

# Curricular Guidance for Associate-Degree Cybersecurity Programs

Cara Tang, Portland Community College  
Melissa Stange, Lord Fairfax Community College

Cindy Tucker,  
Bluegrass Community & Technical College

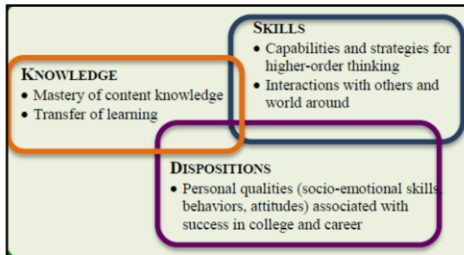
Markus Geissler, Cosumnes River College  
Christian Servin, El Paso Community College

## Goal

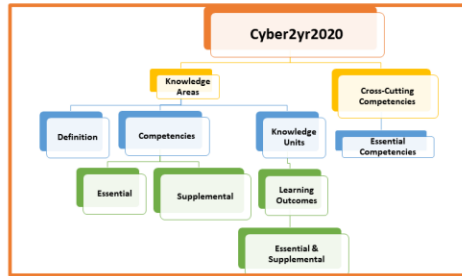
Develop curriculum guidelines for *Cybersecurity Associate-Degree Programs, called Cyber2yr2020*. The curriculum is based on CSEC2017 and other inputs such as the CAE-CD 2Y 2019 knowledge units requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense and the NICE Cybersecurity Workforce Framework.

## Focus

**Competencies = Knowledge + Skills + Dispositions**



## Design



## Knowledge Areas / Domains & Knowledge Units / Subdomains

Knowledge Area / Domain	Knowledge Units / Subdomains
<b>Data</b>	Cryptography Digital Forensics Data Integrity and Authentication Access Control Secure Communication Protocols Cryptography Data Privacy Information Storage Security
<b>Software</b>	Fundamental Principles Design Implementation Analysis and Testing Deployment and Maintenance Documentation Ethics
<b>Component</b>	Component Design Component Procurement Component Testing Component Reverse Engineering
<b>Connection</b>	Physical Media Hardware and Physical Component Interfaces and Connectors Distributed Systems Architecture Network Architecture Network Implementations Network Services Network Defense
<b>System</b>	System Thinking System Management System Access and Control System Testing Common System Architectures
<b>Human</b>	Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms Awareness and Understanding Personal Data Privacy and Security Usable Security and Privacy
<b>Organizational</b>	Risk Management Security Governance & Policy Analytical Tools Systems Administration Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security
<b>Societal</b>	Cybercrime Cyber Law Cyber Ethics Cyber Policy Privacy

## Software Security

**Definition**  
Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

### Essential Competencies

- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

### Supplemental Competencies

- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

### Knowledge Units

Fundamental Principles  
Design  
Implementation  
Analysis and Testing

Deployment and Maintenance  
Documentation  
Ethics

Number Of Competencies & Learning Outcomes Per KA



## Rubrics

### Component Security

Emerging	Learning Outcome - Developed	Highly Developed
Component Design		
Recognize that a component's design may create vulnerabilities in information systems. <i>Remembering</i>	Discuss how a component's design may create vulnerabilities in information systems. <i>Understanding</i> [COM-LO-E01]	Illustrate how a component's design may create vulnerabilities in information systems. <i>Applying</i>
Component Procurement		
List some vulnerabilities, risks, and mitigations for components of an organizational network in a supply chain. <i>Remembering</i>	Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. <i>Understanding</i> [COM-LO-E02]	Analyze vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. <i>Analyzing</i>
Name some security threats and risks to hardware and software in component procurement. <i>Remembering</i>	Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. <i>Understanding</i> [COM-LO-E03]	Outline security threats and risks to both hardware and software in component procurement. <i>Analyzing</i>
Component Testing		
Describe component security testing procedures. <i>Understanding</i>	Perform component security testing. <i>Applying</i> [COM-LO-E04]	Appraise component security testing procedures. <i>Evaluating</i>
Define unit testing and system-level testing. <i>Remembering</i>	Describe unit testing tools and techniques, as distinguished from those used in system-level testing. <i>Understanding</i> [COM-LO-E05]	Compare unit testing tools and techniques with those used in system-level testing, and the role of each in a comprehensive test plan. <i>Analyzing</i>
Component Reverse Engineering		
Recall common reverse engineering scenarios for components of a system. <i>Remembering</i>	Describe common reverse engineering scenarios for components of a system. <i>Understanding</i> [COM-LO-E06]	Perform reverse engineering on components of a system. <i>Applying</i>



More Information Available At  
[ccecc.acm.org/guidance/cybersecurity](https://ccecc.acm.org/guidance/cybersecurity)

# Curricular Guidance for Associate-Degree Cybersecurity Programs

Cara Tang,  
Portland Community College

Cindy Tucker,  
Bluegrass Community &  
Technical College

Markus Geissler,  
Cosumnes River College

Melissa Stange,  
Lord Fairfax Community College

Christian Servin,  
El Paso Community College



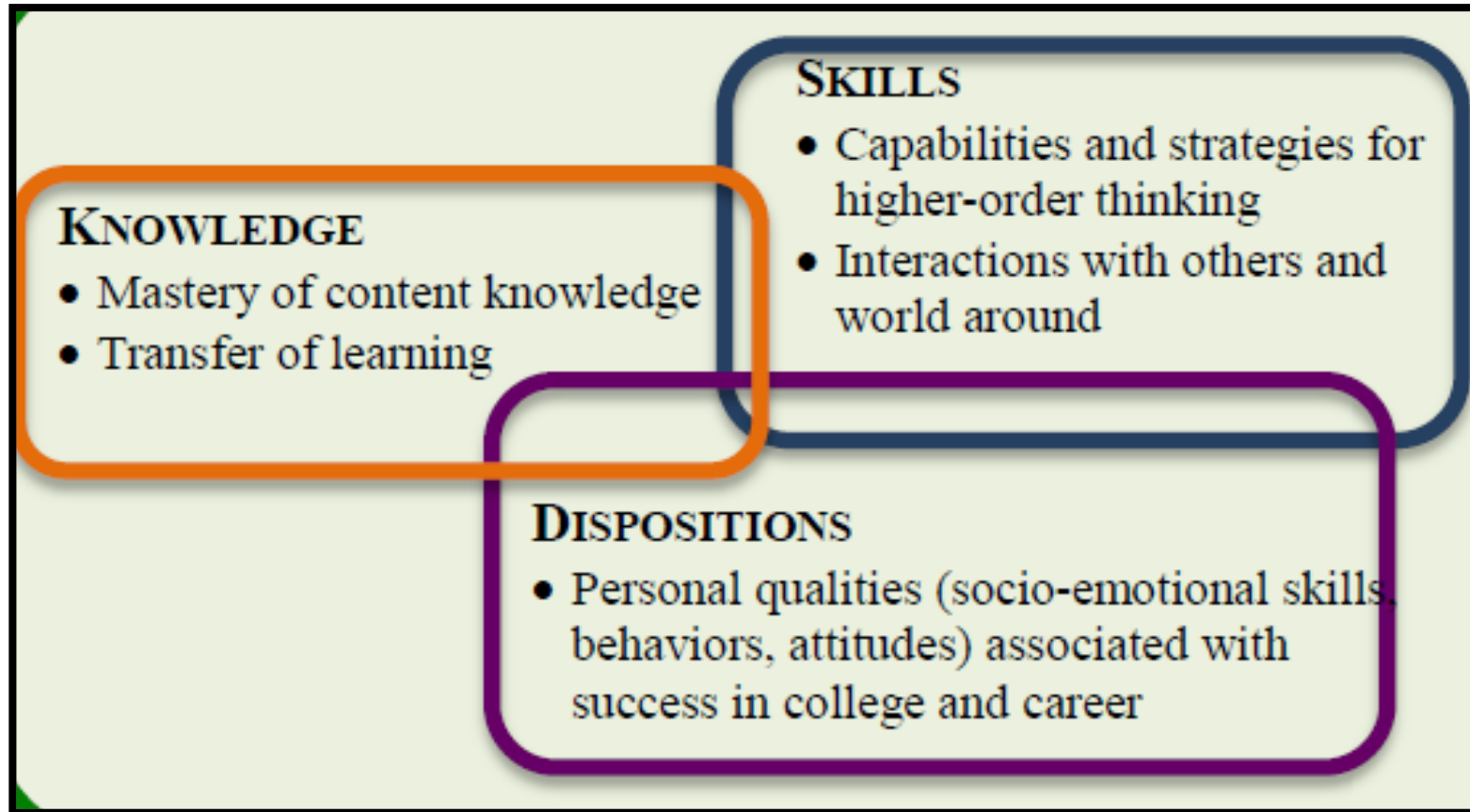
## Goal

Develop curriculum guidelines for *Cybersecurity Associate-Degree Programs*, called *Cyber2yr2020*.

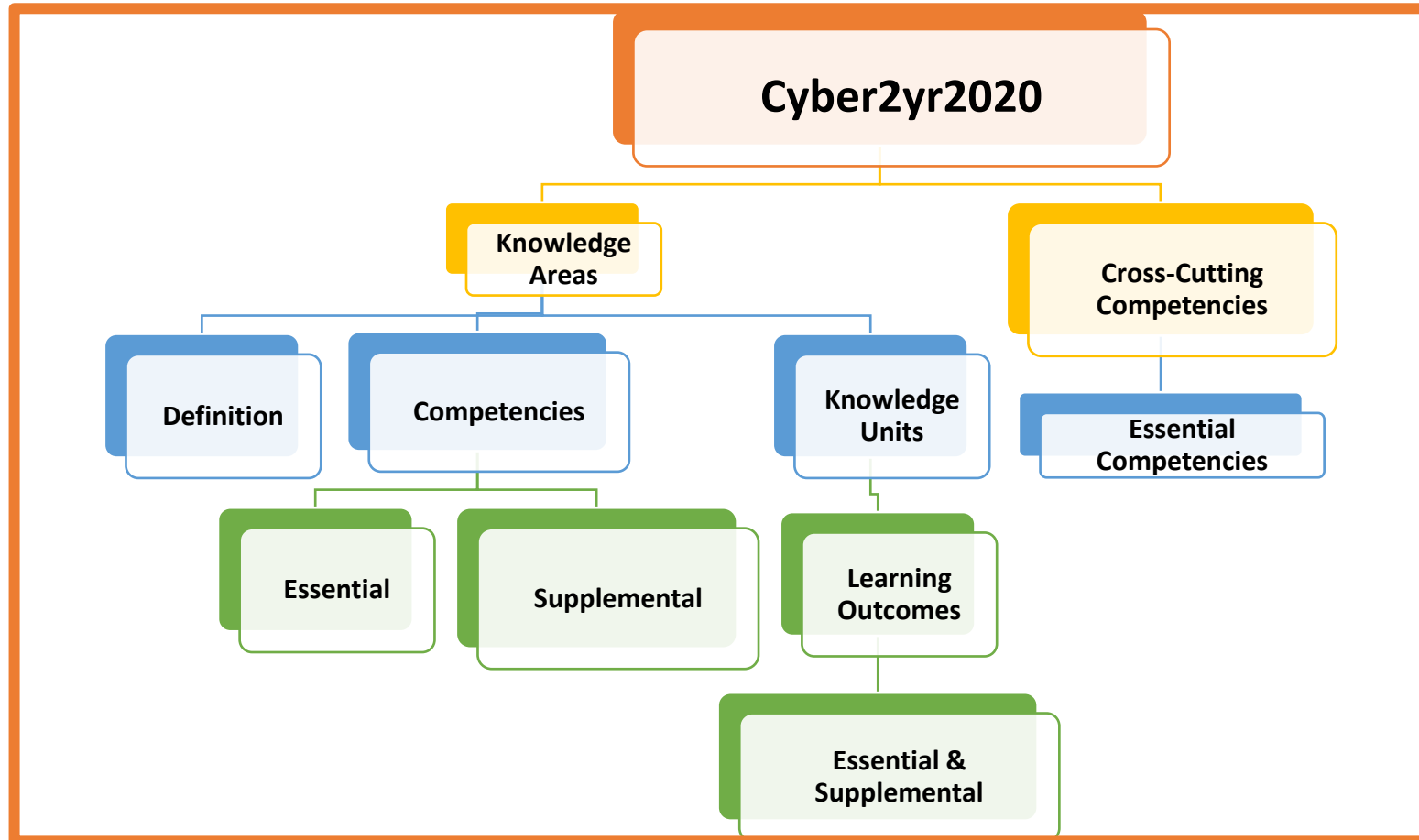
The curriculum is based on CSEC2017 and other inputs, such as the CAE-CD 2Y 2019 Knowledge Units requirements of the NSA and DHS National Centers of Academic Excellence in Cyber Defense, and the NICE Cybersecurity Workforce Framework.

# Focus

***Competencies = Knowledge + Skills + Dispositions***



# Design



# Knowledge Areas / Domains & Knowledge Units / Subdomains

<b>Data</b>	Cryptography Digital Forensics Data Integrity and Authentication Access Control	Secure Communication Protocols Cryptanalysis Data Privacy Information Storage Security
<b>Software</b>	Fundamental Principles Design Implementation Analysis and Testing	Deployment and Maintenance Documentation Ethics
<b>Component</b>	Component Design Component Procurement	Component Testing Component Reverse Engineering
<b>Connection</b>	Physical Media Hardware and Physical Component Interfaces and Connectors Distributed Systems Architecture	Network Architecture Network Implementations Network Services Network Defense
<b>System</b>	System Thinking System Management System Access and Control	System Testing Common System Architectures
<b>Human</b>	Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	Awareness and Understanding Personal Data Privacy and Security Usable Security and Privacy
<b>Organizational</b>	Risk Management Security Governance & Policy Analytical Tools Systems Administration	Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security
<b>Societal</b>	Cybercrime Cyber Law Cyber Ethics	Cyber Policy Privacy

# Software Security

## Definition

Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

## Essential Competencies

- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

## Supplemental Competencies

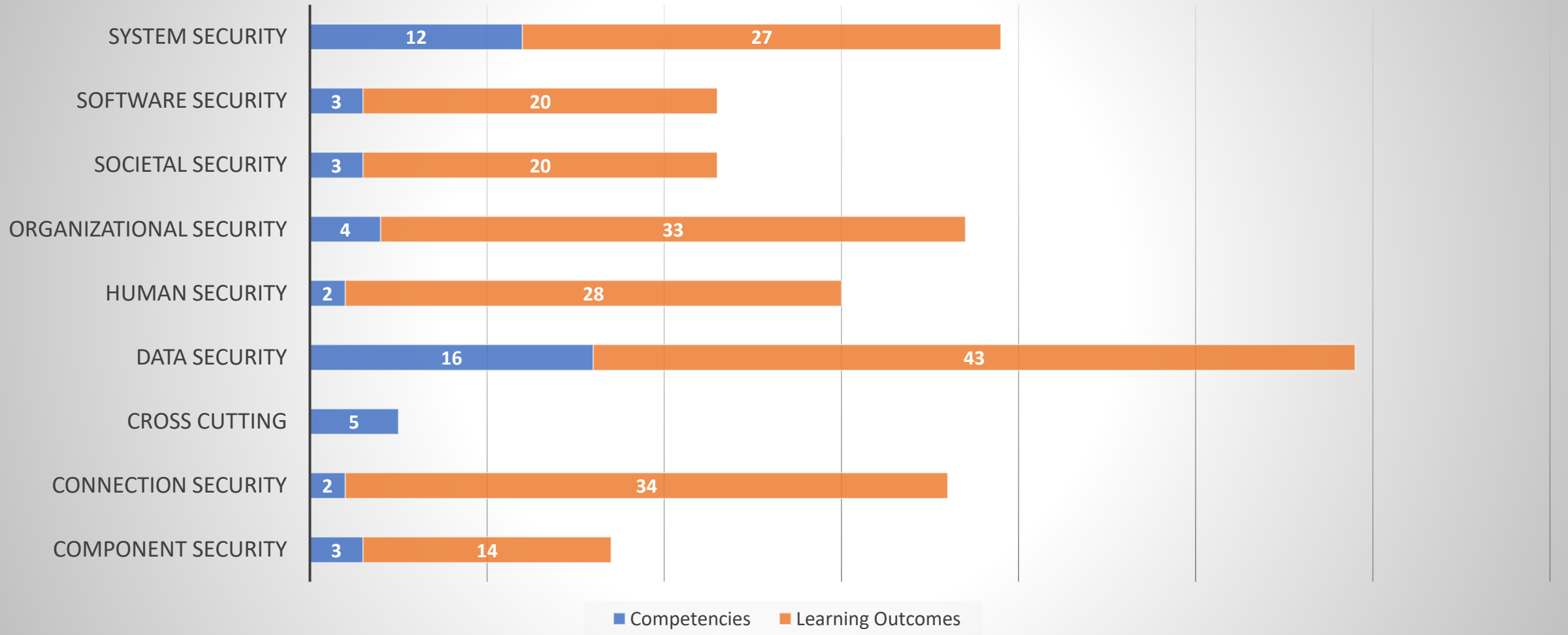
- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

## Knowledge Units

Fundamental Principles  
Design  
Implementation  
Analysis and Testing

Deployment and Maintenance  
Documentation  
Ethics

## Number Of Competencies & Learning Outcomes Per KA





# Rubrics

Component Security		
Emerging	Learning Outcome - Developed	Highly Developed
Component Design		
Recognize that a component's design may create vulnerabilities in information systems. <i>Remembering</i>	Discuss how a component's design may create vulnerabilities in information systems. <i>Understanding</i> [COM-LO-E01]	Illustrate how a component's design may create vulnerabilities in information systems. <i>Applying</i>
Component Procurement		
List some vulnerabilities, risks, and mitigations for components of an organizational network in a supply chain. <i>Remembering</i>	Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. <i>Understanding</i> [COM-LO-E02]	Analyze vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. <i>Analyzing</i>
Name some security threats and risks to hardware and software in component procurement. <i>Remembering</i>	Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. <i>Understanding</i> [COM-LO-E03]	Outline security threats and risks to both hardware and software in component procurement. <i>Analyzing</i>
Component Testing		
Describe component security testing procedures. <i>Understanding</i>	Perform component security testing. <i>Applying</i> [COM-LO-E04]	Appraise component security testing procedures. <i>Evaluating</i>
Define unit testing and system-level testing. <i>Remembering</i>	Describe unit testing tools and techniques, as distinguished from those used in system-level testing. <i>Understanding</i> [COM-LO-E05]	Compare unit testing tools and techniques with those used in system-level testing, and the role of each in a comprehensive test plan. <i>Analyzing</i>
Component Reverse Engineering		
Recall common reverse engineering scenarios for components of a system. <i>Remembering</i>	Describe common reverse engineering scenarios for components of a system. <i>Understanding</i> [COM-LO-E06]	Perform reverse engineering on components of a system. <i>Applying</i>

**More information available at**  
[ccecc.acm.org/guidance/cybersecurity](https://ccecc.acm.org/guidance/cybersecurity)

