Using the NIST NICE Cybersecurity Workforce Framework: mapping curriculum and coursework A Cengage Learning White Paper

Michael E. Whitman, Ph.D, CISM, CISSP
Herbert J. Mattord, Ph.D, CISM, CISSP

Originally published https://blog.cengage.com/using-nist-nice-cybersecurity-workforce-framework-mapping-curriculum-coursework/ in October 2018.

INTRODUCTION

The Cengage Learning NICE Cybersecurity Workforce Framework mapping white paper. The purpose of this white paper is to facilitate the use of the Cengage Learning/NICE mapping document (hereafter referred to as the "Map"). The map is designed to assist a course designer or instructor in achieving a better understanding the NICE Cybersecurity Workforce Framework (hereafter referred to as "the Framework") as well as in selecting textbooks to support curriculum development and provisioning of courses with the highest quality learning support materials.

The map was designed by Cengage text authors specifically to meet the need for a method to link the Framework to specific textbook products. The first section of this white paper describes the Framework and its intended role to support cybersecurity workforce development. It then seeks to prepare the reader to use the Framework in designing curriculum and in selecting texts to support that curriculum. If you have any questions about the use of this document feel free to email us at xxxxxxxx@cengage.com.

ABOUT THE NIST NICE CYBERSECURITY WORKFORCE FRAMEWORK

The Framework was developed in 2011-12 "to provide a common understanding of and lexicon for cybersecurity work."[1] It was designed to support federal agencies but also provided "to the private, public, and academic sectors for describing cybersecurity work and workforces, and related education, training, and professional development."[2] The Framework organizes a wide collection of information security/cybersecurity /information assurance work domains into 31 specialty areas that roughly correspond to areas of work in which an individual employed in the public or private sector could reasonably be expected to work in. The Framework further organizes these 31 areas into 7 domains or categories, as shown in Figure 1. The Framework and supporting documentation may be downloaded from the NIST NICE web site at http://csrc.nist.gov/nice/framework/.

The primary benefit of the Framework is to enable an understanding the Knowledge, Skills and Abilities (KSAs) someone working in a particular specialty area would need to possess and the Tasks they would need to be able to perform to effectively function in that role. The Framework provides detailed lists of both KSAs and Tasks associated with 5 of the 7 categories, with the final two categories (Collect and Operate, Analyze) deemed too specialized to support the development and distribution of KSAs or Tasks.

The specialty areas are shown in Figure 2. There are five general knowledge areas common to all categories and between 12 and 64 specialty KSAs are relatively unique to each area. While some specialty areas may share individual KSAs, but none are identical. Each specialty area also provides a listing of sample job titles commonly associated with an individual working in that area.

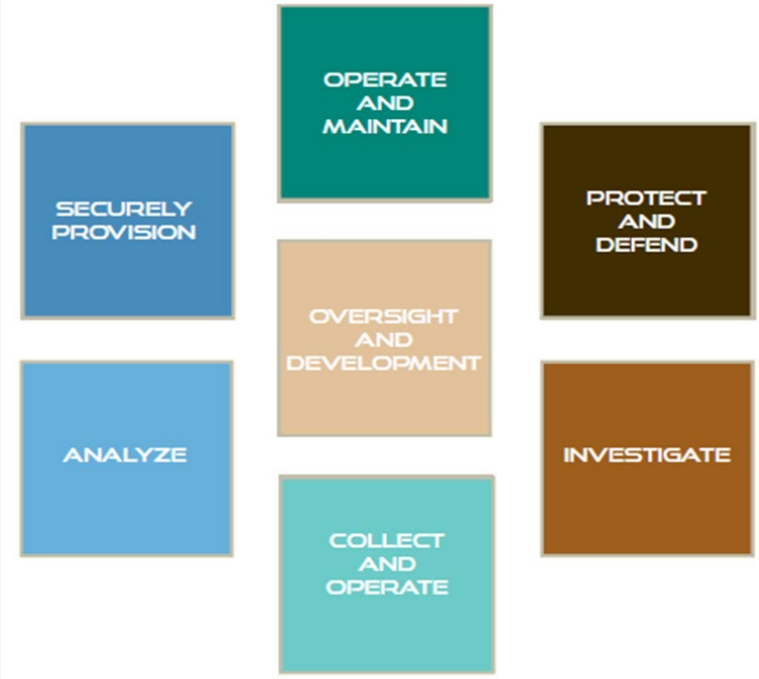

Figure 1: NICE Cybersecurity Workforce Framework Categories
Source: NICE Cybersecurity Workforce Framework

Figure 2: NICE Cybersecurity Workforce Framework Specialty Areas
Source: NICE Cybersecurity Workforce Framework

Figure 3 provides an example set of KSAs for the Data Administration specialty area. Note the "Next Page | Previous Page" indicator at the bottom signaling that there are more KSAs associated with this specialty area than would fit on a single page.

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

OPERATE AND MAINTAIN / DATA ADMINISTRATION

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

TASK / KSA

ID	Statement	Competency
28	Knowledge of data administration and data standardization policies and standards	Data Management
29	**Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools**	**Computer Forensics**
31	Knowledge of data mining and data warehousing principles	Data Management
32	**Knowledge of database management systems, query languages, table relationships, and views**	**Database Management Systems**
35	Knowledge of digital rights management	Encryption
44	**Knowledge of enterprise messaging systems and associated software**	**Enterprise Architecture**
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI])	Identity Management
90	**Knowledge of operating systems**	**Operating Systems**
98	Knowledge of policy-based and risk adaptive access controls	Identity Management
104	**Knowledge of query languages such as Structured Query Language (SQL)**	**Database Management Systems**
120	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
137	**Knowledge of the characteristics of physical and virtual data storage media**	**Data Management**
152	Skill in allocating storage capacity in the design of data management systems	Database Administration
166	**Skill in conducting queries and developing algorithms to analyze data structures**	**Database Management Systems**
178	Skill in designing databases	Database Administration
186	**Skill in developing data dictionaries**	**Data Management**
187	Skill in developing data models	Modeling and Simulation

NEXT PAGE | PREVIOUS PAGE

Data Administration | Knowledge Management | Customer Service and Technical Support | Network Services | System Administration | System Security Analysis

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

Figure 3: NICE Cybersecurity Workforce Framework KSAs for the Data Administration Specialty Area
Source: NICE Cybersecurity Workforce Framework

ABOUT THE CENGAGE LEARNING NICE MAPPING DOCUMENT

Cengage Learning commissioned the development of a project for course designers and instructors locate associations between their curriculum objectives and the Framework and then identify the text or texts that would support their coursework objectives. The resulting Map, provided as a PDF separately from this white paper, provides recommendations as to which texts are most comprehensive in supporting the corresponding specialty area.

What is important to understand is that the specialty areas do not necessarily represent a body of knowledge that can be taught in a single course. It may be most helpful to relate each specialty area with the level of knowledge associated with completing a degree program or concentration.

This will result in the need for multiple courses to provide the student with the *breadth* and *depth* of knowledge necessary to consider a career in that specialty area. Thus when reviewing the Mapping, the most comprehensive and

thus highest recommended text may be best suited for a capstone course or courses associated with that area. For each capstone course or courses, there is also the need for one or more prerequisite courses. Whenever possible, texts that are viewed as supportive of the knowledge base needed for the specialty are also recommended, but not necessarily mapped.

USING THE CENGAGE LEARNING MAPPING

As Tasks and the skill and ability portions of KSAs represent presented in the Framework are more performance based, it is expected that an individual who has become proficient in the knowledge areas of the KSAs would also be able to perform the associated tasks effectively. As such the mapping does not map knowledge-based text materials to the NICE Tasks or to the "SAs" of the KSAs. It does however, provide details for each specialty area's Knowledge areas. For each specialty area you will find one or more textbooks with a summary mapping statement "XX% mapped to General Knowledge Areas" and "YY% mapped to ZZ Specialty Area Knowledge areas", each followed by a number of specific Level details, as shown in Figure 4. The first statement indicates the extent to which the text covers the five general knowledge areas common to all specialty areas. If the text has any level of coverage, regardless of the depth, it is included in this value (5/5 areas = 100%).

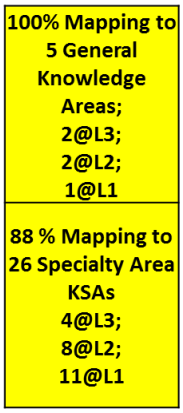

Figure 4: Cengage Learning Mapping summary example
Source: Cengage Learning

The #@L# format corresponds to the depth of coverage, based on the following specifications:

Level	Label	KSA topic coverage:
0 (or blank)	No Coverage	This topic is not covered in this textbook
1	Basic	This topic is introduced and defined.
2	Intermediate	This topic is discussed at length, with additional coverage and detail
3	Advanced	This topic is examined thoroughly, with extensive and detailed discussion, examples and supporting investigation.

As a rule of thumb, the Map associates L1 coverage with "there are one or more paragraphs written on the topic"; L2 coverage with "there are one or more 'A Heads' paragraphs written on the topic" (each text chapter is typically broken into 2-5 high level sections called A-Heads); and L3 coverage with "there are one or more chapters written on the topic".

Thus you can see based on the example shown in Figure 4's summary that there is 100% coverage of the general knowledge and 88% coverage of the specialty area Knowledge areas (percentages rounded to nearest whole number). You can further derive that there is advanced coverage of 4 of the specialty area KSAs, intermediate coverage of 8 KSAs and introductory coverage of 11. If you wish to review the details of coverage, you can request the full spreadsheet with coverage indicate per KSA.

USING THE MAP AND THE FRAMEWORK

In support of this project, we have prepared the following recommendations.

Step 1: Begin with the end in mind (Stephen Covey)

The first task is to determine what you want your program graduates to be able to do – or what specialty area they should be able to perform upon completion of the degree program. Select the specialty area(s) you feel your graduates could or would engage in upon completion of the degree program. If you want your graduates to be able to perform in more than one specialty area, you may need to design a more general program than if you are focused on a single area. The best first step would be to interview businesses in your area to find out what employee skill sets they need, and

then use that information, along with the Framework, to select the suitable knowledge areas, as described in the next step.

If you already have an existing degree program all you may need to do is identify the area(s) that are most closely associated with your current program's objectives, then ensure that you are covering all of the recommended knowledge areas, and have performance assignments closely related to the tasks, skills and abilities not mapped in the Cengage Learning document.

Step 2: Review the NICE Cybersecurity Workforce Framework to identify the Knowledge Areas that have been identified as being needed to succeed in that specialty area.

Next review the Knowledge areas associated with the selected specialty area(s). Do you already have courses that this information is being taught in? What about any prerequisite knowledge? It is most likely you will need a sequence of courses, each with their own texts and experiential labs to build to the capstone experiences most aligned with the specialty areas you have chosen from the Framework.

Step 3: Design the layout of the degree program based on Knowledge Areas and available resources

Now you need to make the determination if you can support the specialty area with existing coursework, or whether new courses will be needed. Development of new curriculum is outside the discussion of this whitepaper however there are many resources available, including programs like Kennesaw State University's Center for Information Security Education (http://infosec.kennesaw.edu). Designing these courses and their learning objectives and program outcomes to suit a particular specialty area may be the most challenging aspect of the process. If you are simply identifying a specialty area to correspond to an existing program, then perhaps you need only make minor revisions to existing courses. In either case, understanding fully the knowledge areas and the resources you will need to teach them is the primary focus of this step.

Step 4: Use the Cengage Learning NICE Map information to select the text(s) you feel would best support the degree program

Next review the Map for your chosen specialty area. You will see a number of texts with varying degrees of support having been mapped. Based on the number of courses you have designed for your degree program in Step 3, you may find you need 1-5 texts to sufficiently cover the Knowledge areas to an acceptable depth. While we do not feel you need to cover every Knowledge area to the *advanced* level, you will need to have sufficient coverage to be able to assert your institution has effectively prepared our students for careers (or at least initial positions) in these areas.

Where appropriate you will also find recommendations for prerequisite courses and texts. Most specialty areas need a strong foundation in information security/cybersecurity fundamentals and many also require managerial content in the domain. Still others may require network security and/or secure programming (software assurance) content. In any event, the content of Step 3 will drive the selection of texts here in Step 4.

Step 5: Roll out the curriculum.

All that remains is to fully develop the individual courses, incorporating the information from the text, plus any supplemental materials necessary to provide acceptable coverage of the specialty area. Here it may be beneficial to select specific Tasks, Skills and Abilities from the Framework to use as assignments, assessments or course deliverables.

RECOMMENDED COURSE STRUCTURES

While each institutions' program will be unique, most programs would benefit from some level of introductory security course, providing the common language and knowledge used by all subsequent courses. For those programs that will be more technical in nature, prerequisite courses in foundations of computing, programming, data communications and networking, and operating systems will likely also be applicable. It is also very likely most programs will need a variety of network security, management of security and operating systems/server security type courses, followed by one or more

capstone courses and/or experiences. It is the process of finding a logical flow of courses, each of which will provide the needed foundation for the following course that will require the attention and diligence of the faculty members designing the course sequence. It is difficult to rise above the natures of our previous disciplines looking at security related curriculum with fresh eyes, rather than simply reiterating the –isms of the past, "they need more math/business".

It is important to keep in mind is that it takes all kinds of security professionals to meet the demands of an organization. Initially there may be a high demand for programmers, help desk workers, and network and systems administrators, each of which could easily progress into and through technical security positions. Eventually many of these individuals and those going through more managerial program will end up as security managers. Businesses will need them all. One program is not any better or worse than another simply because it originated from a particular degree program or because it has a specific focus. With 31 specialty areas in the Framework, there is a very wide range of knowledge and skills needed to fill the many open positions forecast across the country.

ASSOCIATION BETWEEN THE DHS/NSA NATIONAL CENTERS OF ACADEMIC EXCELLENCE PROGRAMS AND THE NICE FRAMEWORK

There currently is discussion within the group responsible for the DHS/NSA National Centers of Academic Excellence program regarding replacing the current curriculum mapping requirements with a mapping to the NIST/NICE Framework – at least some subset of the general knowledge areas and an undetermined number of the specialty areas. For institutions currently possessing the CAE designation or institutions considering pursuing the designation, this could require a detailed investigation of current curriculum offerings compared to the NICE framework. Fortunately there are supporting documents available on the NICE web site and the DHS National Initiative for Cybersecurity Careers and Studies (NICCS) web site at http://niccs.us-cert.gov/ which could help, including the spreadsheet used by the authors to develop this Mapping.

FINAL THOUGHTS

Please keep in mind that the purpose of the NICE framework focused on defining the work specialties of the entire security-related work force, focusing as much on government/public-sector needs as anything else. While it is adaptable to the private/commercial sector, some areas may not readily fit into that environment. What is most important is that academics who seek to use the Framework to help shape the development of new curriculum should remember that even though the Cengage Learning mapping project sought to provide a recommendation for the "best texts" suited toward a specialty area, there will typically be many courses needed to prepare a student for a career in any one of the 31 areas.

References

[1] http://csrc.nist.gov/nice/framework/

[2] http://niccs.us-cert.gov/sites/default/files/documents/files/Framework%20Interactive%20How%20To%20Guide%2002122013.pdf