CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 1, No. 1
July 2022
ISSN: 2832-1006

In this issue:

iscap
Information Systems
&Computing
Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal. Currently the target acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2022 ISCAP Board of Directors

Cybersecurity Pedagogy and Practice Journal

Editors

Going Beyond Considering the Use of Competency-based Education for Designing 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

The National Security Agency (NSA) uses Knowledge Units (KUs) as a way to cover important topics. An institution would document how its courses mapped to the KUs. If an institution covered certain KUs and met other requirements, 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 CAE program. About 2020, they decided that major changes were needed. The 2021 guidance now requires that a KU's learning outcomes and topics to be in one course instead of being in two or more courses. Achieving CAE was changed to being a two-step process. An institution needed to complete the Program of Study step. Then it would need to complete additional requirements before receiving the CAE designation. New applicants and current CAE holders would need to comply with these changes. In 2019, ABET published cybersecurity accreditation criteria. In 2020, the ACM published *Computing Curricula 2020*, which focused on competency-based learning. This paper covers how our university is working to comply with the NSA and with the ABET 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 courses were needed and that changes were needed. We wanted to obtain the National Security Agency's (NSA's) designation as a Center of Academic Excellence in Cybersecurity and to obtain ABET accreditation. Since we had a new program, we were free to make major changes. So we wanted to follow the best educational approach, which appeared to be competency-based education (CBE). A paper presented at EDSIGCON 2021 (Strickland, 2021) reported on our efforts to determine what courses should be added and to shift from knowledge-based learning to competency-based learning. This journal article will review the high points of that paper and provide additional information.

Credentialing

Subject to state-level approval, any institution could create a cybersecurity program. The program could be housed in the Information Technology unit or in the Computer Science unit or in the Business unit. An institution may seek program credentialing from the NSA's National Centers of Academic Excellence (NCAE) in

Cybersecurity program office. The Computing Accreditation Commission (CAC) of the ABET[ii] (2022) looks at programs that have a computing viewpoint.

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 23 cybersecurity programs. The NSA looks at programs in the United States (US) and its possessions and has approved 357 cybersecurity programs.

Program Building Approaches

Most approaches take LOs as a given. In the previous paper (Strickland, 2021), two major approaches were mentioned. The first explored model is what I called the "Japanese approach" (Kim and Beuran, 2018, October 26-28) and it was used to create a cybersecurity academic program. The second approach is the City University of New York (n.d.) ADDIE (Analysis, Design, Development, Implementation, and Evaluation) instructional design process model for building any type of course.

In a survey of the literature, the previous paper (Strickland, 2021) found that many practitioners took the LOs as a given. In *The Theory and Practice of Online Learning* (Anderson, 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 needed 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.

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 in Cyber Defense Education (CAE-CDE) designation in 2018. They wrote about the CAE-CDE changes from 2017 to 2018[iv] and the required additional work. They addressed LOs. Their paper was insightful, but the numerous changes made to the CAE-CDE process has rendered some of their insights as obsolete.

2. COMPETENCY BASED EDUCATION (CBE)

In the previous paper (Strickland, 2021), the second section provided background information on CBE. Information was provided from the Competency-Based Education Network website (n.d.) about how this helped "students [to] acquire and [to] demonstrate their knowledge and skills by engaging in learning exercises, activities[,] and experiences that align with clearly defined programmatic outcomes." And 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."

The rest of the second section went into greater detail on the philosophy and provided information on how different agencies are implementing CBE. Retained for this paper is the information about UMPI, an abridged presentation on the NCAE program, and the credentialing agencies.

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

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 major 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 core KUs. The remaining KUs are based on what is the mission of the program. Table 1 summarizes the NSA's (2020) KU requirements.

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 [vi]

Table 1: Knowledge Unit Requirements

The most recent change is dated January 2022 (Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG), 2022). This codified all the draft changes into a final authoritative document. New applicants and renewing programs must comply with these requirements.

The two largest changes are that an academic course needs to contain all of an individual KU's LOs and required topics and that achieving the CAE is a two-step process. The first step is the Program of Study (PoS) and the second step is the CAE-CDE Designation.

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, the PoS 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 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. 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-CD 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-C Core Values and Guiding Principles.
- 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 CAE-C Post-Designation Reporting Requirements, an institution must submit an annual report, must continue to improve, must continue to meet the CAE-CD Designation requirements, and must attend various meetings. Due to space limitations and the scope of this paper, those details will not be covered here.

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

While the NSA "will rely upon the institutional accreditation [from a regional agency] for sufficiency of program construction and maintenance" (Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG), 2022), there are other agencies that look at the rigor of the actual academic program.

The ACM has published documents pertaining to curricula recommendations. These have tended to be knowledge-based. Recently the ACM and the IEEE[vii] 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 necessitated as the knowledge-based learning paradigm had 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 as presenting to a group, producing useful procedures, or monitoring activities in a work unit.

3. CAE IN NEW ENGLAND AND IN MAINE

See the previous document (Strickland, 2021) for this information.

4. CHANGING UMPI'S CYBERSECURITY PROGRAM

As noted in the introduction, the UMPI cybersecurity program needed to be revised. The NSA's CAE-CD requirements were not being fully addressed. The current program could prepare graduates to serve in any arena, but the graduates could not claim that they had graduated from an NSA approved program.

If UMPI wanted the CAE-CD designation, then the program would need to be changed in order to comply with the current CAE-CD 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, database manager, 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 PoS the first time out.
- And obtain the CAE-CD soon thereafter.
- Program accreditation. A typical person may not understand the value of a program being a holder of the PoS or of the CAE-CD, but he or she would understand accreditation.
    - Of the 22 accredited cybersecurity programs in the US, 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 in Table 1. 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 IT System Components
    - **CSF** Cybersecurity Foundations in UMPI COS 2dd[viii] Cybersecurity Foundations and Principles
    - **CSP** Cybersecurity Principles in UMPI COS 2dd Cybersecurity Foundations and Principles
- 5 Technical Core KUs
    - **BSP** Basic Scripting and Programming in UMPI COS 110 Programming Fundamentals
    - **BNW** Basic Networking in UMPI COS 240 Network Concepts
    - **BCY** Basic Cryptography in UMPI COS 2ad Basic Cryptography
    - **OSC** Operating Systems Concepts in UMPI COS 310 Operating Systems
    - **NDF** Network Defense in UMPI COS 440 Network Security Administration and Defenses
- 14 Program Choice[ix] KUs
    - **DST** Data Structures in UMPI COS 120 Introduction to Data Structures
    - **ALG** Algorithms in UMPI COS 230 Algorithm Theory and Development
    - **DVF** Device Forensics in UMPI COS 232 Device and Digital Forensics

- **DFS** Digital Forensics in UMPI COS 232 Device and Digital Forensics
- **FAC** Forensic Accounting in UMPI BUS/COS 2bb Forensic Accounting
- **SCS** Supply Chain Security in UMPI COS 2ii Supply Chain Security
- **CPM** Cybersecurity Planning and Management in UMPI COS 2ae Cybersecurity Planning and Management
- **IDS** Intrusion Detection/Prevention Systems in UMPI COS 340 Intrusion Detection and Prevention Systems
- **DMS** Database Management Systems in UMPI COS 350 Databases and Database Management Systems
- **DAT** Databases in UMPI COS 350 Databases and Database Management Systems
- **CCR** Cyber Crime in UMPI COS 410 Cyber Crime and Cyber Threats
- **CTH** Cyber Threats in UMPI COS 410 Cyber Crime and Cyber Threats
- **PLE** Policy, Legal, Ethics, and Compliance in UMPI COS 485 Cybersecurity Policy, Legal, Ethics, and Compliance
- **FPM** Fraud Prevention and Management in UMPI COS 4ee Fraud Prevention and Management

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, to be a database manager, 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.[x] Both have a requirement for discrete mathematics. (This paper will not explore the UMPI computer science programs.)

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. In addition, the criteria for accrediting computing programs are updated every cycle.
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 program accreditation, the UMPI cybersecurity program must draw from these resources.

7. DISCUSSION: UMPI AND THE CBE APPROACH FOR DESIGNING THE CYBERSECURITY PROGRAM

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

To track the LOs, these are 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 for UMPI COS 110 Programming Fundamentals course from four sources:

- 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][xi]
- 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][xii]
- COS 110) 14. Trace the execution of a variety of code segments and write summaries of

their computations. [Assessment] [SDF/DM 1][xiii]

- COS 110) 17. Model the way programs store and manipulate data by using numbers or other symbols to represent information. [1A-AP-09][xiv]

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[xv], 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.

In many disciplines, there is a progression from familiarity to expert and this is done over several courses. Since a program designer needs to select 14 out of the 60 KUs available, the NSA has designed the KUs to be independent and the knowledge to understand a concept is included. This approach has been used in many of the UMPI COS courses.

8. DISCUSSION: THE NEXT STEP

The previous paper (Strickland, 2021) provided information on what we wished to do and what we needed to do.

Since the NSA and the CAC of the ABET are still using knowledge-based LOs, these will be recorded. The UMS Academic Program Planning and Assessment Policy (APPA) process uses the word "competencies." From the context, it appears this could be a synonym for LOs.

As course syllabus documents are created, the appropriate subset of the LOs will be listed. A new section will be added that will document the associated skills and dispositions. The calendar contains the assignments, and this will be revised to document the supporting tasks.

The next step is to take the knowledge-based LOs and render into an official University of Maine System approved package. The steps for doing this are documented in *Academic Program Planning and Assessment Policy Manual* (University of Maine at Presque Isle, 2021 October 26).

The APPA guidance stated that proficiency areas are to be documented in a spreadsheet. The reviewers will be able to see how the program competencies align with the corresponding program courses, program proficiencies, and competency priority levels.

In order to capture the tracking requirements of the various agencies, the following columns are used:

- The program competencies. One column for each one.
- Degree Program (CYB, COS, or Both).
- Course Learning Outcome code (i.e., COS 110) 1).
- Competencies (Free text narrative.)
- OPR (Office of Primary Responsibility: ACM, NSA, CSTA).
- Source Document
- Reference Code (How to find the actual text in the source document.)
- Competency Priority Level (See codes below).
- Competency Levels (Cognitive) (See codes below.)
- Competency Levels (Physical) (See codes below.)
- Bloom Taxonomy or ACM Word
- A column for each course. (Use the cognitive competency letter codes from below.)

The competency priority levels will be documented. The codes are:

- 0 = immaterial for all
- 1 = immaterial for most
- 2 = material for some
- 3 = material for most
- 4 = material for all
- 5 = critical for some
- 6 = critical for most
- 7 = critical for all

Cognitive competency (letters) and physical competency (digits) are documented. The codes are:

- A = Awareness/Define
- B = Situational Identification

- C = Universal Application
- D = Compare, Contrast appropriate alternatives, synthesize
- E = Create, innovate, Invent
- H = Historical Context/Origins
- 1 = Perform with Guidance
- 2 = Perform partly without guidance
- 3 = Perform and problem solve
- 4 = Perform with innovation

The last column before the actual course details contains the Bloom Taxonomy.

Table 2 is an extract. This is for a networking concept course. The extract shows some of the NSA's Basic Networking KU LOs, the ACM's cybersecurity LOs, and the ACM's computer science LOs.

A state education department may not require such a detailed document. The NSA does require a document that maps the program-level LOs to each course in the program. Table 3 is an extract for the BS in Cybersecurity. An institution has some freedom in designing the lay-out of the information.

The APPA package will include additional documents such as course sequencing, individual course documentation, and program documentation.

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.

For years, the ACM and the IEEE have emphasized knowledge-based learning. Now they are shifting to competency-based learning (ACM & IEEE, 2020). The two organizations plan to revise all of the curriculum documents to reflect a CBE approach. In the meantime, a website (https://www.cc2020.net/) will be launched that will have resources such as work-in-progress CBE courses. (At this writing, the website has not been launched.)

This will be an on-going process. It may take time to get all of the pieces working.
Established programs may discover that their NSA designation will be revoked. Reviewing our efforts may help them to fix their programs. New programs may be able to avoid numerous missteps by reviewing our efforts.

10. ACKNOWLEDGEMENTS

I wish to acknowledge the insights provided by Jason Johnston, the CTL, fellow professors, and CSTA Maine. This paper was influenced by attendees to the session where I presented the first paper and by the journal reviewers.

11. REFERENCES

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

ABET. (2022). "Criteria for Accrediting Computing Programs, 2022 – 2023." https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2022-2023/

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

Application Process and Adjudication Rubric (APAR) Cyber Defense Working group (CDWG). (2022) *National Centers of Academic Excellence in Cybersecurity CAE 2022 Designation Requirements and Application Process For CAE-Cyber Defense (CAE-CD).* https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-proposed_cae-cd_designation_requirements.pdf

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

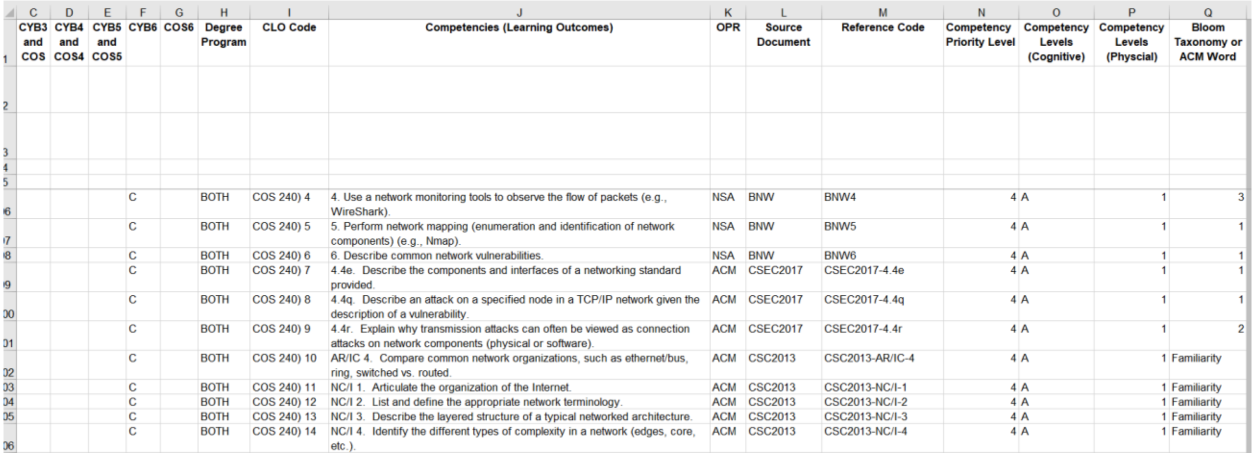
Osters, S., & Tiu, F. S. (n.d.). Writing Measurable Learning Outcomes." https://www.gavilan.edu/research/spd/Writing-Measurable-Learning-Outcomes.pdf

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

Strickland, F. (2021). Using competency-based education to design a cybersecurity curriculum. In EDSIGCON Proceedings 2021. https://proc.iscap.info/2021/pdf/5532.pdf

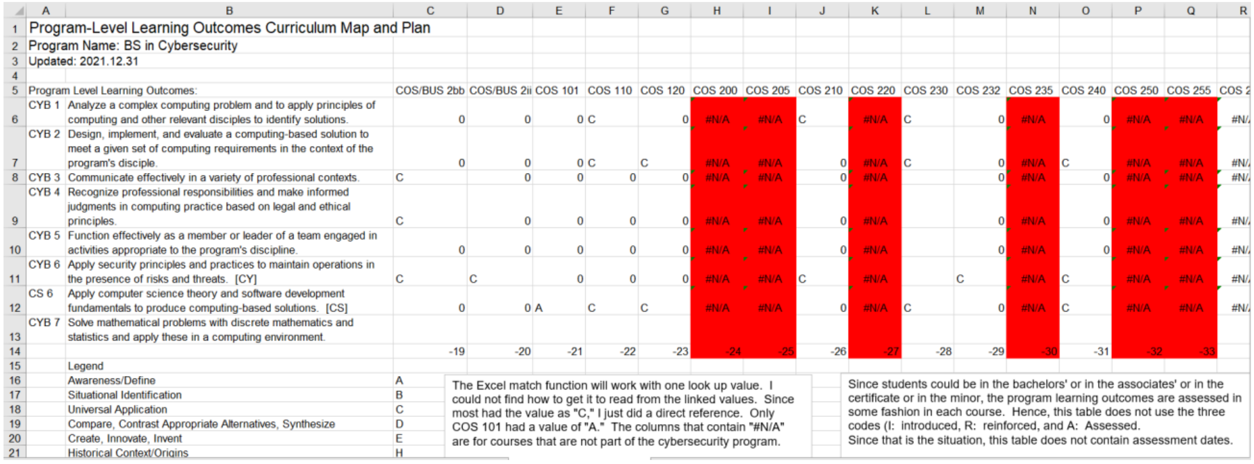
University of Maine at Presque Isle. (2021, October 26). *Academic Program Planning & Assessment Policy Manual*.

Appendix



	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	CYB3 and COS	CYB4 and COS4	CYB5 and COS5	CYB6	COS6	Degree Program	CLO Code	Competencies (Learning Outcomes)	OPR	Source Document	Reference Code	Competency Priority Level	Competency Levels (Cognitive)	Competency Levels (Physcial)	Bloom Taxonomy or ACM Word
2															
3															
4															
5															
6				C		BOTH	COS 240) 4	4. Use a network monitoring tools to observe the flow of packets (e.g., WireShark).	NSA	BNW	BNW4	4	A	1	3
7				C		BOTH	COS 240) 5	5. Perform network mapping (enumeration and identification of network components) (e.g., Nmap).	NSA	BNW	BNW5	4	A	1	1
8				C		BOTH	COS 240) 6	6. Describe common network vulnerabilities.	NSA	BNW	BNW6	4	A	1	1
9				C		BOTH	COS 240) 7	4.4e. Describe the components and interfaces of a networking standard provided.	ACM	CSEC2017	CSEC2017-4.4e	4	A	1	1
00				C		BOTH	COS 240) 8	4.4q. Describe an attack on a specified node in a TCP/IP network given the description of a vulnerability.	ACM	CSEC2017	CSEC2017-4.4q	4	A	1	1
01				C		BOTH	COS 240) 9	4.4r. Explain why transmission attacks can often be viewed as connection attacks on network components (physical or software).	ACM	CSEC2017	CSEC2017-4.4r	4	A	1	2
02				C		BOTH	COS 240) 10	AR/IC 4. Compare common network organizations, such as ethernet/bus, ring, switched vs. routed.	ACM	CSC2013	CSC2013-AR/IC-4	4	A	1	Familiarity
03				C		BOTH	COS 240) 11	NC/I 1. Articulate the organization of the Internet.	ACM	CSC2013	CSC2013-NC/I-1	4	A	1	Familiarity
04				C		BOTH	COS 240) 12	NC/I 2. List and define the appropriate network terminology.	ACM	CSC2013	CSC2013-NC/I-2	4	A	1	Familiarity
05				C		BOTH	COS 240) 13	NC/I 3. Describe the layered structure of a typical networked architecture.	ACM	CSC2013	CSC2013-NC/I-3	4	A	1	Familiarity
06				C		BOTH	COS 240) 14	NC/I 4. Identify the different types of complexity in a network (edges, core, etc.).	ACM	CSC2013	CSC2013-NC/I-4	4	A	1	Familiarity

Table 2: Extract from the "Program Inventory"



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Program-Level Learning Outcomes Curriculum Map and Plan																	
2	Program Name: BS in Cybersecurity																	
3	Updated: 2021.12.31																	
4																		
5	Program Level Learning Outcomes:		COS/BUS 2bb	COS/BUS 2ii	COS 101	COS 110	COS 120	COS 200	COS 205	COS 210	COS 220	COS 230	COS 232	COS 235	COS 240	COS 250	COS 255	COS 2
6	CYB 1	Analyze a complex computing problem and to apply principles of computing and other relevant disciples to identify solutions.	0	0	0	C	0	#N/A	#N/A	C	#N/A	C	0	#N/A	0	#N/A	#N/A	#N/
7	CYB 2	Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's disciple.	0	0	0	C	C	#N/A	#N/A	0	#N/A	C	0	#N/A	C	#N/A	#N/A	#N/
8	CYB 3	Communicate effectively in a variety of professional contexts.	C	0	0	0	0	#N/A	#N/A	0	#N/A		0	#N/A	0	#N/A	#N/A	#N/
9	CYB 4	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	C	0	0	0	0	#N/A	#N/A	0	#N/A		0	#N/A	0	#N/A	#N/A	#N/
10	CYB 5	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	0	0	0	0	0	#N/A	#N/A	0	#N/A		0	#N/A	0	#N/A	#N/A	#N/
11	CYB 6	Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]	C	C	0	0	0	#N/A	#N/A	C	#N/A		C	#N/A	C	#N/A	#N/A	#N/
12	CS 6	Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]	0	0	A	C	C	#N/A	#N/A	0	#N/A	C	0	#N/A	C	#N/A	#N/A	#N/
13	CYB 7	Solve mathematical problems with discrete mathematics and statistics and apply these in a computing environment.																
14			-19	-20	-21	-22	-23	-24	-25	-26	-27	-28	-29	-30	-31	-32	-33	
15		Legend																
16		Awareness/Define	A															
17		Situational Identification	B															
18		Universal Application	C															
19		Compare, Contrast Appropriate Alternatives, Synthesize	D															
20		Create, Innovate, Invent	E															
21		Historical Context/Origins	H															

The Excel match function will work with one look up value. I could not find how to get it to read from the linked values. Since most had the value as "C," I just did a direct reference. Only COS 101 had a value of "A." The columns that contain "#N/A" are for courses that are not part of the cybersecurity program.

Since students could be in the bachelors' or in the associates' or in the certificate or in the minor, the program learning outcomes are assessed in some fashion in each course. Hence, this table does not use the three codes (I: introduced, R: reinforced, and A: Assessed.
Since that is the situation, this table does not contain assessment dates.

Table 3: Extract from the "Curriculum Map and Plan" – BS in Cybersecurity

Footnotes

[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] At EDSIGCON 2021, Ms. Lynne Clark, Chief, NSA/DHS National Centers of Academic Excellence in Cyber Defense was scheduled to appear. Due to a scheduling conflict, another person came in her place. This person stated that the concept of having a technical track and a non-technical track was started in 2018.

[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] The assumption is that the doctoral student has completed a master's degree in a related field.

[vii] 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.

[viii] 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 late Spring 2022.

[ix] The source document uses the word "optional," but a casual reader may think these are not necessary. That is not the case. An institution has a choice of which the 14 KUs might be.

[x] 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.

[xi] Source: NSA's 2020 Knowledge Units: Basic Scripting and Programming (BSP) Knowledge Unit

[xii] 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 pages 33 and 34.

[xiii] Source: *ACM's Computer Science Curricular 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*: Software Development Fundamentals/Fundamental Programming Concepts (SDF/FPC).

[xiv] Source: ACM's *Computer Science Curricular 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*: Software Development Fundamentals/Development Methods (SDF/DM)

[xv] A valuable resource for this effort is the Open Educational Resources (OER). A good starting place is OER Commons.