Using Competency Based Education to Design a Cybersecurity Curriculum

Fred L. Strickland
fred.strickland@maine.edu
College of Arts and Sciences
University of Maine at Presque Isle
Presque Isle Maine 04769, United States

Abstract

Since 1999, the National Security Agency (NSA) has used Knowledge Units (KUs) as a way to cover key areas. An institution would document how its courses mapped to the KUs. If an institution covered certain KUs and met other requirements such as being regionally accredited, offering academic degrees, and so on, then it would be designated as a Center of Academic Excellence (CAE). Reviewers found it hard to determine if an institution was fully covering the KUs. Periodically, the NSA's stakeholders (such as the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the National Institute of Standards and Technology /National Initiative on Cybersecurity Education, the National Science Foundation, the Department of Defense Office of the Chief Information Officer, and US Cyber Command) would review the program. Recently, they decided that major changes were needed. The changes included requiring that an entire individual KU's learning outcomes and topics be in one course instead of being in two or more courses. Achieving CAE was changed to being a two-step process. A program needed to complete the Program of Study validation step. Then a program would need to complete additional requirements before receiving the CAE designation. New applicants and current CAE holders would need to comply with these changes. At nearly the same time, *Computing Curricula 2020* was published, which focused on competency-based learning. This paper covers how our university is working to comply with these new requirements by using the Competency-Based Education approach.

Keywords: Curricula, Competency-Based Education (CBE), National Centers of Academic Excellence (NCAE), Knowledge Units (KUs)

1. INTRODUCTION

With input from outsiders, the University of Maine at Presque Isle (UMPI) cybersecurity program was created. The first class started in Fall 2019. Right away, we realized that 2 of the 13 computing (COS) courses were not true academic courses[i] and more COS courses were needed and that changes were needed. We wanted to follow the best educational approach, which appears to be competency based education (CBE). This paper reports on our efforts to determine what COS courses should be added and to shift from knowledge-based learning to competency-based learning.

Credentialing

Subject to state level approval, any institution can create a cybersecurity program. Beyond this, an institution may seek program credentialing from the Computing Accreditation Commission (CAC) of the ABET[ii] or from the National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE) program office or both.

For these agencies, credentialing means that a program meets certain requirements and covers certain learning outcomes (LOs). ABET looks directly or indirectly[iii] at programs globally and has accredited 19 cybersecurity programs. The NSA looks at programs in the United States (US)

and its possessions and has approved 349 cybersecurity programs.

Program Building Approaches
Most approaches take LOs as a given. The exceptions tend to be weak efforts.

Kim and Beuran (2018, October 26-28) focused on creating a methodology for designing a cybersecurity higher education programs in Japan. Their six-step process included creating education frameworks, reviewing the pedagogical models, and designing curricula. They used a survey of faculty, industry, and students and they used a Japan Business Federation's skill map to determine the specific subjects and topics. They did not use any credentialing agencies' LOs.[iv]

The City University of New York (n.d.) uses the ADDIE (Analysis, Design, Development, Implementation, and Evaluation) instructional design process model for building a course. The LOs are taken as a given.

In *The Theory and Practice of Online Learning* (2008c), most authors (Ally, 2008; Anderson, 2008b, 2008d; Conrad, 2008; Fahy, 2008; Kanuka, 2008; Kondra, Huber, Michalczuk, & Woudtra, 2008; and Parker, 2008) started with the premise that LOs are a given. Davis, Little, & Stewart (2008) did note that LOs needed to be "based upon a good understanding of an institution's or company's core business and values." The authors deviated when they wrote about the need to address the "student market and the needs of the curriculum." The authors did not consider using input from credentialing authorities nor from hiring companies.

Hutchison, Tin, and Cao (2008) pointed out that there is a need to evaluate LOs. Anderson (2008a) was on the same track when he noted that there is a need to assess LOs. However, no details were provided to explain what is needed to be done for evaluating or for assessing the LOs.

Caplan and Graham (2008) wrote about the ideal course development team. The subject matter expert is to "ensure that the content of the online course is an appropriate alternative to the lecture content normally given in a traditional course." The instructional designer needs to write "statements of learning outcomes." But the authors did not mention the source for these LOs.

Parker (2008) came closer to the matter of defining LOs when she wrote:

> *Another tension emanates from the fact that the bulk of what is delivered in the online environment consists of discrete training modules directed to particular job skills or competencies. While there seems to be slippage between what is articulated in the realm of learning outcomes (the skills we expect graduates to demonstrate) and our expectations around the values associated with the liberal arts, it is fair to say that higher education aims should be broader than the goals of the corporate training sector.*

Parker did not answer the question about the sources of those LOs.

As a side note Parker wrote that the Australian Universities Quality Agency has created the environment where there is so much concern about "institutional quality assurance" that mastering course LOs has suffered. She was pleased that the United States is avoiding this trap of destroying the "delicate balance between 'accreditation to assure quality in higher education, the self-regulation of higher education institutions, and the availability of federal money to colleges and universities.'" She saw as noteworthy that the eight regional accrediting commissions have resolved to sustain the value of having 'instructional programs [that] lead to [the award of] degrees that having [any] integrity are [to be] organized around substantive and coherent curricula which define expected learning outcomes." The regional accrediting commissions are not micro-managing the creation of LOs, but have deferred to the institutions.

What is presented in conferences, in workshops, and in other venues is similar to the presentation at the 3rd Annual Texas A&M Assessment Conference where Osters and Tiu (n.d.) stated that "a measurable learning outcome" is about

- Student learning behaviors
- Appropriate assessment methods

- Specific student performance criteria / criteria for success

All these sources failed to address the topic of using standards or authorities for creating course LOs. Instead, they implied or stated that the instructor is the one responsible for defining the knowledge and the skills that students should be mastering in a course. In practice, the instructor may follow what a textbook contains. And textbooks may be organized around the author's own LO list or around a defined "Body of Knowledge" area or around something else.

A noteworthy exception is Clark, Stoker, and Vetter (2019). They wrote about their experience for seeking the CAE-CDE designation in 2018. They wrote about the CAE changes from 2017 to 2018 and the required additional work. They addressed LOs. Their paper was insightful, but the numerous changes made to the CAE in 2020 has rendered some of their insights as obsolete.

2. COMPETENCY BASED EDUCATION (CBE)

Higher education is reinventing itself to serve better adult learners. Efforts have ranged from three-year bachelor's programs to micro-credentials.

CBE was put forth in 2011 as a new approach that is very focused on what is actually taught. As explained on the Competency-Based Education Network website (n.d.), "students acquire and demonstrate their knowledge and skills by engaging in learning exercises, activities[,] and experiences that align with clearly defined programmatic outcomes." Levine and Patrick (2019) wrote that CBE is driven to "transform [the] educational system so all students can and will learn through full engagement and support and through authentic, rigorous learning experiences inside and outside the classroom."

There have been calls for higher education to spell out the paths to completion and what students would have mastered by graduation. This is a major departure from the traditional approach whereby students "log in seat time" and accumulates a defined number of credit hours. Breaking with the traditional approach, CBE institutions will accept mastery of skills gained prior to the beginning of a program or of a course.

CBE uses authentic and measurable assessments whereby students may advance at their own pace. The LOs are packaged in modules that consist of the LO statement, the materials to teach the LOs, and an assessment (tests or projects).

Students may create their own personal pathway through a set of modules. A module could have a pretest whereby a person could "test out" and thus receive credit for the module and access to the next module. The instructor servers as a guide or as a coach.

No matter how a student progresses through the modules, there will be a final assessment. This could be a test or a project.

Various agencies are embracing CBE. The following sub section mentions a few selected agencies.

The New England Commission of Higher Education (NECHE)

In the NECHE *Standards for Accreditation* (2021, January 1), there are eight standards. Standard Eight addressed educational effectiveness. Paragraph 8.3 mentioned competency and is presented in Table 1.

8.3 Assessment of learning is based on verifiable statements of what students are expected to gain, achieve, demonstrate, or know by the time they complete their academic program. The process of understanding what and how students are learning focuses on the course, competency, program, and institutional level. Assessment has the support of the institution's academic and institutional leadership and the systematic involvement of faculty and appropriate staff.

Table 1. Extract from Standards for Accreditation: Standard 8: Educational Effectiveness

Each member state is expected to implement this policy. In the University of Maine System (UMS), guidance has been published in the UMS *Policy Manual – Program Approval, Review, & Elimination* (2019, July 15). The details on this document and the details on how each of the seven state universities are implementing the policy will not be covered in this paper.

UMPI Embracing CBE

UMPI has fully embraced CBE for its on-line degrees (YourPace) and has the Center for Teaching and Learning (CTL) for helping instructors to design courses to use CBE.

YourPace takes advantage of a person's previous knowledge and experiences. Courses are organized as modules called "Learning Outcomes." The person demonstrates mastery of the module's content. Then moves to the next module. Hence, the name of "YourPace."

The CTL has many resources such as instructional designers, a professional development lending library, workshops, and so on. The Curriculum Coordinator[v] works with instructors for crafting their courses along CBE lines.

The National Security Agency's (NSA) National Centers of Academic Excellence (NCAE) Program

Very few individuals were choosing intelligence as a career. In 1999, the NSA created the CAE in Information Assurance Education (CAE-IAE) program (CAE Community, 2019). An institution would receive the CAE-IAE designation if the program had a rigorous curriculum and satisfied other requirements.

This successful approach was expanded to address the shortfall in qualified cybersecurity professionals. In 2004, the US Department of Homeland Security became a co-sponsor (CAE Community, 2019). A research designation was added in 2008 (CAE Community, 2019). In 2017, the program name was changed to the "Center of Academic Excellence in Cyber Defense Education (CAE-CDE)" (CAE Community, 2019).[vi] In 2019, a two-year college pathway was added (CAE Community, 2019).

There are three designations:

- CAE in Cyber Defense Education (CAE-CDE)
- CAE in Research (CAE-R)
- CAE in Cyber Operations (CAE-CO)

Information on all these can be found at https://www.nsa.gov/resources/student-educators/centers-academic-excellence/

The main component is the knowledge unit (KU) requirement. A KU has LOs and required topics. There are 3 foundational KUs that all programs must have. There are 5 objective-driven KUs. The remaining KUs are based on what is the mission of the program.

Academic Level	Foundational KUs	Objective Driven KUs	Program Choice KUs
Associates	Required 3	5 Technical core OR 5 Non-technical core	3
Bachelors			14
Masters	Required 3 or evidence from another program		7 plus a thesis
Doctoral			3 plus a dissertation [vii]

Table 2. Knowledge Unit Requirements

A two-year program must have at least 11 KUs. A bachelors' program must have at least 22 KUs. Graduate level programs assume some undergraduate preparation. Table 2 summaries the NSA's (2020) KU requirements.

Periodically, the NSA's stakeholder[viii] would review the program and make any necessary changes. New applicants would need to comply, but existing programs would be "grandfathered."

Around 2019, the stakeholders decided that major changes were needed. One stakeholder recommended that a course needed to contain all of an individual KU's LOs and required topics. Another recommended the end of grandfathering. Another recommended a two-step process whereby an institution would work through the Program of Study (PoS) and later work on the CAE. These recommendations plus others were adopted.

For the PoS Step, an institution must show its curriculum path and must show that students are enrolled and are successfully completing the curriculum path. And the students must be receiving some type of recognition for the effort. In short, this addressed the curriculum, the student related information, the faculty profiles and their qualifications, and the continuous improvement efforts.

The course listing must be designed to support the program level LOs. The courses listed for the PoS step must be all required courses. Elective courses are not considered. The PoS must be published on the institution's website.

For the NSA to validate a PoS, the program must have been in existence for at least three years and at least one class (minimum of three students) has completed or graduated from the program. No changes may be made during this period. If any changes are made, then the "clock" is reset.

The reviewers would be asking for information on the following items:

- How the program aligns with the National Initiative for Cybersecurity Education (NICE) Framework
- Syllabi for all courses with a KU alignment.
- Identify courses with applied labs and the instructions for those labs.
- Program-Level LOs
- Mapping of the Program-Level LOs to courses.
- Documentation for the assessment indicators for each Program-Level LOs.

- How the KUs align to the PoS.
- Identify which courses support which KU.
- Listing of course LOs for each KU aligned course.
- The academic year when each KU aligned course was last offered.
- Enrollment figures for the last three years.
- At least three redacted student transcripts from the within the past three years.
- Documentation that recognizes the students' completion of the program.
- Samples of students' work.
- Documentation of students' participation in extracurricular activities.
- Faculty information
- Proof of continuous improvement

Program-Level LOs must be identified and on the program's web page. The self-study must document the KUs and the alignment of the KUs to the relevant courses. The new approach means that it is better to fully align a KU to a course than to spread pieces of a KU across two or more courses.

An institution could have several PoS offerings. These could be marketed. If a PoS has been reviewed and validated by the NSA, then that fact could be used as a marketing point.

The institution must have a validated PoS before working on the CAE-CDE Designation step. The institution needs to have the following items:

- Evidence of an institutional cybersecurity posture and plan. Someone designed as the official for overseeing implementation of a plan for protecting the institution's critical information and systems.
- The established of a physical or virtual cybersecurity center.
- The institution must affirm their commitment to the CAE Core Values.
- Proof that the program will continue.
- Professional development opportunities.
- Other degree programs must include some cybersecurity elements.
- Outreach beyond the home institution's campus.
- Transfer of credit agreements.

For the Post CAE-CDE Designation Requirements, an institution must submit an annual report, must continue to improve, must continue to meet the CAE-CDE designation requirements, and must attend various meetings. Due to space limitations and the scope of this paper, the details will not be covered here.

The Association for Computing Machinery (ACM) and IEEE Computer Society (IEEE-CS) Support of CBE.

The ACM and IEEE[ix] CS with input from others published *Computing Curricula 2020* (2020). This report is a major shift from knowledge-based learning to competency-based learning. The change was necessary as the knowledge-based learning paradigm has not been sufficient to prepare ready-to-work graduates. Too many universities produce computing graduates that are intellectually smart, but have difficulties functioning in a workplace setting.

The report stated that knowledge is only one part of a competency. "… the idea of competency as the foundational idea on which to base academic program design permits a stronger alignment between the product of an education and the needs of professional practice in the workplace."

The report provided a framework for creating competencies [Competency = [Knowledge + Skills + Dispositions] in Task].

- Knowledge: The factual understanding of computing concepts. This is the "know-what" dimension.

- Skills: The capability of applying knowledge to complete a task. This is the "know-how" dimension.

- Dispositions: The socio-emotional skills, behaviors, and attitudes that address the desire to carry out tasks and the sensitivity to know when and how to engage in those tasks. This is the "know-why" dimension.

- Task: The "construct that frames the skilled application of knowledge and makes dispositions concrete."

Using a competency model for defining a computing curriculum produces benefits for the many constituencies. A list of competencies can come from many stakeholders. (For example, UMPI is an institution that serves small businesses and agricultural interests. There is an advisory board that communicates the needs of the major constituencies.)

A competency statement describes an area. Then it has a list of required competencies with the needed knowledge and skills. The disposition is presented in the context of activities such a presenting to a group, producing useful procedures, or monitoring activities in a work unit.

3. CAE IN NEW ENGLAND AND IN MAINE

Each New England state has at least one CAE designated program:

- Connecticut has one CAE-R and one CAE-CO.
- Maine has two CAE-CDEs. One is at a community college and the other is at a UMS university.
- Massachusetts has five institutions with approved CAEs. There are two CAE-CDEs, four CAE-Rs, and one CAE-CO.
- New Hampshire has one CAE-R and one CAE-CDE.
- Rhode Island has three institutions with approved CAEs. There are two CAE-CDEs, one CAE-R, and one CAE-2Y (for two-year institutions).
- Vermont has two CAE-CDEs.

Drilling Down on Maine

The University of Maine at Augusta (UMA) cybersecurity program began in 2014. The UMA website does not contain a history page, but clues about the cybersecurity program can be found by reviewing the academic catalogs from 2014 and onward (University of Maine at Augusta, 2014, 2015, 2016, 2017, 2018a, 2019, and 2020). A detailed review of those catalogs is left to the reader to do.

The UMA CAE-CDE was granted in 2014. Degree granting authority started in 2015. The CAE-CDE designation was renewed in 2019 (CAE Community, n.d.).

One CAE-CDE requirement is that an institution must have outreach. UMA satisfied this requirement by founding the Maine Cybersecurity Center (MCC) (University of Maine at Augusta, 2018b) and by helping other UMS institutions to launch their own cybersecurity programs.

4. Changing UMPI's Cybersecurity Program

As noted in the introduction, the UMPI program needed to be revised. The NSA's CAE-CDE requirements were not fully addressed. The current program would prepare graduates to serve in any arena.

If UMPI wanted the CAE-CDE designation, then the program would need to be changed in order to comply with the current CAE-CDE requirements. The planned changes would make it distinctive by being a technical offering that would enable a person to wear additional "hats" (a technology manager, an IT worker, and a software programmer). This would support many of the UMPI's constituencies that are composed of small businesses, small government agencies, and similar entities. As UMPI is located in an agricultural area, the person would learn about supply chain security first hand.

The UMPI distinctiveness would be based on having:

- A CBE approach.
- A solid program that would obtain the CAE-CDE the first time out.
- Program accreditation. A typical person may not understand the value of a program being a holder of the PoS or of the CAE-CDE, but he or she would understand accreditation.
    - Of the 19 accredited cybersecurity programs in the United States, the closest ones to Maine are located in Maryland.
- A think-outside-of-the-box approach by offering something to schoolteachers.

5. UMPI AND THE NSA'S KUs

The NSA requires bachelor's programs to have at least 22 KUs as defined by Table 2. UMPI would comply by having the following KUs covered by these UMPI courses:

- 3 Cybersecurity Foundational KUs
    - ISC IT Systems Components in UMPI COS 210[x]
    - CSF Cybersecurity Foundations in UMPI COS 2dd[xi]
    - CSP Cybersecurity Principles in UMPI COS 2dd
- 5 Technical Core KUs
    - BSP Basic Scripting and Programming in UMPI COS 110
    - BNW Basic Networking in UMPI COS 240
    - BCY Basic Cryptography in UMPI COS 2ad
    - OSC Operating Systems Concepts in UMPI COS 310
    - NDF Network Defense in UMPI COS 440
- 14 Program Choice KUs
    - DST Data Structures in UMPI COS 120
    - ALG Algorithms in UMPI COS 230
    - DVF Device Forensics in UMPI COS 232
    - DFS Digital Forensics in UMPI COS 232
    - FAC Forensic Accounting in UMPI BUS/COS 2bb

- SCS Supply Chain Security in UMPI COS 2ii
- CPM Cybersecurity Planning and Management in UMPI COS 2ae
- IDS Intrusion Detection/Prevention Systems in UMPI COS 340
- DMS Database Management Systems in UMPI COS 350
- DAT Databases in UMPI COS 350
- CCR Cyber Crime in UMPI COS 410
- CTH Cyber Threats in UMPI COS 410
- PLE Policy, Legal, Ethics, and Compliance in UMPI COS 485
- FPM Fraud Prevention and Management in UMPI COS 4ee

Since UMPI's niche is small businesses and small government entities, our graduates would need additional skills. Many of the Choice KUs would enable a graduate to be a knowledgeable business staffer, to be an IT person, and to be a programmer.

6. UMPI AND PROGRAM ACCREDITATION

UMPI has both computer science and cybersecurity programs. The CAC of the ABET considers accreditation based on the program's name. If the name contains the phrase "computer science," then it must satisfy the computer science program requirements. If the name contains the word "cybersecurity," then it must satisfy the cybersecurity program requirements. Both program requirements have the same five program LOs.[xii] Both have a requirement for discrete mathematics.

There are some differences. Computer science programs must have at least 40 semester credit hours of computing courses, 15 semester credit hours of mathematics (discrete mathematics plus courses that have the rigor at least equivalent to introductory calculus), and 6 semester hours of lab-based science courses. Cybersecurity programs must have at least 45 semester credit hours of computing or cybersecurity courses and 6 semester credit hours of mathematics (discrete mathematics and statistics). Cybersecurity programs do not have a lab-based science requirement.

The CAC of the ABET uses the curriculum guidance as provided by certain agencies.

The ACM and the IEEE CS formed the Joint Task Force on Computing Curricula. The final document was published in 2013 as *Computer Science Curricula 2013* (The Joint Task Force on Computing Curricula, 2013).

A few years later, these two entities along with participation from the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) formed the Joint Task Force on Cybersecurity Education. The final document was published in 2017 as *Cybersecurity Curricula 2017* (Joint Task Force on Cybersecurity Education, 2017).

To obtain future program accreditation, the UMPI 2 computer science programs and the UMPI cybersecurity program draw from these resources. The three programs have some common elements.

7. UMPI AND THE CSTA

As part of the thinking-outside-of-the-box approach, UMPI has the long-range goal of adding computer science educator programs to the UMPI College of Education. UMPI would need to seek accreditation from the CSTA. The first document is the *CSTA K-12 Computer Science Standards* (Computer Science Teachers Association, 2017), which covers what students should be taught. The second document is the *Standards for Computer Science Teachers* (Computer Science Teachers Association, 2020), which covers the education and the preparation that K-12 teachers should have.

The second document has five major areas. The first area addressed knowledge and skills. Within this area, there are six indicators of what makes for an effective teacher. These boil down to the content areas that are listed in the first document, which are:

- Algorithms & Programming
- Computing Systems
- Data & Analysis
- Impacts of Computing
- Networks & the Internet

Within these content areas, there are numerous sub-concepts such as cybersecurity, hardware, software, network communications, program development, storage, and so on. Upon closer examination, it turns out the first document is not purely about computer science, but a combination of computer science topics and cybersecurity topics. This document is arranged in columns (Identifier, Grades, Standard, Concept Subconcept, and Practices). The information in the Standard column is a narrative that spells out

the LOs. The following UMPI courses would support these:

- UMPI COS 101 Introduction to Computer Science
- UMPI COS 110 Programming Fundamentals
- UMPI COS 120 Introduction to Data Structures
- UMPI COS 210 IT System Components[xiii]
- UMPI COS 220 Programming Languages
- UMPI COS 230 Algorithm Theory and Development
- UMPI COS 240 Network Concepts
- UMPI COS 2ad Basic Cryptography
- UMPI COS 305 Computational Science
- UMPI COS 310 Operating Systems
- UMPI COS 320 Software Engineering I
- UMPI COS 330 Object-Oriented Programming
- UMPI COS 350 Databases and Database Management Systems[xiv]
- UMPI COS 410 Cyber Crime and Cyber Threats[xv]
- UMPI COS 440 Network Security Administration and Defenses[xvi]
- UMPI COS 485 Cybersecurity Policy, Legal, and Ethics[xvii]

When we do create the computer science educator programs, we envision that a preservice educator would be earning a double major (education and computer science) with a mathematics minor. Thus these educator programs could be accredited by the CAC of the ABET, by the Council for the Accreditation of Educator Preparation,[xviii] by the Maine Department of Education, and by the CSTA.

8. DISCUSSION: UMPI AND THE CBE APPROACH FOR DESIGNING THE COMPUTING PROGRAMS

We looked at the LOs from the NSA, from the CAC of the ABET, from the computing curriculum guidance, and from the CSTA. Once a list was created for a course, then the course would be structured to address each LO.

To track the LOs, these were numbered with the course code and a sequence number as in "COS 110) 1." In the narrative, the source document is cited. This was done so that upon a course review, the reviewer could check to see if the source document has changed. The following shows a sample of LOs from UMPI COS 110 Programming Fundamentals course:

- COS 110) 1. Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g. to automate system administration tasks). [BSP 1][xix]
- COS 110) 5. Analyze and explain the behavior of simple programs involving the fundamental programming constructs variables, expressions, assignments, I/O, control constructs, functions, parameter passing, and recursion. [Assessment] [SDF/FPC 1][xx]
- COS 110) 14. Trace the execution of a variety of code segments and write summaries of their computations. [Assessment] [SDF/DM 1][xxi]
- COS 110) 17. Model the way programs store and manipulate data by using numbers or other symbols to represent information. [1A-AP-09][xxii]

Since we are pulling from several authorities for LOs, a particular concept may appear in two or more sources. We would assign the same course LO code to these. We would retain the duplicates in order to show that we are addressing the LOs from all authorities.

With a firm LO list, then we would find resources that would support each course LO. We have used resources from research papers, from conference papers, from Open Education Resources materials[xxiii], and from high quality websites.

Each class session or module would start with a listing of the LOs to be covered. The students know what would be covered. The instructors know what needs to be covered. Any adjunct or substitute instructor would know what needed to be taught. One or more assignments would be given with the purpose of reinforcing the LOs. The final assessment could be an academic exam or a project.

Most of the modules are independent units. A collection of these would form a course. Some courses would depend upon material presented in another course.

Some LOs are introduced and later modules would go deeper.

9. CONCLUSION

Taking a CBE approach for designing a degree program and each course in that program is labor intensive. It requires reviewing and reworking the weak areas. This is necessary if an institution wishes to teach the important concepts and avoid assigning busy work tasks.

We are still creating new courses and it may take teaching and revising a course a few times, before

we get it exactly the way it should be. When this is done, then a student would have the option of testing out of a module or out of an entire course.

Gone are the days when parents would send their children to a local university in order to keep them out of trouble or to prepare them for taking part in the family's business. Today's students want an education that challenges them and that supports his or her goals by teaching relevant concepts.

For years, the ACM and the IEEE have emphasized knowledge-based learning. Now they are shifting to competency-based learning (ACM & IEEE, 2020). So the CBE approach is gaining more supporters. This is a perfect time to join the CBE movement.

10. ACKNOWLEDGEMENTS

I wish to acknowledge the insights provided by Jason Johnston, the CTL, fellow professors, and CSTA Maine.

11. REFERENCES

ABET. (2015) ABET Constitution. https://www.abet.org/wp-content/uploads/2020/02/Ratified-ABET-Constitution-2015-Public.pdf

ABET. (2021). "Criteria for Accrediting Computing Programs, 2021 – 2022." https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2021-2022/

ACM & IEEE. (2020). *Computing Curricula 2020: Paradigms for Global Computing Education.* https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

Ally, M. (2008). Foundations of educational theory for online learning. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 15-44). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Anderson, T. (2008a). Social software to support distance education learners. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 221-241). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Anderson, T. (2008b). Teaching in an online learning context. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 343-365). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Anderson, T. (Ed.). (2008c). *The Theory and Practice of Online Learnin*g (2nd ed.). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/99z_anderson_2008-theory_and_practice_of_online_learning.pdf

Anderson, T. (2008d). Towards a theory of online learning. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 45-74). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

CAE Community. (2019). "Centers of Academic Excellence in Cybersecurity." https://www.caecommunity.org/content/what-is-a-cae

CAE Community. (n.d.). "UMA University of Maine at Augusta." https://www.caecommunity.org/sites/default/files/CAE_Book_version_1.6-2_93.pdf page 186

Caplan, D. & Graham, R. (2008). The development online courses. In T. Anderson (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 245-263). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

City University of New York. (n.d.). "Course Design & Development Tutorial." https://spscoursedesign.commons.gc.cuny.edu/introduction-to-design-and-development/

Clark, U., Stoker, G., & Vetter, R. (2019). Looking ahead to CAE-CD program changes. In *2019 Proceedings of the EDSIG Conference*. Information Systems and Academic Professionals. http://proc.iscap.info/2019/pdf/4920.pdf

Competency-Based Education Network. (n.d.). "What is competency-Based Education?" https://www.cbenetwork.org/competency-based-education/

Computer Science Teachers Association. (2017). *CSTA K-12 Computer Science Standards, Revised 2017.* http://www.csteachers.org/standards

Computer Science Teachers Association. (2020). *Standards for Computer Science Teachers*. https://csteachers.org/page/standards-for-cs-teachers

Conrad, D. (2008). Situating prior learning assessment and recognition (PLAR) in an online learning environment. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 75-90). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Davis, A., Little P., & Stewart, B. (2008). Developing an infrastructure for online learning. In T. Anderson, T (Ed), The Theory and Practice of Online Learning (2nd ed.). (pp. 121-142). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Fahy, P. (2008). Characteristics of interactive online learning media. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 167-199). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Hutchison, M., Tin, T., & Cao Y. (2008). "In-your-pocket" and "on-the-fly:" Meeting the needs of today's new generation of online learners with mobile learning technology. In T. Anderson (Ed.), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 201-219). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

The Joint Task Force on Computing Curricula. (2013, December 20). *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf

Joint Task Force on Cybersecurity Education. (2017, December 31). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Kanuka, H. (2008). Understanding e-learning technologies-in-practice through philosophies-n-practice. In T. Anderson, T (Ed), The Theory and Practice of Online Learning (2nd ed.). (pp. 91-118). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Kim, E., & Beuran R. (2018, October 26-28). On designing a cybersecurity education program for higher education [Paper presentation]. 2018 10th International Conference on Education Technology and Computers, Tokyo, Japan. https://www.jaist.ac.jp/~razvan/publications/designing_cybersecurity_program.pdf

Kondra, A. Z., Huber, C., Michalczuk, K., & Woudtra, A. (2008). Call centres in distance education. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 367-395). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

Levine E., & Patrick S. (2019). *What is competency-based education? An updated definition*. Vienna, VA: Aurora Institute

National Security Agency. (2020). *2020 Knowledge Units*. https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf

New England Commission of Higher Education. (2021, January 1). *Standards for Accreditation*. https://www.neche.org/wp-content/uploads/2020/12Standards-for-Accreditation-2012pdf

Osters, S., & Tiu, F. S. (n.d.). Writing Measurable Learning Outcomes." https://www.gavilan.edu/research/spd/Writing-Measurable-Learning-Outcomes.pdf

Parker, N. (2008). The quality dilemma in online education revisited. In T. Anderson, T (Ed), *The Theory and Practice of Online Learnin*g (2nd ed.). (pp. 305-340). AU Press. https://biblioteca.pucv.cl/site/colecciones/manuales_u/9z_anderson_2008-theory_and_practice_of_online_learning.pdf

University of Maine at Augusta. (2014). *UMA 2014-2015 UMA Catalog*. https://www.uma.edu/academics/wp-content/uploads/sites/3/2017/03/2014-15-Catalog.pdf

University of Maine at Augusta (2015). *UMA 2015-2016 UMA Catalog*. https://www.uma.edu/academics/wp-

content/uploads/sites/3/2017/03/2015-16-Catalog-ADA-Compliant.pdf See page 35.

University of Maine at Augusta. (2016). *2016/17 catalog*. https://www.uma.edu/academics/wp-content/uploads/sites/3/2017/06/2016-17-Catalog-Final-for-Printing-1.pdf See page 35, 36, 80, and 83.

University of Maine at Augusta. (2017). *2017-2018 Catalog*. https://www.uma.edu/academics/wp-content/uploads/sites/3/2017/03/2017-18-Catalog-Final-Version.pdf

University of Maine at Augusta. (2018a). *2018/19 Catalog*. https://www.uma.edu/academics/wp-content/uploads/sites/3/2018/08/2018-19-Catalog.pdf

University of Maine at Augusta. (2018b). "Maine Cybersecurity Center." https://www.mcc.maine.edu/

University of Maine at Augusta. (2019). *UMA Catalog | 2019/20*. https://www.uma.edu/academics/wp-content/uploads/sites/3/2019/09/2019-20-Catalog-Final-Version.pdf

University of Maine at Augusta. (2020). "Home |Catalog | Cybersecurity (BS) | Mission Statement," http://catalog.uma.edu/content.php?catoid=2&navoid=112

University of Maine at Presque Isle. (2020, May 10). *Academic Program Planning & Assessment Policy Manual*. https://drive.google.com/drive/u/0/folders/1r4t54Q-pWown_MgKPOvCJX1D3p8djFr6

University of Maine System. (2019, July 15). Policy Manual – Program Approval, Review, & Elimination. https://www.maine.edu/board-of-trustees/policy-manual/section-305-1/

Appendices

Details on the UMPI Courses
The first column has the course code. The codes in bold font where the ones that UMA provided course descriptions to help launch the UMPI cybersecurity degree program.

The second column is the current course title. Some of these will be changed.

The third column is the proposed course title for those courses that need a new title.

The next three columns pertain to current degrees.

The last four columns pertain to future degrees.

The information below the degree titles pertain to the National Security Agency's Knowledge Units and to the Computer Science Teachers Association *CSTA K-12 Computer Science Standards, Revised 2017* content areas.

ISSN 2473-4901
v7 n5532

Course Code (Bold font: Listed in the MSCS 2019-20 catalog.)	Current Title	Revised Title (If needed.)	Cybersecurity BS (22 NSA knowledge units.)	Computer Science, Software Development Concentration, BS	Computer Science, Information and Data Management Concentration, BS	Elementary Education, Computer Science Concentration, B.S.	Secondary Education - Computer Science, B.S.	Elementary Education, Computer Science Concentration, B.S. (Canadian Requirements)	Secondary Education - Computer Science, B.S. (Canadian Requirements)
			Active; NSA and ABET	Active, ABET	Active; ABET	Goal is 2022; ABET, CAEP- State Review Option Maine DoE, 020 Endorsement	Goal is 2022; ABET, CAEP- State Review Option, Maine DoE	2022, CAEP	2022 CAEP
COS 101	Introduction to Computer Science		Yes	Yes	Yes	Yes. 1A-CS-02. 1A-CS-03 1A-NI-04 1A-DA-05 1A-AP-08 1A-AP-10 1A-AP-11 1B-NI-04	Yes. 2-DA-07 2-1P-11 3A-NI-05 3A-DA-09 3B-AP-22	Yes. 1A-CS-02. 1A-CS-03 1A-NI-04 1A-DA-05 1A-AP-08 1A-AP-10 1A-AP-11 1B-NI-04	Yes. 2-1P-11 3A-NI-05 3A-DA-09 3B-AP-22
COS 110	Programming Fundamentals		Yes, NSA BSP	Yes, ABET 5a2	Yes, ABET 5a2.	Yes. 1A-AP-09 1A-AP-10 1A-AP-11 1A-AP-12 1A-AP-13 1A-AP-14 1A-AP-15 1B-AP-09 1B-AP-10	Yes. 2-AP-10 2-AP-11 2-AP-12 2-AP-13 2-AP-14 2-AP-16 2-AP-17 2-AP-19 3A-CS-01 3A-AP-14	Yes. 1A-AP-09 1A-AP-10 1A-AP-11 1A-AP-12 1A-AP-13 1A-AP-14 1A-AP-15 1B-AP-09 1B-AP-10	Yes. 2-AP-10 2-AP-11 2-AP-12 2-AP-13 2-AP-14 2-AP-16 2-AP-17 2-AP-19 3A-CS-01 3A-AP-14
COS 120	Introduction to Data Structures		Yes, NSA DST	Yes, ABET 5a2	Yes, ABET 5a2.	Yes	Yes. 2-DA-07 3A-DA-10 3A-AP-14 3A-AP-15	Yes	Yes. 2-DA-07 3A-DA-10 3A-AP-14 3A-AP-15

Table A-1. One hundred level courses

COS 200	Introduction to Web Design			Yes					
COS 205	Multimedia Design			Yes					
COS 210	Introduction to Information Security	IT System Components	Yes, ABET 5a1 and 5a2c. NSA ISC			Lowest Common Denominator 1A-IC-18	Needed. 2-NI-04 2-NI-05 3A-NI-04 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08	Lowest Common Denominator 1A-IC-18	Maybe. 2-NI-04 2-NI-05 3A-NI-04 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08
COS 220	Programming Languages			Yes, ABET 5a1	Yes, ABET 5a1	Yes	Yes. 3A-AP-15 3B-AP-24	Yes	Yes. 3A-AP-15 3B-AP-24
COS 230	Algorithm Theory and Development		Yes, NSA ALG	Yes, ABET 5a1	Yes, ABET 5a1	Yes. 1A-AP-14 1B-AP-08	Yes. 2-AP-10 3A-AP-13 3A-IC-26 3B-AP-10 3B-AP-11 3B-AP-13	Yes. 1A-AP-14 1B-AP-08	Yes. 2-AP-10 3A-AP-13 3A-AP-15 3A-IC-26 3B-AP-10 3B-AP-11 3B-AP-13
COS 232	Introduction to Cyber Forensics	Device and Digital Forensics	Yes, NSA DVF and DFS						
COS 235	Architecture and Organization			Yes, ABET 5a3	Yes, ABET 5a3	Yes	Yes	Yes	Yes
COS 240	Network Concepts		Yes, ABET 5a2d and 5a2e. NSA BNW	Yes, ABET 5a3	Yes, ABET 5a3	Yes. 1B-CS-01 1B-NI-04	Yes. 2-NI-04 2-NI-05 3A-CS-04 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08 3B-NI-03 3B-NI-04	Yes. 1B-CS-01 1B-NI-04 1B-NI-05	Yes. 2-NI-04 2-NI-05 3A-CS-04 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08 3B-NI-03 3B-NI-04
COS 250	Management of Enterprise Data			Yes, ABET 5a3	Yes, ABET 5a3	Yes	Yes	Yes	Yes
COS 252	Data Analytics				Yes	Elective	Elective. 3B-DA-05 3B-DA-06	Elective	Elective. 3B-DA-05 3B-DA-06
COS 290	Special Topics in Cybersecurity	Special Topics in Computing	Optional	Optional	Optional				
BUS/COS 2bb	Forensic Accounting		Yes, ABET 5a2a. NSA FAC						
COS 2bc	Cybersecurity Foundations and Principles		Yes, ABET 5a1 and 5a2. NSA CSF and CSP			Elective. 1B-NI-05	Elective. 2-IC-23	Elective. 1B-NI-05	Elective. 2-IC-23
COS 2bd	Supply Chain Security		Yes, ABET 5a2g. NSA SCS						
COS 2ad	Basic Cryptography		Yes, NSA BCY			Lowest Common Denominator	Needed. 2-NI-06 3B-NI-04	Lowest Common Denominator	Yes. 2-NI-06 3B-NI-04
COS 2ae	Cybersecurity Planning and Management		Yes, ABET 5a2g. NSA CPM			Lowest Common Denominator	Elective. 2-IC-23 3A-NI-06 3A-NI-07 3A-NI-08	Lowest Common Denominator	Elective. 2-IC-23 3A-NI-06 3A-NI-07 3A-NI-08
COS 2aa	Host and Network Forensics								
COS 2ab	Media Forensics								

Table A-2. Two hundred level courses

COS 300	Advanced Web Design			Yes					
COS 305	Computational Science			Yes, ABET 5a4	Yes, ABET 5a4	Yes	Yes 3A-DA-11 3A-DA-12 3A-AP-13 3A-IC-26 3B-DA-07 3B-AP-08	Yes	Yes 3A-DA-11 3A-DA-12 3A-AP-13 3A-IC-26 3B-DA-07 3B-AP-08
COS 310	Operating Systems		Yes, NSA OSC	Yes, ABET 5a3	Yes, ABET 5a3	Yes.	Yes. 3A-CS-01 3A-CS-02 3B-CS-01 3B-CS-02	Yes.	Yes. 3A-CS-01 3A-CS-02 3B-CS-01 3B-CS-02
COS 315	Parallel and Distributed Computing			Yes, ABET 5a3	Yes, ABET 5a3	Yes	Yes	Yes	Yes
COS 320	Software Engineering I			Yes, ABET 5a4	Yes, ABET 5a4	Yes. 1A-AP-15 1B-AP-13 1B-AP-16	Yes. 2-CS-01 2-CS-02 2-AP-15 2-AP-17 2-AP-18 3A-CS-02 3A-AP-19 3A-AP-21 3A-AP-22 3A-AP	Yes. 1A-AP-15 1B-AP-13 1B-AP-16	Yes. 2-CS-01 2-CS-02 2-AP-15 2-AP-17 2-AP-18 3A-CS-02 3A-AP-19 3A-AP-21 3A-AP-22 3A-AP
COS 321	Software Engineering II			Yes					
COS 330	Object-Oriented Programming			Yes, ABET 5a1 ABET 5a2	Yes, ABET 5a1 ABET 5a3	Yes	Yes. 3A-CS-01	Yes	Yes. 3A-CS-01
COS 340	Computer Security	Intrusion Detection and Prevention Systems	Yes, ABET 5a2e. NSA IDS			Elective	Elective. 2-NI-05 3A-NI-08	Elective	Elective. 2-NI-05 3A-NI-08
COS 350	Databases and Database Security	Databases and Database Management Systems	Yes, ABET 5a2a. NSA DMS and DAT	Yes, ABET 5a4	Yes, ABET 5a4	Yes.	Yes.	Yes.	Yes.
COS 355	Bioinformatics				Yes				
COS 360	Management of Agriculture and Natural Resource Data				Yes				
COS/EDU 3ab	Elementary Education Computer Scienc	Teaching Computer Science i	e Elementary Sc	l		Yes. Could be 1A-CS-01 1A-DA-06 1A-DA-07 1A-IC-16 1A-IC-17 1B-CS-03 1B-DA-06 1B-DA-07 1B-1C-18 1B-1C-19 1B-1C-20		Yes. Could be 1A-CS-01 1A-DA-06 1A-DA-07 1A-IC-16 1A-IC-17 1B-CS-03 1B-DA-06 1B-DA-07 1B-1C-18 1B-1C-19 1B-1C-20	
COS/EDU 3ac	Secondary Education Computer Science						Yes. 2-CS-03 2-DA-08 2-DA-09 2-IC-20 2-IC-21 2-IC-22 3A-CS-03 3A-DA-09 3A-DA-10 3A-DA-11 3A-DA-12 3A-AP-20 3A-IC-24 3B-DA-05 3B-DA-06 3B-AP-09 3B-IC-26 3B-IC-27		Yes. 2-CS-03 2-DA-08 2-DA-09 2-IC-20 2-IC-21 2-IC-22 3A-CS-03 3A-DA-09 3A-DA-10 3A-DA-11 3A-DA-12 3A-AP-20 3A-IC-24 3B-DA-05 3B-DA-06 3B-AP-09 3B-IC-26 3B-IC-27

Table A-3. Three hundred level courses

ISSN 2473-4901
v7 n5532

COS 410	Cyber Security I	Cyber Crime and Cyber Threats					1B-NI-05	Yes. 3A-NI-05 3A-IC-28	1B-NI-05	Yes. 3A-NI-05 3A-IC-28
COS 440	Network Security	Network Security Administration and Defenses	Yes, ABET 5a1, 5a2a, 5a2f, 5a2g, 5a2h. NSA CCR and CTH Yes, ABET 5a2d. NSA NDF				Yes. 2-NI-05 2-IC-23	Yes. 2-NI-05 2-IC-23 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08	Yes. 2-NI-05 2-IC-23	Yes. 2-NI-05 2-IC-23 3A-NI-05 3A-NI-06 3A-NI-07 3A-NI-08
COS 485	Cybersecurity Capstone	Cybersecurity Policy, Legal, and Ethics	Yes, ABET 5a1, 5a2f, 5a2g. NSA PLE				Yes	Yes. 3A-IC-28 3A-IC-29 3A-IC-30 3B-IC-28	Yes	Yes. 3A-IC-28 3A-IC-29 3A-IC-30 3B-IC-28
COS 495	Cybersecurity or Computer Science Internship		Yes	Yes			Yes	Yes	Yes	Yes
COS 4ee	Fraud Prevention and Management		Yes, 5a2a, t12f, 5a2g. NSA FPM							

Table A-4. Four hundred level courses

[i] One was a special topics course and the other was an internship course.
[ii] The ABET website does not define the acronym ABET. The full name (Accreditation Board for Engineering and Technology, Inc.) appears in Article One of the ABET Constitution (2015).
[iii] The Seoul Accord is about the mutual recognition of accredited academic computing programs. A non-US program could be accredited by the ABET or it could be accredited by another agency that is part of the Seoul Accord. The result is that the non-US program's accreditation by the Seoul Accord participating agency is the same as being accredited by the ABET. See https://www.seoulaccord.org/ for more information.
[iv] As it turns out, no Japanese institution has any Seoul Accord accreditation.
[v] There is another person involved with YourPace. This is the Academic Success Coach. This person works directly with the students to help ensure their success. They do not work with the faculty for design competencies.
[vi] Sometimes the NSA will express the program name as "National Centers of Academic Excellence in Cybersecurity (NCAE-C)" or just simplify "National Centers of Academic Excellence" (NCAE). Other times, the NSA will drop the National (N) from the phrase. I have not attempt to homogenize the expressions.
[vii] The assumption is that the doctoral student has completed a master's degree in a related field.
[viii] The stakeholders list is long. The main ones are the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the National Institute of Standards and Technology /National Initiative on Cybersecurity Education, the National Science Foundation, the Department of Defense Office of the Chief Information Officer, and US Cyber Command)
[ix] The more common practice is to use IEEE instead of "Institute of Electrical and Electronics Engineers," because the membership includes computing professionals, physicists, medical doctors, and others.
[x] Due to space, the full course name is not provided here. The full list may be found in the appendix.
[xi] At this writing, the cybersecurity program is being revised. Six new courses are needed in order to satisfy numerous requirements. The actual course code will be assigned in Spring 2022.
[xii] ABET uses the phrase "Student Outcome." The definition (ABET, 2021) makes it clear that these are program learning outcomes instead of an individual course outcome. That is, these are what the student are expected to know and to be able to do by the time of graduation.
[xiii] This is a revised course title, which may become official in Spring 2022. This is true for UMPI COS 350, UMPI COS 410, UMPI COS 440, and UMPI COS 485.
[xiv] This is a revised course title, which may become official in Spring 2022. This is true for UMPI COS 350, UMPI COS 410, UMPI COS 440, and UMPI COS 485.
[xv] This is a revised course title, which may become official in Spring 2022. This is true for UMPI COS 350, UMPI COS 410, UMPI COS 440, and UMPI COS 485.
[xvi] This is a revised course title, which may become official in Spring 2022. This is true for UMPI COS 350, UMPI COS 410, UMPI COS 440, and UMPI COS 485.
[xvii] This is a revised course title, which may become official in Spring 2022. This is true for UMPI COS 350, UMPI COS 410, UMPI COS 440, and UMPI COS 485.
[xviii] In 2016, the Council for the Accreditation of Educator Preparation (CAEP) replaced the National Council for Accreditation of Teacher Education (NCATE) and Teacher Education Accreditation Council (TEAC) legacy standards. See http://caepnet.org/about/history/ for more information.
[xix] Source: NSA's 2020 Knowledge Units: Basic Scripting and Programming (BSP) Knowledge Unit
[xx] In the ACM's *Computer Science Curricular 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*, a modified Bloom's Taxonomy is used. See page 33 and 34.
[xxi] Source: *ACM's Computer Science Curricular 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*: Software Development Fundamentals/Fundamental Programming Concepts (SDF/FPC).
[xxii] Source: ACM's *Computer Science Curricular 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*: Software Development Fundamentals/Development Methods (SDF/DM)
[xxiii] A valuable resource for this effort is the Open Educational Resources (OER). A good starting place is OER Commons.