Cyber2yr2020: ACM Curriculum Guidance for Associate Degree Programs in Cybersecurity

National CyberWatch Webcast
May 28, 2020

Cara Tang, Portland Community College, OR
Cindy Tucker, Bluegrass Community & Technical College, KY
Christian Servin, El Paso Community College, TX
Markus Geissler, Cosumnes River College, CA
Melissa Stange, Lord Fairfax Community College, VA

Outline

ACM Curriculum Guidelines

Cyber2yr2020

- Process
- Content
- Mappings: CAE, NICE, ABET
- Program examples

Related Curriculum Guidelines

ACM Curriculum Guidelines for Undergraduate 4-Year Programs

www.acm.org/education

- Computer Engineering – CE2016
- Computer Science – CS2013
- Information Systems – IS2010
- Information Technology – IT2017
- Software Engineering – SE2014
- **Cybersecurity – CSEC2017**

Under Development

- Data Science

CSEC2017

cybered.acm.org

Vision: *The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level.*

Organization

- Knowledge areas, knowledge units, topics
- Cross-cutting concepts - C, I, A, risk, ...
- Disciplinary lenses

CYBERSECURITY CURRICULA 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education

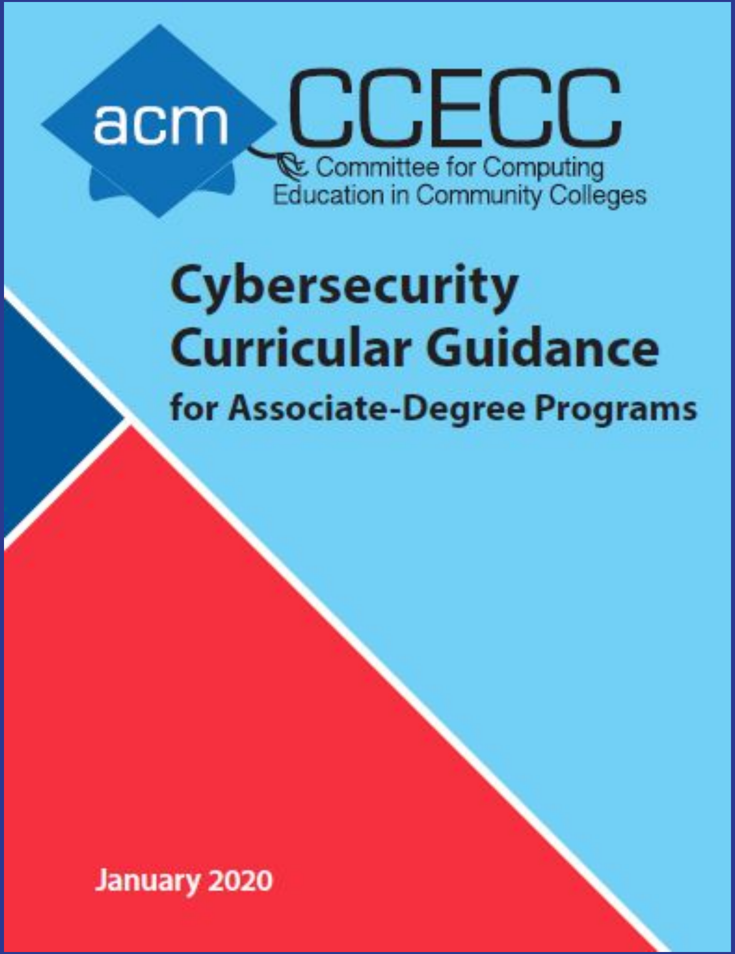
Association for Computing Machinery

- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 1.0 Report
31 December 2017

Cyber2yr2020

Process



acm CCECC Committee for Computing Education in Community Colleges

Cybersecurity Curricular Guidance for Associate-Degree Programs

January 2020

ACM Curriculum Guidelines for 2-Year Programs

ACM CCECC Global Mission
Serve and support community and technical college educators in all aspects of computing education

`ccecc.acm.org`

- Information Technology - IT2yr2014
- Computer Science - CSTransfer2017
- **Cybersecurity - Cyber2yr2020**
- IT Transfer - IT-Transfer2020

acm CCECC Committee for Computing Education in Community Colleges

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

Cyber2yr2020 Advisors

Antonio Bologna | Rapid 7

Elizabeth K. Hawthorne | Union County College

Phil Helsel | Microsoft

Sidd Kaza | Towson University

Sepehr (Sepi) Hejazi Moghadam | Google

Bill Newhouse | NICE (National Initiative for Cybersecurity Education)

Casey O'Brien | National CyberWatch Center

Allen Parrish | Mississippi State University

John Sands | Moraine Valley Community College, CSSIA

Brian Ventura | SANS Instructor

Berk Veral | Microsoft Cybersecurity Solutions Group

Cyber2yr2020 Timeline

2018 April: First Task Group Meeting

2019 February: StrawDog

2019 July: IronDog

2020 Jan: Final Publication

ccecc.acm.org/guidance/cybersecurity

Cyber2yr2020 Presentations and Publications

- Innovation and Technology in Computer Science Education **(ITiCSE)**, Trondheim, Norway, June 15-19, 2020
- National Initiative for Cybersecurity Education **(NICE)** Working Group Meeting, Featured Topic, March 25, 2020
- ACM Special Interest Group on Computer Science Education **(SIGCSE)** Symposium, Portland, OR, USA, March 11-14, 2020
- Innovation and Technology in Computer Science Education **(ITiCSE)**, Aberdeen, UK, July 15-17, 2019
- Community College Cyber Summit **(3CS)**, Shreveport/Bossier City, LA, July 30-August 1, 2019
- ACM Special Interest Group on Computer Science Education **(SIGCSE)** Symposium, Minneapolis, MN, USA, February 27 - March 2, 2019
- IEEE Symposium on Technologies for Homeland Security **(HST)**, Boston, MA, November 5-6, 2019
- Accreditation Board for Engineering and Technology, Inc. **(ABET)** Symposium, Dallas, TX, April 10-12, 2019

Cyber2yr2020 Project Scope

- Curriculum guidelines for associate degree programs (2 years)
  - Transfer programs (A.S. degree)
  - Career programs (A.A.S. degree)
- Based on ACM CSEC2017
- Key influences:
  - CAE2Y knowledge units (KUs) - 2019 Foundational + Technical Core
  - NICE Cybersecurity Workforce Framework

Cyber2yr2020 - Based on CSEC2017

CSEC2017 Structure

Within each of the 8 Knowledge Areas

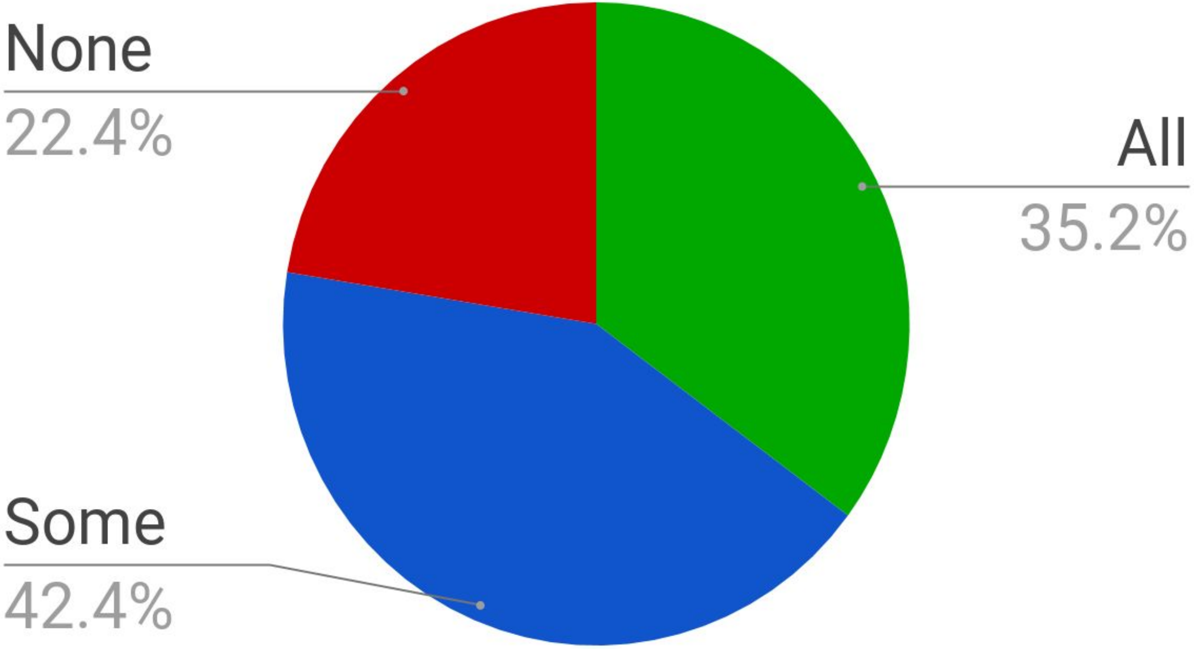
- Knowledge Units
  - **Topics**

Cyber2yr2020 Initial Process

Each CSEC2017 **topic** marked as one of

- **All**: appropriate for all 2-year cyber programs -> **Essential**
- **Some**: appropriate for some 2-year cyber programs -> **Supplemental**
- **None**: not included in 2-year guidance

Cyber2yr2020 Starting from CSEC2017

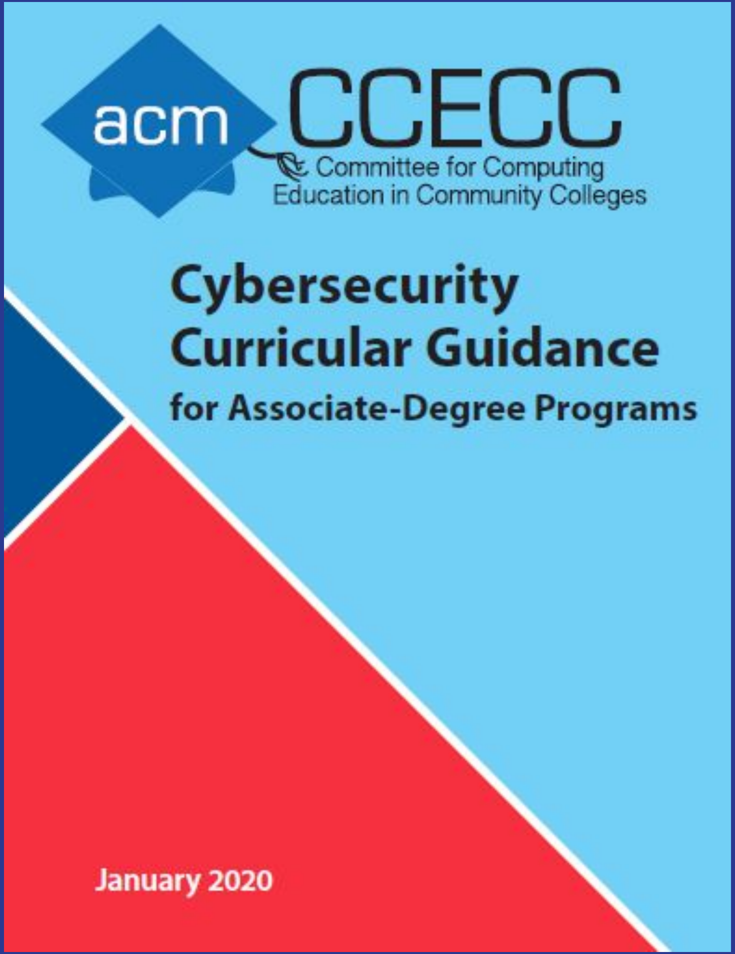


Cyber2yr2020 Incorporating CAE KUs, NICE Framework

- Craft **competencies** and **learning outcomes** instead of topics
- Align Cyber2yr2020 content with CAE KUs (Foundational + Technical Core) and incorporate missing content
- Align Cyber2yr2020 content with NICE Cybersecurity Workforce Framework categories

Cyber2yr2020

Content



acm CCECC Committee for Computing Education in Community Colleges

Cybersecurity Curricular Guidance for Associate-Degree Programs

January 2020

Cyber2yr2020 Knowledge Areas / Domains

Maintain the 8 Knowledge Areas (KAs) of CSEC2017

- Data Security
- Software Security
- Component Security
- Connection Security
- System Security
- Human Security
- Organizational Security
- Societal Security

Competencies and Learning Outcomes

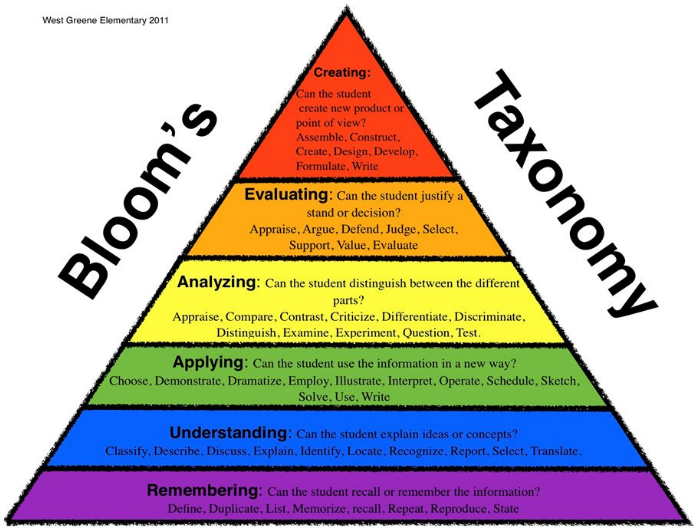
- Competencies (high-level) and learning outcomes (more detailed) instead of topics
- Competency: integrates knowledge, skills, and dispositions in context
  - Dispositions: “attitudinal, behavioral, and socio-emotional qualities of how disposed people are to apply knowledge and skills to solve problems”*
- Focus on **student achievement**
- Avoid traditional body of knowledge focus on topics
- Use Bloom’s Revised Taxonomy

* Frezza et al, 2018. *Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines*

Bloom’s Revised Taxonomy

Six levels of thinking skills in cognitive domain

- Creating
- Evaluating
- Analyzing
- Applying
- Understanding
- Remembering



West Greene Elementary 2011

Creating: Can the student create new product or point of view? Assemble, Construct, Create, Design, Develop, Formulate, Write

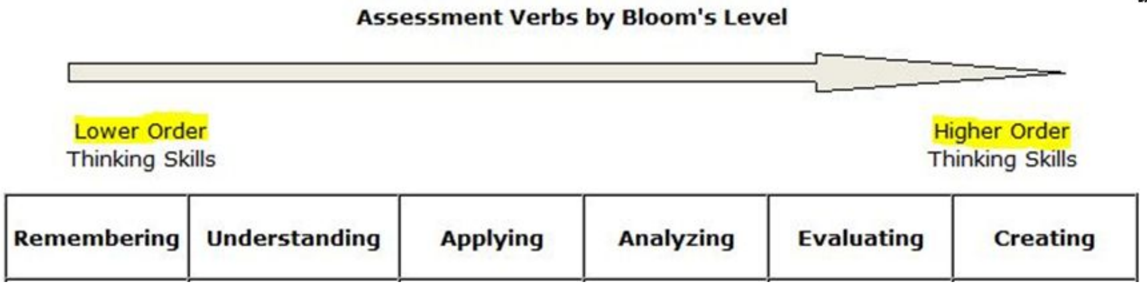
Evaluating: Can the student justify a stand or decision? Appraise, Argue, Defend, Judge, Select, Support, Value, Evaluate

Analyzing: Can the student distinguish between the different parts? Appraise, Compare, Contrast, Criticize, Differentiate, Discriminate, Distinguish, Examine, Experiment, Question, Test.

Applying: Can the student use the information in a new way? Choose, Demonstrate, Dramatize, Employ, Illustrate, Interpret, Operate, Schedule, Sketch, Solve, Use, Write

Understanding: Can the student explain ideas or concepts? Classify, Describe, Discuss, Explain, Identify, Locate, Recognize, Report, Select, Translate,

Remembering: Can the student recall or remember the information? Define, Duplicate, List, Memorize, recall, Repeat, Reproduce, State



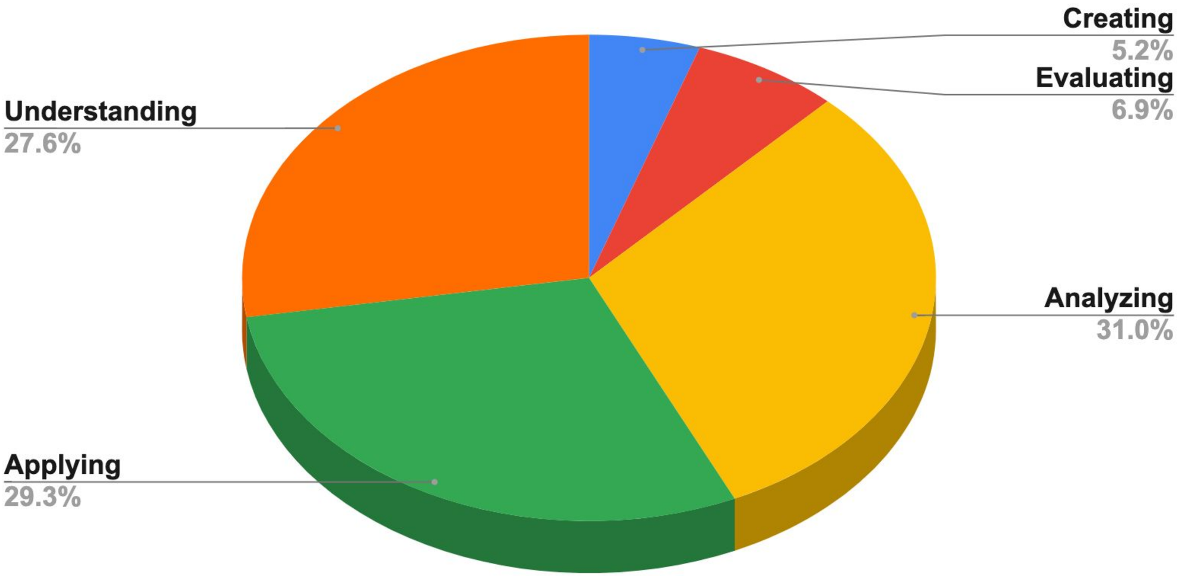
Assessment Verbs by Bloom's Level

Lower Order
Thinking Skills

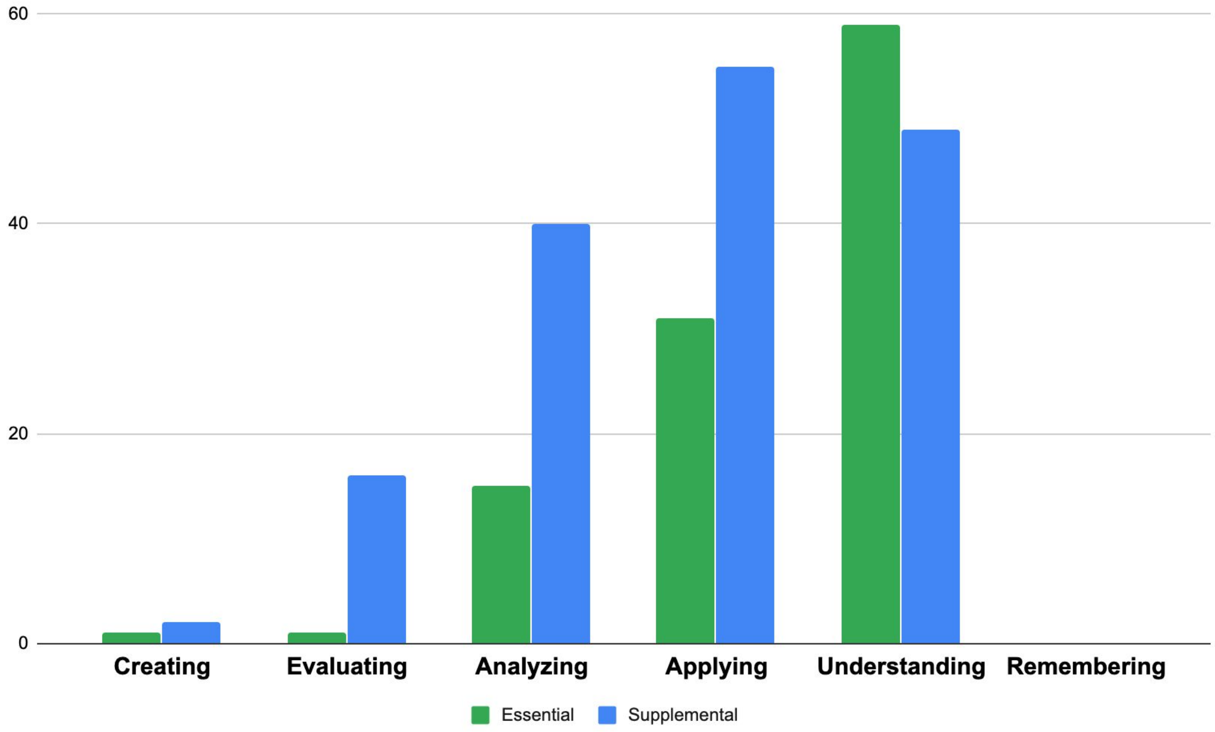
Higher Order
Thinking Skills

Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

Bloom’s Competency Distribution



Bloom’s Learning Outcomes



Selected Competencies - Cross-Cutting Concepts

- Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability. *Analyzing*
- Apply appropriate countermeasures to help protect organizational resources based on an understanding of how bad actors think and operate. *Applying*
- Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem. *Understanding*

Confidentiality, Integrity, Availability

Adversarial Thinking

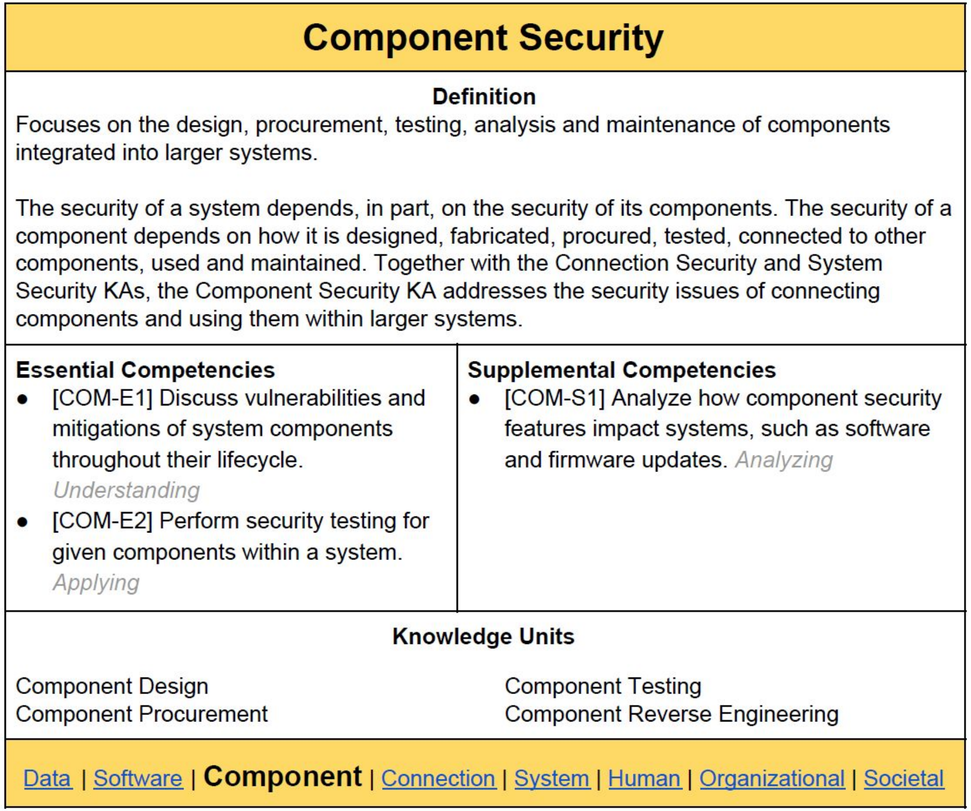
Systems Thinking

Selected Competencies - Software Security

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

Cyber2yr2020 Knowledge Areas

- Cross-Cutting Competencies
- Data Security Competencies
  - Knowledge Units / Subdomains
  - Learning Outcomes
- Software Security
- Component Security
- Connection Security
- System Security
- Human Security
- Organizational Security
- Societal Security



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

How to Use the Guidance

- Conducting program reviews to update and create curriculum
  - For validation or as an incentive for change
- Facilitating program and course articulation
  - To improve transfer pathways
  - To support new articulations
- Aligning with government-sponsored frameworks
  - To illustrate compliance with state and national frameworks
- Interacting with local advisory boards
  - For validation or as an incentive for change

Cyber2yr2020

Mappings

CAE Knowledge Units

NICE Cybersecurity Workforce Framework

ABET 2-year Cybersecurity Accreditation

Mapped to CAE KUs

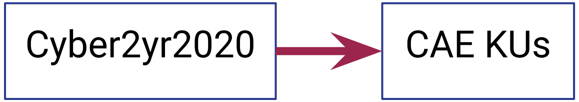
Foundational Core

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

Technical Core

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

100% of CAE KU Outcomes and Topics map to Cyber2yr2020 competencies and/or learning outcomes



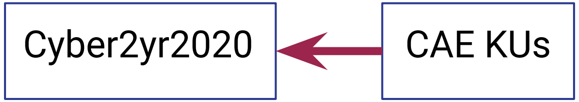
Mapping - Cross-Cutting Concepts

Cyber2yr2020 Cross-Cutting Competency

- [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.

CAE KU: Cybersecurity Foundations (CSF)

- Outcome 1: Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
- Outcome 5: Properly use the vocabulary associated with cybersecurity.
- Topic 10: Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy


Cyber2yr2020

CAE KUs

Mapping - Network Defense (NDF)

CAE KU: Network Defense (NDF)

- Topic 1c: Outline concepts of network defense, such as … (c) Network Hardening

Cyber2yr2020

- Connection Security
  - Competency: [CnSS-3] Implement appropriate defenses throughout an enterprise to harden the network against attackers.
  - Learning Outcome: Implement configuration settings on devices throughout an enterprise to harden the network against attackers.
- *Organizational Security* Learning Outcome: Implement Hardening techniques to protect the operating system.

Map to NICE Cybersecurity Workforce Framework Categories

NICE Category	# of Cyber2yr2020 Competencies
Analyze	4
Collect and Operate	2
Investigate	3
Operate and Maintain	20
Oversee and Govern	6
Protect and Defend	16
Securely Provision	7

Aligning with NICE Framework

NICE Category: Operate & Maintain

- *Cyber2r2020 Knowledge Area:* System Security

- *Cyber2r2020 Competency:* [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.

Aligning with NICE Framework

NICE Category: Protect and Defend

- *Cyber2r2020 Knowledge Area:* Data Security

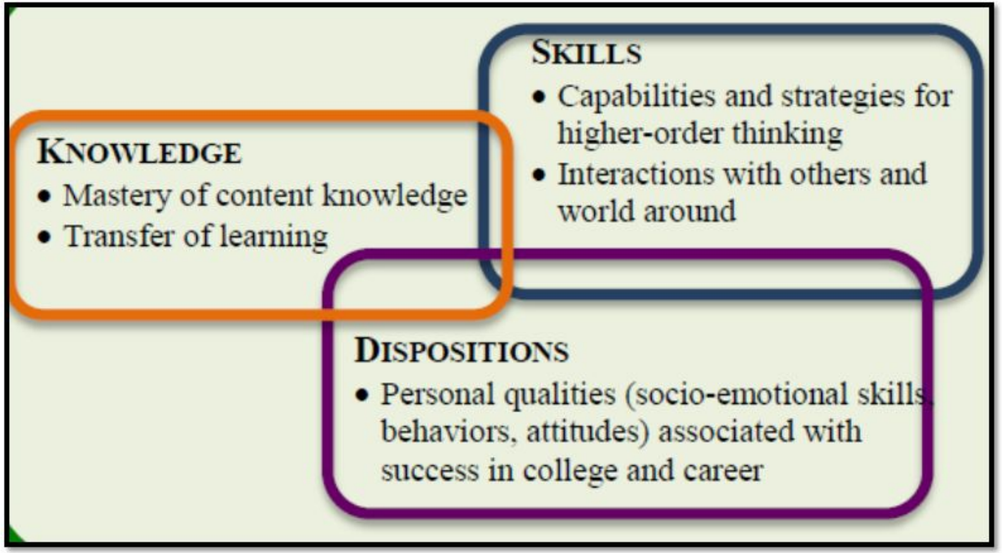
- *Cyber2r2020 Competency:* [DAT-E2] Discuss forensically sound collection and acquisition of digital evidence.

NICE Work Roles vs. Competencies

- Abilities
- Knowledge
- Skills
- Tasks

Cyber2yr2020 competencies

- Broaden NICE Work Roles by including Dispositions
- Less Task-specific



SKILLS

- Capabilities and strategies for higher-order thinking
- Interactions with others and world around

KNOWLEDGE

- Mastery of content knowledge
- Transfer of learning

DISPOSITIONS

- Personal qualities (socio-emotional skills, behaviors, attitudes) associated with success in college and career

ABET Cybersecurity Program Accreditation

ABET accredits 4-year computing programs in

- Computer Science
- Information Systems
- Information Technology
- **Cybersecurity**

ABET released draft criteria for accrediting **2-year cybersecurity programs**

- **Criteria based on Cyber2yr2020**
- Criteria open for public review until June 15, 2020
- Initial pilot programs working on self-studies

Cyber2yr2020 - Classification Mappings

Available on the ACM CCECC website

- http://ccecc.acm.org/guidance/cybersecurity#mappings

Cyber2yr2020

Program Examples

Ivy Tech Community College

Lord Fairfax Community College

Bluegrass Community and Technical College

Your College!

Benefits - Lord Fairfax Community College

- Designated as a Center of Academic Excellence in Cyber Defense in 2015
- Mapping to Cyber2yr2020
    - Initial courses meeting the requirements for CAE were mapped
        - Some pure cybersecurity
        - Some included in Information Systems Technology program
    - New Programming for Cybersecurity Course mapped
- Program Assessment & Review
    - Cyber2yr2020 Learning Outcomes coordination
- Future Curriculum Growth
    - Identified opportunities for new curriculum

Benefits - Lord Fairfax Community College

- Virginia Commonwealth Benefits
  - Validate cybersecurity curriculum (23 community colleges)
  - Curriculum coordination between K-12, 2-year, and 4-year
- LFCC Benefits
  - Re-Designation to updated CAE 2Y Standards
  - ABET Accreditation Criteria Evaluation
  - New initiatives using mappings
    - AS in Cybersecurity Engineering - New curriculum

See LFCC's Program Mappings on CCECC website:
http://ccecc.acm.org/files/reports/Cyber2yr2020-ProgramExample-LFCC.xlsx

Benefits - Bluegrass Community and Technical College

- 1 of 16 community colleges in Kentucky Community and Technical College System
- Shared statewide Computer & Information Technologies curriculum
- Designated as a Center of Academic Excellence in Cyber Defense in 2019
  - 4 courses met the requirements for the CAE mapping
  - The same 4 courses were mapped to Cyber2yr2020
- **4 courses mapped to and met 100%** of CAE KU Outcomes and Topics
- **4 courses mapped to 100%** of the Cyber2yr2020 Essential Competencies
- **4 course mapped to 83%** of the Cyber2yr2020 Essential + Supplemental Competencies

Benefits - Bluegrass Community and Technical College

- Benefits of Mapping to Cyber2yr2020
  - Detailed analysis of curriculum
  - Comparison between statewide curriculum and national guidelines
  - Validate the statewide curriculum
  - Support future updates to curriculum
- New initiatives as a result of mapping
  - AAS degree in Cybersecurity - new degree
  - Cybersecurity Academy - dual credit classes

See BCTC's Cybersecurity Mapping on CCECC website:
http://ccecc.acm.org/files/reports/Cyber2yr2020-ProgramExample-BCTC.xlsx

Submit Your Cyber2yr2020 Program Example

Highlight your Cybersecurity program by submitting a program example at

ccecc.acm.org/correlations

ACM Curriculum Guidelines

Other Computing Disciplines

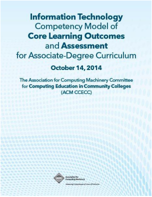
IT-Transfer2020

IT2yr2014

CSTransfer2017

ACM Curriculum Guidelines for Associate-Degree Programs

- Information Technology - IT2yr2014
  - Guidelines for the core of A.A.S. / career programs
  - Infused with cybersecurity



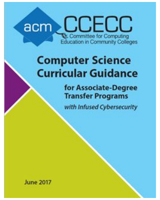
Information Technology
Competency Model of
Core Learning Outcomes
and **Assessment**
for Associate-Degree Curriculum

October 14, 2014

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

ccecc.acm.org

- Computer Science - CSTransfer2017
  - Guidelines for A.S. / transfer programs
  - Infused with cybersecurity

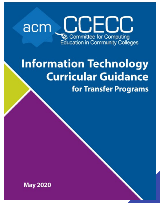


acm CCECC
Committee for Computing
Education in Community Colleges

Computer Science
Curricular Guidance
for Associate-Degree
Transfer Programs
with Infused Cybersecurity

June 2017

- Information Technology Transfer - IT-Transfer2020
  - Guidelines for transfer programs
  - Aligned with IT2017



acm CCECC
Committee for Computing
Education in Community Colleges

Information Technology
Curricular Guidance
for Transfer Programs

May 2020

Questions?

ccecc.acm.org