ABET

Associate-degree Cybersecurity Accreditation Criteria

Elizabeth K. Hawthorne, PhD, CISSP
ekhawthorne@gmail.com

Oregon Council of Computing Chairs (OCCC)

22 April 2022

Beth’s Brief Bio

- Senior Professor Emerita, Computer Science and Cybersecurity, Union County College, NJ
- PI, NSF FORCCE-ATE grant @ Prince George’s CC, MD
    - FORitifying Cybersecurity and Computing Education through ATE grants
- Served on steering committee for the Cyber Education Project (2014)
- Served on several ACM two-year and four-year curricular development steering committees, including CSEC 2017
- Served as past chair of the ACM CCECC (~decade)
- ACM Education Board Co-Chair
- CSAB Board of Directors
- ACM Distinguished Educator (2015)
- ABET Program Evaluator (PEV) for Cybersecurity & Computer Science

Who is ABET?

- A nonprofit, non-governmental agency that accredits programs in applied and natural science, **computing** [e.g., **cybersecurity**], engineering and engineering technology
- ABET **accredits programs**, not institutions (NSA CAE)
- Accreditation for **post-secondary programs** within degree-granting institutions already recognized by national or regional institutional accreditation agencies
- Accreditation is voluntary, and to date, **4,361 programs** at **850 colleges and universities** in **41 countries** have received ABET accreditation
- abet.org/accreditation/

Cybersecurity Criteria History 4YCY

- 2014 – Cyber Education Project formed
- 2017 – CAC approves 4YCY 1st Reading
- 2017 – CAC visits first four 4YCY pilot programs
- 2018 – CAC accredits first four 4YCY programs
- 2018 – CAC approves 4YCY 2nd Reading

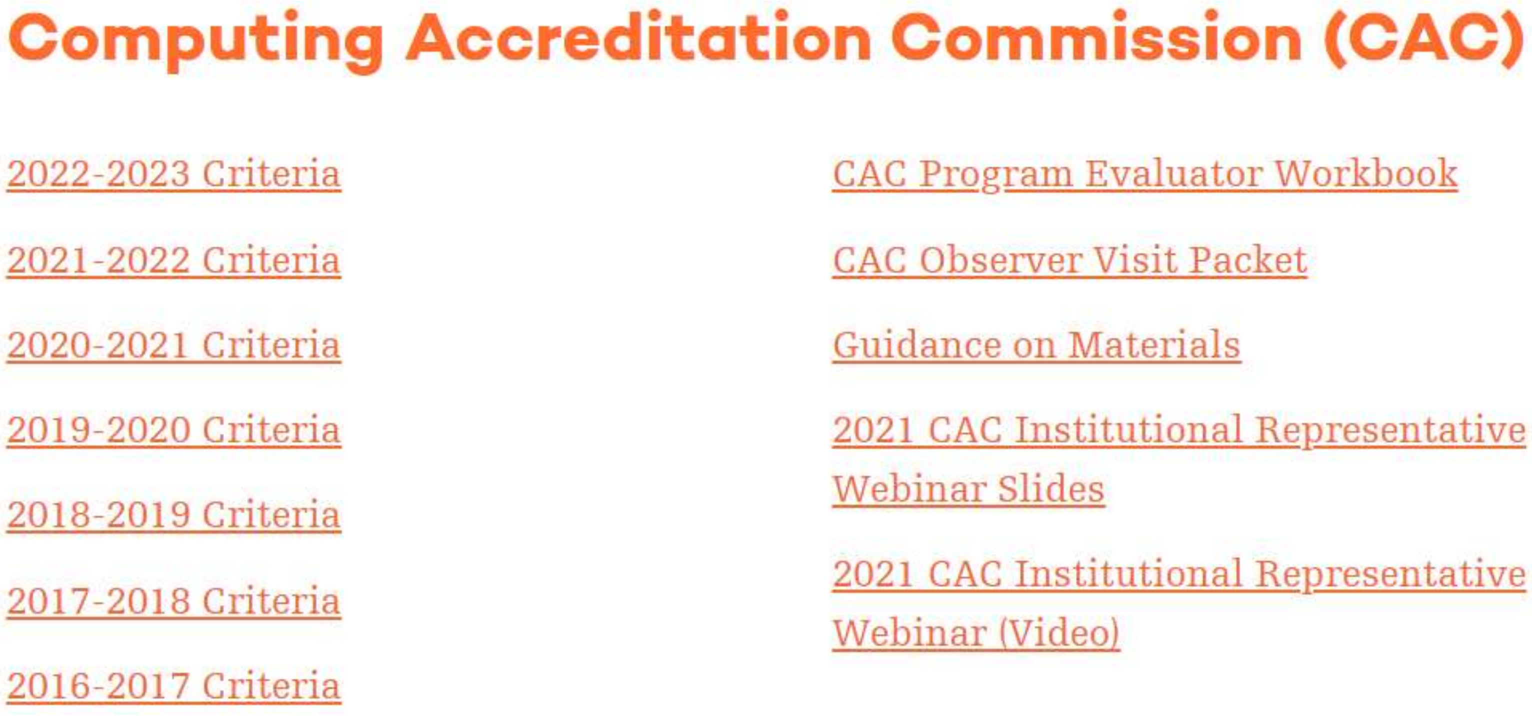
Cybersecurity Criteria History 2YCY

- **Jan-Mar 2019** – Develop initial draft of Criteria from ACM guidelines
- **Mar 2019** – Core Team feedback on First Draft and revision
- **Apr 2019** – Core Team feedback on Second Draft and (minor) revision
- **May 2019** – CAC Commissioner Webinars and feedback
- **Jun 2019** – Revisions to finalize the First Reading Draft
- **July 2019** – Full commission votes First Reading Draft at summer meeting
- **Aug 2019** – Computing Area Delegation (CAD) approval
- **Sept-Dec 2019** – Public review and comment on first reading
- **Jan 2020** – Accept 2YCY Pilot Program Requests for Evaluation
- **Spring 2020** – CAC approves unchanged 2YCY 2nd Reading
- **Fall 2020** – Conduct first 2 pilot 2YCY reviews
- **Summer 2021** – CAC approves 2YCY 2nd Reading in July
- **Fall 2021** – Conduct second round of pilot 2YCY reviews

2YCY Criteria References

- Cybersecurity Curricula 2017 (CSEC 2017)
- Cybersecurity Curricular Guidance for Associate Degree Programs (CSEC2Y or Cyber2yr 2020)
- CAC 4-Year General and Cybersecurity program criteria
- ETAC 2-Year Engineering Technology program criteria
- NSA CAE-2Y requirements
- Existing community college cybersecurity program curricula

Accreditation Criteria



Computing Accreditation Commission (CAC)

- 2022-2023 Criteria
- 2021-2022 Criteria
- 2020-2021 Criteria
- 2019-2020 Criteria
- 2018-2019 Criteria
- 2017-2018 Criteria
- 2016-2017 Criteria

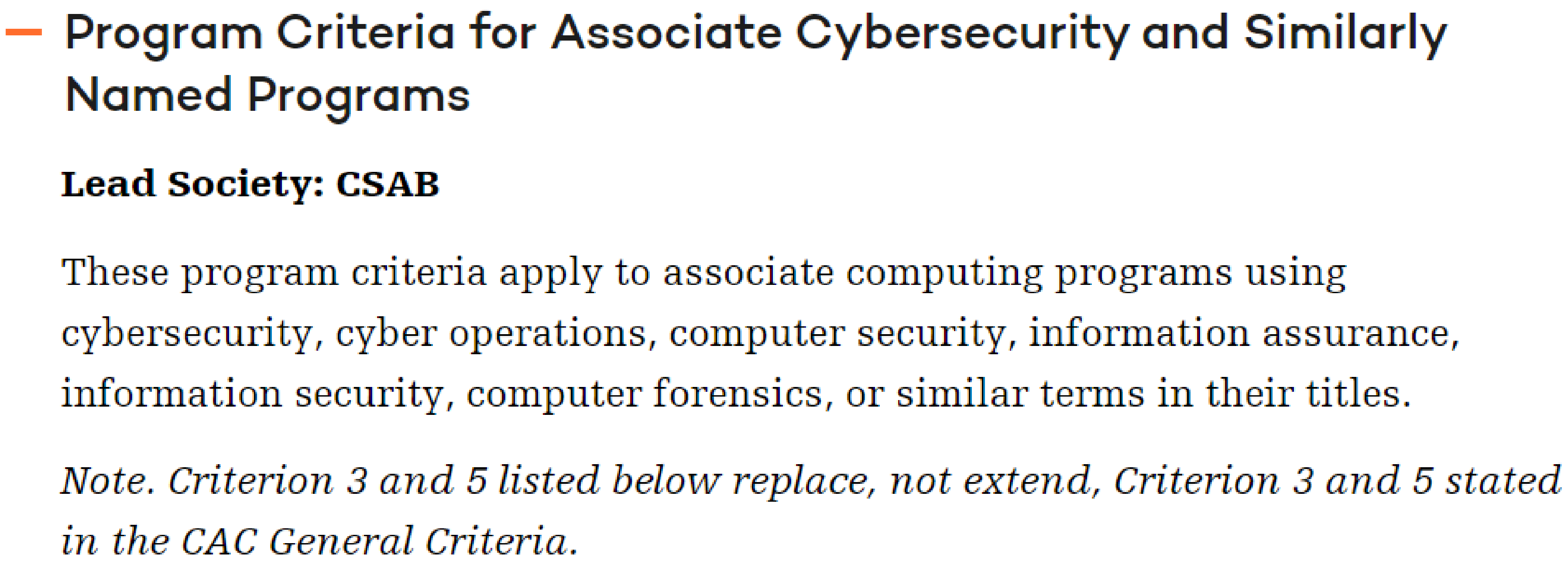
- CAC Program Evaluator Workbook
- CAC Observer Visit Packet
- Guidance on Materials
- 2021 CAC Institutional Representative Webinar Slides
- 2021 CAC Institutional Representative Webinar (Video)

www.abet.org/accreditation/accreditation-criteria/

General Criteria

- Criterion 1. Students
- Criterion 2. Program Educational Objectives
- Criterion 3. Student Outcomes
- Criterion 4. Continuous Improvement
- Criterion 5. Curriculum
- Criterion 6. Faculty
- Criterion 7. Facilities
- Criterion 8. Institutional Support

Cybersecurity Program Criteria



Program Criteria for Associate Cybersecurity and Similarly Named Programs

Lead Society: CSAB

These program criteria apply to associate computing programs using cybersecurity, cyber operations, computer security, information assurance, information security, computer forensics, or similar terms in their titles.

Note. Criterion 3 and 5 listed below replace, not extend, Criterion 3 and 5 stated in the CAC General Criteria.

Criterion 3 – Student Outcomes

The program must have documented and publicly stated student outcomes that include (1) through (5) below. The program may define additional outcomes.

Graduates of the program will have an ability to:

1. Analyze a broadly defined security problem and apply principles of cybersecurity to the design and implementation of solutions.
2. Aply security principles and practices to maintain operations in the presence of risks and threats.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.
5. Function effectively as a member of a team engaged in cybersecurity activities.

Criterion 5 – Curriculum (1 of 2)

The program's requirements must be consistent with its program educational objectives and designed in such a way that each of the student outcomes can be attained. The curriculum must combine technical, professional, and general education components to prepare students for a career and lifelong professional development in the cybersecurity discipline.

The program must include at least **30 semester credit hours** (or equivalent) of up-to-date coverage of cybersecurity topics that include:

1. Application of techniques, skills, and tools necessary for cybersecurity practice.
2. Application of the crosscutting concepts of confidentiality, integrity, availability, risk, adversarial thinking and systems thinking.

Criterion 5 – Curriculum (2 of 2)

3. **Fundamental topics from each of the following:**
    - **Data Security**: protection of data at rest, during processing, and in transit.
    - **Software Security**: development and use of software that reliably preserves the security properties of the protected information and systems.
    - **Component Security**: the security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into larger systems.
    - **Connection Security**: security of the connections between components, both physical and logical.
    - **System Security**: security aspects of systems that use software and are composed of components and connections.
    - **Human Security**: the study of human behavior in the context of data protection, privacy, and threat mitigation.
    - **Organizational Security**: protecting organizations from cybersecurity threats and managing risk to support successful accomplishment of the organizations’ missions.

Resources

- ABET
- ABET Accreditation Criteria for Two-Year Cybersecurity Programs (2022-23)
- The Value of an Accredited Cybersecurity Program (2020)
- ABET Accreditation Fees for Four-Year Programs (will be less for two-year programs; ~$800 vs. $3,350)
- ACM CCECC and Cyber2Y curricular guidelines
- ACM2Y

Q & A