Cybersecurity for Curriculum Alignment

5. Cybersecurity Basics

	KSA Description	Knowledge, Skill, or Ability?	Bloom's Taxonomy Level?	Cross-cutting KSAs	Course Number/Name	Learning Outcome
a	Examine and employ principles of cybersecurity including its goals, objectives, and purposes	Ability	2			
b	Describe the need for security and identify security risks and ssociated security safeguards and methodologies (e.g., auditing).	Knowledge	2			
c	Explain the need for confidentiality, integrity, and availability (CIA) and identify types of controls (e.g., deterrent, preventative, detective, compensating, technical and administrative)	Knowledge	1			
d	Explain security in terms of authentication, authorization, and accounting (AAA) as well as access	Knowledge	3			
e	Understand the purpose and function of cybersecurity technology so identifying and implementing the various tools necessary to improve an organization's resiliency and reduce the possibility of data breaches	Ability	3			
f	Describe, recognize, and mitigate major security threats (e.g., adware, viruses, spyware, trojans, rootkits, logic bombs, worms, spyware, ransomware, spoofing, hacking, phishing, and ploymorphic malware), using the tools standard in the industry	Skill	4			
g	Describe the components of the physical environment (e.g., wiring closets, server rooms, data centers) and physical security systems.	Knowledge	2			
h	Describe the need for security in networking (e.g., firewalls, access controls, encryption, demilitarized zone).	Knowledge	2			
i	Understand the indicators of compromise (IOCs) and their use in determining whether an attack has happened or is in progress	Knowledge	3			
j	Track and catalog computing assets through inventory management, devices and software	Ability	2			
k	Describe the need for security in application development.	Knowledge	2			
l	Describe computer forensic techniques, their importance in incident response, and their relevance to law enforcement	Knowledge	2			
m	Recognize and describe industry threat models (CVE, CWE, threat intel feed, etc).	Skill	2			
n	Demonstrate and recognize common cyber-attack techniques such as the cyber kill chain and the MiTRE ATT&CK framework	Knowledge	3			
o	Describe attackers (black hat, white hat, nation states, etc.) and techniques (cybercriminals, APTs).	Knowledge	2			
p	Describe and understand social engineering attacks (e.g., shoulder surfing, dumpster diving, tailgating, impersonation, hoaxes, phishing, spear phishing, whaling, vishing),	Knowledge	2			
q	Understand the issues with passwords and the tools and techniques available to crack passwords (e.g. brute force, dictionary attacks, birthday attacks, rainbow attacks and other hybrid attacks).	Knowledge	2			
r	Desctribe and discover vulnerabilities, understanding concepts and tools of vulnerability assessment, scanning, and penetration testing, and the work of red .purple and blue teams.	Knowledge	2			
s	Demonstrate an understanding of adversarial thinking using capture the flag (CTF) and other techniques.	Skill	3			
t	Understand the concept of digital trust computing and the Zero Trust principles	Knowledge	2			
u	Describe cyber threat intelligence (CTI) and its role in cybersecurity	Knowledge	2			

Cybersecurity for Curriculum Alignment						
v	Recognize that an enterprise security requires a holistics strategy that considers people, process, and technology.	Knowledge	2			
w	Categorize system contrils in compliance with government and industry standards including NIST Cybersecurity Framework, FISMA, FEDRAMP, PCI/DSS and ISO standards	Knowledge	4			