IT SKILL STANDARDS 2020 AND BEYOND

“Infrastructure Connectivity Management and Engineering”

Job Cluster

Acknowledgements

The development and publication of these skill standards has been a joint and collaborative effort between business and industry representatives and the education community. We are grateful to the industry personnel who participated in the development and validation process. Industry subject matter experts, technical executives, supervisors and technicians donated their time and effort to assure the relevancy of the standards 12 to 36 months into the future.

We gratefully acknowledge funding from the National Science Foundation and the leadership by the team on the IT Skill Standards 2020 and Beyond grant, based at Collin College.

Our leaders are strategically divided into Central, Western, and Eastern teams.

Central

Dr. Ann Beheler, Principal Investigator

Christina Titus, Program Director

Deborah Roberts, Co-Principal Investigator

Helen Sullivan, Senior Staff

West Coast

Terryll Bailey, Co-Principal Investigator

Dr. Suzanne Ames, Co-Principal Investigator

East Coast

Peter Maritato, Co-Principal Investigator

Gordon Snyder, Senior Staff

This material is based upon work supported by the National Science Foundation under Grant No. 1838535. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

itskillstandards.org

Infrastructure Connectivity, Management and Engineering

The definition for Infrastructure Connectivity, Management and Engineering as developed by approximately 100 Thought Leaders (mostly Chief Technology Officers and Chief Information Officers) through three meetings and follow-up surveys to gain consensus is:

> Infrastructure Connectivity covers hardware, wired, optical, wireless, satellite, cloud, and any other means of connectivity for data transmission.
>
> Infrastructure Management and Engineering ensures that the Information Technology and Communications Infrastructure is sufficiently robust, scalable, secure and efficient to deliver integrated services. It supports the design installation processes, physical resources, and operations required for developing, integrating, operating, and sustaining IT applications. It also addresses the day-to-day management and maintenance of IT services, systems, and applications. This definition was adapted from mitre.org with input from national IT Thought Leaders.

This packet includes…

Job skills as developed by subject matter experts (SMEs) via multiple synchronous meetings (Page 5).

The tasks, knowledge, skills and abilities (KSAs) were developed with a focus 12 to 36 months in the future for an entry-level employee working in that specific cluster.

More specific definitions can be found within the KSA list.

The average was calculated from the subject matter expert votes.

- A vote of "4" indicated the item must be covered in the curriculum.
- A vote of "3" indicated the item should be covered in the curriculum.
- A vote of "2" indicated that it would be nice for the item to be covered in the curriculum.
- A vote of "1" indicated the item should not be covered in the curriculum.

Employability Skills as developed by SMEs via multiple synchronous meetings (Page 12).

Employability competencies are essential for every IT job and are based on what the work requires. SMEs were offered three clearly-defined “levels of proficiency” for each employability skill. The proficiency scale is defined as Level 1 – basic: Level 2- intermediate; and Level 3 - advanced. The levels are cumulative, so a “Level 3” assumes the employee can perform all characteristics of “Level 1” and “Level 2.”

For each employability skill, SMEs selected the competency level that best aligned with what would be expected from an entry-level worker for the job cluster in question.

Key Performance Indicators (KPIs) as developed by SMEs (Page 13).

Key Performance Indicators answer the question, “How do we know when a task is performed well?”

A search was performed to locate validated/verified KPIs for technician level work in IT fields. Sources included the Texas Skill Standards System, National Skill Standards Board, National Institute of Standards and Technology and other sources. The identified KPIs were then cross-referenced to the tasks for the ITSS 2020 job clusters. They were reviewed and revised by a group of the same subject matter experts who developed the tasks and KSAs for the cluster in a structured, facilitated verification session.

Student Learning Outcomes (SLOs) as identified by educators attending the KSA meetings (Page 15).

The SLOs are for use in the creation of curriculum to help define what the students will know and be able to demonstrate. Each of these SLOs can be observed, measured, and demonstrated.

Degree Expectations as identified by educators (Page 22).

A pool of 20 community college and four-year university faculty members from across the country were asked to categorize each knowledge, skill, ability, and task below. The question posed to them: would these KSA+Ts be reasonably included in a two-year AAS program, a four-year Bachelor's program, both, or neither? These results provide another tool for educators to use in assessing how to best incorporate each knowledge, skill, ability, and task.

Infrastructure Connectivity Management and Engineering Tasks and KSAs

Tasks

SPECIFIC THINGS an entry level person would BE EXPECTED TO PERFORM on the job WITH LITTLE SUPERVISION.

	Install	Avg
T-1	Configure network, routers, and switches (e.g., higher-level protocols, tunneling).	3.00
T-2	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patch network vulnerabilities to safeguard information.	3.35
T-3	Install or replace network, routers, and switches.	3.40
T-4	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	2.86
T-5	Validate/update baseline system security according to organizational policies.	3.10
T-6	Install, update, and troubleshoot systems/servers.	3.24
T-7	Installation, implementation, configuration, and support of system components.	3.33
	Troubleshoot	
T-8	Diagnose network connectivity problem.	3.20
T-9	Troubleshoot hardware/software interface and interoperability problems.	3.10
	Document	
T-10	Follow SOP and validate/update documentation of compliance.	3.38
	Monitor, Maintain, Operate	
T-11	Integrate new systems into existing network architecture.	2.90
T-12	Monitor network capacity and performance.	3.05
T-13	Test and maintain network infrastructure including software and hardware devices.	3.15
T-14	Conduct functional and connectivity testing to ensure continuing operability.	3.48
T-15	Follow group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	2.90
T-16	Manage basic functionality around accounts, network rights, and access to systems and equipment.	2.95
T-17	Provide ongoing optimization and problem-solving support.	3.15
T-18	Check system hardware availability, functionality, integrity, and efficiency.	3.33
T-19	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	3.19
T-20	Implement local network usage policies and procedures.	2.90
T-21	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	3.05
T-22	Monitor and maintain system/server configuration.	3.24

Knowledge

Knowledge focuses on the understanding of concepts. It is theoretical. An individual may have an understanding of a topic or tool or some textbook knowledge of it but have no experience applying it. For example, someone might have read hundreds of articles on health and nutrition, many of them in scientific journals, but that doesn't make that person qualified to dispense advice on nutrition.

K-1	Knowledge of computer networking concepts and protocols, and network security methodologies.	3.90

K-2	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (e.g. PCI, PII, PHI, GDPR).	2.76
K-3	Knowledge of cybersecurity and privacy principles.	3.33
K-4	Knowledge of cyber threats and vulnerabilities.	3.24
K-5	Knowledge of impacts of cybersecurity lapses.	3.19
K-6	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	3.57
K-7	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	3.65
K-8	Knowledge of risk management, cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	3.10
K-9	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.62
K-10	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	3.43
K-11	Knowledge of measures or indicators of system performance and availability.	3.24
K-12	Knowledge of remote access technology concepts.	3.19
K-13	Knowledge of server administration and systems engineering theories, concepts, and methods.	3.19
K-14	Knowledge of Virtual Private Network (VPN) security.	3.43
K-15	Knowledge of concepts, terminology, and operations of a wide range of baseband and broadband communications transmission media and protocols (computer and telecommunications networks, satellite, fiber, wireless).	3.43
K-16	Knowledge of network tools (e.g., ping, traceroute, nslookup).	3.71
K-17	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	3.38
K-18	Knowledge of Voice over IP (VoIP).	3.14
K-19	Knowledge of the common attack vectors on the network layer.	3.29
K-20	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	3.33
K-21	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	3.24
K-22	Knowledge of concepts of certificates, key management and usage.	3.19
K-23	Knowledge of where to find details on wired and wireless transmission standards (e.g. Ethernet, Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, and satellite communications.)	3.10
K-24	Knowledge of jamming and interference patterns so they can be recognized as a challenge for the network itself applied to wireless networkds.	2.81
K-25	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	3.71
K-26	Knowledge of controls related to the use, processing, storage, and transmission of data.	3.24
K-27	Knowledge of performance tuning tools and techniques.	2.95
K-28	Knowledge of the enterprise information technology (IT) architecture.	3.24
K-29	Knowledge of the type and frequency of routine hardware maintenance (e.g. Linux/Unix OS, Windows Server OS).	3.24

K-30	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) including network storage and servers with emphasis on extensions.	3.05
K-31	Knowledge of virtualization technologies and virtual machine development and maintenance.	3.29
K-32	Knowledge of system administration, network, and operating system hardening techniques.	3.14
K-33	Knowledge of system/server diagnostic tools and fault identification techniques.	3.24
K-34	Knowledge of operating system command-line tools.	3.33
K-35	Knowledge of principles and methods for integrating system components including network storage and servers.	3.24
K-36	Knowledge of script automation and application programming interfaces.	3.24
K-37	Knowledge of network backup and recovery procedures.	3.19
K-38	Knowledge of how to patch network vulnerabilities to ensure that information is safeguarded against outside parties.	3.38
K-39	Knowledge of system administration, network, and operating system concepts and hardening techniques.	3.43
K-40	Knowledge of asset management and why it's important to the business.	2.95
K-41	Knowledge of risks associated with storing various types of data in different physical locations.	3.05
K-42	Knowledge of infrastructure data storage capabilities and storage clusters.	3.10
K-43	Knowledge of IoT end devices and connectivity.	3.05
K-44	Knowledge of Software Defined Networking concepts.	3.19
K-45	Knowledge of Continuous Quality Improvement Principles (of particular value: Lean and Agile).	2.43
K-46	Knowledge of how to identify organizational goals that align with architecture and how do you identify your value to the organization.	2.71
K-47	Knowledge of Python or other scripting languages.	3.05
K-48	Knowledge of the differences or similarities between Private, Public, and Hybrid Cloud Implementations.	3.48
K-49	Knowledge of the difference or similarities between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	3.43
K-50	Awareness of framework concepts, their selection and use.	2.90
K-51	Awareness of the pros or cons behind using Frameworks.	2.86
K-52	Knowledge of the term benchmarks and the reasons for their use.	3.10
K-53	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure or organization.	3.19
K-54	Knowledge of the concept of Service Level Agreement, why they are used, when they are used, and its application within Cloud implementations.	3.38
K-55	Knowledge of who owns or should own the data/information in a Cloud implementation.	3.00
K-56	Knowledge of the key Management/Operational/Security/Privacy challenges potential faced when considering or implementing a Cloud capability.	3.10
K-57	Knowledge of the different organizational roles needed as one plans for Cloud implementation or manages an existing Cloud capability.	2.85
K-58	Knowledge of the incident response challenges potentially faced within a Cloud implementation.	2.95
K-59	Knowledge of Web Services technologies.	2.90
K-60	Knowledge of cloud network storage including cloud object -based storage and local system storage.	3.05

K-61	Knowledge of the different Cloud computing database types (RDS).	2.76
K-62	Knowledge of how to scale a Cloud database.	2.43
K-63	Knowledge of region failover and redundancy vs local failover and redundancy and how that needs to be applied to your data centers (cloud, hybrid, on-prem).	3.14
K-64	Knowledge of the differences between SQL and Non-SQL Databases.	2.76
K-65	Knowledge of Cloud IAM (Identity and Access Management) - cloud and hybrid.	3.14
K-66	Knowledge of Cloud IAM users, groups, roles and policies - cloud and hybrid.	3.14
K-67	Knowledge of Cloud Computing shared security responsibility model - cloud and hybrid.	3.19
K-68	Knowledge of Cloud Regions - cloud and hybrid.	3.29
K-69	Knowledge of Cloud Availability Zone - cloud and hybrid.	3.10
K-70	Knowledge of Recovery Time Objective (RTO).	2.95
K-71	Knowledge of Recovery Point Objective (RPO).	3.00
K-72	Knowledge of High Availability factors (Fault-tolerance, recoverability, and scalability).	3.19
K-73	Knowledge of microservices and containerization (e.g. Kubernetes and Docker).	2.90
K-74	Knowledge of Auto Scaling and Load Balancing.	2.95
K-75	Knowledge of the differences between Cloud vs. On-Premises.	3.67
K-76	Knowledge in preparing and deploying a cloud database solution that meets application requirements.	2.32
K-77	Knowledge of database management systems, query languages, table relationships, and views.	2.33
K-78	Knowledge of Azure.	3.14
K-79	Knowledge of AWS.	3.24
K-80	Knowledge of Google Cloud.	2.95
K-81	Knowledge of emerging technology (e.g. blockchain, quantum computing)	2.71
K-82	Knowledge of making recommendations for migration of a physical network to a cloud-based architecture.	2.67
K-83	Knowledge of creating a cloud-based network infrastructure to meet requirements for a software application.	2.76
K-84	Knowledge of the OSI model and understand that OSI is the framework for all problem solving and troubleshooting. Provide basic framework for how it all works, including how cloud computing has impacted the conceptualization of the seven layers. Plus an awareness of IP multimedia services.	3.67
K-85	Knowledge of preparing and deploying a Cloud High Availability and Business Continuity Solution.	2.57
K-86	Knowledge of implementing auto scaling and load balancing.	2.57
K-87	Knowledge of assessing and evaluating the technical benefits of implementation of a cloud computing architecture.	2.43
Skills The capabilities or proficiencies developed through training or hands-on experience. Skills are the practical application of theoretical knowledge. Someone can take a course to gain knowledge of concepts without developing the skills to apply those concepts. Development of skills requires hands-on application of the concepts.		
S-1	Understand that OSI is the framework for all problem solving and troubleshooting	3.48
S-2	Skill in establishing a routing schema.	3.29
S-3	Skill in implementing, maintaining established network security practices.	3.38

S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, and switches.	3.62
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	3.38
S-6	Skill in securing network communications. (e.g., logical)	3.38
S-7	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	3.48
S-8	Skill in basic configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	3.52
S-9	Skill in testing network infrastructure contingency and recovery plans.	3.10
S-10	Skill in applying various subnet techniques (e.g., CIDR).	3.05
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	3.38
S-12	Skill in configuring and basic optimizing software.	2.90
S-13	Skill in diagnosing connectivity problems.	3.71
S-14	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).	2.86
S-15	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	3.24
S-16	Skill in using Cloud (e.g. Amazon Elastic Compute Cloud).	3.05
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	2.62
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	3.43
S-19	Skill in interfacing with customers.	3.29
S-20	Skill in conducting system/server management and maintenance.	3.10
S-21	Skill in correcting physical and technical problems that impact system/server performance.	3.19
S-22	Skill in troubleshooting failed system components (i.e., servers).	3.38
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	3.29
S-24	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).	3.43
S-25	Skill in monitoring and optimizing basic system/server/cloud performance.	3.24
S-26	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).	3.19
S-27	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	3.05
S-28	Skill in applying Software Defined Networking concepts.	3.05
S-29	Skill in identifying and distinguishing Private, Public, and Hybrid Cloud Implementations.	3.19
S-30	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	3.29
S-31	Skill in executing Test Cases for identified functional or non-functional requirements.	3.00
S-32	Skill in documenting results of executed test cases showing whether according to developed success criteria the test case passes, fails, or partially passes.	3.05
S-33	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	3.00
S-34	Skill in preparing written reports.	3.14
S-35	Skill in preparing presentations.	3.10

S-36	Skill in producing Virtual Machines from a Cloud image.	3.00
S-37	Skill in producing Virtual Machines within a Cloud region.	2.76
S-38	Skill in demonstrating how to customize virtual networks with IP Address Range, subnets, routing tables and gateways.	3.05
S-39	Skill in analyzing and troubleshooting Cloud Virtual Networks.	2.86
S-40	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	3.10
S-41	Skill in deploying cloud storage technologies with the assistance of a senior technician.	3.00
S-42	Skill in analyzing and troubleshooting different cloud storage technologies.	2.81
S-43	Skill in applying permissions from the IAM (Identity and Access Management).	3.05
S-44	Skill in applying permissions for IAM (Identity and Access Management) Group(s).	3.10
S-45	Skill in applying permissions for IAM (Identity and Access Management) user(s).	3.10
S-46	Skill in analyzing and troubleshooting containers.	2.74
S-47	Skill in using tools like Chef, Puppet, etc.	2.48
S-48	Skill in managing changes/updates for both internal and external customers when policies and procedures change.	2.90
S-49	Skill in assessing or monitoring system for cyberattacks.	3.05
S-50	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	3.05
S-51	Skill in identifying areas where there are issues/gaps in a cloud implementation and develop a working solution.	2.52
S-52	Skill in leveraging cloud/hybrid managed services to enable greater flexibility and resilience in an secure infrastructure.	2.76
S-53	Skill in identifying appropriate cloud services that provide the compute power needed to solve a technical business problem while optimizing cost.	2.71
S-54	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	2.95
S-55	Skill in importing/ exporting/migrating/protecting/securing data from one data source to another.	2.19
S-56	Skill in applying security concepts in the automation of resource provisioning.	3.00
S-57	Skill in identifying the necessary components of a physical network and a cloud-based network.	3.05
S-58	Skill in using Azure .	2.86
S-59	Skill in using AWS.	2.95
S-60	Skill in Google Cloud.	2.57
Abilities Abilities have historically been used to describe the innate traits or talents that a person brings to a task or situation. Many people can learn to negotiate competently by acquiring knowledge about it and practicing the skills it requires. A few are brilliant negotiators because they have the innate ability to persuade. In reality, abilities may be included under skills or may be separated out.		
A-1	Ability to install network equipment including routers, switches, servers, transmission media, and related hardware.	3.52
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	3.62
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	3.65
A-4	Ability to operate the organization's LAN/WAN pathways.	3.14

A-5	Ability to monitor measures or indicators of system performance and availability.	3.33
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	3.05
A-7	Ability to monitor traffic flows across the network.	3.38
A-8	Ability to recognize and escalate the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	3.52
A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	3.29
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	3.00
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).	3.05
A-12	Ability to collaborate effectively with others.	3.81
A-13	Ability to function effectively in a dynamic, fast-paced environment.	3.75
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.33
A-15	Ability to maintain automated security control assessments.	3.00
A-16	Ability to communicate effectively (written and oral) within and among team members and associated stakeholders (i.e. different audiences and organizational levels). This includes communicating complex technical issues and business implications.	3.62
A-17	Ability to work under stress.	3.81
A-18	Ability to problem solve.	3.86
A-19	Ability to analyze and interpret customer input for expressed and implied requirements.	3.38
A-20	Ability to translate technical language into lay terminology when needed.	3.48
A-21	Ability to read and interpret technical documents, diagrams, and decision trees.	3.71
A-22	Ability to listen and understand what people say.	3.95
A-23	Ability to recognize and understand details.	3.76
A-24	Ability to order and arrange items.	3.52
A-25	Ability to create appropriate presentation visuals for technical material.	3.24

Infrastructure Connectivity Management and Engineering Employability Skills

Workplace Professionalism & Work Ethics	Level 1 - Employee learns expectations of workplace environment (professional behavior and ethics) and adheres to practices with some guidance. Level 2 - Employee exhibits sound professionalism, judgment, and integrity and accepts responsibility for own behavior. Employee exhibits these qualities without guidance but occasionally refers to policies as needed.
Written Communication	Level 1 - Employee understands written instructions and executes tasks with guidance and feedback from supervisor. Employee clearly communicates concepts in writing. Level 2 - Employee comprehends and executes written instructions with minimal guidance. Employee composes well-organized written documents.
Oral Communication	Level 1 - Employee understands oral instructions and executes tasks with guidance and feedback from supervisor. Employee communicates concepts orally while clarifying for meaning. Employee develops listening skills. Level 2 - Employee comprehends and executes oral instructions with minimal guidance and exhibits good listening skills. Employee clarifies for meaning without needing prompting from supervisor.
Teamwork	Level 1 - With guidance and feedback from supervisor, employee obeys team rules and understands team member roles. Employee actively participates in team activities, volunteers for special tasks, and establishes rapport with co-workers.
Problem Solving & Critical Thinking	Level 1 - Employee identifies the problem and relevant facts and principles with guidance and feedback from supervisor. Employee summarizes existing ideas and demonstrates creative thinking process while problem solving. Level 2 - With minimal supervision, employee analyzes underlying causes, considers risks and implications, and uses logic to draw conclusions. Employee applies rules and principles to processes and recommends solutions.
Organization and Planning	Level 1 - Employee prepares schedule for self, monitors and adjusts task sequence, and analyzes work assignments with guidance from supervisor. Level 2 - Employee manages timelines and recommends timeline adjustments. Employee escalates timeline-impacting issues as appropriate.
Adaptability and Flexibility	Level 1 - With guidance and feedback from supervisor, employee is able to adjust ways of doing work based on changing dynamics. Working under pressure is difficult, but employee makes it through the project with guidance and oversight.
Initiative	Level 1 - Employee finishes a step in a project and waits for direction before going on to the next step. Level 2 - Employee finishes multiple steps in a project and appropriately begins working on the next step without being asked.
Accuracy	Level 1 - Employee makes mistakes routinely but is committed to learning to adjust work habits to prevent them in the future. Level 2 - Employee occasionally makes mistakes but quickly makes adjustments to work habits to avoid making the same mistake twice.
Cultural Competence	Level 1 - Employee is inexperienced with working with diverse teams. With support and guidance and getting to know team members, employee develops working relationships. Level 2 - Employee is committed to working with diverse teams but struggles when differences arise. Employee identifies those challenges and works with colleagues to find ways to work effectively.
Self and Career Development	Level 1 - Employee requires feedback and direction from supervisor regarding improvement needed in professional and technical skills. Employee follows through with skills development with monitoring by supervisor. Level 2 - Employee builds upon self-assessment experience and can develop a professional and technical skills improvement plan in conjunction with supervisor. Employee completes development plan without prompting from supervisor.

frastructure Connectivity Management and Engineering Key Performance Indicato

For the entry-level employee, all tasks are typically done under supervision for much of the first year and then with some

	Task	Key Performance Indicators
	Install	
T-1	Configure and optimize network, routers, and switches (e.g., higher-level protocols, tunneling).	Installation or upgrade plan is complete and accurate and company guidelines are followed. All components and devices (including IoT) are properly connected. Operating system and application software and upgrades are installed and configured according to specifications. Required network protocols are correctly installed and tested. System hardware and software are configured to specification. Network interfaces (e.g. LAN to WAN) are correctly connected and configured. Network security devices and software (e.g., firewall, routers, anti-virus software) are correctly installed by peer reviews or supervisor. Accounts are set up following standard operating procedures. Final overall tests to ensure full network resilience and functionality are properly performed. Current software upgrades including operating system patches anti-virus database are installed. Requirements for systems security are properly identified by peer reviews or supervisor. Communication regarding changes in procedures is distributed to all necessary parties in a timely manner.
T-2	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patching network vulnerabilities to safeguard information.	
T-3	Install or replace network, routers, and switches.	
T-4	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	
T-5	Validate/update baseline system security according to organizational policies.	
T-6	Install, update, and troubleshoot systems/servers.	
T-7	Installation, implementation, configuration, and support of system components.	
	Troubleshoot	
T-8	Diagnose network connectivity problems.	Appropriate data analysis and troubleshooting techniques per organizational standard are used to diagnose the problem. Problem is correctly identified and causes are isolated per organizational standard. Solutions are thoroughly tested and implemented with minimal risk to network performance per organizational standard. Problems, solutions, and implementation processes are thoroughly documented and clearly communicated per organizational standard.
T-9	Troubleshoot hardware/software interface and interoperability problems.	
	Document	
T-10	Follow SOP and validate/update documentation of compliance.	New configuration, system specifications, installation, and test results are clearly and completely documented. Systems security procedures are properly documented and approved in accordance with company guidelines. Documentation follows company format and standards and is at the appropriate level of detail. Inventory of parts includes accurate identification, tagging, and location. Accurate and up-to-date records (e.g., device configuration and user accounts) are maintained to ensure system integrity.

Monitor, Maintain, Operate		
T-11	Integrate new systems into existing network architecture.	Integration and testing are performed according to project and company schedules, priorities, and guidelines. Preventive maintenance plan and monitoring procedures are updated. Documented performance requirements are used to monitor network and recommend system improvement. System configuration is optimized to meet user needs with minimal disruption. Performance is monitored according to procedures and is compared to baseline performance for discrepancies; reports are generated. Traffic capacity and performance characteristics are monitored, and technician knows how to involve others to handle concerns. Component and connectivity problems are monitored and reported. Functional verifications, system audits, and backups are performed according to proper procedures. Patches are applied to affected software and hardware in a timely manner, and are properly tested. Disruptions, outages, security violations, and attacks of network services are monitored, recognized, and escalated in a timely manner according to company procedures. Diagnostic software is run to verify that the components are operating, and tests are performed. System backups and other maintenance tasks are performed and documented according to scope, schedule, and procedure. System back-ups are verified and periodic test restores are performed. Components are correctly programmed, integrated into the system and backed up, and all security procedures are followed. Tests for functionality and safety of equipment and systems are completed. Communication regarding changes in procedures is distributed to all necessary parties in a timely manner.
T-12	Monitor network capacity and performance.	
T-13	Test and maintain network infrastructure, including software and hardware devices.	
T-14	Conduct functional and connectivity testing to ensure continuing operability.	
T-15	Follow group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	
T-16	Manage basic functionality around accounts, network rights, and access to systems and equipment.	
T-17	Provide ongoing optimization and problem-solving support.	
T-18	Check system hardware availability, functionality, integrity, and efficiency.	
T-19	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	
T-20	Implement local network usage policies and procedures.	
T-21	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	
T-22	Monitor and maintain system/server configuration.	

Infrastructure Connectivity Management and Engineering Student Learning Outcomes		
	Knowledge	**Student Learning Outcomes**
K-8	Knowledge of risk management, cybersecurity, and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Explain information security principles and fundamentals. Describe laws, regulations, and ethical behavior related to cybersecurity and privacy globally.
K-2	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (e.g., PCI, PII, PHI, GDPR).	
K-3	Knowledge of cybersecurity and privacy principles.	
K-4	Knowledge of cyber threats and vulnerabilities.	Explain how to assess network vulnerabilities and attacks. Describe the operational implications to the organization resulting from cybersecurity lapses.
K-5	Knowledge of impacts of cybersecurity lapses.	
K-40	Knowledge of asset management and why it's important to the business.	Describe the network system components and their inter-relationships. Summarize the key role asset management plays in organizational operations. Explain the components of storage infrastructure including subsystems
K-42	Knowledge of infrastructure data storage capabilities and storage clusters.	
K-17	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	Differentiate between different enterprise network architecture and topologies, such as Local Area Networks (LANs), Wide Area Networks (WANs).
K-28	Knowledge of the enterprise information technology (IT) architecture.	
K-12	Knowledge of remote access technology concepts.	Explain the OSI model and different network protocols, such as TCPIP. Describe technology concepts for remote access.
K-26	Knowledge of controls related to the use, processing, storage, and transmission of data.	Explain the controls related to the use, processing, storage, and transmission of data. List resources for gaining more information on wired and wireless transmission standards.
K-23	Knowledge of where to find details on wired and wireless transmission standards (e.g., Ethernet, Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, and satellite communications).	
K-25	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Install and configure TCPIP protocols such as DHCP, DNS, and directory services. Describe the current concepts of telecommunications. Explain the capabilities of different electronic communication systems and methods.
K-6	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	
K-15	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	
K-43	Knowledge of IoT end devices and connectivity.	Describe commonly used IoT end devices and their connectivity.
K-1	Knowledge of computer networking concepts and protocols, and network security methodologies.	Identify and summarize techniques and protocols related to networks, including network security. Explain the principles of Voice over IP (VoIP).
K-18	Knowledge of Voice over IP (VoIP).	
K-7	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Discuss appropriate uses of different network hardware equipment in a business environment. Discuss concepts of bandwidth management in a LAN/WAN networks.
K-10	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	
K-13	Knowledge of server administration and systems engineering theories, concepts, and methods.	Explain the concepts and methods of server administration.
K-16	Knowledge of network tools (e.g., ping, traceroute, nslookup).	Explain how different network commands and tools can be used to monitor and manage network performance.
K-21	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	
K-27	Knowledge of performance tuning tools and techniques.	
K-39	Knowledge of system administration, network, and operating system concepts and hardening techniques.	Explain concepts and hardening techniques for systems administration, network, and operating systems.
K-29	Knowledge of the type and frequency of routine hardware maintenance (e.g., Linux/Unix OS, Windows Server OS).	Summarize a typical organization's recommended schedule and procedures for routine hardware maintenance. Explain different file systems and extensions, including network storage, servers, and file transfer protocols.
K-30	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) including network storage and servers.	

K-31	Knowledge of virtualization technologies and virtual machine development and maintenance.	Outline the concepts of network virtualization, including virtual machine development and maintenance.
K-32	Knowledge of system administration, network, and operating system hardening techniques.	Describe how to administer a network operating system, including hardening techniques.
K-33	Knowledge of system/server diagnostic tools and fault identification techniques.	Explain a typical organization's recommended system/server diagnostic tools and fault identification techniques.
K-34	Knowledge of operating system command-line tools.	Explain commonly used operating system command-line tools.
K-35	Knowledge of principles and methods for integrating system components including network storage and servers.	Describe the principles and methods used to integrate network system components.
K-37	Knowledge of network backup and recovery procedures.	Describe the organization's network backup and restoration process.
K-55	Knowledge of metrics, how they are developed in general, their purpose, and why they are used.	Discuss the latest tools for network traffic metrics and system performance.
K-11	Knowledge of measures or indicators of system performance and availability.	Explain typical measures used to evaluate system performance and availability.
K-19	Knowledge of the common attack vectors on the network layer.	Explain common attack vectors on the network layer.
K-20	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Describe concepts of network security architecture, including Network Security Devices, Protocols, and Topologies.
K-14	Knowledge of Virtual Private Network (VPN) security.	Explain the administration of a Virtual Private Network (VPN).
K-22	Knowledge of concepts of certificates, key management, and usage.	Explain the concepts of Key Management and Certificate Lifecycles.
K-9	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Identify and describe various information technology security principles and methods.
K-38	Knowledge of how to patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Explain Network Vulnerability Assessment and Data Security at physical and cloud locations, including how and when to patch network vulnerabilities.
K-41	Knowledge of risks associated with storing various types of data in different physical locations.	
K-36	Knowledge of script automation and application programming interfaces.	Describe the importance of APIs and use of script automation in network environment.
K-48	Knowledge of the differences or similarities between private, public, and hybrid cloud implementations.	Compare and contrast public, private, and hybrid cloud.
K-49	Knowledge of the difference or similarities between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	Compare and contrast different XaaS tools and technology models.
K-50	Awareness of framework concepts, their selection, and use.	Discuss the selection and use of cloud framework concepts, including the pros and cons of using frameworks.
K-51	Awareness of the pros or cons behind using frameworks.	
K-52	Knowledge of the term benchmarks and the reasons for their use.	Describe benchmarks as performance metrics.
K-53	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure, or organization.	Explain how to design resilience into projects and components of an organization.
K-54	Knowledge of the concept of service level agreement (SLA), why they are used, when they are used, and their application within cloud implementations.	Describe how, why, and when Service Level Agreements (SLA) are implemented in a cloud environment. Define and explain the applicability of high availability service levels.
K-55	Knowledge of who owns or should own the data/information in a cloud implementation.	Explain data ownership in a cloud implementation.
K-56	Knowledge of the key Management/Operational/Security/Privacy challenges potential faced when considering or implementing a Cloud capability.	Describe management, operational, security, and privacy challenges when considering cloud implementation.
K-57	Knowledge of the different organizational roles needed as one plans for Cloud implementation or manages an existing Cloud capability.	Classify organizational roles needed for a planned cloud implementation.
K-58	Knowledge of the incident response challenges potentially faced within a Cloud implementation.	Discuss incident response challenges typically encountered in a cloud implementation.
K-60	Knowledge of cloud network storage including cloud object-based storage and local system storage.	Describe different cloud storage systems including local, network, and object-based.

K-61	Knowledge of the different Cloud computing database types (RDS).	Differentiate and describe the scalability of cloud-based databases such as RDS, SQL, and Non-SQL. Describe how to implement a cloud database solution that can scale and meet the requirements. Document best practices in database fail-over processes.
K-62	Knowledge of how to scale a cloud database.	
K-64	Knowledge of the differences between SQL and Non-SQL databases.	
K-65	Knowledge of Cloud IAM (Identity and Access Management) - cloud and hybrid.	Summarize and explain the life cycle of users with Identity and Access Management in both Cloud and Hybrid environments.
K-66	Knowledge of Cloud IAM users, groups, roles, and policies - cloud and hybrid.	
K-67	Knowledge of Cloud Computing shared security responsibility model - cloud and hybrid.	Describe the cloud computing shared security responsibility model.
K-68	Knowledge of Cloud Regions - cloud and hybrid.	Explain cloud regions and availability zones in cloud infrastructure.
K-69	Knowledge of Cloud Availability Zone - cloud and hybrid.	
K-70	Knowledge of Recovery Time Objective (RTO).	Compare and contrast Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
K-71	Knowledge of Recovery Point Objective (RPO).	
K-72	Knowledge of High Availability factors (fault-tolerance, recoverability, and scalability).	Explain high availability factors in a cloud environment.
K-74	Knowledge of Auto Scaling and Load Balancing.	Describe capabilities of cloud auto-scaling and load balancing.
K-75	Knowledge of the differences between Cloud vs. On-Premise.	Describe the difference between cloud technologies and traditional networks.
K-24	Knowledge of jamming and interference patterns so they can be recognized as a challenge for the network itself applied to wireless networks.	Define the concept of jamming in the context of wireless networks. Explain the various types of interference patterns that can affect wireless networks.
K-44	Knowledge of Software Defined Networking concepts.	Define Software Defined Networking (SDN) and articulate its fundamental concepts.
K-45	Knowledge of Continuous Quality Improvement Principles (of particular value: Lean and Agile).	Describe Continuous Quality Improvement (CQI) and articulate its importance in organizational processes. Explain the key principles of Lean and Agile methodologies and their relevance to CQI.
K-46	Knowledge of how to identify organizational goals that align with architecture and how do you identify your value to the organization.	Identify key elements of organizational architecture and articulate their alignment with broader organizational goals. Define the concept of personal and professional value within an organizational context.
K-47	Knowledge of Python or other scripting languages.	Discuss the role and importance of scripting languages, with a focus on Python.
K-59	Knowledge of Web Services technologies.	Define the concept of web services and their role in modern software development.
K-63	Knowledge of region failover and redundancy vs local failover and redundancy and how that needs to be applied to your data centers (cloud, hybrid, on-prem).	Define the concept of region failover and redundancy in the context of data center architecture. Define the concept of local failover and redundancy in the context of data center architecture. Differentiate between local failover and redundancy and region failover and redundancy.
K-76	Knowledge in preparing and deploying a cloud database solution that meets application requirements.	Define the fundamentals of cloud databases and their role in modern application architecture.
K-77	Knowledge of database management systems, query languages, table relationships, and views.	Explain the purpose, functions, and key components of a Database Management System (DBMS). Define the concept of query languages in the context of databases.
K-78	Knowledge of Azure.	Identify and differentiate the cloud services provided by Azure, AWS, and Google Cloud.
K-79	Knowledge of AWS.	
K-80	Knowledge of Google Cloud.	
K-81	Knowledge of emerging technology (e.g., blockchain, quantum computing).	Define the key concepts and principles of blockchain technology. Identify the fundamental principles of quantum computing.
K-82	Knowledge of making recommendations for migration of a physical network to a cloud-based architecture.	Describe the benefits of migrating from a physical network to a cloud-based architecture.
K-87	Knowledge of assessing and evaluating the technical benefits of implementation of a cloud computing architecture.	

K-83	Knowledge of creating a cloud-based network infrastructure to meet requirements for a software application.	Summarize the fundamental concepts of cloud-based network infrastructure in terms of meeting the needs of a given application.
K-84	Knowledge of the OSI model and understand that OSI is the framework for all problem solving and troubleshooting. Provide basic framework for how it all works, including how cloud computing has impacted the conceptualization of the seven layers. Plus an awareness of IP multimedia services.	Explain the OSI (Open Systems Interconnection) model and identify its different layers. Differentiate the purpose of each OSI layer and the interactions between layers during data communication as well as how it applies to cloud computing.
K-85	Knowledge of preparing and deploying a Cloud High Availability and Business Continuity Solution.	Describe the concepts of High Availability (HA) and Business Continuity (BC) in the context of cloud computing architecture.
K-86	Knowledge of implementing auto scaling and load balancing.	Explain auto-scaling and load balancing concepts.
	Skills	**Student Learning Outcomes**
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers and switches.	Install network components and perform configuration. Effectively test network security configuration backup and recovery plans.
S-9	Skill in testing network infrastructure contingency and recovery plans.	
S-2	Skill in establishing a routing schema.	Establish a routing schema and apply subnetting TCP/IP consents to that schema.
S-10	Skill in applying various subnet techniques (e.g., CIDR).	
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	Demonstrate skills in installing and configuring network hardware, software, and cable, including firewalls and other devices. Demonstrate skill in diagnosing network connectivity problems.
S-12	Skill in configuring and basic optimizing software.	
S-13	Skill in diagnosing connectivity problems.	
S-14	Skill in maintaining directory services (e.g., Microsoft Active Directory, LDAP, etc.).	Operate and articulate file system and directory services operations. Design and develop different types of virtual machines. Design and develop apps using containerized software tools.
S-15	Skill in using virtual machines (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	Apply basic software security measures to protect network devices. Perform troubleshooting services including software upgrade/downgrade and installation of appropriate network devices. Perform system/server management and maintenance.
S-20	Skill in conducting system/server management and maintenance.	
S-22	Skill in troubleshooting failed system components (i.e., servers).	
S-24	Skill in installing system and component upgrades (i.e., servers, appliances, network devices).	
S-25	Skill in monitoring and optimizing basic system/server/cloud performance.	Create and maintain an effective network performance baseline by monitoring and troubleshooting network performance.
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	
S-21	Skill in correcting physical and technical problems that impact system/server performance.	
S-26	Skill in recovering failed systems/servers (e.g., recovery software, failover clusters, replication, etc.).	Perform the recovery process for a failed system or server. Create, administer, and maintain user accounts and groups in a network environment.
S-27	Skill in operating system administration (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	
S-1	Understand that OSI is the framework for all problem solving and troubleshooting.	Utilize the latest tools to analyze network traffic and identify patterns to improve performance using the OSI model as a reference.
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	
S-6	Skill in securing network communications (e.g., logical).	Take appropriate actions to mitigate vulnerability and risk from potential network attacks.
S-7	Skill in protecting a network against malware (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	
S-8	Skill in basic configuring and utilizing network protection components (e.g., firewalls, VPNs, network intrusion detection systems).	
S-3	Skill in implementing, maintaining established network security practices.	Apply established practices to secure a network.
S-19	Skill in interfacing with customers.	Demonstrate effective interactions with customers.

S-29	Skill in identifying and distinguishing private, public, and hybrid cloud implementations.	Evaluate public, private, and hybrid cloud technologies. Assess and apply different XaaS tools and technologies models. Operate and manage cloud technologies. Perform different functional and non-functional cloud tests to ensure business requirements. Summarize and document cloud testing results against developed criteria.
S-30	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	
S-16	Skill in using cloud (e.g., Amazon Elastic Compute Cloud).	
S-31	Skill in executing test cases for identified functional or non-functional requirements.	
S-32	Skill in documenting results of executed test cases showing whether according to developed success criteria the test case passes, fails, or partially passes.	
S-33	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	
S-36	Skill in producing virtual machines from a cloud image.	Demonstrate setting up virtual machine(s) using cloud technologies.
S-37	Skill in producing virtual machines within a cloud region.	
S-38	Skill in demonstrating how to customize virtual networks with IP address range, subnets, routing tables and gateways.	Devise customized virtual machine(s) based on different network topologies. Detect troubleshoot issues with virtual machine(s).
S-39	Skill in analyzing and troubleshooting cloud virtual networks.	
S-40	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	
S-43	Skill in applying permissions from the IAM (Identity and Access Management).	Apply permissions for IAM (Identify and Access Management) for groups and users.
S-44	Skill in applying permissions for IAM (Identity and Access Management) group(s).	
S-45	Skill in applying permissions for IAM (Identity and Access Management) user(s).	
S-46	Skill in analyzing and troubleshooting containers.	Analyze and troubleshoot containers.
S-41	Skill in deploying cloud storage technologies with the assistance of a senior technician.	Deploy different cloud storage systems with assistance from a senior technician. Analyze and troubleshoot different cloud storage systems.
S-42	Skill in analyzing and troubleshooting different cloud storage technologies.	
S-47	Skill in using management tools like Chef, Puppet, etc.	Utilize management tools for improving infrastructure automation.
S-34	Skill in preparing written reports.	Deliver information in an appropriate manner to each type of audience.
S-35	Skill in preparing presentations.	
S-28	Skill in applying Software Defined Networking concepts.	Deploy SDN components such as OpenFlow protocols to enable communication between the control and data planes.
S-48	Skill in managing changes/updates for both internal and external customers when policies and procedures change.	Apply established change management processes to assess the impact of policy and procedure changes.
S-49	Skill in assessing or monitoring system for cyberattacks.	Apply knowledge of cybersecurity tools and technologies used for system assessment and monitoring (e.g., intrusion detection systems, antivirus software, firewalls). Configure and use security information and event management (SIEM) tools for log analysis and correlation.
S-50	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	Detect system performance degradation using data to pinpoint potential bottlenecks. Use performance trends and anomalies to determine the root causes of degradation.
S-51	Skill in identifying areas where there are issues/gaps in a cloud implementation and develop a working solution.	Apply knowledge of cloud service models (IaaS, PaaS, SaaS) to identify issues specific to each model. Evaluate cloud architectures to identify potential gaps in scalability, redundancy, and fault tolerance.
S-52	Skill in leveraging cloud/hybrid managed services to enable greater flexibility and resilience in an secure infrastructure.	Implement cloud/management services that enhance the flexibility of the infrastructure, allowing for rapid adaptation to business needs. Apply knowledge of managed security services to enhance the overall security posture of a hybrid cloud infrastructure.
S-53	Skill in identifying appropriate cloud services that provide the compute power needed to solve a technical business problem while optimizing cost.	Compare cost structures of different compute services and models in the cloud that are needed to solve technical business problems.

S-54	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Write simple scripts in Perl and VBScript on Windows and UNIX systems to perform specified tasks based on specific requirements.
S-55	Skill in importing/ exporting/migrating/protecting/securing data from one data source to another.	Apply techniques for importing data into various data sources. Choose methods for exporting data from different sources. Apply strategies for migrating data between different systems or platforms. Formulate security measures to protect sensitive data during transfer.
S-56	Skill in applying security concepts in the automation of resource provisioning.	Investigate security best practices when designing and implementing automated resource provisioning workflows.
S-57	Skill in identifying the necessary components of a physical network and a cloud-based network.	Identify and label physical network components within a given infrastructure. Demonstrate the ability to trace physical connections and understand their roles in data transmission. Identify and configure virtualized components in a cloud-based network, including virtual machines, virtual networks, and subnets. Implement and manage load balancers, firewalls, and other cloud-specific components.
S-58	Skill in using Azure.	Create and manage virtual machines, storage, and networking components in a cloud environment for Azure, AWS, and GCP.
S-59	Skill in using AWS.	
S-60	Skill in Google Cloud.	
	Abilities	**Student Learning Outcomes**
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	Apply techniques and protocols to data communication network systems.
A-1	Ability to install network equipment including routers, switches, servers, transmission media, and related hardware.	Integrate LAN/WAN network connectivity by installing network hardware, software, and cabling. Operate the organization's LAN/WAN pathways.
A-4	Ability to operate the organization's LAN/WAN pathways.	
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	Ensure network architecture aligns with organization's goals and objectives. Demonstrate the use of OS command line tools.
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	
A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	Assess and troubleshoot issues submitted to the organization's ticketing system.
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	Measure network system traffic by using network tools to monitor network performance.
A-5	Ability to monitor measures or indicators of system performance and availability.	
A-7	Ability to monitor traffic flows across the network.	
A-8	Ability to recognize and escalate the information collected by network tools (e.g., nslookup, ping, and traceroute).	Analyze the data collected from network tools to identify problems and escalate when needed.
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Execute organization's cybersecurity, privacy, and security controls for the network environment.
A-15	Ability to maintain automated security control assessments.	
A-11	Ability to update and/or maintain standard operating procedures (SOPs).	Update the organization's standard operating procedures (SOPs) as needed.
A-12	Ability to collaborate effectively with others.	Demonstrate effective collaboration skills to work with a team to achieve project goals.
A-16	Ability to communicate effectively (written and oral) within and among team members and associated stakeholders (i.e., different audiences and organizational levels). This includes communicating complex technical issues and business implications.	Demonstrate effective communication skills (both oral and written) when working with team members and stakeholders. Effectively communicate technical jargon in simple terms to team members and stakeholders. Demonstrate effective listening skills. Analyze and interpret input to determine implicit and explicit customer requirements.
A-20	Ability to translate technical language into lay terminology when needed.	
A-22	Ability to listen and understand what people say.	
A-19	Ability to analyze and interpret customer input for expressed and implied requirements.	

A-13	Ability to function effectively in a dynamic, fast-paced environment.	Demonstrate the ability to successfully perform job functions in a fast-paced and dynamic work environment. Demonstrate the ability to successfully perform job functions in stressful situations.
A-17	Ability to work under stress.	
A-18	Ability to problem solve.	Demonstrate the ability to understand details, prioritize items, and use available information to solve problems.
A-23	Ability to recognize and understand details.	
A-24	Ability to order and arrange items.	
A-21	Ability to read and interpret technical documents, diagrams, and decision trees.	Analyze and interpret technical documents and diagrams. Develop presentation visuals to deliver technical information to an appropriate audience.
A-25	Ability to create appropriate presentation visuals for technical material.	

Infrastructure Degree Expectations

A pool of 20 community college and four-year university faculty members from across the country were asked to categorize each knowledge, skill, ability, and task below. The question posed to them: would these KSA+Ts be reasonably included in a two-year AAS program, a four-year Bachelor's program, both, or neither? These results provide another tool for educators to use in assessing how to best incorporate each knowledge, skill, ability, and task.

		% Best Estimate			
	Tasks	2 Year AAS	Both 2 yr AAS and 4 yr Academic Degree	4 Year Academic Degree	Number of responses
T-1	Configure network, routers, and switches.	35%	50%	15%	20
T-2	Diagnose network connectivity problem.	35%	65%	0%	20
T-3	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patch network vulnerabilities to safeguard information.	35%	55%	10%	20
T-4	Install or replace network, routers, and switches.	50%	45%	5%	20
T-5	Integrate new systems into existing network architecture.	20%	40%	40%	20
T-6	Monitor basic network capacity and performance.	35%	55%	10%	20
T-7	Test and maintain network infrastructure including software, hardware devices, software-defined networks, and network applications.	26%	58%	16%	19
T-8	Conduct functional and connectivity testing to ensure continuing operability.	37%	63%	0%	20
T-9	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	20%	65%	15%	20
T-10	Support group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	20%	45%	35%	20
T-11	Follow SOP and validate/update documentation of compliance.	15%	45%	40%	20
T-12	Validate/update baseline system security according to organizational policies.	20%	55%	25%	20
T-13	Manage accounts, network rights, and access to systems and equipment.	40%	55%	5%	20
T-14	Provide ongoing optimization and problem-solving support.	15%	65%	20%	20
T-15	Install, update, and troubleshoot systems/servers.	30%	70%	0%	20
T-16	Check system hardware availability, functionality, integrity, and efficiency.	25%	50%	20%	20
T-17	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	50%	45%	5%	20
T-18	Implement local network usage policies and procedures.	30%	50%	20%	20
T-19	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	35%	40%	25%	20
T-20	Monitor and maintain system/server configuration.	45%	55%	0%	20
T-21	Installation, implementation, configuration, and support of system components.	30%	65%	5%	20
T-22	Troubleshoot hardware/software interface and interoperability problems.	30%	60%	10%	20
	Knowledge				
K-1	Knowledge of computer networking concepts and protocols, and network security methodologies.	35%	55%	10%	20
K-2	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (e.g. PCI, PII, PHI, GDPR). Note connection to K-8 below.	20%	45%	35%	20
K-3	Knowledge of cybersecurity and privacy principles.	30%	70%	0%	20
K-4	Knowledge of cyber threats and vulnerabilities.	25%	70%	5%	20
K-5	Knowledge of specific operational impacts of cybersecurity lapses.	20%	75%	5%	20

K-6	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	25%	60%	15%	20
K-7	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	35%	60%	5%	20
K-8	Knowledge of risk management, cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	15%	65%	20%	20
K-9	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	25%	75%	0%	20
K-10	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	35%	65%	0%	20
K-11	Knowledge of measures or indicators of system performance and availability.	26%	58%	16%	19
K-12	Knowledge of remote access technology concepts.	35%	65%	0%	20
K-13	Knowledge of server administration and systems engineering theories, concepts, and methods.	25%	65%	10%	20
K-14	Knowledge of Virtual Private Network (VPN) security.	30%	65%	5%	20
K-15	Knowledge of concepts, terminology, and operations of a wide range of baseband and broadband communications transmission media and protocols (computer and telecommunications networks, satellite, fiber, wireless).	25%	70%	5%	20
K-16	Knowledge of network tools (e.g., ping, traceroute, nslookup).	45%	55%	0%	20
K-17	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	25%	65%	10%	20
K-18	Knowledge of Voice over IP (VoIP).	33%	50%	17%	18
K-19	Knowledge of the common attack vectors on the network layer.	35%	55%	10%	20
K-20	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	26%	68%	5%	20
K-21	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	15%	60%	25%	20
K-22	Knowledge of concepts of certificates, key management and usage.	30%	65%	5%	20
K-23	Knowledge of wired and wireless transmission standards (e.g. Ethernet, Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, and satellite communications.)	26%	68%	5%	20
K-24	Knowledge of jamming and interference patterns so they can be recognized as a challenge for the network itself, especially as this applies to wireless networks.	16%	58%	26%	19
K-25	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	35%	65%	0%	20
K-26	Knowledge of controls related to the use, processing, storage, and transmission of data.	25%	65%	10%	20
K-27	Knowledge of performance tuning tools and techniques.	20%	60%	20%	20
K-28	Knowledge of the enterprise information technology (IT) architecture.	22%	50%	28%	18
K-29	Knowledge of the type and frequency of routine hardware maintenance (e.g. Linux/Unix OS, Windows Server OS).	37%	63%	0%	19
K-30	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) including network storage and servers.	35%	60%	5%	20
K-31	Knowledge of virtualization technologies and virtual machine development and maintenance.	25%	70%	5%	20
K-32	Knowledge of system administration, network, and operating system hardening techniques.	30%	65%	5%	20
K-33	Knowledge of system/server diagnostic tools and fault identification techniques.	21%	58%	21%	19

K-34	Knowledge of operating system command-line tools.	30%	70%	0%	20
K-35	Knowledge of principles and methods for integrating system components including network storage and servers.	26%	58%	16%	19
K-36	Knowledge of script automation and application programming interfaces.	20%	50%	30%	20
K-37	Knowledge of network backup and recovery procedures.	30%	70%	0%	20
K-38	Knowledge of patch network vulnerabilities to ensure that information is safeguarded against outside parties.	30%	70%	0%	20
K-39	Knowledge of system administration, network, and operating system concepts and hardening techniques.	35%	60%	5%	20
K-40	Knowledge of asset management and why it's important to the business.	15%	50%	35%	20
K-41	Knowledge of risks associated with storing various types of data in different physical locations.	26%	68%	5%	19
K-42	Knowledge of infrastructure data storage capabilities and storage clusters.	25%	55%	20%	20
K-43	Knowledge of IoT end devices and connectivity.	30%	65%	5%	20
K-44	Knowledge of Software Defined Networking concepts.	15%	50%	35%	20
K-45	Knowledge of database theory as it relates both to network latency and replication and also to the three states of data (in the data center, in the cloud, and in a co-location).	16%	53%	32%	19
K-46	Knowledge of Continuous Quality Improvement Principles (of particular value: Lean and Agile).	10%	30%	60%	20
K-47	Knowledge of how to identify organizations goals that align with system architecture (i.e. know your business)	10%	40%	50%	20
K-48	Knowledge of Python or other scripting languages.	30%	65%	5%	20
K-49	Knowledge of the differences or similarities between Private, Public, and Hybrid Cloud Implementations.	32%	58%	11%	20
K-50	Knowledge of the difference or similarities between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	30%	65%	5%	20
K-51	Awareness of framework concepts, their selection and use.	11%	72%	17%	18
K-52	Awareness of the pros or cons behind using Frameworks.	17%	50%	33%	18
K-53	Knowledge of the term benchmarks and the reasons for their use.	25%	70%	5%	20
K-54	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure or organization.	20%	65%	15%	20
K-55	Knowledge of the concept of Service Level Agreement, why they are used, when they are used, and its application within Cloud implementations.	15%	75%	10%	20
K-56	Knowledge of who owns or should own the data/information in a Cloud implementation.	15%	70%	15%	20
K-57	Knowledge of the key Management/Operational/Security/Privacy challenges potential faced when considering or implementing a Cloud capability.	15%	65%	20%	20
K-58	Knowledge of the different organizational roles needed as one plans for Cloud implementation or manages an existing Cloud capability.	10%	55%	35%	20
K-59	Knowledge of the incident response challenges potentially faced within a Cloud implementation.	15%	60%	25%	20
K-60	Knowledge of Web Services technologies.	30%	55%	15%	20
K-61	Knowledge of cloud network storage including cloud object -based storage and local system storage.	25%	60%	15%	20
K-62	Knowledge of the different Cloud computing database types (RDS).	15%	50%	35%	20
K-63	Knowledge of how to scale a Cloud database.	15%	40%	45%	20
K-64	Knowledge of region failover and redundancy vs local failover and redundancy and how that needs to be applied to your data centers (cloud, hybrid, on-prem).	10%	75%	15%	20
K-65	Knowledge of the differences between SQL and Non-SQL Databases.	25%	45%	30%	20
K-66	Knowledge of Cloud IAM (Identity and Access Management) - cloud and hybrid.	16%	58%	26%	20

K-67	Knowledge of Cloud IAM users, groups, roles and policies - cloud and hybrid.	21%	53%	26%	20
K-68	Knowledge of Cloud Computing shared security responsibility model - cloud and hybrid.	16%	53%	32%	19
K-69	Knowledge of Cloud Regions - cloud and hybrid.	16%	58%	26%	19
K-70	Knowledge of Cloud Availability Zone - cloud and hybrid.	16%	53%	32%	19
K-71	Knowledge of Recovery Time Objective (RTO).	10%	80%	10%	20
K-72	Knowledge of Recovery Point Objective (RPO).	11%	79%	11%	19
K-73	Knowledge of High Availability factors (Fault-tolerance, recoverability, and scalability).	21%	74%	5%	19
K-74	Knowledge of microservices and containerization (e.g. Kubernetes and Docker).	11%	47%	42%	19
K-75	Knowledge of Auto Scaling and Load Balancing.	20%	55%	25%	20
K-76	Knowledge of the differences between Cloud vs. On-Premises.	40%	60%	0%	20
K-77	Knowledge in preparing and deploying a cloud database solution that meets application requirements.	10%	50%	40%	20
K-78	Knowledge of database impacts to network systems.	20%	60%	20%	20
K-79	Knowledge of Azure.	35%	60%	5%	20
K-80	Knowledge of AWS.	35%	60%	5%	20
K-81	Knowledge of Google Cloud.	35%	60%	5%	20
K-82	Knowledge of emerging technology (e.g. blockchain, quantum computing)	10%	65%	25%	20
K-83	Knowledge of building scalable distributed systems supporting parallel processing of customer jobs on a large fleet of devices.	11%	37%	53%	19
K-84	Knowledge of making recommendations for migration of a physical network to a cloud-based architecture.	15%	40%	45%	20
K-85	Knowledge of creating a cloud-based network infrastructure to meet requirements for a software application.	10%	35%	55%	20
K-86	Knowledge of assessing and evaluating the technical benefits of implementation of a cloud computing architecture.	10%	50%	40%	20
K-87	Knowledge of the OSI model and understand that OSI is the framework for all problem solving and troubleshooting. Provide basic framework for how it all works, including how cloud computing has impacted the conceptualization of the seven layers. Plus an awareness of IP multimedia services.	35%	60%	5%	20
K-88	Knowledge of preparing and deploying a Cloud High Availability and Business Continuity Solution.	16%	47%	37%	19
K-89	Knowledge of implementing auto scaling and load balancing.	16%	68%	16%	20
K-90	Knowledge of DevSecOps concepts.	11%	42%	47%	19
K-91	Knowledge of the trend of technology's increasing "interconnectivity" and the end of rigid workplace silos.	10%	55%	35%	20
K-92	Knowledge of online professional resource forums (e.g. GitHub, Reddit, Signal) and an understanding of both the benefits and risks associated with using them.	16%	79%	5%	19
K-93	Knowledge of basic AI and machine learning concepts/tools (e.g. ChatGPT).	20%	65%	15%	20
Skills					
S-1	Understand that OSI is the framework for all problem solving and troubleshooting	44%	56%	0%	18
S-2	Skill in establishing a routing schema.	35%	45%	20%	20
S-3	Skill in implementing, maintaining established network security practices.	45%	50%	5%	20
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, and switches.	40%	60%	0%	20
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	40%	55%	5%	20
S-6	Skill in securing network communications. (e.g., logical)	32%	58%	11%	19

S-7	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	37%	53%	11%	19
S-8	Skill in basic configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	40%	50%	10%	20
S-9	Skill in testing network infrastructure contingency and recovery plans.	30%	35%	35%	20
S-10	Skill in applying various subnet techniques (e.g., CIDR).	35%	65%	0%	20
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	35%	60%	5%	20
S-12	Skill in configuring and basic optimizing software.	47%	42%	11%	19
S-13	Skill in diagnosing connectivity problems.	45%	55%	0%	20
S-14	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).	42%	58%	0%	19
S-15	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	35%	50%	15%	20
S-16	Skill in using Cloud (e.g. Amazon Elastic Compute Cloud).	30%	55%	15%	20
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	16%	47%	37%	20
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	35%	60%	5%	20
S-19	Skill in interfacing with customers.	11%	89%	0%	19
S-20	Skill in conducting system/server management and maintenance.	35%	55%	10%	20
S-21	Skill in correcting physical and technical problems that impact system/server performance.	20%	55%	20%	20
S-22	Skill in troubleshooting failed system components (i.e., servers).	37%	58%	5%	19
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	37%	53%	11%	19
S-24	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).	45%	50%	5%	20
S-25	Skill in monitoring and optimizing basic system/server/cloud performance.	37%	47%	16%	19
S-26	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).	35%	35%	30%	20
S-27	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	40%	45%	15%	20
S-28	Skill in applying Software Defined Networking concepts.	21%	47%	32%	19
S-29	Skill in identifying and distinguishing Private, Public, and Hybrid Cloud Implementations.	20%	65%	15%	20
S-30	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	20%	65%	15%	20
S-31	Skill in executing Test Cases for identified functional or non-functional requirements.	10%	45%	45%	20
S-32	Skill in documenting results of executed test cases showing whether according to developed success criteria the test case passes, fails, or partially passes.	16%	47%	37%	19
S-33	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	11%	58%	32%	19
S-34	Skill in preparing written reports.	10%	80%	10%	20
S-35	Skill in preparing presentations.	15%	75%	10%	20
S-36	Skill in producing Virtual Machines from a Cloud image.	29%	53%	18%	17
S-37	Skill in producing Virtual Machines within a Cloud region.	22%	44%	33%	18
S-38	Skill in demonstrating how to customize virtual networks with IP Address Range, subnets, routing tables and gateways.	25%	60%	15%	20
S-39	Skill in analyzing and troubleshooting Cloud Virtual Networks.	15%	40%	45%	20

S-40	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	25%	50%	25%	20
S-41	Skill in deploying cloud storage technologies with the assistance of a senior technician.	35%	50%	15%	20
S-42	Skill in analyzing and troubleshooting different cloud storage technologies.	32%	37%	32%	19
S-43	Skill in applying permissions from the IAM (Identity and Access Management).	30%	45%	25%	20
S-44	Skill in applying permissions for IAM (Identity and Access Management) Group(s).	32%	42%	26%	19
S-45	Skill in applying permissions for IAM (Identity and Access Management) user(s).	30%	45%	25%	20
S-46	Skill in analyzing and troubleshooting containers.	25%	35%	40%	20
S-47	Skill in using tools like Chef, Puppet, Ansible, etc.	5%	37%	58%	19
S-48	Skill in managing changes/updates for both internal and external customers when policies and procedures change.	16%	47%	37%	19
S-49	Skill in assessing or monitoring system for cyberattacks.	21%	68%	11%	19
S-50	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	11%	47%	42%	19
S-51	Skill in leveraging cloud/hybrid managed services to enable greater flexibility and resilience in an secure infrastructure.	11%	32%	58%	19
S-52	Skill in identifying appropriate cloud services that provide the compute power needed to solve a technical business problem while optimizing cost.	11%	33%	56%	18
S-53	Skill in building, and operating key pieces of serverless and cloud native applications using appropriate cloud services.	11%	42%	47%	19
S-54	Skill in using a continuous integration (CI) / continuous delivery (CD) pipeline to deploy applications.	6%	39%	56%	18
S-55	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	15%	55%	30%	20
S-56	Skill in importing, exporting, migrating, protecting, and securing data from one data source to another.	20%	55%	25%	20
S-57	Skill in applying security concepts in the automation of resource provisioning.	15%	25%	60%	20
S-58	Skill in identifying the necessary components of a physical network and a cloud-based network.	25%	60%	15%	20
S-59	Skill in using Azure.	26%	58%	16%	19
S-60	Skill in using AWS.	30%	55%	15%	20
S-61	Skill in Google Cloud.	33%	44%	22%	18
S-62	Skill in using IBM Cloud.	17%	42%	42%	12
S-63	Skill in using Oracle Cloud.	23%	39%	39%	13
S-64	Skill in using Cisco Cloud.	33%	33%	33%	15
S-65	Skill in using VirtualBox.	37%	58%	5%	19
Abilities					
A-1	Ability to install network equipment including routers, switches, servers, transmission media, and related hardware.	45%	50%	5%	20
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	40%	60%	0%	20
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	45%	55%	0%	20
A-4	Ability to operate the organization's LAN/WAN pathways.	37%	53%	11%	19
A-5	Ability to monitor measures or indicators of system performance and availability.	30%	55%	15%	20

A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	26%	47%	26%	19
A-7	Ability to monitor traffic flows across the network.	32%	53%	16%	19
A-8	Ability to recognize and escalate the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	40%	60%	0%	20
A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	32%	58%	11%	19
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	21%	32%	47%	19
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).	30%	35%	35%	20
A-12	Ability to collaborate effectively with others.	20%	80%	0%	20
A-13	Ability to function effectively in a dynamic, fast-paced environment.	16%	79%	5%	19
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	15%	75%	10%	20
A-15	Ability to maintain automated security control assessments.	25%	50%	25%	20
A-16	Ability to communicate effectively (written and oral) within and among team members and associated stakeholders (i.e. different audiences and organizational levels). This includes communicating complex technical issues and business implications.	15%	70%	15%	20
A-17	Ability to work under stress.	16%	74%	11%	19
A-18	Ability to problem solve.	15%	85%	0%	20
A-19	Ability to analyze and interpret customer input for expressed and implied requirements.	10%	75%	15%	20
A-20	Ability to translate technical language into lay terminology when needed.	10%	85%	5%	20
A-21	Ability to read and interpret technical documents, diagrams, and decision trees.	10%	85%	5%	20
A-22	Ability to listen and understand what people say.	15%	85%	0%	20
A-23	Ability to recognize and understand details.	15%	85%	0%	20
A-24	Ability to order and arrange items.	15%	85%	0%	20
A-25	Ability to create appropriate presentation visuals for technical material.	15%	75%	10%	20