August 13, 2021

Based on feedback from an initial round of pilot visits, these criteria were slightly modified, resubmitted to, and approved by the CAC last month. They will be before the Computing Area Delegation/ABET for second reading approval in October.

WITHOUT MARKUP

PROGRAM CRITERIA FOR ASSOCIATE CYBERSECURITY AND SIMILARLY NAMED COMPUTING PROGRAMS

Approved July 20, 2019 for Public Review and Comment
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.

Criterion 1. Students

Student performance must be evaluated. Student progress must be monitored to foster success in attaining student outcomes, thereby enabling graduates to attain program educational objectives. Students must be advised regarding curriculum and career matters.

The program must have and enforce policies for accepting both new and transfer students, awarding appropriate academic credit for courses taken at other institutions, and awarding appropriate academic credit for work in lieu of courses taken at the institution. The program must have and enforce procedures to ensure and document that students who graduate meet all graduation requirements.

Criterion 2. Program Educational Objectives

The program must have published program educational objectives that are consistent with the mission of the institution, the needs of the program’s various constituencies, and these criteria. There must be a documented, systematically utilized, and effective process, involving program constituencies, for the periodic review of these program educational objectives that ensures they remain consistent with the institutional mission, the program’s constituents’ needs, and these 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. Apply 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 4. Continuous Improvement

The program must regularly use appropriate, documented processes for assessing and evaluating the extent to which the student outcomes are being attained. The results of these evaluations must be systematically utilized as input for the continuous improvement of the program. Other available information may also be used to assist in the continuous improvement of the program.

Criterion 5. Curriculum

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 that includes:

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.

3. Cybersecurity topics from each of the following areas:

   - **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.
   - **Societal Security**: aspects of cybersecurity that broadly impact society as a whole.

4. Programming or scripting skills.

5. Advanced cybersecurity topics that build on the above crosscutting concepts and cybersecurity topics.

The program must ensure its students have the mathematical skills required to meet its student outcomes and program educational objectives.

Criterion 6. Faculty

Each faculty member teaching in the program must have expertise and educational background consistent with the contributions to the program expected from the faculty member. The competence of faculty members must be demonstrated by such factors as education, professional credentials and certifications, professional experience, ongoing professional development, contributions to the discipline, teaching effectiveness, and communication skills. Collectively, the faculty must have the breadth and depth to cover all curricular areas of the program.

The faculty serving in the program must be of sufficient number to maintain continuity, stability, oversight, student interaction, and advising. The faculty must have sufficient responsibility and authority to improve the program through definition and revision of program educational objectives and student outcomes as well as through the implementation of a program of study that fosters the attainment of student outcomes.

Criterion 7. Facilities

Classrooms, offices, laboratories, and associated equipment must be adequate to support attainment of the student outcomes and to provide an atmosphere conducive to learning. Modern tools, equipment, computing resources, and laboratories appropriate to the program must be available, accessible, and systematically maintained and upgraded to enable students to attain the student outcomes and to support program needs. Students must be provided appropriate guidance regarding the use of the tools, equipment, computing resources, and laboratories available to the program.

The library services and the computing and information infrastructure must be adequate to support the scholarly and professional activities of the students and faculty.

Criterion 8. Institutional Support

Institutional support and leadership must be adequate to ensure the quality and continuity of the program.

Resources including institutional services, financial support, and staff (both administrative and technical) provided to the program must be adequate to meet program needs. The resources available to the program must be sufficient to attract, retain, and provide for the continued professional development of a qualified faculty. The resources available to the program must be sufficient to acquire, maintain, and operate infrastructures, facilities and equipment appropriate for the program, and to provide an environment in which student outcomes can be attained.

WITH MARKUP

PROGRAM CRITERIA FOR ASSOCIATE CYBERSECURITY AND SIMILARLY NAMED COMPUTING PROGRAMS
Approved July 20, 2019 for Public Review and Comment
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.

Criterion 1. Students

Student performance must be evaluated. Student progress must be monitored to foster success in attaining student outcomes, thereby enabling graduates to attain program educational objectives. Students must be advised regarding curriculum and career matters.

The program must have and enforce policies for accepting both new and transfer students, awarding appropriate academic credit for courses taken at other institutions, and awarding appropriate academic credit for work in lieu of courses taken at the institution. The program must have and enforce procedures to ensure and document that students who graduate meet all graduation requirements.

Criterion 2. Program Educational Objectives

The program must have published program educational objectives that are consistent with the mission of the institution, the needs of the program's various constituencies, and these criteria. There must be a documented, systematically utilized, and effective process, involving program constituencies, for the periodic review of these program educational objectives that ensures they remain consistent with the institutional mission, the program's constituents' needs, and these 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. Apply 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 4. Continuous Improvement

The program must regularly use appropriate, documented processes for assessing and evaluating the extent to which the student outcomes are being attained. The results of these evaluations must be systematically utilized as input for the continuous improvement of the program. Other available information may also be used to assist in the continuous improvement of the program.

Criterion 5. Curriculum

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 that includes:~~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.

3. ~~Fundamental t~~Cybersecurity topics from each of the following areas:

    - **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.
    - **Societal Security**: aspects of cybersecurity that broadly impact society as a whole.

4. Programming or scripting skills.

~~4.~~5. Advanced cybersecurity topics that build on the above crosscutting concepts and ~~fundamental~~ cybersecurity topics.

The program must ensure its students have the mathematical skills ~~and an understanding of the scripting and programming concepts~~ required ~~for cybersecurity practice~~ to meet its student outcomes and program educational objectives.

Criterion 6. Faculty

Each faculty member teaching in the program must have expertise and educational background consistent with the contributions to the program expected from the faculty member. The competence of faculty members must be demonstrated by such factors as education, professional credentials and certifications, professional experience, ongoing professional development, contributions to the discipline, teaching effectiveness, and communication skills. Collectively, the faculty must have the breadth and depth to cover all curricular areas of the program.

The faculty serving in the program must be of sufficient number to maintain continuity, stability, oversight, student interaction, and advising. The faculty must have sufficient responsibility and authority to improve the program through definition and revision of program educational objectives and student outcomes as well as through the implementation of a program of study that fosters the attainment of student outcomes.

Criterion 7. Facilities

Classrooms, offices, laboratories, and associated equipment must be adequate to support attainment of the student outcomes and to provide an atmosphere conducive to learning. Modern tools, equipment, computing resources, and laboratories appropriate to the program must be available, accessible, and systematically maintained and upgraded to enable students to attain the student outcomes and to support program needs. Students must be provided appropriate guidance regarding the use of the tools, equipment, computing resources, and laboratories available to the program.

The library services and the computing and information infrastructure must be adequate to support the scholarly and professional activities of the students and faculty.

Criterion 8. Institutional Support

Institutional support and leadership must be adequate to ensure the quality and continuity of the program.

Resources including institutional services, financial support, and staff (both administrative and technical) provided to the program must be adequate to meet program needs. The resources available to the program must be sufficient to attract, retain, and provide for the continued professional development of a qualified faculty. The resources available to the program must be sufficient to acquire, maintain, and operate infrastructures, facilities and equipment appropriate for the program, and to provide an environment in which student outcomes can be attained.