Cybersecurity for Curriculum Alignment

8. Network Security

	KSA Description	Knowledge, Skill, or Ability?	Bloom's Taxonomy Level?	Cross-cutting KSAs	Course Number/Name	Learning Outcome
a	Apply networking fundamentals to infrastructure in an organization including Defense in Depth	Skill	3			
b	Select network storage interfaces (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB]).	Skill	3			
c	Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring).	Skill	4			
d	Demonstrate an understanding of network security devices (IDS, IPS, FW, NGFW, WAF, CDN, etc.).	Kowledge	3			
e	Design a secure small office/home office (SOHO) network	Skill	3			
f	Apply network protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP, etc.) and their impact on security	Skill	3			
g	Apply Ipv4 and IPv6 securely	Skill	2			
h	Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, antenna placement, power level controls).	Skill	2			
i	Apply the principles of secure network design (e.g., DMZ, subnetting, NAT/PAT, remote access, telephony, virtualization, honeypots).	Skill	3			
j	Implement port security, including an undersanding of port scanning and network traffic monitoring	Skill	2			
k	Understand how to mitigate network threats (e.g., flood guards, loop protection, implicit deny, network separation, log analysis, Unified Threat Management, peripheral and removable media).	Knowledge	2			
l	Describe the characteristics and uses of networks, network devices, and components	Knowledge	2			
m	Design a basic network diagram given a specific need and set of hosts.	Skill	3			
n	Install and configure network security mechanisms (firewalls, switches, load balancers, proxies, security gateways, spam filters, IDS/IPS, VPN, etc.).	Skill	3			
o	Understand and use basic network assessment tools (e.g. Wireshark, NMAP, port scanner)	Knowledge	3			
p	Understand, setup, and maintain the key cybersecurity principles in network defense (defense in depth, minimizing exposure, etc.).	Skill	4			
q	Understand the process of vulnerability identification and assessment.	Knowledge	2			
r	Understand, setup and maintain user roles and system management techniques (e.g., password, groups, user privilege policies and monitoring).	Knowledge	2			
s	Monitor and manage a network using Unified Threat Management (UTM)	Skill	3			
t	Manage PKI and certificates (transport encryption, non-repudiation, hashing, digital signatures).	Skill	2			
u	Understand the concept of opening/extending the network perimeter and the role of a cloud access security broker (CASB).	Knowledge	2	Networking 1i		
v	Identify threats using discovery tools and utilities (e.g., protocol analyzer, vulnerability scanner, honeypots, honeynets, port scanner).	Ability	3			