describe social aspects related to software development. *Understanding*
[SOF-LO-S29] Summarize legal aspects and regulations regarding software development. *Understanding*
[SOF-LO-S30] Defend an ethical approach to software development and vulnerability disclosure. *Evaluating*

Component Security

Definition

Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

Essential Competencies

- [COM-E1] Discuss vulnerabilities and mitigations of system components throughout their lifecycle. *Understanding*
- [COM-E2] Perform security testing for given components within a system. *Applying*

Supplemental Competencies

- [COM-S1] Analyze how component security features impact systems, such as software and firmware updates. *Analyzing*

Knowledge Units

Component Design
Component Procurement
Component Testing
Component Reverse Engineering

Data | Software | **Component** | Connection | System | Human | Organizational | Societal

Component Security Learning Outcomes

Component Design

Essential Learning Outcomes

[COM-LO-E01] Discuss how a component's design may create vulnerabilities in information systems. *Understanding*

Supplemental Learning Outcomes

[COM-LO-S01] Describe the various phases of the component lifecycle. *Understanding*
[COM-LO-S02] Compare various secure component design principles. *Analyzing*

Component Procurement

Essential Learning Outcomes

[COM-LO-E02] Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Understanding*

[COM-LO-E03] Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. *Understanding*

Component Testing

Essential Learning Outcomes

[COM-LO-E04] Perform component security testing. *Applying*

[COM-LO-E05] Describe unit testing tools and techniques, as distinguished from those used in system-level testing. *Understanding*

Supplemental Learning Outcomes

[COM-LO-S03] Use tools and techniques, such as fuzz testing, for testing the security properties of a component beyond its functional correctness. *Applying*

Component Reverse Engineering

Essential Learning Outcomes

[COM-LO-E06] Describe common reverse engineering scenarios for components of a system. *Understanding*

Connection Security

Definition

Focuses on the security of the connections between components including both physical and logical connections.

It is critical that every cybersecurity professional have a basic knowledge of digital communications and networking. Connections are how components interact. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.

Essential Competencies

- [CON-E1] Illustrate the construction and proper configuration of computer networks which adhere to current industry standards and organizational guidelines. *Applying*
- [CON-E2] Investigate the impact of various connection and transmission attacks on network hardware and software. *Applying*

Supplemental Competencies

- [CON-S1] Examine characteristics of commonly used physical networking media and interfaces. *Analyzing*
- [CON-S2] Distinguish vulnerabilities and example exploits as they apply to network services, architectures, and protocols. *Analyzing*
- [CON-S3] Implement appropriate defenses throughout an enterprise to harden the network against attackers. *Applying*
- [CON-S4] Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. *Creating*

Knowledge Units

Physical Media
Hardware and Physical Component Interfaces and Connectors
Distributed Systems Architecture
Network Architecture
Network Implementations
Network Services
Network Defense

Data | Software | Component | **Connection** | System | Human | Organizational | Societal

Connection Security Learning Outcomes

Physical Media

Supplemental Learning Outcomes

[CON-LO-S01] Diagram transmission flow in a medium. *Applying*

[CON-LO-S02] Contrast the communications characteristics of shared and point -to-point media. *Analyzing*

[CON-LO-S03] Explain various schemes for sharing media between multiple clients, including PPP and CSMA/CD. *Understanding*

[CON-LO-S04] Examine characteristics of common networking standards including frame structure, including IEEE 802.3 and 802.11. *Analyzing*

Hardware and Physical Component Interfaces and Connectors

Supplemental Learning Outcomes

[CON-LO-S05] Manipulate physical components of an organizational network and their interfaces, such as network cables, motherboards, memory, current CPU chips, and buses. *Applying*

[CON-LO-S06] Explain various standards for network connector hardware, such as RJ-11, RJ-45, ST, and SC. *Understanding*

[CON-LO-S07] Perform installation and configuration of device drivers for network components in an organization. *Applying*

Distributed Systems Architecture

Essential Learning Outcomes

[CON-LO-E01] Describe architectures for running processes in a distributed system and enabling communication between them. *Understanding*

[CON-LO-E02] Summarize the evolution of the Internet as a distributed platform, including the role of the world-wide-web. *Understanding*

[CON-LO-E03] Compare the OSI model and the TCP/IP model. *Analyzing*

[CON-LO-E04] Categorize commonly used network protocols based on the layers of the OSI model. *Analyzing*

[CON-LO-E05] Explain common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. *Understanding*

[CON-LO-E06] Classify various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). *Understanding*

[CON-LO-E07] Perform the setup and configuration of a virtual machine in a hypervisor environment. *Applying*

Supplemental Learning Outcomes

[CON-LO-S08] Describe use cases for high performance computing (HPC). *Understanding*

[CON-LO-S09] Distinguish vulnerabilities and example exploits as they apply to interfaces used in hypervisors, virtual networking, physical networking, and interprocess communication. *Analyzing*

Network Architecture

Essential Learning Outcomes

[CON-LO-E08] Diagram common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards. *Applying*

[CON-LO-E09] Distinguish various network topologies and their transmission characteristics. *Analyzing*

[CON-LO-E10] Describe various types of virtualization, including native virtualization (Type 1) and hosted virtualization (Type 2). *Understanding*

Supplemental Learning Outcomes

[CON-LO-S10] Compare the various IEEE 802 network architecture implementations. *Analyzing*

[CON-LO-S11] Distinguish various networks based on their physical characteristics (LANs, MANs, etc.). *Analyzing*

[CON-LO-S12] Illustrate packet forwarding in general and in the context of software-defined networking. *Applying*

[CON-LO-S13] Examine routing algorithms, such as link-state and distance vector, and how they populate forwarding tables. *Analyzing*

[CON-LO-S14] Discuss emerging technologies and their impact as they emerge, such as software-defined networking, the Internet of Things, and adding routing to layer 2 with enhanced learning bridges. *Understanding*

Network Implementations

Essential Learning Outcomes

[CON-LO-E11] Differentiate between various connection attacks, such as SYN-scanning, and associated vulnerabilities, and how they can affect an organization's network. *Understanding*

[CON-LO-E12] Differentiate between various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization's network. *Understanding*

Supplemental Learning Outcomes

[CON-LO-S15] Analyze the various fields available in Internet Protocol packets at various layers of the Open Systems Interconnection (OSI) and TCP/IP models. *Analyzing*

[CON-LO-S16] Demonstrate examples of network vulnerabilities, such as ARP poisoning as a man-in-the-middle attack. *Understanding*

[CON-LO-S17] Discuss examples of physical security vulnerabilities, including Universal Serial Bus (USB) and other serial connections. *Understanding*

Network Services

Essential Learning Outcomes

[CON-LO-E13] Describe the concept of an operating system service or daemon, and how it could be vulnerable to exploitation. *Understanding*

Supplemental Learning Outcomes

[CON-LO-S18] Compare network service models, including client-server and peer-to-peer. *Analyzing*

[CON-LO-S19] Describe methods by which components connect, including procedure calls, IPC requests, Interface Definition Languages with stub code, and private protocols over a socket. *Understanding*

[CON-LO-S20] Explain specific services and how their protocols are implemented, including SMTP, HTTP, SNMP, REST, CORBA, and Application layer protocols for specialty devices. *Understanding*

[CON-LO-S21] Describe service virtualization as a method to emulate the behavior of specific components, such as cloud-based applications and service-oriented architecture. *Understanding*

[CON-LO-S22] Write a security policy that provides guidance and requirements for the services provided by the network along with the measures to be used to see that the policies are followed. *Applying*

[CON-LO-S23] Illustrate examples of network vulnerabilities of client-server, peer-to-peer, and virtualization network services, such as common service signatures. *Applying*

Network Defense

Essential Learning Outcomes

[CON-LO-E14] Explain how network defenses should be structured using layering, segmentation, and other controls to achieve maximum confidentiality, integrity, and availability (CIA). *Understanding*

Supplemental Learning Outcomes

[CON-LO-S24] Implement configuration settings on devices throughout an enterprise to harden the network against attackers. *Applying*

[CON-LO-S25] Demonstrate how intrusion detection and intrusion prevention services can be used to protect a network and audit network traffic. *Understanding*

[CON-LO-S26] Discuss appropriate uses of host-, server-, and internetworking device-based firewalls. *Understanding*

[CON-LO-S27] Implement a simple virtual private network. *Applying*

[CON-LO-S28] Describe the purpose and function of honeypots, honeynets, and padded cells within an overall network defense strategy. *Understanding*

[CON-LO-S29] Operate commonly used monitoring network tools and devices. *Applying*

[CON-LO-S30] Analyze logs associated with commonly used monitoring network tools and devices. *Analyzing*

[CON-LO-S31] Manipulate a commonly used network protocol analyzer to capture and analyze packets flowing through the network. *Applying*

[CON-LO-S32] Discuss threat hunting, attack pattern detection, and similar network traffic analysis techniques. *Understanding*

[CON-LO-S33] Use tools and techniques for finding and mitigating vulnerabilities through looking at potential weaknesses. *Applying*

[CON-LO-S34] Discuss tools and techniques for limiting the flow of packets based upon rules for packet content, including network admission control techniques; machine certificates; machine profiling techniques; and probing with SNMP, DHCP, HTTP, DNS, LDAP, and NMAP. *Understanding*

[CON-LO-S35] Diagram a Demilitarized Zone (DMZ) and its components, including isolated networks and special servers, such as proxy servers, mail servers, and web servers. *Applying*

[CON-LO-S36] Develop procedures that are used to operate the network in light of applicable security policies and business requirements. *Creating*

[CON-LO-S37] Use penetration testing tools and techniques to test the network by attempting to exploit vulnerabilities. *Applying*

[CON-LO-S38] Discuss the role of machine learning to detect patterns in attack vectors, such as in proactive threat hunting. *Understanding*

System Security

Definition

Focuses on the security aspects of systems that are composed of components and connections, and use software.

Understanding the security of a system requires viewing it not only as a set of components and connections, but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems.

Essential Competencies

- [SYS-E1] Discuss security aspects of system management in common system architectures. *Understanding*
- [SYS-E2] Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. *Analyzing*
- [SYS-E3] Perform system security testing with an understanding of normal, secure operation, and document results. *Applying*

Supplemental Competencies

- [SYS-S1] Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal. *Evaluating*
- [SYS-S2] Outline a security threat model and how system monitoring tools and mechanisms can be used. *Analyzing*
- [SYS-S3] Examine appropriate models for managing authentication, access control and authorization across systems in an organization. *Analyzing*
- [SYS-S4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying*
- [SYS-S5] Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis. *Understanding*
- [SYS-S6] Construct virtual environments including disk and memory structures to meet organization needs. *Creating*

Knowledge Units

System Thinking
System Management
System Access and Control
System Testing
Common System Architectures

System Security Learning Outcomes

System Thinking

Essential Learning Outcomes

[SYS-LO-E01] Describe how components work together to secure a system. *Understanding*
[SYS-LO-E02] Apply a security threat model to a given scenario. *Applying*
[SYS-LO-E03] Explain fundamental principles of secure systems. *Understanding*

Supplemental Learning Outcomes

[SYS-LO-S01] Discuss the components used to secure special-purpose systems. *Understanding*
[SYS-LO-S02] Justify security requirements throughout the system development lifecycle. *Evaluating*

System Management

Essential Learning Outcomes

[SYS-LO-E04] Describe the components of a security policy for a system. *Understanding*
[SYS-LO-E05] Discuss methods and tools for system monitoring and recovery. *Understanding*
[SYS-LO-E06] Describe the use of vulnerability reports and patching in maintaining the security of a system. *Understanding*

Supplemental Learning Outcomes

[SYS-LO-S03] Carry out elements of an automation plan, such as data mining, machine learning, and related techniques. *Applying*
[SYS-LO-S04] Examine reasons for commissioning, decommissioning, and disposing of a system under attack. *Analyzing*
[SYS-LO-S05] Contrast various system monitoring tools and mechanisms. *Analyzing*
[SYS-LO-S06] Evaluate various system recovery methods. *Evaluating*
[SYS-LO-S07] Implement defenses to protect a system against an insider threat. *Evaluating*
[SYS-LO-S08] Apply a process to document baseline system functions. *Understanding*

System Access and Control

Essential Learning Outcomes

[SYS-LO-E07] Contrast various system-related methods for authentication, authorization, and access control. *Analyzing*
[SYS-LO-E08] Write documentation for a system with security considerations in mind. *Applying*
[SYS-LO-E09] Differentiate among types of malware. *Understanding*
[SYS-LO-E10] Describe how malicious activity can be detected, including the use of intrusion detection systems. *Understanding*

[SYS-LO-E11] Describe potential system attacks and the actors that might perform them. *Understanding*

Supplemental Learning Outcomes

[SYS-LO-S09] Critique the strengths and weaknesses of various access control models and mechanisms. *Evaluating*

[SYS-LO-S10] Investigate models for managing authorization across systems. *Applying*

[SYS-LO-S11] Analyze logs to detect intruders. *Analyzing*

[SYS-LO-S12] Carry out a penetration test on a system. *Applying*

[SYS-LO-S13] Analyze system requirements for performing forensic analysis. *Analyzing*

[SYS-LO-S14] Paraphrase legal ramifications that can affect day-to-day network administration, such as litigation holds. *Understanding*

[SYS-LO-S15] Discuss recovery and resilience mechanisms that help ensure system availability. *Understanding*

System Testing

Essential Learning Outcomes

[SYS-LO-E12] Execute system security test protocols. *Applying*

[SYS-LO-E13] Discuss the differences between unit testing and system testing. *Understanding*

Supplemental Learning Outcomes

[SYS-LO-S16] Examine system requirements to determine whether they meet system objectives. *Analyzing*

[SYS-LO-S17] Critique plans for testing secure systems in a given scenario. *Evaluating*

Common System Architectures

Essential Learning Outcomes

[SYS-LO-E14] Discuss system security issues related to common system architectures such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems. *Understanding*

Supplemental Learning Outcomes

[SYS-LO-S18] Construct virtual environments including disk and memory structures. *Creating*

[SYS-LO-S19] Describe the components of a SCADA industrial control system. *Understanding*

[SYS-LO-S20] Diagram an Internet of Things system. *Applying*

Human Security

Definition

Focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.

Humans have responsibility to ensure the confidentiality, integrity, and availability (CIA) of their organizational and personal computer systems.

Essential Competencies

- [HUM-E1] Discuss identity management in the context of attacks and mitigations. *Understanding*
- [HUM-E2] Analyze the security of an individual's data and privacy in the context of an organization and in their personal lives. *Analyzing*
- [HUM-E3] Describe trends in human behavior which pose risks to individual and organizational privacy and security. *Understanding*

Supplemental Competencies

- [HUM-S1] Analyze a variety of physical access controls. *Analyzing*
- [HUM-S2] Use a variety of tools and techniques to detect and mitigate social engineering threats. *Applying*
- [HUM-S3] Examine techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms. *Analyzing*

Knowledge Units

Identity Management
Social Engineering
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms
Awareness and Understanding
Personal Data Privacy and Security
Usable Security and Privacy

Data | Software | Component | Connection | System | **Human** | Organizational | Societal

Human Security Learning Outcomes

Identity Management

Essential Learning Outcomes

[HUM-LO-E01] Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and multifactor systems. *Analyzing*

[HUM-LO-E02] Discuss attacks and mitigations associated with identity management, such as brute force attacks, spoofing attacks, strong password policies, and restricted access systems. *Understanding*

Supplemental Learning Outcomes

[HUM-LO-S01] Examine various physical assets access controls, such as Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control(RAC), and Roles-based Access Control (RBAC). *Analyzing*

[HUM-LO-S02] Explain the benefits and challenges of identity management as a service (IaaS). *Understanding*

Social Engineering

Essential Learning Outcomes

[HUM-LO-E03] Compare various social engineering attacks, such as phishing, vishing, email compromise, and baiting, along with suitable mitigations. *Analyzing*

[HUM-LO-E04] Describe psychological and behavioral factors which contribute to social engineering attacks, such as adversarial thinking, cognitive biases, and trust building. *Understanding*

Supplemental Learning Outcomes

[HUM-LO-S03] Use various tools and approaches to detect and/or mitigate different social engineering threats, such as using email filtering and blacklists. *Applying*

Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms

Essential Learning Outcomes

[HUM-LO-E05] Analyze one's personal social media use with respect to organizational policies, rules, and ethical norms. *Analyzing*

Supplemental Learning Outcomes

[HUM-LO-S04] Summarize various ways in which systems are misused and users misbehave to cause intentional and unintentional threats and attacks, such as unintentional system misuse, naïve behavior, and cyber bullying. *Understanding*

[HUM-LO-S05] Debate methods and techniques to persuade individuals to follow rules, policies, and ethical norms related to cybersecurity. *Evaluating*

[HUM-LO-S06] Summarize methods and techniques to employ when an individual is uncertain how to respond to a given cybersecurity situation. *Understanding*

[HUM-LO-S07] Investigate privacy theories from social psychology and social science, including tradeoffs and risks. *Applying*

[HUM-LO-S08] Debate various organizational rules and policies, and ethical norms related to personal social media privacy and security. *Evaluating*

Awareness and Understanding

Essential Learning Outcomes

[HUM-LO-E06] Carry out formal or informal security education, training, and awareness program tasks. *Applying*

Supplemental Learning Outcomes

[HUM-LO-S09] Compare various mental models and their impact on how users perceive, judge, communicate, and respond to cybersecurity risks. *Analyzing*

[HUM-LO-S10] Evaluate security education, training, and awareness program tasks. *Evaluating*

[HUM-LO-S11] Assess individual responsibilities related to cyber hygiene, such as password creation, maintenance, and storage; mitigation tools; identification and use of safe websites; and identifying and using appropriate privacy settings. *Evaluating*

Personal Data Privacy and Security

Essential Learning Outcomes

[HUM-LO-E07] Evaluate potential risks to personal data privacy and security for a given scenario. *Evaluating*

Supplemental Learning Outcomes

[HUM-LO-S12] Examine various types of sensitive personal data (SPD) and associated risks and impact of misuse. *Analyzing*

[HUM-LO-S13] Evaluate how personal tracking techniques and an individual's digital footprint impact privacy and security. *Evaluating*

Usable Security and Privacy

Essential Learning Outcomes

[HUM-LO-E08] Describe the impact usability and user experience have on security and privacy, including compliance with laws such as HIPAA and FERPA. *Understanding*

[HUM-LO-E09] Describe human factors which impact privacy and security, such as the psychology of adversarial thinking, resistance to biometric authentication, and the economics of security. *Understanding*

Supplemental Learning Outcomes

[HUM-LO-S14] Describe the benefits and challenges of following cybersecurity design guidelines, such as providing secure defaults, and reducing unintentional security and privacy errors. *Understanding*

Organizational Security

Definition

Focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission.

Organizations have responsibility to meet the needs of many constituencies and those needs must inform risk management, security governance, business continuity, and security program management.

Essential Competencies

- [ORG-E1] Describe policies, procedures, and ethical considerations to protect information security. *Understanding*
- [ORG-E2] Describe security features in operating system and database administration in a local or cloud environment. *Understanding*
- [ORG-E3] Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters. *Understanding*
- [ORG-E4] Describe physical security features to protect an organization's computing and information resources. *Understanding*

Supplemental Competencies

- [ORG-S1] Analyze risks to information assets in an organization and communicate them to stakeholders. *Analyzing*
- [ORG-S2] Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. *Evaluating*
- [ORG-S3] Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. *Analyzing*
- [ORG-S4] Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. *Understanding*

Knowledge Units

Risk Management
Security Governance & Policy
Analytical Tools
Systems Administration
Cybersecurity Planning
Business Continuity, Disaster Recovery, and Incident Management
Security Program Management
Personnel Security

Data | Software | Component | Connection | System | Human | **Organizational** | Societal

Organizational Security Learning Outcomes

Risk Management

Essential Learning Outcomes

[ORG-LO-E01] Classify organizational risk factors due to security failure, such as financial loss, operational disruption, and reputational damage. *Understanding*

[ORG-LO-E02] Describe the components that contribute to an organization's security posture. *Understanding*

Supplemental Learning Outcomes

[ORG-LO-S01] Distinguish information assets in an organization and threats to those assets. *Analyzing*

[ORG-LO-S02] Analyze risks in an organization including the potential for both accidental and intentional losses. *Analyzing*

[ORG-LO-S03] Describe the risk of insider threat in an organization, including motive-means-opportunity behaviors. *Understanding*

[ORG-LO-S04] Apply a risk management model to measure, evaluate, and communicate risk to stakeholders. *Applying*

[ORG-LO-S05] Outline risk control in an organization using the categories of Avoid, Reduce, Transfer, and Accept. *Analyzing*

Security Governance & Policy

Essential Learning Outcomes

[ORG-LO-E03] Perform tasks in compliance with information security governance and policy. *Applying*

[ORG-LO-E04] Summarize relevant independent and government-sponsored cybersecurity frameworks. *Understanding*

[ORG-LO-E05] Discuss the importance of ethical codes of conduct for cybersecurity professionals and their organizations. *Understanding*

Supplemental Learning Outcomes

[ORG-LO-S06] Examine the cost of cybersecurity to an organization. *Analyzing*

Analytical Tools

Supplemental Learning Outcomes

[ORG-LO-S07] Use tools to collect and analyze data to generate security intelligence including threats and adversary capabilities. *Applying*

Systems Administration

Essential Learning Outcomes

[ORG-LO-E06] Describe components that secure the operating system and system database from vulnerabilities. *Understanding*

[ORG-LO-E07] Demonstrate administrative functions, such as using group membership to assign permissions. *Understanding*

[ORG-LO-E08] Discuss security features that are embedded within a cloud environment. *Understanding*

Supplemental Learning Outcomes

[ORG-LO-S08] Decompose administrative procedures for protecting the physical system from attack. *Analyzing*

[ORG-LO-S09] Assess processes that ensure availability of system access and functions. *Evaluating*

[ORG-LO-S10] Implement hardening techniques to protect the operating system. *Applying*

Cybersecurity Planning

Supplemental Learning Outcomes

[ORG-LO-S11] Apply Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis in an organization. *Applying*

Business Continuity, Disaster Recovery, and Incident Management

Essential Learning Outcomes

[ORG-LO-E09] Explain the components of a business continuity plan, such as contingency planning, incident response, emergency response, backup, and recovery efforts. *Understanding*

[ORG-LO-E10] Describe a disaster recovery plan that ensures minimal down time and quick recovery. *Understanding*

Security Program Management

Supplemental Learning Outcomes

[ORG-LO-S12] Perform project management tasks that provide for security of data. *Applying*

[ORG-LO-S13] Analyze the meaning and use of various security metrics used in protecting the network. *Analyzing*

[ORG-LO-S14] Describe the use of quality assurance and quality control to prevent mistakes and increase the quality of a system. *Understanding*

Personnel Security

Supplemental Learning Outcomes

[ORG-LO-S15] Describe the proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool in various contexts, such as physical security, password security, and social engineering. *Understanding*

[ORG-LO-S16] Classify components of third party security services. *Understanding*

[ORG-LO-S17] Discuss components that ensure the protection of personally identifiable information. *Understanding*

Societal Security

Definition

Focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse.

Cybercrime, law, ethics, policy, privacy and their relation to each other are the key concepts of this knowledge area. The threat of cybercrime across global society is serious and growing. Laws, ethics and policies are vital to the security of corporate and government secrets and assets, as well as to the protection of individual privacy and identity.

Essential Competencies

- [SOC-E1] Interpret applicable cyber policies and ethics for a given scenario. *Understanding*
- [SOC-E2] Summarize applicable national, international, and global security policies and legislation. *Understanding*
- [SOC-E3] Distinguish social dynamics of computer attackers in a global context. *Analyzing*

Supplemental Competencies

- [SOC-S1] Attribute specific cyber laws and potential economic impact for a given cybercrime scenario. *Analyzing*
- [SOC-S2] Compare different cyber ethics theories that impact on individuals and society. *Analyzing*

Knowledge Units

Cybercrime
Cyber Law
Cyber Ethics
Cyber Policy
Privacy

Data | Software | Component | Connection | System | Human | Organizational | **Societal**

Societal Security Learning Outcomes

Cybercrime

Essential Learning Outcomes

[SOC-LO-E01] Categorize different types of cybercrime. *Analyzing*

[SOC-LO-E02] Investigate the economic impact of cybersecurity and cybercrime for a given city, state, or nation. *Applying*

Supplemental Learning Outcomes

[SOC-LO-S01] Categorize challenges associated with the enforcement and prosecution of cybercrime. *Analyzing*

Cyber Law

Essential Learning Outcomes

[SOC-LO-E03] Describe various categories of global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property. *Understanding*

Supplemental Learning Outcomes

[SOC-LO-S02] Investigate legislative and executive powers relevant to cyber law, along with those addressed in constitutional amendments. *Applying*

[SOC-LO-S03] Examine the core doctrines of intellectual property in cyber law. *Analyzing*

[SOC-LO-S04] Describe privacy law as it relates to contemporary dilemmas involving social media, electronic surveillance, and Internet privacy. *Understanding*

[SOC-LO-S05] Explain a data security or privacy law in the context of a recent event. *Understanding*

[SOC-LO-S06] Apply case law and common law to current legal dilemmas related to computer hacking. *Applying*

Cyber Ethics

Essential Learning Outcomes

[SOC-LO-E04] Analyze given cyber ethics scenarios, including topics on codes of conduct and professional ethics. *Analyzing*

[SOC-LO-E05] Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war. *Analyzing*

Supplemental Learning Outcomes

[SOC-LO-S07] Compare ethical practices and legal codes for given scenarios. *Analyzing*

[SOC-LO-S08] Discuss ethical issues related to nation-state conflicts, including cyber espionage and Just War Theory. *Understanding*

Cyber Policy

Essential Learning Outcomes

[SOC-LO-E06] Discuss cyber policies and related liability issues. *Understanding*

Supplemental Learning Outcomes

[SOC-LO-S09] Examine the cost of cybersecurity to a nation. *Analyzing*

Privacy

Essential Learning Outcomes

[SOC-LO-E07] Contrast privacy and transparency from a societal perspective, including goals and tradeoffs. *Analyzing*

[SOC-LO-E08] Investigate cultural differences in the existence of privacy norms and boundaries. *Applying*

Supplemental Learning Outcomes

[SOC-LO-S10] Debate human right to privacy contrasting the need for transparency. *Evaluating*

[SOC-LO-S11] Explain conditions for ethical and lawful use of privacy enhancing technology. *Understanding*

[SOC-LO-S12] Analyze potential solutions that address circumstances when data privacy is compromised in a societal context. *Analyzing*

References

[1] ABET. 2018. *ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs*. https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/ Accessed June 2019.

[2] American Association of Community Colleges. 2019. *AACC Fast Facts 2019*. https://www.aacc.nche.edu/wp-content/uploads/2019/05/AACC2019FactSheet_rev.pdf. Accessed June 2019.

[3] American Association of Community Colleges. *Research*. https://www.aacc.nche.edu/research-trends/. Accessed June 2019.

[4] Association for Computing Machinery (ACM). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics. Accessed June 2019.

[5] ACM Committee for Computing Education in Community Colleges. 2017. *Computer Science Curricular Guidance for Associate-Degree Transfer Programs with Infused Cybersecurity*. ACM, New York, NY. DOI: http://dx.doi.org/10.1145/3108241.

[6] ACM Committee for Computing Education in Community Colleges. 2014. *Information Technology Competency Model of Core Learning Outcomes and Assessment for Associate-Degree Curriculum*. ACM, New York, NY, USA. DOI: http://dx.doi.org/10.1145/2686614.

[7] Lorin Anderson, David Krathwohl, et al. 2001. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. Addison Wesley Longman, Inc.

[8] Benjamin Bloom. 1956. *Taxonomy of Educational Objectives: The Classification of Educational Goals*. Longmans, Green.

[9] Cybersecurity Ventures. *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021*. 2018. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. Accessed November 2019.

[10] Cyberseek.org. *Cybersecurity Supply/Demand Interactive Heat Map*. https://www.cyberseek.org/heatmap.html Accessed November 2019.

[11] Peter Denning, Matti Tedre. 2019. *Computational Thinking*. MIT Press.

[12] EC-Council. *EC-Council Code of Ethics*. https://www.eccouncil.org/code-of-ethics/. Accessed June 2019.

[13] Stephen Frezza, Mats Daniels, Arnold Pears, Åsa Cajander, Viggo Kann, Amanpreet Kapoor, Roger McDermott, Anne-Kathrin Peters, Mihaela Sabin, and Charles Wallace. 2018. Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '18 Companion), July 2-4, 2018, Larnaca, Cyprus*. ACM, New York, NY, USA, 27 pages. https://doi.org/10.1145/3293881.3295782

[14] Information Systems Security Association. *ISSA Code of Ethics*. https://www.issa.org/page/CodeofEthics. Accessed June 2019.

[15] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. ACM, New York, NY, USA. DOI: https://dx.doi.org/10.1145/3184594.

[16] National Initiative for Cybersecurity Education (NICE). 2017. *NICE Cybersecurity Workforce Framework*. NIST Special Publication 800-181. DOI: https://doi.org/10.6028/NIST.SP.800-181.

[17] Nationwide Mutual Insurance Company. *Nearly Half of Business Owners Have Been Victims of Cyberattacks - But Didn't Know It*. 2017. https://www.nationwide.com/personal/about-us/newsroom/press-release?title=100917-cyber-security. Accessed February 2019.

[18] NSA and DHS, *Centers of Academic Excellence in Cyber Defense (CAE-CD) 2019 Knowledge Units*, https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf. Accessed June 2019.

[19] U.S. Bureau of Labor Statistics. *Information Security Analysts*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1. Accessed November 2019.

Appendix A: Competencies by NICE Framework Category

NICE Analyze

Knowledge Area	Competency
Cross-Cutting	[CC-1] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability.
Human Security	[HUM-E2] Analyze the security of an individual's data and privacy in the context of an organization and in their personal lives
	[HUM-E3] Describe trends in human behavior which pose risks to individual and organizational privacy and security.
Organizational Security	[ORG-S1] Analyze risks to information assets in an organization and communicate them to stakeholders.

NICE Collect and Operate

Knowledge Area	Competency
Data Security	[DAT-S2] Outline complex technical concepts to technical and non-technical audiences as they relate to data security.
System Security	[SYS-S2] Outline a security threat model and how system monitoring tools and mechanisms can be used.

NICE Investigate

Knowledge Area	Competency
Data Security	[DAT-S1] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment.
Societal Security	[SOC-E3] Distinguish social dynamics of computer attackers in a global context.
	[SOC-S2] Compare different cyber ethics theories that impact on individuals and society.

NICE Operate and Maintain

Knowledge Area	Competency
Cross-Cutting	[CC-3] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them.
Data Security	[DAT-E4] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks.
Component Security	[COM-E2] Perform security testing for given components within a system.
Connection Security	[CON-E1] Illustrate the construction and proper configuration of computer networks which adhere to current industry standards and organizational guidelines.
	[CON-S1] Examine characteristics of commonly used physical networking media and interfaces.
	[CON-S3] Implement appropriate defenses throughout an enterprise to harden the network against attackers.
	[CON-S4] Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines.
System Security	[SYS-E1] Discuss security aspects of system management in common system architectures.

	[SYS-E2] Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another
	[SYS-E3] Perform system security testing with an understanding of normal, secure operation, and document results.
	[SYS-S1] Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal.
	[SYS-S3] Examine appropriate models for managing authentication, access control and authorization across systems in an organization.
	[SYS-S4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems.
	[SYS-S5] Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis.
	[SYS-S6] Construct virtual environments including disk and memory structures to meet organization needs.
Organizational Security	[ORG-E1] Describe policies, procedures, and ethical considerations to protect information security.
	[ORG-E2] Describe security features in operating system and database administration in a local or cloud environment.
	[ORG-E3] Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters.
	[ORG-S2] Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization.
	[ORG-S3] Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data.

NICE Oversee and Govern

Knowledge Area	Competency
Software Security	[SOF-S5] Examine social and legal aspects of software development from a security perspective.
Human Security	[HUM-S3] Examine techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms.
Organizational Security	[ORG-S4] Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool.
Societal Security	[SOC-E1] Interpret applicable cyber policies and ethics for a given scenario.
	[SOC-E2] Summarize applicable national, international, and global security policies and legislation.
	[SOC-S1] Attribute specific cyber laws and potential economic impact for a given cybercrime scenario.

NICE Protect and Defend

Knowledge Area	Competency
Cross-Cutting	[CC-2] Assess and respond appropriately to various risks which can affect the expected operation of information systems.
	[CC-4] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate.
	[CC-5] Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem.
Data Security	[DAT-E1] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization.

	[DAT-E2] Discuss forensically sound collection and acquisition of digital evidence.
	[DAT-E3] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents.
	[DAT-E5] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime.
Software Security	[SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario.
Component Security	[COM-E1] Discuss vulnerabilities and mitigations of system components throughout their lifecycle.
	[COM-S1] Analyze how component security features impact systems, such as software and firmware updates
Connection Security	[CON-E2] Investigate the impact of various connection and transmission attacks on network hardware and software.
	[CON-S2] Distinguish vulnerabilities and example exploits as they apply to network services, architectures, and protocols.
Human Security	[HUM-E1] Discuss identity management in the context of attacks and mitigations.
	[HUM-S1] Analyze a variety of physical access controls.
	[HUM-S2] Use a variety of tools and techniques to detect and mitigate social engineering threats.
Organizational Security	[ORG-E4] Describe physical security features to protect an organization’s computing and information resources.

NICE Securely Provision

Knowledge Area	**Competency**
Software Security	[SOF-E1] Write secure code with appropriate documentation for a software system and its related data.
	[SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle.

	[SOF-S1] Implement isolation to secure a process or application.
	[SOF-S2] Discuss the relationship between an organization’s mission and secure software design.
	[SOF-S3] Write software specifications, including security specifications, for a given process or application
	[SOF-S4] Assess a given test plan, from a security perspective.
	[SOF-S6] Develop user documentation for software installation with security appropriately included.

Appendix B: Competencies Mapped to CAE KUs

Many schools with cybersecurity programs are interested in the designation by the NSA (National Security Agency) and DHS (Department of Homeland Security) of Center of Academic Excellence (CAE) in Cybersecurity [18]. These Cyber2yr2020 guidelines have been mapped to the CAE knowledge units (KUs) in the Foundational Core as well as the Technical Core, which are the two areas that two-year technically-oriented cybersecurity programs may be interested in mapping their curriculum to. Each CAE KU consists of Outcomes and Topics. The CAE KUs in the Foundational Core and Technical Core are the following [18]:

CAE Foundational Core KUs:

- Cybersecurity Foundations (CSF)
- Cybersecurity Principles (CSP)
- IT Systems Components (ISC)

CAE Technical Core KUs:

- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)

The Cyber2yr2020 competencies and learning outcomes map to **100%** of the outcomes and topics in the Foundational Core and Technical Core CAE KUs. The full mapping can be found on the CCECC web site at ccecc.acm.org/guidance/cybersecurity/classification-mappings. In this appendix we present a few examples from the mapping.

The table below shows, for the Cyber2yr2020 Cross-Cutting Competencies, the Outcomes (O) and Topics (T) from the CAE KUs to which each competency maps.

Cyber2yr2020 Competency	**CAE KU Outcome (O) or Topic (T)**
[CC-1] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*	**CSF Cybersecurity Foundations** O1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security. O5. Properly use the vocabulary associated with cybersecurity. T10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy. **CSP Cybersecurity Principles** O1. Define the principles of cybersecurity.

	ISC IT Systems Components O4. Properly use the Vocabulary associated with cyber security.
[CC-2] Assess and respond appropriately to various risks which can affect the expected operation of information systems. *Evaluating*	**CSF Cybersecurity Foundations** T4. Basic risk assessment. **NDF Network Defense** T3. Network Operations. a. Network security monitoring; b. Network traffic analysis
[CC-3] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. *Applying*	**CSP Cybersecurity Principles** O4. Given a specific scenario, identify the design principles involved or needed. **ISC IT Systems Components** O2. Describe the basic security implications of modern computing environments. **BCY Basic Cryptography** O4 Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc. **NDF Network Defense** T1. Outline concepts of network defense, such as a. Defense in depth; b. Network attacks; c. Network hardening; d. Minimizing exposure (attack surface and vectors)
[CC-4] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. *Applying*	**CSF Cybersecurity Foundations** T15. Appropriate Countermeasures
[CC-5] Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. *Understanding*	**BCY Basic Cryptography** O1. Students will be able to identify the elements of a cryptographic system. **OSC Operating System Concepts** O1. Describe the role and basic functions of an operating system, and how operating systems interact with hardware and software applications.

The table below shows, for the CAE Foundational KU Cybersecurity Foundations (CSF), the competencies and learning outcomes from Cyber2yr2020 that each CSF Outcome (O) maps to.

CAE KU Outcomes and Topics	**Cyber2yr2020 KA - KU Competency or Learning Outcome**
CSF Cybersecurity Foundations	
O1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.	**Cross Cutting** [CC-1] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing* **System Security - System Thinking (E)** Explain fundamental principles of secure systems. *Understanding*
O2. Describe potential system attacks and the actors that might perform them.	**System Security - System Access and Control** Describe potential system attacks and the actors that might perform them. *Understanding*
O3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.	**System Security** [SySS-4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying*
O4. Describe appropriate measures to be taken should a system compromise occur.	**System Security** [SYS-S4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying*
O5. Properly use the Vocabulary associated with cyber security.	**Cross Cutting** [CC-1] Outline via appropriate methods, and using industry-standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*

Appendix C: Rubrics

Rubrics are presented for all of the Essential learning outcomes, organized by knowledge area/domain. The rubric is three-tiered, with the middle tier, Developed, being the learning outcome itself. The lower tier, Emerging, represents an emerging grasp of the desired outcome, without yet achieving it. The higher tier, Highly Developed, represents going beyond the learning outcome.

Data Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Cryptography		
Summarize cryptographic protocols, tools, and techniques. *Understanding*	Analyze which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation. *Analyzing* [DAT-LO-E01]	Justify which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation for a given scenario. *Evaluating*
Explain symmetric and asymmetric algorithms. *Understanding*	Apply symmetric and asymmetric algorithms as appropriate for a given scenario. *Applying* [DAT-LO-E02]	Compare the tradeoffs of symmetric and asymmetric algorithms for a given scenario. *Analyzing*
Explain hash functions for checking integrity and protecting authentication data. *Understanding*	Investigate hash functions for checking integrity and protecting authentication data. *Applying* [DAT-LO-E03]	Examine hash functions for checking integrity and protecting authentication data. *Analyzing*
Describe some historical ciphers. *Understanding*	Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher,	Contrast historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill

	and Enigma machine, to encrypt and decrypt data. *Applying* [DAT-LO-E04]	cipher, and Enigma machine, for encrypting and decrypting data. *Analyzing*
Digital Forensics		
Define the concept of digital forensics. *Remembering*	Discuss the concept, need, and value of digital forensics. *Understanding* [DAT-LO-E05]	Illustrate the concept, need, and value of digital forensics. *Applying*
Recognize components of a digital investigation, sources of digital evidence, and limitations of forensics. *Remembering*	Describe components of a digital investigation, sources of digital evidence, limitations of forensics, and ethical considerations. *Understanding* [DAT-LO-E06]	Debate sources of digital evidence, limitations of forensics, and ethical considerations. *Evaluating*
List key rules, laws, policies, and procedures that impact digital forensics. *Remembering*	Discuss key rules, laws, policies, and procedures that impact digital forensics. *Understanding* [DAT-LO-E07]	Debate key rules, laws, policies, and procedures that impact digital forensics. *Evaluating*
State the purpose of the chain of custody for digital evidence. *Remembering*	Explain how to preserve the chain of custody for digital evidence. *Understanding* [DAT-LO-E08]	Carry out the steps necessary to preserve the chain of custody for digital evidence. *Applying*
Describe fundamental incident response functions including detecting, responding, and recovering from security incidents. *Understanding*	Perform fundamental incident response functions including detecting, responding, and recovering from security incidents. *Applying* [DAT-LO-E09]	Integrate fundamental incident response functions including detecting, responding, and recovering from security incidents. *Analyzing*
Data Integrity and Authentication		

Describe the concepts and techniques to achieve authentication, authorization, access control, and data integrity. *Understanding*	Contrast the concepts and techniques to achieve data integrity, authentication, authorization, and access control. *Analyzing* [DAT-LO-E10]	Justify the concepts and techniques to achieve authentication, authorization, access control, and data integrity. *Evaluating*
Recognize the benefits and challenges of multifactor authentication. *Remembering*	Summarize the benefits and challenges of multifactor authentication. *Understanding* [DAT-LO-E11]	Illustrate the benefits and challenges of multifactor authentication. *Applying*
Explain one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools. *Remembering*	Execute one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools. *Applying* [DAT-LO-E12]	Examine one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools. *Analyzing*
Summarize basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers. *Understanding*	Apply basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers. *Applying* [DAT-LO-E13]	Analyze basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers. *Analyzing*
Access Control		
Recognize access control best practices, such as separation of duties, job rotation, and clean desk policy. *Remembering*	Describe access control best practices, such as separation of duties, job rotation, and clean desk policy. *Understanding* [DAT-LO-E14]	Illustrate access control best practices, such as separation of duties, job rotation, and clean desk policy. *Applying*

Define physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction. *Remembering*	Discuss physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction. *Understanding* [DAT-LO-E15]	Outline physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction. *Analyzing*
Describe data access control to manage identities, credentials, privileges, and related access. *Understanding*	Implement data access control to manage identities, credentials, privileges, and related access. *Applying* [DAT-LO-E16]	Choose data access control to manage identities, credentials, privileges, and related access. *Evaluating*
List different types of identities. *Understanding*	Differentiate among the different types of identities, such as federated identities. *Understanding* [DAT-LO-E17]	Distinguish among the different types of identities, such as federated identities. *Analyzing*
Recognize access control models, including role-based, rule-based, and attribute-based. *Remembering*	Differentiate access control models, including role-based, rule-based, and attribute-based. *Understanding* [DAT-LO-E18]	Compare access control models, including role-based, rule-based, and attribute-based. *Analyzing*
Secure Communication Protocols		
Define end-to-end data security. *Remembering*	Explain end-to-end data security. *Understanding* [DAT-LO-E19]	Outline end-to-end data security. *Understanding*
Demonstrate important application and transport layer protocols. *Understanding*	Illustrate important application and transport layer protocols, such as HTTP, HTTPS, SSH, SSL/TLS, IPsec and VPN technologies. *Applying* [DAT-LO-E20]	Examine important application and transport layer protocols, such as HTTP, HTTPS, SSH, SSL/TLS, IPsec and VPN technologies. *Analyzing*
Cryptanalysis		

List various cryptanalysis attacks. *Remembering*	Classify various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force. *Understanding* [DAT-LO-E21]	Carry out various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force. *Applying*
Data Privacy		
Discuss various ways that privacy can be jeopardized by using contemporary technology, including social media. *Understanding*	Examine various ways that privacy can be jeopardized by using contemporary technology, including social media. *Analyzing* [DAT-LO-E22]	Appraise various ways that privacy can be jeopardized by using contemporary technology, including social media. *Evaluating*
Information Storage Security		
Recognize storage device encryption implemented at the hardware and software levels. *Remembering*	Discuss storage device encryption implemented at the hardware and software levels. *Understanding* [DAT-LO-E23]	Compare storage device encryption implemented at the hardware and software levels. *Analyzing*
Describe techniques for data erasure. *Understanding*	Contrast techniques for data erasure and their limitations in implementation. *Analyzing* [DAT-LO-E24]	Critique techniques for data erasure and their limitations in implementation. *Evaluating*

Software Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Fundamental Principles		

Describe fundamental design principles for system and application software. *Understanding*	Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. *Applying* [SOF-LO-E01]	Evaluate the fundamental design principles used, including least privilege, open design, and abstraction, for a given software development scenario. *Evaluating*
Classify access decisions and permissions based on explicit need. *Understanding*	Execute access decisions and permissions based on explicit need. *Applying* [SOF-LO-E02]	Analyze access decisions and permissions based on explicit need. *Analyzing*
Describe a simple secure application design. *Understanding*	Diagram a simple secure application design. *Applying* [SOF-LO-E03]	Develop a simple secure application design for a given scenario. *Creating*
Summarize select aspects of software security controls in an open design. *Understanding*	Explain software security controls in an open design. *Understanding* [SOF-LO-E04]	Use software security controls in an open design. *Applying*
Explain techniques for reducing the levels of abstraction to a single layer of abstraction, for a given piece of software. *Understanding*	Modify the levels of abstraction in a given piece of software to provide single layer abstraction whenever possible. *Applying* [SOF-LO-E05]	Create a simple software system or application which has a single layer of abstraction. *Creating*
Summarize how software can be designed as a system of secure co-operating components. *Understanding*	Implement software as a system of secure co-operating components. *Applying* [SOF-LO-E06]	Develop a simple software system with secure co-operating components. *Creating*
Recognize the role of session management in securing web-based applications and services. *Remembering*	Explain session management and its role in securing web-based applications and services. *Understanding* [SOF-LO-E07]	Implement secure session management in a web-based application or service. *Applying*
Design		

List select security requirements in software design for a given scenario. *Remembering*	Explain security requirements in software design for a given scenario. *Understanding* [SOF-LO-E08]	Write security requirements in software design for a given scenario. *Applying*
Explain the waterfall and agile development models' relationship to software security. *Understanding*	Examine the waterfall and agile development models' relationship to software security. *Analyzing* [SOF-LO-E09]	Design secure software using the waterfall or agile development model. *Creating*
Name programming languages which have type-safe issues. *Remembering*	Describe what makes a programming language type-safe. *Understanding* [SOF-LO-E10]	Implement a given piece of software using type-safe features of a programming language. *Applying*
Implementation		
List a few implementation issues which may arise in a secure software life cycle. *Remembering*	Discuss significant implementation issues in a secure software life cycle. *Understanding* [SOF-LO-E11]	Diagram implementation issues in a secure software life cycle, for a given scenario. *Applying*
Explain how secure code can perform input validation and prevent buffer overflow, integer range violations, and input type violations. *Applying*	Write secure code which implements input validation and prevents buffer overflow, integer range violations, and input type violations. *Applying* [SOF-LO-E12]	Examine security vulnerabilities in a given piece of software in relation to improper input validation, buffer overflow, integer range violations, and input type violations. *Analyzing*
Describe appropriate restrictions to process privileges. *Understanding*	Apply appropriate restrictions to process privileges. *Applying* [SOF-LO-E13]	Analyze appropriate restrictions to process privileges, for a given scenario. *Analyzing*
Describe features of appropriate error handling and user notification. *Understanding*	Implement appropriate error and exception handling and user notification. *Applying* [SOF-LO-E14]	Examine appropriate error and exception handling and user notification, for a given scenario. *Analyzing*

Implement a secure application or script using defensive programming techniques. *Applying*	Develop a secure application or script using defensive programming techniques. *Creating* [SOF-LO-E015]	Develop a complex secure application or script using defensive programming techniques. *Creating*
Analysis and Testing		
Summarize generic security-related testing procedures. *Understanding*	Carry out security-related testing procedures, for a given piece of software. *Applying* [SOF-LO-E16]	Examine security-related testing procedures to be used for a given piece of software. *Analyzing*
Define static and dynamic software analysis and testing. *Remembering*	Explain the difference between static and dynamic software analysis and testing. *Understanding* [SOF-LO-E17]	Carry out static and dynamic software analysis and testing, for a given piece of software. *Applying*
Deployment and Maintenance		
Summarize security-related tasks related to software installation, configuration, maintenance, and patching. *Understanding*	Perform software installation, configuration, maintenance, and patching tasks in a secure manner. *Applying* [SOF-LO-E18]	Evaluate software installation, configuration, maintenance, and patching tasks from a security perspective. *Applying*
List a few potential security implications for software decommissioning and retiring. *Remembering*	Explain potential security implications for software decommissioning and retiring. *Understanding* [SOF-LO-E19]	Investigate potential security implications for software decommissioning and retiring, for a given piece of software. *Applying*
Documentation		
Explain security notations within software documentation, for a given piece of software. *Applying*	Write appropriate security notations within software documentation. *Applying* [SOF-LO-E20]	Analyze security notations within software documentation, for a given piece of software. *Analyzing*

Use available documentation to resolve security-related issues throughout the software life cycle. *Applying*	Use available documentation to resolve security-related issues throughout the software life cycle. *Applying* [SOF-LO-E21]	Use available documentation to resolve security-related issues throughout the software life cycle. *Applying*
Ethics		
List a few ethical aspects related to software development. *Remembering*	Explain various ethical aspects related to software development, including vulnerability disclosure. *Understanding* [SOF-LO-E22]	Compare various ethical aspects in software development, including vulnerability disclosure. *Analyzing*

Component Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Component Design		
Recognize that a component's design may create vulnerabilities in information systems. *Remembering*	Discuss how a component's design may create vulnerabilities in information systems. *Understanding* [COM-LO-E01]	Illustrate how a component's design may create vulnerabilities in information systems. *Applying*
Component Procurement		
List some vulnerabilities, risks, and mitigations for components of an organizational network in a supply chain. *Remembering*	Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Understanding* [COM-LO-E02]	Analyze vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Analyzing*
Name some security threats and risks to hardware and	Discuss security threats and risks to both hardware and software in component	Outline security threats and risks to both hardware and

software in component procurement. *Remembering*	procurement, such as malware attached during manufacturing or transportation. *Understanding* [COM-LO-E03]	software in component procurement. *Analyzing*
Component Testing		
Describe component security testing procedures. *Understanding*	Perform component security testing. *Applying* [COM-LO-E04]	Appraise component security testing procedures. *Evaluating*
Define unit testing and system-level testing. *Remembering*	Describe unit testing tools and techniques, as distinguished from those used in system-level testing. *Understanding* [COM-LO-E05]	Compare unit testing tools and techniques with those used in system-level testing, and the role of each in a comprehensive test plan. *Analyzing*
Component Reverse Engineering		
Recall common reverse engineering scenarios for components of a system. *Remembering*	Describe common reverse engineering scenarios for components of a system. *Understanding* [COM-LO-E06]	Perform reverse engineering on components of a system. *Applying*

Connection Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Distributed Systems Architecture		
Recognize architectures for running processes in a distributed system and enabling communication between them. *Remembering*	Describe architectures for running processes in a distributed system and enabling communication between them. *Understanding* [CON-LO-E01]	Implement a distributed system and enable communication between processes. *Applying*

Identify important events in the evolution of the Internet as a distributed platform, including the role of the world-wide-web. *Remembering*	Summarize the evolution of the Internet as a distributed platform, including the role of the world-wide-web. *Understanding* [CON-LO-E02]	Examine the evolution of the Internet as a distributed platform, including the role of the world-wide-web. *Analyzing*
Describe the layers of the OSI model and the TCP/IP model. *Understanding*	Compare the OSI model and the TCP/IP model. *Analyzing* [CON-LO-E03]	Debate the use of the OSI model over the TCP/IP model for a given scenario. *Evaluating*
Discuss commonly used network protocols based on the layers of the OSI model. *Understanding*	Categorize commonly used network protocols based on the layers of the OSI model. *Analyzing* [CON-LO-E04]	Choose commonly used network protocols based on the layers of the OSI model. *Evaluating*
Identify common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. *Remembering*	Explain common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. *Understanding* [CON-LO-E05]	Contrast common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. *Analyzing*
Identify various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). *Remembering*	Classify various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). *Understanding* [CON-LO-E06]	Implement various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). *Applying*
Discuss the setup and configuration of a virtual machine in a hypervisor environment. *Understanding*	Perform the setup and configuration of a virtual machine in a hypervisor environment. *Applying* [CON-LO-E07]	Examine the setup and configuration of a virtual machine in a hypervisor environment. *Analyzing*
Network Architecture		

Summarize common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards. *Understanding*	Diagram common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards. *Applying* [CON-LO-E08]	Compare common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards. *Analyzing*
Diagram various network topologies and their transmission characteristics. *Applying*	Distinguish various network topologies and their transmission characteristics. *Analyzing* [CON-LO-E09]	Evaluate various network topologies and their transmission characteristics. *Evaluating*
Recognize various types of virtualization, including native virtualization (Type 1) and hosted virtualization (Type 2). *Remembering*	Describe various types of virtualization, including native virtualization (Type 1) and hosted virtualization (Type 2). *Understanding* [CON-LO-E10]	Compare various types of virtualization, including native virtualization (Type 1) and hosted virtualization (Type 2). *Analyzing*
Network Implementations		
Define various connection attacks, such as SYN-scanning, and associated vulnerabilities, and how they can affect an organization's network. *Remembering*	Differentiate between various connection attacks, such as SYN-scanning, and associated vulnerabilities, and how they can affect an organization's network. *Understanding* [CON-LO-E11]	Investigate various connection attacks, such as SYN-scanning, and associated vulnerabilities, and how they can affect an organization's network. *Applying*
Define various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization's network. *Remembering*	Differentiate between various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization's network. *Understanding* [CON-LO-E12]	Investigate various transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities, and how they can affect an organization's network. *Applying*
Network Services		

Define the concept of an operating system service or daemon and various security vulnerabilities. *Remembering*	Describe the concept of an operating system service or daemon, and how it could be vulnerable to exploitation. *Understanding* [CON-LO-E13]	Apply configuration settings to an operating system service or daemon that reduce its vulnerability to exploitation. *Applying*
Network Defense		
Explain the concepts of confidentiality, integrity, and availability (CIA). *Understanding*	Explain how network defenses should be structured using layering, segmentation, and other controls to achieve maximum confidentiality, integrity, and availability (CIA). *Understanding* [CON-LO-E14]	Implement a network defense structure that uses layering, segmentation, and other controls to achieve maximum confidentiality, integrity, and availability (CIA). *Applying*

System Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
System Thinking		
List some components that work to secure a system. *Remembering*	Describe how components work together to secure a system. *Understanding* [SYS-LO-E01]	Illustrate how components work together to secure a system. *Applying*
Explain a security threat model. *Understanding*	Apply a security threat model to a given scenario. *Applying* [SYS-LO-E02]	Critique a security threat model for a given scenario. *Evaluating*
Name some fundamental principles of secure systems. *Remembering*	Explain fundamental principles of secure systems. *Understanding* [SYS-LO-E03]	Outline elements of fundamental principles of secure systems. *Analyzing*
System Management		

Recognize components of a security policy for a system. *Remembering*	Describe the components of a security policy for a system. *Understanding* [SYS-LO-E04]	Implement components of a security policy for a system. *Applying*
Define methods and tools for system monitoring and recovery. *Remembering*	Discuss methods and tools for system monitoring and recovery. *Understanding* [SYS-LO-E05]	Apply methods and tools for system monitoring and recovery. *Applying*
State the role of patching in maintaining the security of a system. *Remembering*	Describe the use of vulnerability reports and patching in maintaining the security of a system. *Understanding* [SYS-LO-E06]	Analyze the use of vulnerability reports and patching in maintaining security for a given system. *Analyzing*
System Access and Control		
Describe various system-related methods for authentication, authorization, and access control. *Understanding*	Contrast various system-related methods for authentication, authorization, and access control. *Analyzing* [SYS-LO-E07]	Design system-related methods for authentication, authorization, and access control. *Creating*
Interpret documentation for a system with focus on security considerations. *Understanding*	Write documentation for a system with security considerations in mind. *Applying* [SYS-LO-E08]	Evaluate documentation for a system with security considerations in mind. *Evaluating*
List types of malware. *Remembering*	Differentiate among types of malware. *Understanding* [SYS-LO-E09]	Contrast types of malware. *Analyzing*
Define intrusion detection systems. *Remembering*	Describe how malicious activity can be detected, including the use of intrusion detection systems. *Understanding* [SYS-LO-E10]	Use an intrusion detection system to detect malicious activity. *Applying*
Identify potential system attacks and the actors that	Describe potential system attacks and the actors that	Decompose potential system attacks and the actors that

might perform them. *Remembering*	might perform them. *Understanding* [SYS-LO-E11]	might perform them. *Analyzing*
System Testing		
Describe system security test protocols. *Understanding*	Execute system security test protocols. *Applying* [SYS-LO-E12]	Structure system security test protocols. *Analyzing*
Identify differences between unit testing and system testing. *Remembering*	Discuss the differences between unit testing and system testing. *Understanding* [SYS-LO-E13]	Illustrate the differences between unit testing and system testing. *Applying*
Common System Architectures		
List some system security issues related to common system architectures. *Remembering*	Discuss system security issues related to common system architectures such as virtual machines, industrial control systems, embedded systems, autonomous systems, mobile systems and general-purpose systems. *Understanding* [SYS-LO-E14]	Investigate system security issues related to a variety of common system architectures. *Applying*

Human Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Identity Management		
Execute various methods of identity management, identification, authentication, and access authorization. *Applying*	Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and	Verify various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and

	multifactor systems. *Analyzing* [HUM-LO-E01]	multifactor systems. *Evaluating*
List attacks and mitigations associated with identity management. *Remembering*	Discuss attacks and mitigations associated with identity management, such as brute force attacks, spoofing attacks, strong password policies, and restricted access systems. *Understanding* [HUM-LO-E02]	Analyze a variety of attacks and mitigations associated with identity management. *Analyzing*
Social Engineering		
Perform various social engineering attacks and suitable mitigations. *Applying*	Compare various social engineering attacks, such as phishing, vishing, email compromise, and baiting, along with suitable mitigations. *Analyzing* [HUM-LO-E03]	Defend against various social engineering attacks with suitable mitigations. *Evaluating*
Identify psychological and behavioral factors which contribute to social engineering attacks. *Remembering*	Describe psychological and behavioral factors which contribute to social engineering attacks, such as adversarial thinking, cognitive biases, and trust building. *Understanding* [HUM-LO-E04]	Investigate psychological and behavioral factors which contribute to social engineering attacks, such as adversarial thinking, cognitive biases, and trust building. *Applying*
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms		
Summarize one's personal social media use with respect to organizational policies, rules, and ethical norms. *Understanding*	Analyze one's personal social media use with respect to organizational policies, rules, and ethical norms. *Analyzing* [HUM-LO-E05]	Develop one's personal social media use with respect to organizational policies, rules, and ethical norms. *Creating*
Awareness and Understanding		

Describe formal or informal security education, training, and awareness program tasks. *Understanding*	Carry out formal or informal security education, training, and awareness program tasks. *Applying* [HUM-LO-E06]	Critique formal or informal security education, training, and awareness program tasks. *Evaluating*
Personal Data Privacy and Security		
Investigate potential risks to personal data privacy and security. *Applying*	Evaluate potential risks to personal data privacy and security for a given scenario. *Evaluating* [HUM-LO-E07]	Formulate a protective plan to reduce potential risks to personal data privacy within a given security scenario. *Creating*
Usable Security and Privacy		
Identify the impact usability and user experience have on security and privacy, including compliance with laws. *Remembering*	Describe the impact usability and user experience have on security and privacy, including compliance with laws such as HIPAA and FERPA. *Understanding* [HUM-LO-E08]	Compare the impact usability and user experience have on security and privacy, including compliance with laws. *Analyzing*
Identify human factors which impact privacy and security. *Remembering*	Describe human factors which impact privacy and security, such as the psychology of adversarial thinking, resistance to biometric authentication, and the economics of security. *Understanding* [HUM-LO-E09]	Describe human factors which impact privacy and security, such as the psychology of adversarial thinking, resistance to biometric authentication, and the economics of security. *Understanding*

Organizational Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Risk Management		

Identify organizational risk factors due to security failure. *Remembering*	Classify organizational risk factors due to security failure, such as financial loss, operational disruption, and reputational damage. *Understanding* [ORG-LO-E01]	Analyze organizational risk factors due to security failure. *Analyzing*
Identify some components that contribute to an organization's security posture. *Remembering*	Describe the components that contribute to an organization's security posture. *Understanding* [ORG-LO-E02]	Illustrate the components that contribute to an organization's security posture. *Applying*
Security Governance & Policy		
Summarize tasks required in order to comply with information security governance and policy. *Understanding*	Perform tasks in compliance with information security governance and policy. *Applying* [ORG-LO-E03]	Examine tasks with respect to compliance with information security governance and policy. *Analyzing*
Recognize relevant independent and government-sponsored cybersecurity frameworks. *Remembering*	Summarize relevant independent and government-sponsored cybersecurity frameworks. *Understanding* [ORG-LO-E04]	Investigate relevant independent and government-sponsored cybersecurity frameworks. *Applying*
State the importance of ethical codes of conduct for cybersecurity professionals and their organizations. *Remembering*	Discuss the importance of ethical codes of conduct for cybersecurity professionals and their organizations. *Understanding* [ORG-LO-E05]	Apply tenets from ethical codes of conduct for cybersecurity professionals in an organization. *Applying*
Systems Administration		
Name some components that secure the operating system and system database from vulnerabilities. *Remembering*	Describe components that secure the operating system and system database from vulnerabilities. *Understanding* [ORG-LO-E06]	Manipulate components that secure the operating system and system database from vulnerabilities in order to increase security. *Applying*

List some administrative functions in an operating system. *Remembering*	Demonstrate administrative functions, such as using group membership to assign permissions. *Understanding* [ORG-LO-E07]	Perform administrative functions in an operating system. *Applying*
Identify security features relevant in a cloud environment. *Remembering*	Discuss security features that are embedded within a cloud environment. *Understanding* [ORG-LO-E08]	Compare security features that are embedded within a cloud environment. *Analyzing*
Business Continuity, Disaster Recovery, and Incident Management		
Label components of a business continuity plan. *Remembering*	Explain the components of a business continuity plan, such as contingency planning, incident response, emergency response, backup, and recovery efforts. *Understanding* [ORG-LO-E09]	Deconstruct components of a business continuity plan. *Analyzing*
Recognize a disaster recovery plan that ensures minimal down time and quick recovery. *Remembering*	Describe a disaster recovery plan that ensures minimal down time and quick recovery. *Understanding* [ORG-LO-E10]	Diagram a disaster recovery plan that ensures minimal down time and quick recovery. *Applying*

Societal Security

Emerging	**Learning Outcome - Developed**	**Highly Developed**
Cybercrime		
Differentiate among different types of cybercrime. *Understanding*	Categorize different types of cybercrime. *Analyzing* [SOC-LO-E01]	Assess different types of cybercrime. *Evaluating*
Describe the economic implications of a society	Investigate the economic implications of a society	Examine the economic implications of a society

impacted by cybercrimes, including crimes that involve cryptocurrencies. *Understanding*	impacted by cybercrimes, including crimes that involve cryptocurrencies. *Applying* [SOC-LO-E02]	impacted by cybercrimes, including crimes that involve cryptocurrencies. *Analyzing*
Cyber Law		
Recognize various categories of global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property. *Remembering*	Describe various categories of global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property. *Understanding* [SOC-LO-E03]	Investigate various categories of global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property. *Applying*
Cyber Ethics		
Investigate given cyber ethics scenarios, including topics on codes of conduct and professional ethics. *Applying*	Analyze given cyber ethics scenarios, including topics on codes of conduct and professional ethics. *Analyzing* [SOC-LO-E04]	Debate given cyber ethics scenarios, including topics on codes of conduct and professional ethics. *Evaluating*
Summarize ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war. *Understanding*	Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war. *Analyzing* [SOC-LO-E05]	Critique ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war. *Evaluating*
Cyber Policy		
Recall cyber policies and related liability issues. *Remembering*	Discuss cyber policies and related liability issues. *Understanding* [SOC-LO-E06]	Examine cyber policies and related liability issues. *Analyzing*
Privacy		
Infer privacy and transparency from a societal	Contrast privacy and transparency from a societal	Argue privacy and transparency from a societal

perspective, including goals and tradeoffs. *Understanding*	perspective, including goals and tradeoffs. *Analyzing* [SOC-LO-E07]	perspective, including goals and tradeoffs. *Evaluating*
Discuss cultural differences in the existence of privacy norms and boundaries. *Understanding*	Investigate cultural differences in the existence of privacy norms and boundaries. *Applying* [SOC-LO-E08]	Analyze cultural differences in the existence of privacy norms and boundaries. *Analyzing*

Appendix D: Program Examples

The two Cybersecurity programs shown here give examples of how a program can align with the Cyber2yr2020 competencies presented in this guidance. Additional program examples are available on the ACM CCECC web site at ccecc.acm.org/correlations, and more program examples are welcome. If your college is interested in submitting a program example, visit ccecc.acm.org/correlations for instructions, and contact the CCECC with any questions at ccecc.acm.org/contact.

Ivy Tech Community College

Program Name: Cybersecurity / Information Assurance
Program Type: AAS Degree
Program URL: www.ivytech.edu/cyber-security
NSA/DHS Center of Academic Excellence in Cyber Defense: Yes
Submitter: Pam Schmelz

Notes:
We used INFM 109, SDEV 120, SVAD 111, CSIA 105, NETI 105, and CSIA 225 to map the KUs for the CAE designation we have. CSIA 260 is an elective in our program.

Course Descriptions:

CSIA 105 Introduction to Cyber Security / Information Assurance
Prerequisites: ITSP 135. The students will explore the field of Cyber Security/Information Assurance focusing on the technical and managerial aspects of the discipline. Students will be introduced to the basic terminology, concepts, and best practices of computer/network security and the roles and responsibilities of management/security personnel. The students will learn the technologies used and techniques involved in creating a secure computer networking environment including authentication and the types of attacks against an organization.

CSIA 225 Ethical Hacking
Prerequisites: NETI 105 and SVAD 111. Students will learn threats and defense mechanisms; web applications and data servers; Linux, Macintosh and mobile systems; and secure network infrastructures. Hands-on practical application will be included as preparation for the Certified Ethical Hacker exam by EC-Council.

CSIA 210 Network Protocol Analysis
Prerequisites: NETI 105 and ITSP 135. Offers in-depth coverage of all the salient models, protocols, services, and standards that govern TCP/IP and that guide its behavior on modern networks. Specific guidance is given to reinforce the concepts introduced and to help prepare students to interact with TCP/IP on the vast majority of networks in use today. As a hands-on course, students are provided firsthand experience in installing, configuring, analyzing, using, and managing TCP/IP on a network.

Included are case projects that pose problems and require creative solutions that should prepare students for the kinds of situations faced on a real, live network.

CSIA 135 Digital Forensics

Prerequisites: ITSP 135. Provides students with an understanding of the detailed methodological approach to computer forensics and evidence analysis. Students will acquire hands-on experience with various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

NETI 105 Network Fundamentals

Prerequisites: Demonstrated competency through appropriate assessment or earning a grade of “C” or better in ENGL 083 or ENGL 095. Covers the fundamentals of networking. Students will learn both the practical and conceptual skills that build the foundation for understanding basic networking. Human versus network communication are compared, and the parallels between them are presented. Students are introduced to the two major models used to plan and implement networks. The functions and services of the Open System Interconnection and Transport Control Protocol/Internet Protocol Models are examined in detail. Various network devices, network addressing schemes, and the types of media used to carry data across the network are also presented. Designed to be a study of local area networks, topologies, and functions while providing a general understanding of basic local area network protocols.

SVAD 111 Linux and Virtualization Technologies Fundamentals

Prerequisites: ITSP 135. Corequisites: ITSP 135. Designed as a dual purpose course, providing students with the necessary skills to understand and apply Linux and virtualization concepts while maintaining a clear division between subjects. Students will apply fundamental concepts with project-based content exercises. Students will have a strong understanding of critical Linux and virtual technologies. Students will demonstrate the ability to install, manage, monitor, configure, and troubleshoot the fundamental systems and services available in most major Linux operating system distributions. Further study concentrates on the file system organization service, command line language, file system, and print service permissions found in the Linux operating system. Virtualization technologies including the exploration, installation, and troubleshoot various virtualization software packages to obtain the skillset necessary to choose and implement hypervisor environments for client-level operating systems. Students are required to demonstrate course objectives through the appropriate Linux certification exam and the fee for the exam is assessed upon enrollment in the course.

ITSP 135 Hardware / Software Support

Prerequisites: INFM 109 or CSCI 101. Corequisites: INFM 109 or CSCI 101. Delivers the necessary competencies with hands-on experience in the lab for an entry-level Information Technology professional. Students will have the knowledge required to assemble components based on customer requirements, install, configure and maintain devices/software for end users, understand the basics of networking and security, properly and safely diagnose, resolve and document common hardware and software issues while applying troubleshooting skills. Students will also learn appropriate customer support, understand the basics of virtualization, desktop imaging, and deployment.

CSIA 215 Perimeter Defense

Prerequisites: NETI 115. Provides an advanced understanding of the concepts involved in firewalls, routers, intrusion detection, intrusion prevention and Virtual Private Networks (VPNs) in relationship to the

overall enterprise network strategy. Students will learn advanced network security installation techniques; advanced network security troubleshooting; and how to make intelligent choices in firewall and router technology. Additionally, the students will have a comprehensive look at the use of routers and switches with other network security components in configuring De-Militarized Zones (DMZ) and VPNs for optimal perimeter security. Students will study such topics as packet filtering, proxy servers, authentication, encryption, and securing host computers.

CSIA 260 Business Continuity in an Information World

Prerequisites: CSIA105. Students will learn principles of incident response and disaster recovery. Identification of vulnerabilities and appropriate countermeasures to prevent and mitigate risks to an organization will be discussed. Students will learn risk assessment, incident response, contingency planning, and prioritizing systems for disaster recovery. The importance of management's roles and interaction with other organizational members will be discussed. Students will learn how to create a hardened network by developing system specific plans for the protection of intellectual property, the implementation of access controls, and patch/change management. Students will gain an understanding of information assurance including the governing rules and guidelines.

Cyber2yr2020 Competency	CSIA 105	CSIA 225	CSIA 210	CSIA 135	NETI 105	SVAD 111	ITSP 135	CSIA 215	CSIA 260
[CC-1] Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*	X	X							
[CC-2] Assess and respond appropriately to various risks which can affect the expected operation of information systems. *Evaluating*	X								
[CC-3] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. *Applying*	X	X							
[CC-4] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. *Applying*	X	X							
[CC-5] Discuss how changes in	X								

one part of a system may impact other parts of a cybersecurity ecosystem. *Understanding*									
[DAT-E1] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. *Applying*	X	X							
[DAT-E2] Discuss forensically sound collection and acquisition of digital evidence. *Understanding*				X					
[DAT-E3] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents. *Applying*	X							X	
[DAT-E4] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks. *Applying*	X				X	X			
[DAT-E5] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. *Understanding*	X			X					
[DAT-S1] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. *Applying*				X					
[DAT-S2] Outline complex technical concepts to technical and non-technical audiences as they relate to data security. *Analyzing*	X								
[SOF-E1] Write secure code						X			

with appropriate documentation for a software system and its related data. *Applying*									
[SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*	X								
[SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*	X							X	
[SOF-S1] Implement isolation to secure a process or application. *Applying*									
[SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*									
[SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*									
[SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*									
[SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*									
[SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*									
[COM-E1] Discuss vulnerabilities and mitigations of system components throughout their lifecycle. *Understanding*	X				X				

[COM-E2] Perform security testing for given components within a system. *Applying*	X	X			X				
[COM-S1] Analyze how component security features impact systems, such as software and firmware updates. *Analyzing*									
[CON-E1] Illustrate the construction and proper configuration of computer networks which adhere to current industry standards and organizational guidelines. *Applying*					X				
[CON-E2] Investigate the impact of various connection and transmission attacks on network hardware and software. *Applying*	X	X			X				
[CON-S1] Examine characteristics of commonly used physical networking media and interfaces. *Analyzing*					X		X		
[CON-S2] Distinguish vulnerabilities and example exploits as they apply to network services, architectures, and protocols. *Analyzing*	X	X	X					X	
[CON-S3] Implement appropriate defenses throughout an enterprise to harden the network against attackers. *Applying*									
[CON-S4] Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. *Creating*					X				
[SYS-E1] Discuss security aspects of system management in common system architectures.	X							X	

Understanding									
[SYS-E2] Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. *Analyzing*	X								
[SYS-E3] Perform system security testing with an understanding of normal, secure operation, and document results. *Applying*		X							
[SYS-S1] Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal. *Evaluating*									
[SYS-S2] Outline a security threat model and how system monitoring tools and mechanisms can be used. *Analyzing*									
[SYS-S3] Examine appropriate models for managing authentication, access control and authorization across systems in an organization. *Analyzing*	X								
[SYS-S4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying*		X							
[SYS-S5] Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis. *Understanding*				X					
[SYS-S6] Construct virtual environments including disk and memory structures to meet						X			

organization needs. *Creating*									
[HUM-E1] Discuss identity management in the context of attacks and mitigations. *Understanding*	X								
[HUM-E2] Analyze the security of an individual's data and privacy in the context of an organization and in their personal lives. *Analyzing*	X		X					X	
[HUM-E3] Describe trends in human behavior which pose risks to individual and organizational privacy and security. *Understanding*	X	X							
[HUM-S1] Analyze a variety of physical access controls. *Analyzing*	X								
[HUM-S2] Use a variety of tools and techniques to detect and mitigate social engineering threats. *Applying*		X							
[HUM-S3] Examine techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms. *Analyzing*								X	
[ORG-E1] Describe policies, procedures, and ethical considerations to protect information security. *Understanding*	X							X	
[ORG-E2] Describe security features in operating system and database administration in a local or cloud environment. *Understanding*	X					X			
[ORG-E3] Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters.	X								

Understanding									
[ORG-E4] Describe physical security features to protect an organization's computing and information resources. *Understanding*	X								X
[ORG-S1] Analyze risks to information assets in an organization and communicate them to stakeholders. *Analyzing*									X
[ORG-S2] Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. *Evaluating*								X	X
[ORG-S3] Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. *Analyzing*									
[ORG-S4] Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. *Understanding*								X	
[SOC-E1] Interpret applicable cyber policies and ethics for a given scenario. *Understanding*	X			X					
[SOC-E2] Summarize applicable national, international, and global security policies and legislation. *Understanding*	X								
[SOC-E3] Distinguish social dynamics of computer attackers in a global context. *Analyzing*	X								
[SOC-S1] Attribute specific	X			X					

cyber laws and potential economic impact for a given cybercrime scenario. *Analyzing*									
[SOC-S2] Compare different cyber ethics theories that impact on individuals and society. *Analyzing*									

Bluegrass Community and Technical College (BCTC)

Program Name: Computer & Information Technologies (CIT)
Program Type: AAS Degree
Program URL: https://bluegrass.kctcs.edu/education-training/programs/cit/index.aspx
NSA/DHS Center of Academic Excellence in Cyber Defense: Yes
Submitter: Cindy Tucker

Notes:
BCTC used four courses, CIT 111, CIT 120, CIT 170, and CIT 180, to map to and earn the NSA/DHS CAE-CD designation. Each of these courses is a core course required for the CIT AAS degree. Consequently, any student who earns an AAS CIT degree, regardless of the track they choose, will have achieved the learning outcomes associated with the CAE outcomes and topics for the BCTC designation. Many students study cybersecurity in more depth within their chosen track.

Course Descriptions:
CIT 111 Computer Hardware and Software
Prerequisite: (CIT 105 AND MAT 065). Presents a practical view of computer hardware and client operating systems. Covers computer hardware components; troubleshooting, repair, and maintenance; operating system interfaces and management tools; networking components; computer security; and operational procedures.

CIT 120 Computational Thinking
Prerequisite or Corequisite: MAT 085 or (MAT 126 or higher). Promotes understanding of computer programming and logic by teaching students to think like a computer. Covers skills needed to develop and design language-independent solutions to solve computer-related problems. Covers development and design basics including use of variables, control and data structures, and principles of command line and object-oriented languages.

CIT 170 Database Design Fundamentals

Prerequisite: (CIT 105 OR OST 105 OR IMD 100) AND (MAT 085 OR MAT 126). Provides an overview of database and database management system concepts, internal design models, normalization, network data models, development tools, and applications.

CIT 180 Security Fundamentals
Prerequisite: (CIT 160 OR CIT 161). Introduces basic computer and network security concepts and methodologies. Covers principles of security; compliance and operational security; threats and vulnerabilities; network security; application, data, and host security; access control and identity management; and cryptography. Helps to prepare students for the COMPTIA Security+ examination.

Cyber2yr2020 Competency	CIT 111	CIT 120	CIT 170	CIT 180
[CC-1] Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*		X	X	X
[CC-2] Assess and respond appropriately to various risks which can affect the expected operation of information systems. *Evaluating*	X	X	X	X
[CC-3] Investigate current and emerging cyberthreats and incorporate best practices to mitigate them. *Applying*	X			X
[CC-4] Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. *Applying*	X			X
[CC-5] Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. *Understanding*		X		X
[DAT-E1] Implement data security by selecting appropriate cryptographic procedures, algorithms, and tools based on security policy and level of risk in an organization. *Applying*	X	X		X
[DAT-E2] Discuss forensically sound collection and acquisition of digital evidence. *Understanding*				X
[DAT-E3] Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents. *Applying*		X	X	X
[DAT-E4] Use appropriate levels of authentication, authorization, and access control to ensure data integrity and security for information systems and networks. *Applying*	X			X

[DAT-E5] Infer gaps in data security considering current and emerging technologies and the current state and prevailing trends in cybercrime. *Understanding*				X
[DAT-S1] Perform a forensic analysis on a local network, on stored data within a system as well as mobile devices for an enterprise environment. *Applying*				X
[DAT-S2] Outline complex technical concepts to technical and non-technical audiences as they relate to data security. *Analyzing*				
[SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*		X		
[SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*		X		
[SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*		X		
[SOF-S1] Implement isolation to secure a process or application. *Applying*		X		
[SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*				
[SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*				
[SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*		X		X
[SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*		X		
[SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*				
[COM-E1] Discuss vulnerabilities and mitigations of system components throughout their lifecycle. *Understanding*	X	X	X	X
[COM-E2] Perform security testing for given components within a system. *Applying*		X	X	X
[COM-S1] Analyze how component security features impact systems, such as software and firmware updates. *Analyzing*	X	X		
[COM-E1] Illustrate the construction and proper configuration of computer networks which adhere to current industry standards and organizational guidelines. *Applying*	X			X
[COM-E2] Investigate the impact of various connection and transmission attacks on network hardware and software.	X			X

Applying				
[CON-S1] Examine characteristics of commonly used physical networking media and interfaces. *Analyzing*	X			X
[CON-S2] Distinguish vulnerabilities and example exploits as they apply to network services, architectures, and protocols. *Analyzing*	X			X
[CON-S3] Implement appropriate defenses throughout an enterprise to harden the network against attackers. *Applying*				X
[CON-S4] Construct and properly configure computer networks which adhere to current industry standards and organizational guidelines. *Creating*	X			X
[SYS-E1] Discuss security aspects of system management in common system architectures. *Understanding*				X
[SYS-E2] Contrast various methods for authentication and access control in an enterprise, and why one might choose one over another. *Analyzing*	X			X
[SYS-E3] Perform system security testing with an understanding of normal, secure operation, and document results. *Applying*		X		X
[SYS-S1] Critique security throughout the system lifecycle, including security requirements, system management, system testing, and system disposal. *Evaluating*	X	X	X	X
[SYS-S2] Outline a security threat model and how system monitoring tools and mechanisms can be used. *Analyzing*				X
[SYS-S3] Examine appropriate models for managing authentication, access control and authorization across systems in an organization. *Analyzing*	X	X		X
[SYS-S4] Apply cyber defense methods to prepare a system against attacks, including penetration testing, log analysis, resilience mechanisms, and the use of intrusion detection systems. *Applying*				X
[SYS-S5] Discuss legal aspects of system and network requirements, such as support for litigation holds and forensic analysis. *Understanding*				
[SYS-S6] Construct virtual environments including disk and memory structures to meet organization needs. *Creating*	X			X
[HUM-E1] Discuss identity management in the context of attacks and mitigations. *Understanding*	X			X

[HUM-E2] Analyze the security of an individual's data and privacy in the context of an organization and in their personal lives. *Analyzing*		X	X	X
[HUM-E3] Describe trends in human behavior which pose risks to individual and organizational privacy and security. *Understanding*	X	X	X	X
[HUM-S1] Analyze a variety of physical access controls. *Analyzing*	X			X
[HUM-S2] Use a variety of tools and techniques to detect and mitigate social engineering threats. *Applying*				X
[HUM-S3] Examine techniques to encourage personal compliance with cybersecurity rules, policies, and ethical norms. *Analyzing*		X		X
[ORG-E1] Describe policies, procedures, and ethical considerations to protect information security. *Understanding*	X	X	X	X
[ORG-E2] Describe security features in operating system and database administration in a local or cloud environment. *Understanding*	X	X	X	X
[ORG-E3] Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters. *Understanding*				X
[ORG-E4] Describe physical security features to protect an organization's computing and information resources. *Understanding*	X			X
[ORG-S1] Analyze risks to information assets in an organization and communicate them to stakeholders. *Analyzing*				
[ORG-S2] Assess administrative procedures for protecting systems from attack and ensuring the availability of system access and functions in an organization. *Evaluating*				
[ORG-S3] Analyze the meaning and use of various security metrics and data with the aid of tools, to ensure quality control and security of data. *Analyzing*				
[ORG-S4] Discuss issues related to personnel security in an organization, including the protection of personally identifiable information, and proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool. *Understanding*				X
[SOC-E1] Interpret applicable cyber policies and ethics for a given scenario. *Understanding*	X	X	X	X

[SOC-E2] Summarize applicable national, international, and global security policies and legislation. *Understanding*				X
[SOC-E3] Distinguish social dynamics of computer attackers in a global context. *Analyzing*	X	X	X	X
[SOC-S1] Attribute specific cyber laws and potential economic impact for a given cybercrime scenario. *Analyzing*				
[SOC-S2] Compare different cyber ethics theories that impact on individuals and society. *Analyzing*				

Appendix E: Bloom's Revised Taxonomy

The foundational *Taxonomy of Educational Objectives: The Classification of Educational Goals* was established in 1956 by Dr. Benjamin Bloom, an educational psychologist, and is often referred to as Bloom's Taxonomy [8]. This classification divided educational objectives into three learning domains: Cognitive (knowledge), Affective (attitude) and Psychomotor (skills). In 2000, Lorin Anderson and David Krathwohl updated Bloom's seminal framework to create Bloom's Revised Taxonomy [7], focusing on the Cognitive and Affective Domains. The ACM Committee for Computing Education in Community Colleges has adopted Bloom's Revised Taxonomy for the assessment of student learning outcomes in its computing curricula.

It is important to note that in the framework of Bloom's Revised Taxonomy learners need not start at the lowest taxonomic level and work up; rather, the learning process can be initiated at any point, and the lower taxonomic levels will be subsumed within the learning scaffold. To wit:

- Before we can understand a concept we have to remember it;
- Before we can apply the concept we must understand it;
- Before we analyze it we must be able to apply it;
- Before we can evaluate its impact we must have analyzed it; and
- Before we can create, we must have remembered, understood, applied, analyzed and evaluated.

In its computing curricula, the ACM Committee for Computing Education in Community Colleges uses the Cognitive domain to assess student mastery of learning outcomes. There are six levels in the taxonomy for the Cognitive domain, progressing from the lowest order processes to the highest:

1. Remembering - Retrieving, recalling, or recognizing information from memory. Students can recall or remember information. Note: This process is the most basic thinking skill.
2. Understanding - Constructing meaning or explaining material from written, spoken or graphic sources. Students can explain ideas or concepts.
3. Applying - Using learned materials or implementing materials in new situations. Students can use/apply information in a new way.
4. Analyzing - Breaking material or concepts into parts, determining how the parts relate or interrelate to one another or to an overall structure or purpose. Students can distinguish between different parts.
5. Evaluating - Assessing, making judgments and drawing conclusions from ideas, information, or data. Students can justify a stand or decision.
6. Creating - Putting elements together or reorganizing them into a new way, form or product. Students can create a new product. Note: This process is the most difficult mental function.

Remembering	***Understanding***	***Applying***	***Analyzing***	***Evaluating***	***Creating***
Define	Classify	Apply	Analyze	Appraise	Assemble
Duplicate	Convert	Calculate	Attribute	Argue	Construct
Find	Demonstrate	Carry out	Categorize	Assess	Create
Identify	Describe	Edit	Compare	Choose	Design
Label	Differentiate	Diagram	Contrast	Critique	Develop
List	Discuss	Execute	Decompose	Debate	Devise
Locate	Exemplify	Illustrate	Deconstruct	Defend	Formulate
Memorize	Explain	Implement	Deduce	Estimate	Hypothesize
Name	Infer	Investigate	Discriminate	Evaluate	Invent
Recall	Interpret	Manipulate	Distinguish	Judge	Make
Recognize	Paraphrase	Modify	Examine	Justify	Plan
Retrieve	Report	Operate	Integrate	Support	
Select	Summarize	Perform	Organize	Test	
State	Translate	Produce	Outline	Value	
		Solve	Structure	Verify	
		Use			
		Write			

CCECC.ACM.org

Association for
Computing Machinery

Advancing Computing as a Science & Profession