	Infrastructure KSAs - updated Summer 2023	# votes (4 = most important)				green cells ≥ 2.60
		4	3	2	1	Avg
	Tasks SPECIFIC THINGS an entry level person would BE EXPECTED TO PERFORM on the job WITH LITTLE SUPERVISION.					
T-1	Configure network, routers, and switches	9	3	1	0	3.62
T-2	Diagnose network connectivity problem.	10	2	1	0	3.69
T-3	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patch network vulnerabilities to safeguard information.	6	6	1	0	3.38
T-4	Install or replace network, routers, and switches.	9	2	2	0	3.54
T-5	Integrate new systems into existing network architecture.	5	7	1	0	3.31
T-6	Monitor basic network capacity and performance.	8	5	0	0	3.62
T-7	Test and maintain network infrastructure including software, hardware devices, software-defined networks, and network applications.	5	8	0	0	3.38
T-8	Conduct functional and connectivity testing to ensure continuing operability.	6	7	0	0	3.46
T-9	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	4	7	2	0	3.15
T-10	Support group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	6	5	2	0	3.31
T-11	Follow SOP and validate/update documentation of compliance.	9	2	2	0	3.54
T-12	Validate/update baseline system security according to organizational policies.	7	2	3	1	3.15
T-13	Manage accounts, network rights, and access to systems and equipment.	6	6	1	0	3.38
T-14	Provide ongoing optimization and problem-solving support.	5	7	1	0	3.31
T-15	Install, update, and troubleshoot systems/servers.	7	5	1	0	3.46
T-16	Check system hardware availability, functionality, integrity, and efficiency.	8	3	2	0	3.46
T-17	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	5	6	2	0	3.23
T-18	Implement local network usage policies and procedures.	5	7	1	0	3.31
T-19	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	4	9	0	0	3.31
T-20	Monitor and maintain system/server configuration.	8	5	0	0	3.62
T-21	Installation, implementation, configuration, and support of system components.	5	7	0	0	3.42
T-22	Troubleshoot hardware/software interface and interoperability problems.	8	5	0	0	3.62
	Knowledge Knowledge focuses on the understanding of concepts. It is theoretical and not practical. 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.	12	1	0	0	3.92
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.	4	7	2	0	3.15
K-3	Knowledge of cybersecurity and privacy principles.	5	7	1	0	3.31
K-4	Knowledge of cyber threats and vulnerabilities.	5	7	1	0	3.31
K-5	Knowledge of specific operational impacts of cybersecurity lapses.	8	4	1	0	3.54
K-6	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	7	6	0	0	3.54
K-7	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	9	4	0	0	3.69
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.	4	8	1	0	3.23
K-9	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	9	4	0	0	3.69
K-10	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	9	2	2	0	3.54

K-11	Knowledge of measures or indicators of system performance and availability.	10	3	0	0	3.77
K-12	Knowledge of remote access technology concepts.	8	4	1	0	3.54
K-13	Knowledge of server administration and systems engineering theories, concepts, and methods.	3	9	1	0	3.15
K-14	Knowledge of Virtual Private Network (VPN) security.	8	4	1	0	3.54
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).	7	5	1	0	3.46
K-16	Knowledge of network tools (e.g., ping, traceroute, nslookup).	11	2	0	0	3.85
K-17	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	10	3	0	0	3.77
K-18	Knowledge of Voice over IP (VoIP).	2	8	2	1	2.85
K-19	Knowledge of the common attack vectors on the network layer.	5	8	0	0	3.38
K-20	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	7	4	2	0	3.38
K-21	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	7	5	1	0	3.46
K-22	Knowledge of concepts of certificates, key management and usage.	5	7	1	0	3.31
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.)	4	7	1	1	3.08
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.	1	6	6	0	2.62
K-25	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	11	2	0	0	3.85
K-26	Knowledge of controls related to the use, processing, storage, and transmission of data.	4	8	1	0	3.23
K-27	Knowledge of performance tuning tools and techniques.	2	9	2	0	3.00
K-28	Knowledge of the enterprise information technology (IT) architecture.	4	9	0	0	3.31
K-29	Knowledge of the type and frequency of routine hardware maintenance (e.g. Linux/Unix OS, Windows Server OS).	6	5	2	0	3.31
K-30	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT], Zettabyte File System [ZFS]) including network storage and servers.	4	6	2	1	3.00
K-31	Knowledge of virtualization technologies and virtual machine development and maintenance.	7	6	0	0	3.54
K-32	Knowledge of system administration, network, and operating system hardening techniques.	6	5	2	0	3.31
K-33	Knowledge of system/server diagnostic tools and fault identification techniques.	4	7	1	1	3.08
K-34	Knowledge of operating system command-line tools.	7	6	0	0	3.54
K-35	Knowledge of principles and methods for integrating system components including network storage and servers.	4	7	2	0	3.15
K-36	Knowledge of script automation and application programming interfaces.	4	8	1	0	3.23
K-37	Knowledge of network backup and recovery procedures.	7	5	1	0	3.46
K-38	Knowledge of patch network vulnerabilities to ensure that information is safeguarded against outside parties.	7	5	1	0	3.46
K-39	Knowledge of system administration, network, and operating system concepts and hardening techniques.	8	4	1	0	3.54
K-40	Knowledge of asset management and why it's important to the business.	6	3	4	0	3.15
K-41	Knowledge of risks associated with storing various types of data in different physical locations.	3	7	3	0	3.00
K-42	Knowledge of infrastructure data storage capabilities and storage clusters.	4	6	3	0	3.08
K-43	Knowledge of IoT end devices and connectivity.	4	8	1	0	3.23
K-44	Knowledge of Software Defined Networking concepts.	7	6	0	0	3.54
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).	1	8	3	1	2.69
K-46	Knowledge of Continuous Quality Improvement Principles (of particular value: Lean and Agile).	4	6	3	0	3.08
K-47	Knowledge of how to identify organizations goals that align with system architecture (i.e. know your business)	3	4	6	0	2.77
K-48	Knowledge of Python or other scripting languages.	3	6	4	0	2.92

K-49	Knowledge of the differences or similarities between Private, Public, and Hybrid Cloud Implementations.	6	6	1	0	3.38
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.	7	6	0	0	3.54
K-51	Awareness of framework concepts, their selection and use.	2	6	5	0	2.77
K-52	Awareness of the pros or cons behind using Frameworks.	2	5	6	0	2.69
K-53	Knowledge of the term benchmarks and the reasons for their use.	4	6	2	1	3.00
K-54	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure or organization.	2	8	3	0	2.92
K-55	Knowledge of the concept of Service Level Agreement, why they are used, when they are used, and its application within Cloud implementations.	5	8	0	0	3.38
K-56	Knowledge of who owns or should own the data/information in a Cloud implementation.	3	8	2	0	3.08
K-57	Knowledge of the key Management/Operational/Security/Privacy challenges potential faced when considering or implementing a Cloud capability.	3	7	2	0	3.08
K-58	Knowledge of the different organizational roles needed as one plans for Cloud implementation or manages an existing Cloud capability.	2	9	2	0	3.00
K-59	Knowledge of the incident response challenges potentially faced within a Cloud implementation.	4	6	3	0	3.08
K-60	Knowledge of Web Services technologies.	2	6	4	1	2.69
K-61	Knowledge of cloud network storage including cloud object -based storage and local system storage.	3	5	5	0	2.85
K-62	Knowledge of the different Cloud computing database types (RDS).	1	7	4	1	2.62
K-63	Knowledge of how to scale a database.	0	2	2	1	2.20
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).	1	12	0	0	3.08
K-65	Knowledge of the differences between SQL and Non-SQL Databases.	1	6	3	3	2.38
K-66	Knowledge of Cloud IAM (Identity and Access Management) - cloud and hybrid.	4	8	0	1	3.15
K-67	Knowledge of Cloud IAM users, groups, roles and policies - cloud and hybrid.	4	7	1	1	3.08
K-68	Knowledge of Cloud Computing shared security responsibility model - cloud and hybrid.	5	7	1	0	3.31
K-69	Knowledge of Cloud Regions - cloud and hybrid.	4	6	2	0	3.17
K-70	Knowledge of Cloud Availability Zone - cloud and hybrid.	3	7	2	0	3.08
K-71	Knowledge of Recovery Time Objective (RTO).	3	8	2	0	3.08
K-72	Knowledge of Recovery Point Objective (RPO).	3	7	3	0	3.00
K-73	Knowledge of High Availability factors (Fault-tolerance, recoverability, and scalability).	6	7	0	0	3.46
K-74	Knowledge of microservices and containerization (e.g. Kubernetes and Docker).	3	7	2	0	3.08
K-75	Knowledge of Auto Scaling and Load Balancing.	4	6	3	0	3.08
K-76	Knowledge of the differences between Cloud vs. On-Premises.	9	4	0	0	3.69
K-77	Knowledge in preparing and deploying a cloud database solution that meets application requirements.	0	5	6	1	2.33
K-78	Knowledge of database impacts to network systems.	0	4	1	0	2.80
K-79	Knowledge of Azure.	3	8	1	1	3.00
K-80	Knowledge of AWS.	5	6	1	1	3.15
K-81	Knowledge of Google Cloud.	2	7	3	1	2.77
K-82	Knowledge of emerging technology (e.g. blockchain, quantum computing)	3	5	4	1	2.77
K-83	Knowledge of building scalable distributed systems supporting parallel processing of customer jobs on a large fleet of devices.	1	5	5	0	2.64
K-84	Knowledge of making recommendations for migration of a physical network to a cloud-based architecture.	2	5	5	0	2.75
K-85	Knowledge of creating a cloud-based network infrastructure to meet requirements for a software application.	1	9	2	1	2.77
K-86	Knowledge of assessing and evaluating the technical benefits of implementation of a cloud computing architecture.	3	7	3	0	3.00
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.	9	3	1	0	3.62
K-88	Knowledge of preparing and deploying a Cloud High Availability and Business Continuity Solution.	1	8	3	1	2.69
K-89	Knowledge of implementing auto scaling and load balancing.	3	7	3	0	3.00

K-90	Knowledge of DevSecOps concepts.	1	3	1	0	2.80
K-91	Knowledge of the trend of technology's increasing "interconnectivity" and the end of rigid workplace silos.	0	5	0	0	3.00
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.	0	5	0	0	3.00
K-93	Knowledge of basic AI and machine learning concepts/tools (e.g. ChatGPT).	1	2	2	0	2.80
	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 on investing in financial futures, and therefore has knowledge of it. But getting experience in trading these instruments adds skills.					
S-1	Understand that OSI is the framework for all problem solving and troubleshooting	10	2	1	0	3.69
S-2	Skill in establishing a routing schema.	7	6	0	0	3.54
S-3	Skill in implementing, maintaining established network security practices.	6	7	0	0	3.46
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, and switches.	7	6	0	0	3.54
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	9	4	0	0	3.69
S-6	Skill in securing network communications. (e.g., logical)	7	6	0	0	3.54
S-7	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	6	7	0	0	3.46
S-8	Skill in basic configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	9	4	0	0	3.69
S-9	Skill in testing network infrastructure contingency and recovery plans.	2	10	1	0	3.08
S-10	Skill in applying various subnet techniques (e.g., CIDR).	7	4	2	0	3.38
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	6	7	0	0	3.46
S-12	Skill in configuring and basic optimizing software.	4	5	4	0	3.00
S-13	Skill in diagnosing connectivity problems.	9	4	0	0	3.69
S-14	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).	6	5	2	0	3.31
S-15	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	8	4	1	0	3.54
S-16	Skill in using Cloud (e.g. Amazon Elastic Compute Cloud).	5	6	2	0	3.23
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	6	3	2	0	3.36
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	6	6	1	0	3.38
S-19	Skill in interfacing with customers.	8	4	1	0	3.54
S-20	Skill in conducting system/server management and maintenance.	4	6	2	0	3.17
S-21	Skill in correcting physical and technical problems that impact system/server performance.	6	6	1	0	3.38
S-22	Skill in troubleshooting failed system components (i.e., servers).	6	7	0	0	3.46
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	5	6	2	0	3.23
S-24	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).	6	5	2	0	3.31
S-25	Skill in monitoring and optimizing basic system/server/cloud performance.	7	6	0	0	3.54
S-26	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).	4	6	3	0	3.08
S-27	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	5	6	2	0	3.23
S-28	Skill in applying Software Defined Networking concepts.	5	5	2	0	3.25
S-29	Skill in identifying and distinguishing Private, Public, and Hybrid Cloud Implementations.	8	4	1	0	3.54
S-30	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	9	4	0	0	3.69
S-31	Skill in executing Test Cases for identified functional or non-functional requirements.	3	7	3	0	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	8	2	0	3.08
S-33	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	3	8	1	1	3.00
S-34	Skill in preparing written reports.	4	8	1	0	3.23

S-35	Skill in preparing presentations.	4	5	4	0	3.00
S-36	Skill in producing Virtual Machines from a Cloud image.	3	7	2	0	3.08
S-37	Skill in producing Virtual Machines within a Cloud region.	2	8	1	1	2.92
S-38	Skill in demonstrating how to customize virtual networks with IP Address Range, subnets, routing tables and gateways.	6	5	2	0	3.31
S-39	Skill in analyzing and troubleshooting Cloud Virtual Networks.	2	9	2	0	3.00
S-40	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	5	7	1	0	3.31
S-41	Skill in deploying cloud storage technologies with the assistance of a senior technician.	3	7	2	1	2.92
S-42	Skill in analyzing and troubleshooting different cloud storage technologies.	3	6	2	1	2.92
S-43	Skill in applying permissions from the IAM (Identity and Access Management).	4	8	1	0	3.23
S-44	Skill in applying permissions for IAM (Identity and Access Management) Group(s).	4	7	1	0	3.25
S-45	Skill in applying permissions for IAM (Identity and Access Management) user(s).	4	8	1	0	3.23
S-46	Skill in analyzing and troubleshooting containers.	3	7	1	1	3.00
S-47	Skill in using tools like Chef, Puppet, Ansible, etc.	4	3	4	0	3.00
S-48	Skill in managing changes/updates for both internal and external customers when policies and procedures change.	3	8	2	0	3.08
S-49	Skill in assessing or monitoring system for cyberattacks.	4	6	2	0	3.17
S-50	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	4	8	1	0	3.23
S-51	Skill in leveraging cloud/hybrid managed services to enable greater flexibility and resilience in an secure infrastructure.	2	6	5	0	2.77
S-52	Skill in identifying appropriate cloud services that provide the compute power needed to solve a technical business problem while optimizing cost.	0	6	7	0	2.46
S-53	Skill in building, and operating key pieces of serverless and cloud native applications using appropriate cloud services.	2	5	5	0	2.75
S-54	Skill in using a continuous integration (CI) / continuous delivery (CD) pipeline to deploy applications.	2	6	2	0	3.00
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).	4	6	3	0	3.08
S-56	Skill in importing, exporting, migrating, protecting, and securing data from one data source to another.	3	5	5	0	2.85
S-57	Skill in applying security concepts in the automation of resource provisioning.	3	6	3	0	3.00
S-58	Skill in identifying the necessary components of a physical network and a cloud-based network.	5	8	0	0	3.38
S-59	Skill in using Azure.	3	5	3	1	2.83
S-60	Skill in using AWS.	4	4	3	1	2.92
S-61	Skill in Google Cloud.	2	4	4	2	2.50
S-62	Skill in using IBM Cloud.	0	2	5	5	1.75
S-63	Skill in using Oracle Cloud.	0	3	6	3	2.00
S-64	Skill in using Cisco Cloud.	0	3	5	4	1.92
S-65	Skill in using VirtualBox.	1	3	6	1	2.36
	Abilities Often confused with skills, yet there is a subtle but important difference. Abilities are 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.					
A-1	Ability to install network equipment including routers, switches, servers, transmission media, and related hardware.	9	4	0	0	3.69
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	10	3	0	0	3.77
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	11	2	0	0	3.85
A-4	Ability to operate the organization's LAN/WAN pathways.	7	6	0	0	3.54
A-5	Ability to monitor measures or indicators of system performance and availability.	8	5	0	0	3.62
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	5	7	1	0	3.31
A-7	Ability to monitor traffic flows across the network.	7	6	0	0	3.54
A-8	Ability to recognize and escalate the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	11	2	0	0	3.85

A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	7	6	0	0	3.54
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	2	8	3	0	2.92
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).	4	7	2	0	3.15
A-12	Ability to collaborate effectively with others.	10	2	1	0	3.69
A-13	Ability to function effectively in a dynamic, fast-paced environment.	9	3	1	0	3.62
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4	9	0	0	3.31
A-15	Ability to maintain automated security control assessments.	3	6	3	0	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.	9	3	1	0	3.62
A-17	Ability to work under stress.	11	1	1	0	3.77
A-18	Ability to problem solve.	11	2	0	0	3.85
A-19	Ability to analyze and interpret customer input for expressed and implied requirements.	8	4	1	0	3.54
A-20	Ability to translate technical language into lay terminology when needed.	7	5	1	0	3.46
A-21	Ability to read and interpret technical documents, diagrams, and decision trees.	9	4	0	0	3.69
A-22	Ability to listen and understand what people say.	11	1	1	0	3.77
A-23	Ability to recognize and understand details.	11	2	0	0	3.85
A-24	Ability to order and arrange items.	10	3	0	0	3.77
A-25	Ability to create appropriate presentation visuals for technical material.	3	7	3	0	3.00
Certifications Certifications show deeper level of interest, commitment, and follow-through, but can also help job applicants get past HR gatekeeprs and passed along to the hiring manager. They are "door openers."						
Cert-1	A+	2	4	4	2	2.50
Cert-2	Network+	4	4	3	1	2.92
Cert-3	Security+	5	3	3	1	3.00
Cert-4	CCNA	2	7	2	1	2.83
Cert-5	SSCP/CISSP	3	6	3	1	2.85
Cert-6	CWNP	0	6	3	1	2.50
Cert-7	CWNA (i.e. "broad wireless")	0	7	1	4	2.25
Cert-8	AWS Cloud Practitioner	4	3	4	1	2.83
Cert-9	Azure Fundamentals	2	5	4	1	2.67