# Competency in Cybersecurity Education

Version 2. Updated March 2024

*A handbook for educators at NCAE-C designated institutions.*

NORWICH™
UNIVERSITY

# Competency in Cybersecurity Education:

*Presented by:*

Vincent Nestler, vnestler@csusb.edu

Zoe Fowler, zfowler@norwich.edu

*This Careers Preparation National Center product was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-22-1-0329), which is part of the National Security Agency.*

# Contents

# The Purpose of this Handbook

*The purposes of this e-handbook are:*

- To provide a definition of competency and to articulate its importance in relation to the current talent shortages in cybersecurity.
- To explain the five essential elements (ABCDE) of competency and to explain how these facilitate more effective communication between educators and employers.
- To offer a step-by-step guide for educators at NCAE-C (National Centers in Academic Excellence in Cybersecurity) designated institutions in designing, building, facilitating and evaluating competency experiences.
- To demonstrate how competencies can be implemented throughout the student experience, including classroom activities, cyber-clubs, competitions, internships, conferences and more.
- To provide guidance on uploading competency statements into an NCAE-C e-library that will be shared across the CAE-C community.
- To benefit the students within NCAE-C designation institutions through providing them with greater understanding of cybersecurity work roles, inspiring their career choices, preparing them for job interviews and the recruitment process, and increasing their competitiveness within the workplace.

***Many thanks to members of the Competencies Working Group for their guidance in writing this handbook:***

**Anne Kohnke, Ben Lampe, Blair Taylor, Cynthia Irvine, Dan Manson, Edward Vasko, Gary Sparks, Glenn Dietrich, Greg White, Gretchen Bliss, Isaac (Chip) Thornsberg, Jake Mihevc, Jeffrey Hanson, Karen Wetzel, Kim Muschalek, Kristin Hayes, Madeline Russell, Martin Bencic, Michael Franz, Morgan Zantua, Nancy LaTourette, Nate Evans, Paige Flores, Ran Hinrichs, Shakur Abuzneid, Sharon Hamilton, Sidd Kaza, Stephen Miller, Stephen Troupe, Susan Frank, Tirthankar Ghosh, Tyler Moore, William Butler, Yair Levy.**

# Introduction

The national shortage of both cybersecurity capacity and capability threatens to compromise not only the security of individual enterprises, but also our national security and public safety. Demand for cybersecurity professionals across the US continues to outpace the supply of competent recruits, both in terms of quality and quantity. How can we effectively provide the talented cybersecurity workforce which our country urgently needs?

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is managed by NSA's National Cryptologic School and includes federal partners from the Department of Defense Office of the Chief Information Officer (DoD-CIO), U.S. Cyber Command (USCYBERCOM), Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST) / National Initiative on Cybersecurity Education (NICE), and the National Science Foundation (NSF). Over four hundred CAE-designated community colleges, colleges and universities are recognized for leading good practices in cybersecurity curriculum, academic excellence, and building competency in their graduating students. This handbook focuses upon building and sharing good practices in relation to developing the competencies of students within our institutions. If our students are going to be the workforce of the future, we need to ensure they are prepared for the workplaces where they will be employed.

A focus on competency provides an effective bridge between the classroom and the workplace. Both NICE and the DoD maintain frameworks of work roles and the tasks they contain. The challenge facing the cybersecurity educator is how best to educate their student body so that graduates are both knowledgeable about cybersecurity and proficient within the specific work roles relating to the careers they want to build. Through developing opportunities to build competency, we can support our students in successfully integrating their knowledge, skills and attitudes in ways that enable them to be proficient in the workplace.

This handbook provides an effective approach for building the competency of our students. We are not proposing that our schools and colleges should become vocational institutions or shift towards solely competency-based education; instead, we imagine augmenting existing courses through furthering their connections with the workplace and mapping learning onto existing and future work roles. Drawing on work from several NCAE-C initiatives and discussions with leading stakeholders and thinkers within cybersecurity education, we have developed an approach to competency that is beneficial for our educators, employers and students; we have established a definition that is easy to state, easy to remember and easy to implement; and we have identified five key elements of competency. Within this handbook, we provide ideas, support and inspiration for building our students' competencies so that they might be better prepared for the cybersecurity workplace of today and of the future.

> *Students in my Intro to PC Operating Systems enjoy knowing that they are gaining competency with a task that will eventually prepare them for a work role in cybersecurity. Each competency helps them build confidence in their abilities to work in a cybersecurity job.*
>
> —Kim Muschalek

# Defining Competency

We have found that the most effective tool for building communication between educators, employers and students is the development of a shared language. Clarity and consistency are important. A plethora of definitions of competency exist and these have historically complicated an already complicated situation. To increase communication and understanding between the classroom and the workplace, we established a definition of competency which has now been adopted by the NCAE's Careers Preparation National Center (CPNC) and is accepted by both the NSA and the DoD.  This definition provides the bedrock upon which future competency education work within the NCAE-C community is being built–

*Competency is the ability for the student to complete a task within the context of a work role.*

When we talk about competency, we are talking about things our students actually do. Unlike descriptions of knowledge and skills, competency is not abstract.  Competency is observable. Competency is the ability for the student to complete a task within the context of a work role. Competency is situational (located in an actual place and time), social (involving people) and normative (framed by expected ways of doing things).

Within every competency, there are five elements. An actor (A) performs a behavior (B) within a context (C) to an acceptable degree (D) according to the normative expectations of an employer (E). These are the five essential elements of competency. Any competency can be described through using this ABCDE method. Some competency statements might be long and complex, whereas others might be simple and straightforward.

Competency statements might be used in the following ways:

- A statement of competency might be used to design, describe and/or evaluate an educational opportunity (see figure 1).
- A statement of competency might be used by employers to articulate their needs for new hires.
- A statement of competency might form the basis of a conversation between students and potential employers, enabling them to narrate what they did and to make explicit connections to work role tasks.

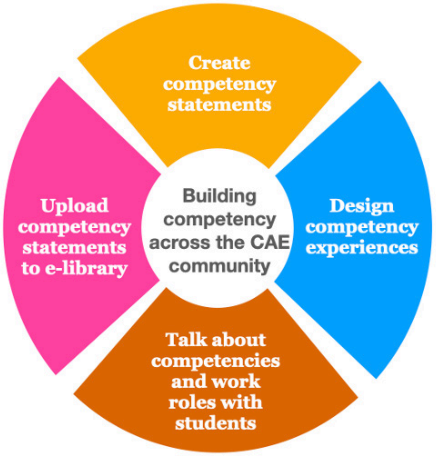

Create competency statements
Upload competency statements to e-library
Building competency across the CAE community
Design competency experiences
Talk about competencies and work roles with students

***Figure 1:*** *How competency statements might be used by educators*

*The next section of the  handbook breaks competency down into the five ABCDE elements.*

**Competency is the ability for the student to complete a task within the context of a work role.**

# The Five Essential Elements of Competency

The educationalist Robert Mager argued that learning objectives should contain specific, measurable objectives which guide instructors and aid students in the learning process; a learning objective is "a description of a performance you want learners to be able to exhibit before you consider them competent" (Mager, 1997, p. 3 [1]) Mager's ABCD model for learning objectives includes four elements: audience, behavior, condition, and degree of mastery needed. We have adapted this model for our work on competency and, importantly, brought in a further category — E for employability — because of competency's role in connecting the classroom and the workplace.

Describing competency using the essential elements of ABCDE provides the means to situate abstract knowledge and skills within the actual practices of a cybersecurity work role. The ABCDE model provides a standardized syntax which increases clarity between educators, employers and students.

[1] Mager, R. F. (1997). Preparing Instructional Objectives, Lake Publishing Company: Belmont, California

# A, the actor

Competencies relate to what we want our students to do and what we observe our students to be doing. Through educational opportunities, we are facilitating opportunities for them to act. While Mager's model focused on teaching and the students were conceptualized as the audience of the teaching, our model is focused on providing opportunities for our students to enact behaviors: our students, therefore, are the actors within the competency statement.

The description of the actor requires the identification of the knowledge, skills and experience a student needs to have already acquired if they are to be able to enact this competency successfully. This might, for example, identify course they have previously taken or knowledge and skills they have already mastered. For example,

- The description of the actor might list previous courses a student will have needed to have studied or completed before enacting this competency.
- The description of the actor might identify whether they are undergraduates or graduates, whether they are college juniors, seniors or high schoolers.

Example 1: "A student in a cybersecurity program taking a 200-level introductory course to networking." Such a statement would suggest this competency event could be reasonably completed by other students in similar programs at similar levels.

Example 2: "A student in a capstone class for a cybersecurity degree". This suggests the student will have completed all, or almost all, the relevant coursework for a degree program and would be familiar with the knowledge and skills taught within that program.

## Why does the actor matter?

**For educators:** Identifying the intended actor ensures the competency is accessible to a specific cohort. Identifying the intended actor will also support educators in sequencing their teaching to ensure the competency is attainable by their students — they will understand what courses and knowledge units they will have needed to teach prior to introducing the student to this competency experience.

**For employers:** An employer will be able to infer a degree of proficiency. It would be reasonable, for example, to assume a Masters-level student will be able to enact a competency at a higher level of competency than a first year undergraduate.

**For students:** Students will gain an understanding of what they need to have done to prepare for this competency - what knowledge and skills will they need to have achieved if they are to successfully access this competency experience.

# B, the behavior

The behavior references a task within an established work role. Tasks and work roles are central to our definition of competency: competency is the ability for the individual to complete a task within the context of a work role.

Although there are several published task lists for work roles, we have made use of the NIST NICE Workforce Framework SP 800-181 (https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final) and the DoD's DCWF (https://public.cyber.mil/cw/dcwf/). The NICE Framework currently identifies 52 cybersecurity work roles and lists the knowledge and skills required by those work roles as well as listing the tasks. The DCWF contains similar information and also includes the domains of Cyber IT Workforce, Cyber Enablers, Cyber Effects, Data/AI, Intelligence and Software Engineering. While the tasks listed in both frameworks are not perfect or complete, they provide a good starting point for identifying the task in relation to which the actor needs to be competent.

Identifying the task makes a direct connection between the educational activity and the workplace. While not all learning objectives and educational activities relate to the workplace, the purpose of the competency statement is to identify the bridges between education and employment.

**Example 3:** "An Entry level community college student (grade 13-Freshman) will troubleshoot system hardware and software (T0237)". This references a task from the NICE framework and does not need to provide further information as the task stands alone within the competency statement.

**Example 4:** "Cybersecurity students on a IS136 Disaster Recovery Business Continuity level community college course who have completed courses including Introduction to Information Systems, Introduction to Operating Systems and Networking Security Fundamentals, will perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). (T0549)" This qualifies and extends the description of the task to ensure sufficient detail is given to someone reading this competency statement.

## Why does the behavior (task) matter?

**For educators:** The identification of a task and the articulation of this within a competency statement ensures the educational opportunity is directly related to the workplace. Our approach to competency is intended to provide opportunities for educators to make direct and explicit links between their teaching and work role tasks — B is central to making those connections.

**For employers:** Linking education and work roles enables employers to better understand what is being taught within colleges. B demystifies what educators deliver in the classroom. Employers can use a task-based framework to to communicate their needs to local educators and to understand how courses might have been designed to prepare students for specific work roles.

**For students:** Connecting learning activities to workplace tasks provides students with insights into the different work roles in cybersecurity. Research evidence shows that when students begin to relate their participation in cyber-competitions to NICE tasks, they increase their potential employability, both in terms of recognizing what kind of work they most want to do within cybersecurity and in relation to being able to articulate their competency in ways that are attractive to potential employers. This promotes their self-efficacy in terms of pursuing a career path in which they know they have a passion or particular interest.

*NOTE: Task statements on their own generally are quite broad. Without context, one can say a "task" was completed even though it was not completed in a way that is realistic to the workplace. For example, the task diagnose network connectivity issues: without context, the student may have been asked to troubleshoot two Windows computers connected by a single cable. While it is a task fulfilling the behavior, it is far from a realistic context of what that task would look like when performed in a work role. This is a key piece toward establishing competency, developing self efficacy, and being able to identify gaps in learning.*

> *I found reviewing existing course projects in the context of a defined competency framework insightful. Particularly helpful was aligning our projects with specific work roles. In the case of Northeast Lakeview College, we aligned competency projects with two work roles of Cyber Defense Analyst and Cyber Incident Responder to provide a focused approach for instructors and students.*
>
> —Isaac Thornsberg

# C, the context

*NOTE: Competency is the ability for the student to complete a task within the context of a work role.*

The workforce frameworks provide abstract congregation of tasks organized by work role. In contrast, a competency statement contextualizes how an actor will carry out that task within an actual situation. Every situation is unique whereas work roles are generic. The 'C' element refers to the description of context, these are the unique elements of the competency which situate the task within an actual event. The context is the description of the specifics of this situation. C, the context, provides the "story" of the competency event.

A description of the context might include:

- the technology provided to the student,
- any documents associated with this competency,
- and any limitations or constraints that were in place within this competency activity.

C also provides an opportunity to identify any additional resources the student will be able to access. This is relevant because some classroom activities might restrict student access to the internet or additional guides etc.

*NOTE: The context of a competency statement shared with educators might not be identical to the context description shared with the student. For example, if I present the student with a computer with 3 pieces of malware on it, I may not want to tell the student how much malware is on it. Just that the student is to check the computer since it "was acting strange".*

**Example 5:** "An entry-level community college student will troubleshoot system hardware and software (T0237) in the role of a technical support specialist and given a computer connected to the network and internet. They will work without the aid of reference, without consulting others, and should be able to download antivirus/malware software, scan computer drives and remove viruses and malware from the system." The context of this competency statements clearly describes what is provided to the actor and what restrictions are in place within this competency experience.

## Why does the context matter?

**For the educator:** As educators, we design learning opportunities. As we support students in the development of their competences, we design activities which allow them to grow and demonstrate competence. The context describes how we make a task taken from a workforce framework accessible and meaningful to our students. Another educator, reading our competency statement, might emulate this activity or use it as food for thought. If the behavior is the raw ingredients, the context provides the recipe for how we have transformed these raw ingredients into something our students might digest.

**For employers:** A description of context provides the employer with insights into the validity of how this task is being enacted within this competency. An employer would be able to make connections between how the listed task is carried out without their own organization and might provide useful feedback to the educator on the design of this competency experience.

**For students:** The context provides the story the student might tell within a job interview. It provides the information they need to describe what they did.

A, B and C **describe** the competency activity. They identify **who** will be engaging with the activity, **what** task relates to the competency and how that task will be enacted. These are the who, what and how of the competency statement.

D and E provide more evaluative aspects, identifying **how much** the student has achieved in relation to this competency and **why** they have behaved in certain ways while enacting the competency.

# D, the degree

Degree introduces a quantitative evaluation of the activity **– how much**.

- **How much time?** A student who resolves a networking issue in 30 minutes might be seen to be competent, whereas a student who takes 3 hours to do this task might not be seen as competent.
- **How much completion?** Academic courses are designed around a principle of the possibility of 100% completion within the semester, but this sense of completion rarely exists in a workplace where objectives and priorities are constantly evolving. Thinking about competency invites us to think about the employer's perspective – in relation to this task, what might an employer consider to be an adequate degree of completion?
- **How much accuracy?** Grading within the university assumes there is the possibility of 100% accuracy, the possibility of a perfect GPA. In contrast, workplaces are often structured around the principle of 'good enough'. In relation to the task enacted within this competency statement, what would be good enough for an employer to consider hiring the individual?

Generally, competency events can reasonably be done in the context of a class, a club or competition. Competencies that take months may not be appropriate, however if your unique situation is appropriate for it then the degree of time might be significant.

**Example 6:** "First term undergraduate students in a Fundamentals of Cybersecurity course will take on the work role of an IT security administrator for a small corporate network whose president has received several suspicious emails (relevant to DCWF 940B). They will determine whether the emails in the company president's inbox are hazardous and handle them accordingly by deciding (a) whether they are legitimate (keep) or (b) whether they are attempts at social engineering (delete). Within 10 minutes, they will successfully identify the five emails which are social engineering attempts, delete them, and keep the remaining seven legitimate emails in the company president's inbox."

## Why does degree matter?

**For educators:** Competency has an evaluative aspect. Unlike academic grading where an educator provides a grade out of 100 (or some other total which implies perfection), within a competency event the educator is constantly asking, "would this be good enough for an employer?" Parameters of accuracy, completion and time relate to normative expectations of 'good enough'.

**For employers:** Degree can imply proficiency. A student who has successfully scanned drives and removed viruses in twenty minutes might be seen as more proficient than a student who has required several hours to complete this task.

**For students:** Students gain valuable insights into the workplace by understanding what is expected from them in relation to a competency. In the workplace, tasks are rarely completed in full, for example. Expectations may relate to 'good enough' rather than an aspiration towards perfection. Completion of a task might be dependent upon team work rather than operating as an individual. It is valuable for educators to spend time talking with students about the expectations of 'degree' and why the competency has been framed in this way. Encouraging students to understand workplace practices is an important aspect of developing competency experiences.

*An undergraduate student enrolled in the Introduction to Cybersecurity class at a 4-year institution will be able to act as a Cyber Operator to conduct network scouting and vulnerability analyses of systems within a network (NICE T0616). The student will be provided with a virtual network and various tools to discover hosts and services on the network and to identify potential vulnerabilities that adversaries could exploit. Additionally, the student will review and research the identified vulnerabilities using the publicly available vulnerability database. The student must complete all scans and analyses and report the findings with recommended remediations within 2 hours. The student must correctly identify all the open ports and high-severity vulnerabilities on the target and summarize at least three high-severity vulnerabilities identified during their analysis. For each vulnerability, they must identify the severity, describe the issue, and recommend remediation. To demonstrate this competency, the student must be able to think critically and use technology effectively.*

# E, for employability

Competencies relate to the workplace. It is important to remember that a person can be technically adept but remain unemployable. E provides an opportunity to document many of the qualitative aspects that make an individual competent within a work role — those qualities that make an individual employable. Think of the following:

- an individual who completes tasks in an unethical way that jeopardizes the mission of an organization;
- a technical wizard who is unable to communicate to others and who refuses to collaborate with members of his or her team;
- a person who is unable to creatively problem-solve when new situations arise.

Regardless of technical ability, it is unlikely an employer would want these individuals on their organization's team. The employability section of a competency statement becomes, therefore, arguably the most important aspect of recognizing competency.

> *Students who gain competition experience demonstrate their competencies with confidence and self-awareness. This includes technical skills, communication skills, leadership, empathy, conflict resolution, and teamwork.*
>
> —Morgan Zantua

To be successful within the workplace one needs to have professional skills, such as teamwork, communication and problem-solving, as well as established ethical values. Work conducted within the NCAE-C's Careers Preparation National Center by Montreat College identifies the following as key attributes necessary for employability:

- **Critical thinking**
  - Critical thinking is disciplined thinking that is clear, rational, open-minded, and informed by evidence
- **Communication**
  - Effective communication enables ideas to be clearly and confidently articulated to others through reports, letters, public speaking, emails, etc. A competent communicator is able to articulate thoughts appropriately with a wide variety of individuals.
- **Leadership**
  - Leadership involves using interpersonal skills, managing personal emotions, coaching, and developing others, along with organizing, planning, and delegating work. A competent leader is able to manage his/herself as well as leverage the strengths of others to achieve common goals. (Based on The Leadership Challenge by James M. Kouzes and Barry Z. Posner, 2017)
- **Teamwork**
  - Teamwork involves building collaborative relationships with colleagues and customers representing diverse cultures, races, ages, genders, religions, and viewpoints. A competent team player is able to work within a team structure and can negotiate and manage conflict
- **Reponsibility and Integrity**
  - Responsibility and integrity include: being willing to accept personal accountability and to take ownership of the strengths and weaknesses of one's own or one's team's work; to acknowledge the impact of one's actions on others; to effectively manage time and workload; and to act with self-control and integrity.
- **Ethical Judgement and Reasoning**
  - While ethical judgment matters in every workplace, cybersecurity organizations in particular rely upon having an ethical workforce. Ethical judgment is demonstrated by making good decisions in your personal and professional life and acting with integrity by aligning actions with beliefs about what is right and wrong.

Alongside a commitment to teaching technical knowledge and skills, cybersecurity educators have a responsibility for enhancing the employability of their students through providing opportunities for them to develop and demonstrate their employability. Please note: a competency does not need to reference each one of these aspects of employability.

**Example 7:** "First term undergraduate students in a Fundamentals of Cybersecurity course will take on the work role of an IT security administrator for a small corporate network whose president has received several suspicious emails (relevant to DCWF 940B). They will determine whether the emails in the company president's inbox are hazardous and handle them accordingly by deciding (a) whether they are legitimate (keep) or (b) whether they are attempts at social engineering (delete). Within 10 minutes, they will successfully identify the five emails which are social engineering attempts, delete them, and keep the remaining seven legitimate emails in the company president's inbox. This competency will require students to demonstrate ethical problem-solving and effective time management."

## Why does employability matter?

**For educators:** Educators are successfully teaching knowledge and skills within their classrooms. The focus of this competency work it to encourage further connections with established work roles and workplace practices. The consideration of employability within a competency statement provides the stimulus for educators to provide their students with opportunities to develop the practices which employers consider to be desirable.

**For employers:** Research conducted within this project shows that employers consider the behaviors contained within 'E' to be extremely desirable in new hires. Including E within a competency statement enables these professional skills to be evidenced.

**For students:** Research shows that students who can effectively articulate their professional skills enhance their employability.

## Competency Statement Template

| | | |
|---|---|---|
| Name of Competency | | |
| Type of Activity | | |
| Associated work role as listed in DCWF or NICE | | |
| Essential Elements: ABCDE | | |
| Actor | Type of Student | |
| | Necessary knowledge and/or skills | |
| Behavior | Task (Name and code from NICE or DCWF frameworks) | |
| Context | Scenario | |
| | Technology | |
| | Documentation | |
| | Limitations | |
| Degree | % Complete (if stated) | |
| | % Correct (if stated) | |
| | Amount of Time (if stated) | |
| Employability | (use Montreat 360) | |
| Notes (Optional) | | |

## Competency Statement Example Using Template

| | | |
|---|---|---|
| **Name of Competency** | | Cyberdome Cybersecurity Analyst (Boise State) |
| **Type of Activity** | | Internship |
| **Associated work role as listed in DCWF or NICE** | | Cyber Defense Analyst |
| **Essential Elements: ABCDE** | | |
| **Actor** | **Type of Student** | Cybersecurity/computer science students within the last 6 months of their degree program |
| | **Necessary knowledge and/or skills** | Basic understanding of networks, operating systems, and cybersecurity elements (CIA-triad) |
| **Behavior** | **Task (Name and code from NICE or DCWF frameworks)** | NICE task T0214: "Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts." |
| **Context** | **Scenario** | Depending on the traffic of the clients' networks and the resulting correlation analysis of the tools used, the student examines an identified alert. The alert provides details elements such as (but not limited to): source/ destination IP addresses, identified possible ATTACK framework element, date/time stamp. The student takes this alert information, examines the client's documentation set, which outlines prior false/true positive information for possible immediate (de) escalation requirements. If that examination does not enable a decision to be made, the student then utilizes identified OSINT tools to "create a story" around the alert and determine if the alert requires escalation to the client. As the student develops this story, they may engage other students / mentors into the decisioning process. |
| | **Technology** | Open source and commercial tools such as: Security Information Event Management (SIEM) Network Detec<on & Response (NDR) End-point Detec<on & Response (EDR) Threat Intelligence / OSINT tools Ticketing systems and workflows |
| | **Documentation** | |
| | **Limitations** | |
| **Degree** | **% Complete (if stated)** | Last 6 months of a degree program: 75% complete for associate degree seekers 87.75% complete for bachelor's degree seekers ~83% complete for post-baccalaureate degree seekers |
| | **% Correct (if stated)** | |
| | **Amount of Time (if stated)** | Interns spend a total of 6-months in the program. In the case of this task, the intern has to make a determination within 2-hours of whether an alert is a false/true positive and then establish alerting client points of contact via pre- determined channels of communication. |
| **Employability** | **(use Montreat 360)** | Communication. The student, ader examining the alert and client details, will update client-specific documentation and/ or alert the client via the prescribed appropriate channels (e.g., text, email, phone call). The choice of communication channel is dependent upon the criticality of the alert.<br>Critical Thinking: Think Creatively Learn & Problem Solve Communicate Graciously<br>Teamwork: Contribute to a common goal.<br>Technology: adapt to new technology and cyber threats, use technology to create efficiencies.<br>Intercultural and global fluency.<br>Responsibility & Integrity: Accept Personal Accountability Demonstrate Commitment & Work Ethic Manage Time & Workload Act with Self-Control and Integrity Take Ownership of Results Ethical Judgment & Reasoning: Decision Making Ethical Communication Social Responsibility |
| **Notes (Optional)** | | |

# Discussion of Competency Statements

### Competency statement Example 1:

Cybersecurity students taking an IS136 Disaster Recovery Business Continuity level community college course who have completed Introduction to Information Systems, Information to Operating Systems and Networking Security Fundamentals will act as vulnerability assessment analysts (VAM) with access to the risk assessments of Dr. Know's  medical office network and the CSET 10.3 tool to perform technical and non-technical risk and vulnerability assessments of the local computing environment (T0549). They will identitfy 5 key risks within 4 hours and produce a risk assessment and recommendations report which cleaerly communicates the found risks for a non-technical user.

What does example 1 tell us about ABCDE?

What information do we know about the actor?

What is the behavior being enacted?

What affordances and limitations are placed upon this task?

What degrees of measurement relate to this competency?

What wider employability skills are identified?

### Competency statement Example 2:

Third year Computer and Network Forensics students who have taken Computer Networks and Fundamentals of Cybersecurity will conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion (T0027) through performing two FTP application and capturing the transmission once via Wireshark and again via NetWitness Investigator. They will identify: (a) FTP login credentials as part of a forensic investigation; (b) identify FTP client/server TCP/IP communications and dialogue; (c) compare Wireshark and NetWitness investigator reports as a forensic analysis for protocol analysis. They will successfully conduct all file transfers within 30 minutes and present a written report of their results.

What does example 2 tell us about ABCDE?

What information do we know about the actor?

What is the behavior being enacted?

What affordances and limitations are placed upon this task?

What degrees of measurement relate to this competency?

What wider employability skills are identified?

# Competency Statements and Experiential Learning

The next section of this handbook provides examples drawn from different parts of the CPNC. These examples and reflections are intended to provide insights into how the above approach to competency is influencing educational activities in cybersecurity, including competitions, exercises and internships.

To briefly recap, a competency statement (or description of a competency experience) would include the following:

| | |
|---|---|
| **Actor**<br>**Who?** | *Class level.* Prerequisite skills and knowledge necessary to successfully access this competency |
| **Behavior**<br>**What?** | *Work role.* Mapped onto an existing framework such as the NICE framework or the DoD's DCWF.<br>Task. Listed within the description of the work role.<br>Details. Any additional information needed to describe the generic task. |
| **Context**<br>**How?** | *Scenario.* Description of activity scenario.<br>Given documents.<br>Given technology.<br>Limitations. |
| **Degree**<br>**How much?** | Required completeness<br>Required correctness<br>Time limitations. |
| **Employability** | Cross reference Montreat's 360 competencies for descriptions of 'professional' skills needed in this work role. |
| **Notes:** | Bring in any additional notes or teaching materials. |

To draft a competency statement based around your own teaching, it might be useful to make use of the following template.

*A competency statement might end up looking like the following:*

A student who has completed 200 courses related to networking, Operating Systems, virtualization and introductory cloud computing courses (Microsoft AZ900, Cloud+ or AWS ACF) level course and acting as a cloud/enterprise architect will be able to meet with a requirements team, design a hybrid cloud infrastructure, and implement a hybrid cloud architecture (A0060). The implementation will require the architect to set up a Site-to-Site IPSEC VPN tunnel to a cloud tenant from an existing on premises network. The architect will (a) provision appropriate networks, apply correct subnet ranges, and create VPN gateways as needed in both on-premises and the cloud tenant. The architect should be able to (b) right-size the gateway and throughout to ensure it meets the needs of the requirements team. The architect should be able to (c) select appropriate encryption and authentication (AES, 3DES, SHA) settings to ensure the tunnel both establishes correctly and is secure. The architect should be able to design this architecture, craft draft documentation, implement and test by sending ICMP packets (ingress/egress) from both networks. The task should be completed within one business day and the appropriate documentation should be made available to team members. Successfully meeting the requirements demonstrates Critical Thinking, Communication and Teamwork Employability skills.

**In short:**

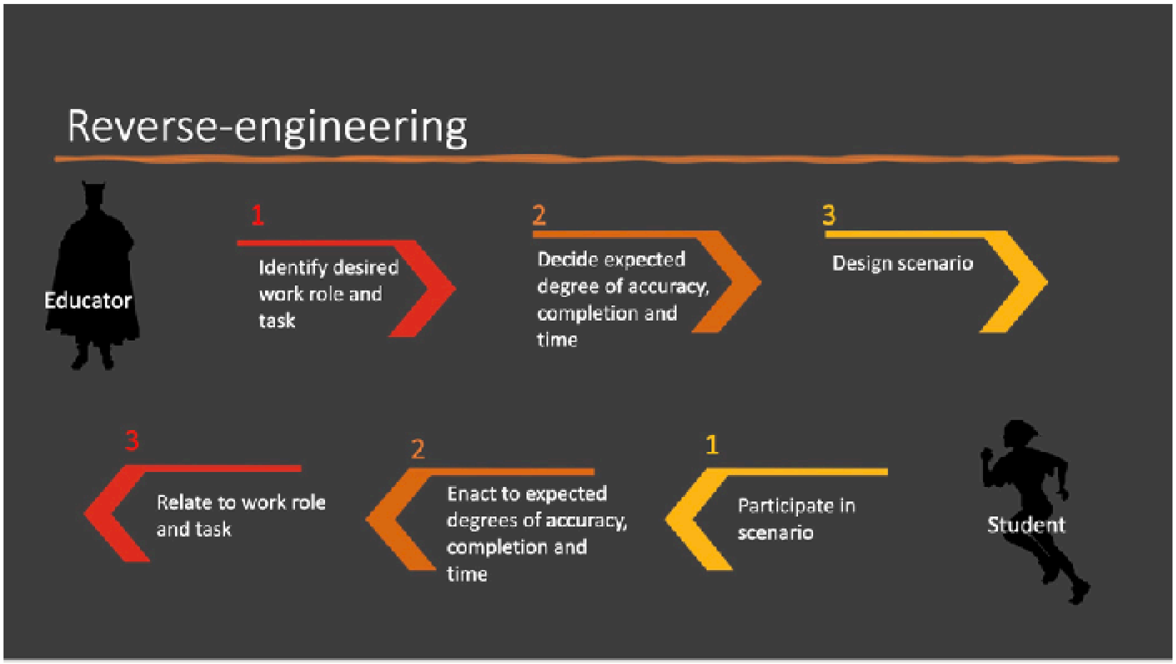
1. Focus on activities, exercises or assessments in existing course curricula that relate to the cybersecurity workplace.
2. Cross-reference the skill, task or competency to the NICE or DoD DCWF frameworks.
3. Draft a competency statement structured around the 5 headings (ABCDE model).

## Using Competency Statements in the Classroom

Bringing competency statements into classroom-based activities is not a push for vocational education. A competency statement is a learning outcome, but not all learning outcomes are competency statements. Developing a few competency experiences in the classes you are teaching will go a long way. One of the values of adding competency experiences is to help students discover the many different areas in cybersecurity where they can apply their acquired knowledge and skills. It can also give them a sense of what they enjoy doing, and what they might loathe. As the saying goes, “find a job you love, and you will never work a day in your life.” When a person finds a job they love, everyone benefits!

In most cybersecurity classrooms, learning opportunities already exist that can, with slight modifications, be used to create competency statements. If you are teaching a cybersecurity class, you may already have lab assignments that fit well as a competency experience. You may just need to put the details of what you are doing in the ABCDE elements format and perhaps make some modification to context. Crafting a competency statement in many cases should not be too heavy a lift. Identifying competencies you want your students to develop can help you design new activities.

If you decide to develop a class beginning with a competency statement, the process is one of reverse engineering. Figure 2 shows the ways that an educator might build a classroom activity from a competency statement, and how the student might then engage with the competency statement and, through engaging with this competency, better understand the task and work role associated with it.



Reverse-engineering

Educator

1 Identify desired work role and task

2 Decide expected degree of accuracy, completion and time

3 Design scenario

Student

1 Participate in scenario

2 Enact to expected degrees of accuracy, completion and time

3 Relate to work role and task

***Figure 2:*** *Building a classroom activity from a competency statement*

### A word about designing instruction:

*In the Backward Design approach to instructional design, there are three steps: (1) Determine the desired outcome, (2) Determine the acceptable evidence, (3) Develop the learning plan. With the ABCDE approach, the first two steps are essentially covered. ABC describe the acceptable results. You may already have ideas as to the learning plan that will prepare the student to perform the compentency. However, you are not expected to become instructional designers in the creation of the competency statements. If you find that you might need help with the learning plan that leads to a competency experience there are resources to assist you. Many institutions have instructional designers on staff that might be helpful. There is also CLARK CENTER that has a large repository of cybersecurity lesson plans. And of course you can always reach out to the CAE Community for assistance.*

Another approach to bringing competency into the classroom might be to encourage students to research work roles and tasks which relate to the classroom activities through studying the various frameworks themselves. Students can take the lead in identifying connections between their classroom activities and possible competencies. This can also provide the motivation to explore the various work roles which exist in cybersecurity and to identify the directions in which they want to take their careers.

### Validating competency statements (Encouraged but not required)

*It would be great value to include professionals who are working in or with work roles for which you are developing competencies. For example, you might collaborate in building a competency from scratch or ask for their feedback on a competency you are already using in your class. Ask the employer whether the competency represents an actual piece of work an individual would need to complete if they were working in the work role in question. You might also ask whether the employer would hire someone who was able to do this task and articulate their experience. While one task is not enough to determine if someone would be hireable, good feedback is useful.*

## Using Competency Statements in Competitions

*(by Dan Manson and Morgan Zantua)*

The National Institute of Cybersecurity Education (NICE) describes cybersecurity competitions as follows: "Cybersecurity competitions are interactive, scenario-based events or exercises, in person or virtual, where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy and ethics. Competitions encourage players to practice, hone cybersecurity skills, and build confidence in a controlled, real-world environment and are available for all ages and levels, from as young as elementary school and for those considered experts in the field. Achievements may be measured and evaluated against a large field of competitors. While they are not the only method for educating, developing skills, and measuring performance, cybersecurity competitions play an integral role in stimulating interest."

Using the ABCDE elements, cybersecurity competition competencies include the following:

**Actor –** In a cybersecurity competition, the actor is the individual student or student team being judged and scored in competition activities.

**Behavior –** In a cybersecurity competition, the behavior is the measurable task being judged and scored during competition activities.  Similar to measuring competency in a cyber range or classroom, the behavior is the task that a person working in a particular workrole would have to do.

**Context –** In a cybersecurity competition, the context describes the competition technology provided to compete, and the role performed by the individual or team competing.

**Degree –** In a cybersecurity competition, the degree includes the time allowed for a behavior, the level of completeness and accuracy of the behavior.  For example, a blue team is asked to perform an inject is performed within a specific time, is scored according to a defined rubric that includes completeness and accuracy measurements.

**Employability –** In a cybersecurity competition, employability connects the competition competency to the workplace. Employable student cybersecurity competitors demonstrate their competencies with confidence and self-awareness. This includes technical skills, communication skills, leadership, empathy, conflict resolution, and teamwork.

Documenting competencies in cybersecurity competitions should include more than a competition score. Students should be able to reflect and describe competences measured, how well they performed competencies, and how these measurements relate to their real-world workforce experience. The reflection process is an essential element to ensure students integrate the ABCDE components and can confidently discuss their competition achievements. The reflection and articulation process cements the ABCDE model. When competition participants respond to the questions and reflect on their competition experience, they gain insight and find the language to relate their experience.

The language and insights discovered during the reflection are beneficial to students during interviews, team projects, and professional engagements. The reflection component bridges competitions to the digital portfolio and the articulation of the workplace-based “soft skills” which are now deemed critical skills in the hiring process.   If time is spent developing the employability skills in the classroom, during competitions participants experience all four stages of the competency framework.  A structured reflection process allows participants to articulate their technical and non-technical accomplishments and strengths.

## Using Competency Statements in Internships

Unlike the majority of planned classroom activities, internships tend to have high degrees of serendipity and unplanned opportunities. Students are immersed in an actual work environment, and not all events can be planned in advance. However, competency statements have a role in the design and evaluation of internships, as piloted by the SECURE internship program within the CPNC.

Prior to the internship, students were each provided with three statements of competencies they were expected to develop. The competencies used the ABCDE framework and made explicit connections with the DCWF tasks (B). This framed student expectations and provided a rigorous understanding of the purposes of the internship placement. Throughout the internship experience, students were therefore able to make connections with intended work roles and tasks, and this informed the evaluation process following the internship. Students received coaching in how to talk about what they had done in their internship to demonstrate their competence to employers in interview conversations.

## Using Competency Statements in Exercises

Tabletop exercises provide a simulation of a work environment. Participants are allocated specific work roles and behave in accordance to these roles within a shared scenario. Desirable competency statements can be identified prior to the design of the exercise, and opportunities to demonstrate these competencies can then be built into the exercise.

Within the CPNC, Norwich University Applied Research Institutes (NUARI) piloted this kind of competency statement-led approach to a tabletop exercise. Prior to the exercise, students were allocated work roles and encouraged to read through the relevant tasks they would be expected to enact within the exercise. These were cross-referenced with the DCWF framework. During the exercise, focus was also given to (E), the employability skills listed by Montreat and at the end of the exercise, students were asked to draft ‘elevator pitches’ which described what they had done and achieved. This pitch was structured around the ABCDE framework.

During these exercises, students gained understanding of different work roles, and evaluators and observers (some of whom were drawn from employers and industry partners) were able to observe competence and to provide feedback not only on student performance, but also on how the scenario (C) might be further refined to enhance opportunities to develop and demonstrate this competence.

The ABCDE framework was seen as an effective tool for establishing consistency between employers, educators and students in relation to workplace roles and expectations.

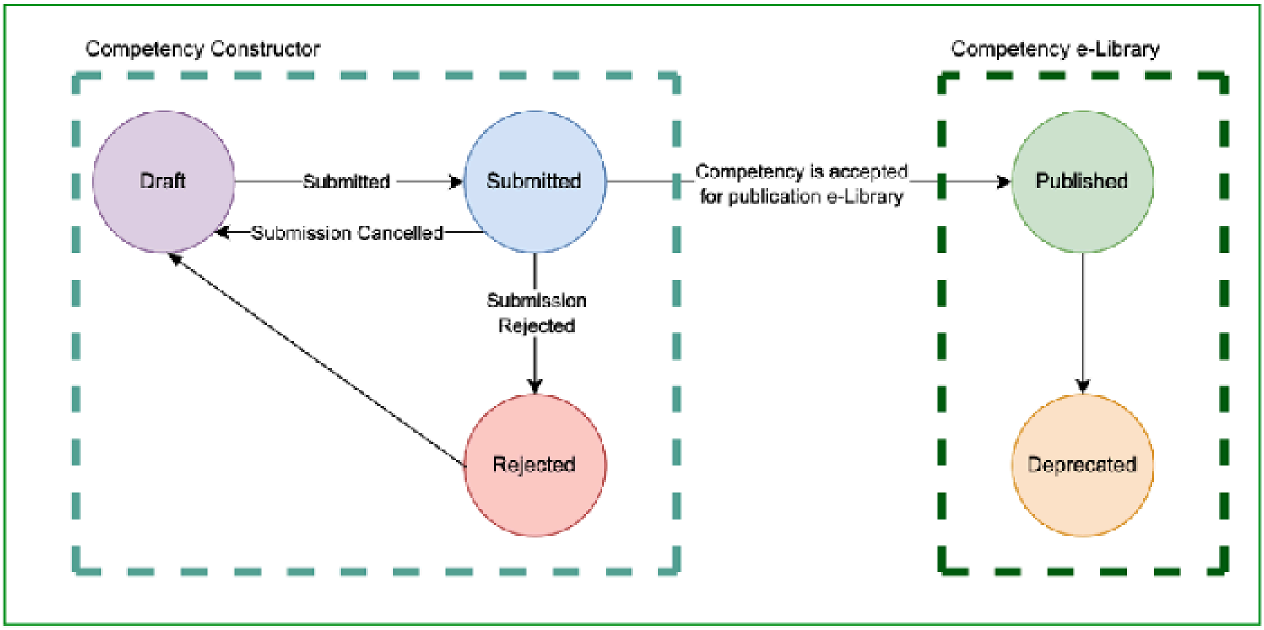
# The NCAE-C Cyber Competencies Ecosystem

## *(Competency Constructor and the the e-library of Competency Statements)*

Competency Constructor and e-Library are two applications within the NCAE-C Cyber Competencies Ecosystem that work together to support the creation, curation, retrieval and maintenance of competencies produced by the NCAE-C Community. The Competency Constructor provides the ability to create and upload competency statements and the e-Library supports the ability to browse competencies. Both applications use the ABCDE model outlined in this eHandbook. All competencies submitted to the constructor using the ABCDE model will undergo a curation process to ensure they are of the highest quality and are ready to be shared across the NCAE-C Community. After each competency is curated and has been published, they are then available through the e-Library. The e-Library application facilitates the retrieval of competencies that can be used in classroom activities, competitions, and experiential learning activities across the NCAE-C Community.

Competency Constructor can be accessed via https://cybercompetencies.com/. You must register for an account and verify your email after registering in order to create competencies. For detailed information about creating and submitting your competency statements, please visit the Competency Constructor Help pages via https://cybercompetencies.com/help/. The e-Library application will be available in Fall 2023.

The NCAE-C Cyber Competencies Ecosystem is designed, built, and hosted by SecurEd Inc. For any inquiries, you may reach us through email via info@secured.team.



# Students Explaining Their Competency Experience (STAR)

The primary focus of this handbook has been upon explaining the importance of  competency experiences and providing guidance on how to develop these. These experiences are of value when students discuss them with prospective employers and other professionals within the cybersecurity industry, and research shows that students who are able to connect their learning to the workplace increase their employability. However, it is not uncommon for a student to have excellent skills and to have succeeded on their college course, but to struggle to explain to potential employers what they did. Discussing with students how to narrate their experiences in relation to the workplace enhances the value of these experiences.

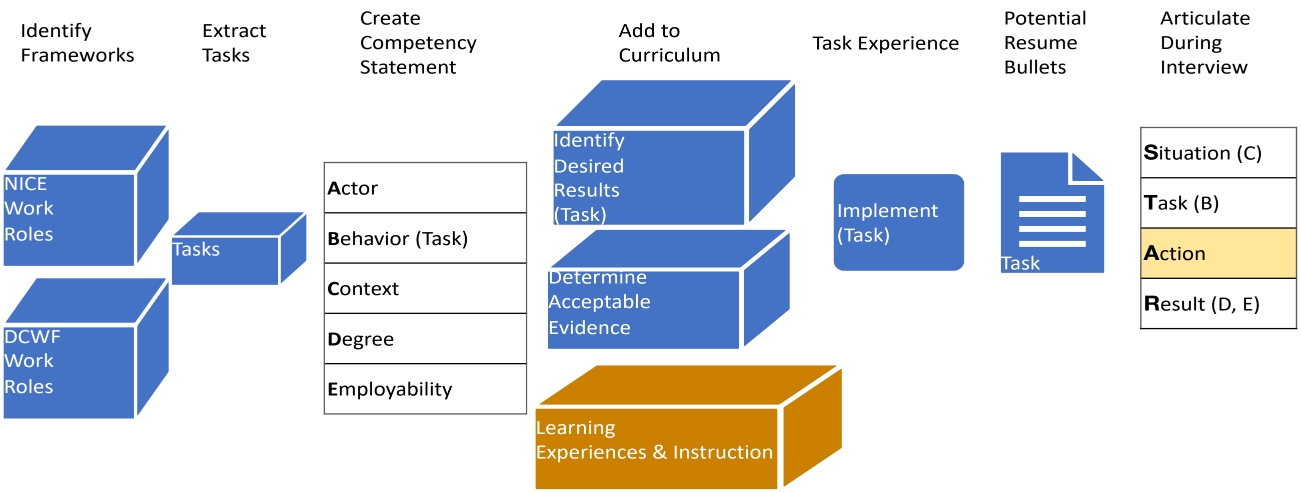
The STAR method is often recommended as an acronym to aid people in presenting themselves in job interviews. This acronym can help students organize their thoughts in a cogent manner. STAR stands for Situation, Task, Action, Results. The student learns to describe the situation, articulate the task, explain their actions and reflect upon the results.

This approach maps relatively neatly onto the ABCDE model of competency.

Situation maps to context,
Task maps to behavior,
Results map to degree and employability.

Although Action does not fit cleanly into the ABCDE model, this would be the specific steps or approach a student took toward completing the task. The actions taken may vary significantly from student to student depending on the task. Having the students take the time to think about how they would explain what they did to someone else, therefore developing a conscious awareness of their practice, is extremely valuable. A good activity is to have students practice explaining it to a person who is not very technical, and again to someone who is very technical. They should be able to explain their experiences to both types of people as either can be the person at an interview.

After doing a competency experience, consider sharing the STAR method and role playing a job interview. Encourage the student to try to describe their experience in front of the class. You can solicit feedback from the class to see if they hit all the key points in a clear and concise manner.



Competency - ability to complete a task in the context of a work role

# Activity A

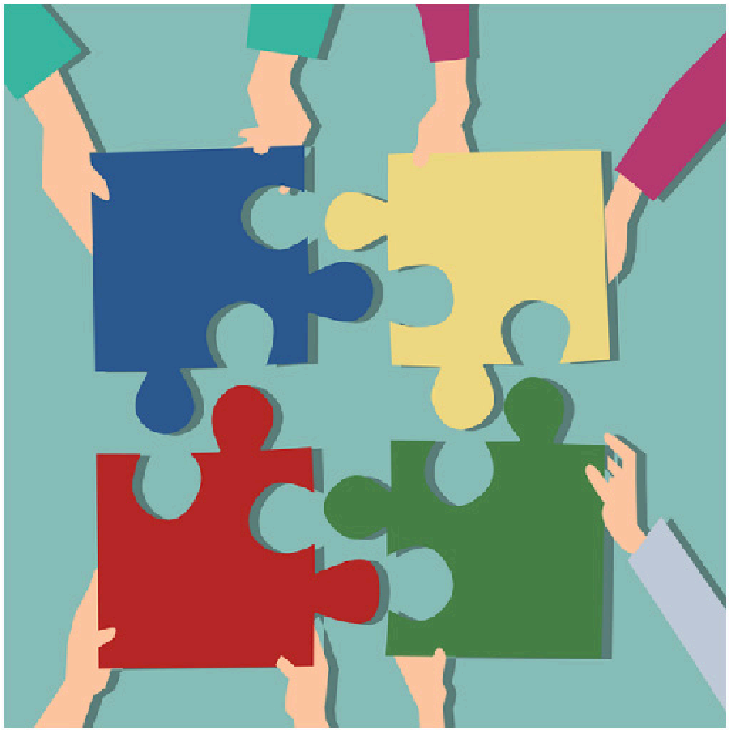
Think of a course you teach, or have taught. What courses did your students need to have studied before engaging with this activity? What skills do they need to already possess? What knowledge do they already need to have? Can you write a sentence which clearly identifies what students need to know and to have achieved before engaging with your classroom activity? *"How tall do they need to be to ride the ride?"*

**Note:** this might relate to the technical knowledge and skills they need to have acquired, but it might also refer to their ability to write a report, build a datasheet, or present a series of PowerPoint slides of the findings.

For many statements, the assumed prerequisite knowledge and skills will be encompassed in the description of the grade level. However, if your activity requires a specialty that is not usual for other programs but which is necessary for this competency, you would need to include reference to this. For example, "and has an in-depth knowledge of FedRAMP".

# Activity B

Think of a course you teach, or have taught. Use the DCWF or NIST NICE Framework (https://niccs.cisa.gov/workforce-development/nice-framework/work-roles) to identify the tasks included in your activity. What would happen if you invited your students to make this connection? Are your students already familiar with the NICE framework? Are they able to identify workplace tasks within their course learning?



Invite your students to make these connections and to talk about whether this makes them think differently about the activity.

## What do you want to be when you grow up?

*Many students studying cybersecurity are not familiar with many of the over 50 work roles that exist. Have the students visit https://niccs.cisa.gov/workforce-development/nice-framework or https://public.cyber.mil/wid/dcwf/ and read all of the work roles and their definitions. Have them identitfy the three work roles they are most interested in and likely to want to do upon graduation. Have them also identify the three tasks for each that they are most interested in doing.*

# Activity C

In activity B, you identified a task (or tasks) from the NICE framework which currently fit into a class you teach. How do you teach these tasks? Think about what technology and resources you provide to your students and any restrictions you place upon them. How does your approach mirror the workplace? To what extent is your approach constrained by the practical logistics of your organization (for example, how many machines you have available).

Write the first part of a competency statement including (a) the actor, (b) the behavior (task), and (c) describing the context.

# Activity D

The following table is useful for identifying E for employability. If this professional skill is not relevant, leave it blank.

| | |
|---|---|
| Critical thinking | |
| Communication | |
| Leadership | |
| Teamwork | |
| Intercultural and global fluency | |
| Responsibility and integrity | |
| Ethical judgement and reasoning | |

Which of these professional skills are central to the competencies you are teaching?

Have you explicitly discussed these with your students?

1. (Optional) To further students' connections between class learning and the workplace, encourage students to articulate how they completed the task, and why they completed the task in this way.
2. (Optional) To increase resonance between curriculum and employer needs, share this competency statement(s) with employers and ask for their feedback (for example, would they consider hiring a student who could complete this task to this degree in this context).

# Overcoming Objections

*by Kristin Hayes*

Below are possible responses an educator might make to resistance from faculty or other teaching colleagues. Implementing competency statements brings a slight cultural shift to how we think about the relationship between education and employment. Hayes considers these responses can be helpful in facilitating productive discussions and dealing with objections.

### *"I don't teach to specific roles"*

"Thank you for sharing your concern. I understand that there are different approaches to teaching. It is not the intention of this process to ask you to modify your teaching style. While teaching competency skills may not be your primary focus, it's important to acknowledge that many students attend college with the goal of obtaining a degree that will prepare them for a specific career. By incorporating relevant skill-based competencies into your teaching, you are helping to develop the practical skills required to be successful. This also helps our students to make meaningful connections between their coursework and real-world applications."

### *"Employers should expect to train new employees. This is not my job"*

"I understand that there are different opinions regarding the responsibilities of professors in preparing students for the workforce. While it is true that employers have a responsibility to train their employees, it is important to recognize that professors also have a role in helping students develop their foundational knowledge and the skills necessary to apply that knowledge in a real-world setting. Knowledge without an understanding of how to apply it is not meaningful."

### *"What is in it for me? Why should I care?"*

"Empowering our students with competencies will greatly benefit the faculty. By developing our student's competencies at a higher level, this will increase student confidence and create opportunities for deeper and more meaningful in class discussion. This will further continue to improve the quality of students graduating from our program which will keep our school competitive and drive future student enrollment."

### *“I already have too many things to do. I don’t have time for this”*

“I understand that faculty workloads can already feel overwhelming. Many faculty members originally felt the same way as you. However, I would ask you to consider this from another perspective. In all reality, the competency statement takes a minimal amount of time to write. In fact, once the database is fully developed there will be a lot of shared resources for faculty use. Your curriculum remains your own and is driven with full academic freedom. These competency statements are a way to employ hands-on, role-play experiences to complement that learning. This allows the students to take what they are already learning in your class, and understand how to applies it in a real-world professional setting.”

***or***

“I understand that faculty workloads can already feel overwhelming, but let me explain the benefits of this task. Developing our student’s competency skills will increase student employability and confidence. The school also benefits by graduating students that are prepared to competently enter the workforce. By creating a program of excellence this will continue to attract students and build our future student pipeline. Finally, remember that you are not alone. There are a lot of available resources to help make this process easy to implement. How can I best provide support?”

# Useful links

Workforce frameworks:

- The NIST NICE Workforce Framework SP 800-181 https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

- DoD's DCWF https://public.cyber.mil/cw/dcwf/

Resources relating to work roles in cybersecurity:

- The Women in Cybersecurity organization has a wonderful set of videos show-casing different jobs within cybersecurity. These can be accessed at https://www.wicys.org/resources/nice-workforce-framework-wicys-video-album/

Curriculum resources:

- Clark supports a wide range of freely available curricula and learning materials. These can be accessed at https://clark.center/home

# Notes

35

# Notes

# Notes

37

NORWICH™
UNIVERSITY

Norwich.edu