

Shaping ACM Cybersecurity Curriculum Guidelines

3CS 2019

July 31, 2019

Cara Tang, Portland Community College, OR

Cindy Tucker, Bluegrass Community & Tech. College, KY

Christian Servin, El Paso Community College, TX

Markus Geissler, Cosumnes River College, CA

Melissa Stange, Lord Fairfax Community College, VA

Outline

- ACM CCECC and Curricular Guidelines
- CSEC2Y Background
- CSEC2Y IronDog Draft
- Group Breakouts and Feedback

ACM CCECC and Curricular Guidelines

ACM Curriculum Guidelines for Undergraduate Programs

www.acm.org/education

CC2005 (Computing Curricula 2005): The Overview Report

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

Under Development

- CC2020
- Data Science

Introduction to ACM CCECC



Committee for Computing Education in Community Colleges

- 40++ years of service to computing education
- Standing committee of the ACM Education Board for 25+ years

Global Mission

Serve and support community and technical college educators in all aspects of computing education

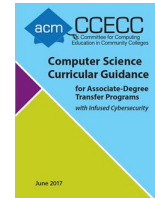
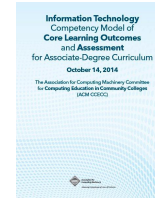
Engage in curriculum and assessment development, community building, and advocacy in service to this sector of higher education

ccecc.acm.org

ACM Curriculum Guidelines for Associate-Degree Programs

Produced by the CCECC

- Information Technology - IT Competency Model 2014
 - Guidelines for the core of A.A.S. / career programs
 - Infused with cybersecurity
- Computer Science - CTransfer2017
 - Guidelines for A.S. / transfer programs
 - Infused with cybersecurity



Current Projects

- Cybersecurity - CSEC2Y
- IT Transfer

CSEC2Y Background

CSEC2Y 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
- Updated for currency & appropriateness at the two-year college level
- Other influences:
 - CAE2Y knowledge units (KUs) - 2019 Foundational + Technical Core
 - NICE Cybersecurity Workforce Framework

CSEC2017

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.*

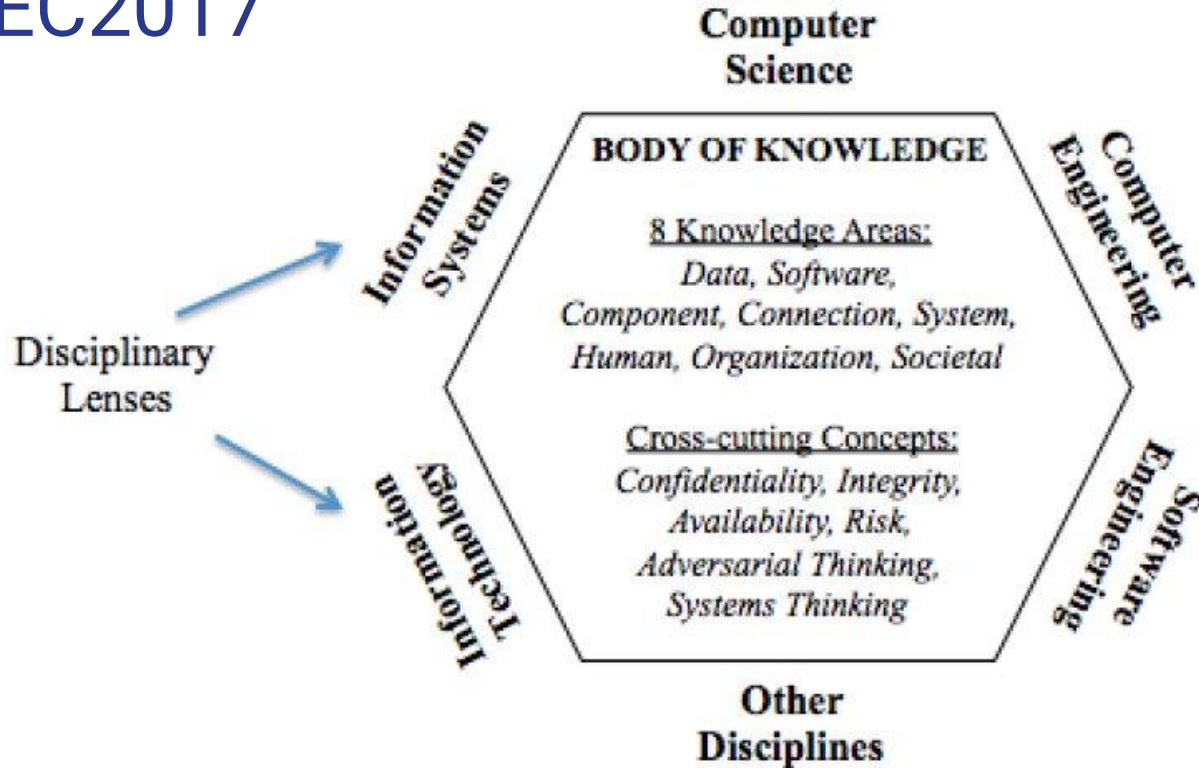
Organization

- Knowledge areas, knowledge units, topics
- Cross-cutting concepts
- Disciplinary lenses

cybered.acm.org



CSEC2017



CSEC2Y 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

CSEC2Y Advisors

Antonio Bologna | Rapid 7

Elizabeth 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

CSEC2Y Timeline

2018 April: First Task Group Meeting

2019 February: StrawDog

2019 July: IronDog - **comments due August 15**

2019 Dec: Final Version

Project overview and status:

ccecc.acm.org/guidance/cybersecurity

CSEC2Y
IronDog

CSEC2Y Draft

Maintain the 8 Knowledge Areas (KAs) of CSEC2017:

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

CSEC2Y Draft

CSEC2017 Structure

Within each of the 8
Knowledge Areas

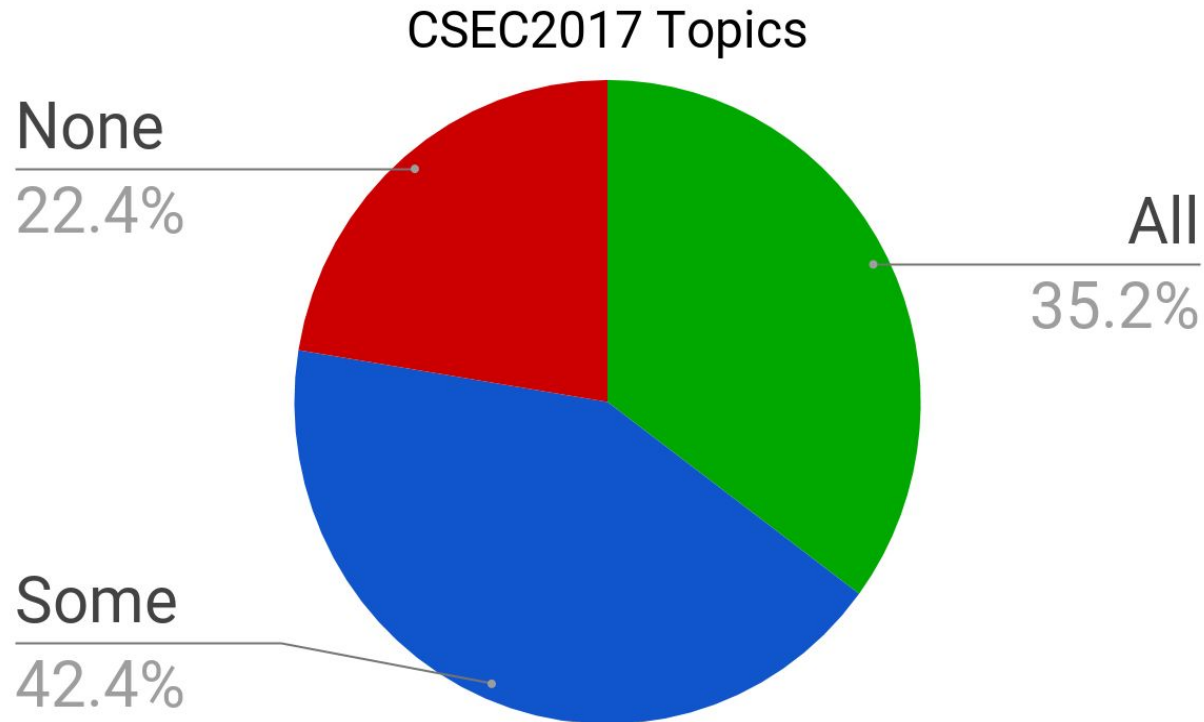
- Essentials
- Knowledge Units
 - **Topics**

CSEC2Y 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

CSEC2Y Draft



Competencies and Learning Outcomes 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”*
- Learning outcomes focus on **student achievement**
- Avoid traditional body of knowledge focus on topics
- Use Bloom’s Revised Taxonomy

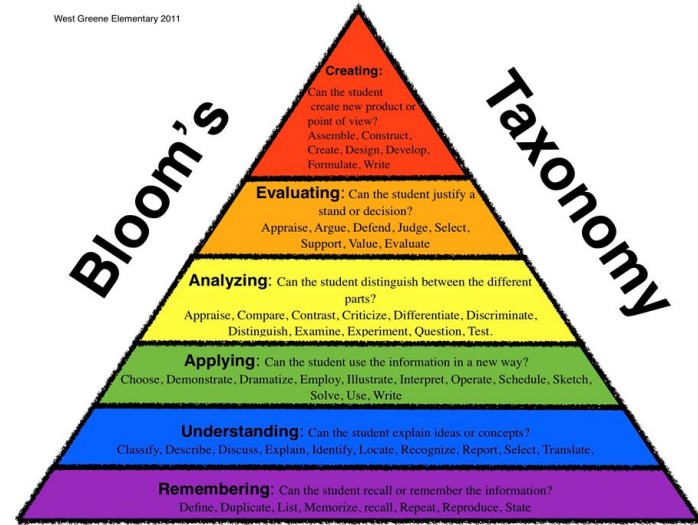
* Frezza et al, 2018. *Modelling Competencies for Computing Education beyond 2020: A Research Based Approach to Defining Competencies in the Computing Disciplines*

Bloom's Revised Taxonomy

Six levels of thinking skills in cognitive domain

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

West Greene Elementary 2011



Assessment Verbs by Bloom's Level



Lower Order
Thinking Skills

Higher Order
Thinking Skills

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

CSEC2Y Curricular Framework Structure

Essential

- Cross-Cutting Competencies
- 8 Knowledge Areas
 - Competencies
 - Knowledge Units
 - Learning Outcomes

Supplemental

- 8 Knowledge Areas
 - Competencies
 - Knowledge Units
 - 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.

*Confidentiality,
Integrity,
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*

*Adversarial
Thinking*

*Systems
Thinking*

Selected Competencies - Software Security

- Demonstrate techniques of defensive programming and secure coding in a software system. *Understanding*
- Analyze the software development life cycle and explain and discuss how security can be incorporated into the software development life cycle.
Analyzing
- Use documentation or a knowledge base to resolve a security challenge in an identified computing scenario. *Applying*



CSEC2Y IronDog Table of Contents

Introduction

- Overview
- How to use these Guidelines
- Two-year/Community College Environment
- Diversity in the Computing Profession
- Ethics and Professionalism
- Mathematics Requirement
- The Cybersecurity Discipline

Cybersecurity Curricular Framework

Essential

- Cross-Cutting Competencies
- 8 Knowledge Areas
 - Competencies
 - Knowledge Units
 - Learning Outcomes

Supplemental

- (same as Essential)

References

Appendix: Competencies

Group Breakout

Review Essential and Supplemental Competencies

Questions to Consider:

- Input on specific competencies
- How clear is Essential & Supplemental?
- What would make the guidelines (more) useful?
- Would adding rubrics help you?
- Any other input

Report Out

Questions to Consider:

- Input on specific competencies
- How clear is Essential & Supplemental?
- What would make the guidelines (more) useful?
- Would adding rubrics help you?
- Any other input

Review CSEC2Y IronDog



Review the IronDog draft and complete the feedback survey to offer your input and help shape the next version of the guidelines!

- Input on specific competencies
- What would make the guidelines more useful?
- Would adding rubrics help you?
- Any other input

Feedback deadline:
August 15

Find IronDog and the feedback survey at:

ccecc.acm.org

Related Cybersecurity Initiatives

ABET Cybersecurity Program Accreditation

ABET accredits 4-year computing programs in

- Computer Science
- Information Systems
- Information Technology
- **Cybersecurity** - new; first 4 schools accredited in pilot round 2017-2018

ABET is developing criteria for accrediting **2-year cybersecurity programs**.

- **Criteria will be based on CSEC2Y**

