	Infrastructure KSAs - updated Summer 2020 * Skills for an entry-level IT worker looking for a job 12-36 months from Fall 2020 * Be sure ITIL (change management and root/cause analysis) elements are covered as needed in every course. ISO 9000/9001 Quality Management criteria * Consider on-site tours.	Avg
	Tasks SPECIFIC THINGS an entry level person would BE EXPECTED TO PERFORM on the job WITH LITTLE SUPERVISION.	
T-1	Configure and optimize network, routers, and switches (e.g., higher-level protocols, tunneling).	3.4
T-2	Diagnose network connectivity problem.	3.8
T-3	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware) which would include patch network vulnerabilities to safeguard information.	3.3
T-4	Install or replace network, routers, and switches.	3.4
T-5	Integrate new systems into existing network architecture.	3.1
T-6	Monitor network capacity and performance.	3.4
T-7	Test and maintain network infrastructure including software and hardware devices.	3.3
T-8	Conduct functional and connectivity testing to ensure continuing operability.	3.5
T-9	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	3.4
T-10	Support group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	3.5
T-11	Follow SOP and validate/update documentation of compliance.	3.3
T-12	Validate/update baseline system security according to organizational policies.	3.3
T-13	Manage accounts, network rights, and access to systems and equipment.	3.2

T-14	Provide ongoing optimization and problem-solving support.	3.5
T-15	Install, update, and troubleshoot systems/servers.	3.4
T-16	Check system hardware availability, functionality, integrity, and efficiency.	3.4
T-17	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	3.2
T-18	Implement local network usage policies and procedures.	3.3
T-19	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	3.1
T-20	Monitor and maintain system/server configuration.	3.3
T-21	Installation, implementation, configuration, and support of system components.	3.1
T-22	Troubleshoot faulty system/server hardware.	3.3
T-23	Perform repairs on faulty system/server hardware.	3.2
T-24	Troubleshoot hardware/software interface and interoperability problems.	3.2
	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.	3.9
K-2	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	3.1
K-3	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (e.g. PCI, PII, PHI, GDPR).	3.1
K-4	Knowledge of cybersecurity and privacy principles.	3.4
K-5	Knowledge of cyber threats and vulnerabilities.	3.4

K-6	Knowledge of specific operational impacts of cybersecurity lapses.	3.4
K-7	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	3.4
K-8	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	3.6
K-9	Knowledge of how to assess existing infrastructure (LAN, WAN).	3.5
K-10	Knowledge of risk management, cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	3.2
K-11	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.7
K-12	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	3.5
K-13	Knowledge of measures or indicators of system performance and availability.	3.4
K-14	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI]).	3.5
K-15	Knowledge of remote access technology concepts.	3.5
K-16	Knowledge of server administration and systems engineering theories, concepts, and methods.	3.1
K-17	Knowledge of telecommunications concepts (e.g., will change all the time).	3.2
K-18	Knowledge of Virtual Private Network (VPN) security.	3.5
K-19	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	3.4
K-20	Knowledge of network tools (e.g., ping, traceroute, nslookup).	3.8
K-21	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	3.5
K-22	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	3.3

K-23	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	3.3
K-24	Knowledge of Wi-Fi.	3.5
K-25	Knowledge of Voice over IP (VoIP).	3.3
K-26	Knowledge of the common attack vectors on the network layer.	3.4
K-27	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	3.3
K-28	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	3.3
K-29	Knowledge of concepts of certificates, key management and usage.	3.1
K-30	Knowledge of transmission types (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques and interference techniques.	3.0
K-31	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	3.6
K-32	Knowledge of controls related to the use, processing, storage, and transmission of data.	3.1
K-33	Knowledge of performance tuning tools and techniques.	3.1
K-34	Knowledge of server and client operating systems.	3.6
K-35	Knowledge of systems administration concepts.	3.4
K-36	Knowledge of the enterprise information technology (IT) architecture.	3.3
K-37	Knowledge of the type and frequency of routine hardware maintenance (e.g. Linux/Unix OS, Windows Server OS).	3.2
K-38	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) including network storage and servers.	3.1

K-39	Knowledge of virtualization technologies and virtual machine development and maintenance.	3.6
K-40	Knowledge of information technology (IT) user security policies (e.g., account creation, password rules, access control).	3.4
K-41	Knowledge of system administration, network, and operating system hardening techniques.	3.3
K-42	Knowledge of systems concepts and methods.	3.2
K-43	Knowledge of system/server diagnostic tools and fault identification techniques.	3.4
K-44	Knowledge of operating system command-line tools.	3.3
K-45	Knowledge of principles and methods for integrating system components including network storage and servers.	3.3
K-46	Knowledge of Cloud and Cloud Services.	3.6
K-47	Knowledge of script automation and application programming interfaces.	3.4
K-48	Knowledge of network backup and recovery procedures.	3.4
K-49	Knowledge of patch network vulnerabilities to ensure that information is safeguarded against outside parties.	3.6
K-50	Knowledge of asset management and why it's important to the business.	3.0
K-51	Knowledge of infrastructure data storage capabilities and storage cluster.	3.2
K-52	Knowledge of risks associated with storing various types of data in different physical locations.	3.3
K-53	Knowledge of infrastructure data storage capabilities and storage clusters.	3.1
K-54	Knowledge of voice, video and data transmission protocols.	3.3
K-55	Knowledge of IoT end devices and connectivity.	3.2
K-56	Knowledge of metrics, how they are developed in general, their purpose, and why they are used.	2.9

Cloud K-1	Knowledge of the differences or similarities between private, public, and hybrid cloud implementations.	3.3
Cloud K-2	Knowledge of the difference or similarities between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	3.3
Cloud K-3	Awareness of framework concepts, their selection and use.	2.8
Cloud K-4	Awareness of the pros or cons behind using frameworks.	2.6
Cloud K-5	Knowledge of the term benchmarks and the reasons for their use.	3.0
Cloud K-6	Knowledge of the term resilience and how resilience can be designed into a project, program, infrastructure or organization.	3.0
Cloud K-7	Knowledge of the concept of service level agreement (SLA), why they are used, when they are used, and its application within cloud implementations.	3.0
Cloud K-8	Knowledge of who owns or should own the data/information in a cloud implementation.	3.1
Cloud K-9	Knowledge of the key management, operational, security, and/or privacy challenges potentially faced when considering or implementing a cloud capability.	3.2
Cloud K-10	Knowledge of the key key management, operational, security, and/or privacy monitoring challenges potentially faced when considering or implementing a cloud capability.	3.1
Cloud K-11	Knowledge of the different organizational roles needed as one plans for cloud implementation or manages an existing cloud capability.	2.8
Cloud K-12	Knowledge of the incident response challenges potentially faced within a cloud implementation.	3.0
Cloud K-13	Knowledge of web services technologies.	3.0
Cloud K-14	Knowledge of cloud network storage.	3.1
Cloud K-15	Knowledge of cloud object-based Storage.	2.9
Cloud K-16	Knowledge of cloud local system storage.	3.0
Cloud K-17	Knowledge of the different cloud computing database types (RDS).	2.8

Cloud K-18	Knowledge of how to scale a cloud database.	2.9
Cloud K-19	Knowledge of cloud database fail-over best practices.	3.1
Cloud K-20	Knowledge of the differences between SQL and Non-SQL databases.	2.7
Cloud K-21	Knowledge of cloud IAM (Identity and Access Management).	3.0
Cloud K-22	Knowledge of cloud IAM (Identity and Access Management) users, groups, roles and policies.	3.0
Cloud K-23	Knowledge of cloud computing shared security responsibility model.	3.3
Cloud K-24	Knowledge of cloud regions.	2.6
Cloud K-25	Knowledge of cloud availability zone.	2.6
Cloud K-26	Knowledge of high availability service levels (SLA).	3.3
Cloud K-27	Knowledge of recovery time objective (RTO).	3.1
Cloud K-28	Knowledge of recovery point objective (RPO).	3.1
Cloud K-29	Knowledge of high availability factors (fault-tolerance, recoverability, and scalability).	3.1
Cloud K-30	Knowledge of microservices and containerization (e.g. Kubernetes and Docker).	3.1
Cloud K-31	Knowledge of auto scaling and load balancing.	2.9
Cloud K-32	Knowledge of the differences between cloud vs. on-premises.	3.5
Cloud K-33	Knowledge (not skill) in preparing and deploying a cloud database solution that meets application requirements.	2.6
	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	Skill in analyzing network traffic capacity and performance characteristics.	3.6

S-2	Skill in establishing a routing schema.	3.2
S-3	Skill in implementing, maintaining established network security practices.	3.4
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, and switches.	3.6
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	3.6
S-6	Skill in securing network communications. (e.g., logical).	3.4
S-7	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	3.4
S-8	Skill in basic configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	3.4
S-9	Skill in testing network infrastructure contingency and recovery plans.	3.0
S-10	Skill in applying various subnet techniques (e.g., CIDR).	3.5
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	3.7
S-12	Skill in configuring and basic optimizing software.	3.0
S-13	Skill in diagnosing connectivity problems.	3.8
S-14	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).	3.4
S-15	Skill in using virtual machines (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	3.3
S-16	Skill in using Cloud (e.g. Amazon Elastic Compute Cloud).	3.3
S-17	Skills in using microservices and containers (e.g., Docker, Kubernetes, ECS) and understanding monitoring dashboards.	3.1
S-18	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	3.3

S-19	Skill in interfacing with customers.	3.6
S-20	Skill in conducting system/server management and maintenance.	3.4
S-21	Skill in correcting physical and technical problems that impact system/server performance.	3.2
S-22	Skill in troubleshooting failed system components (i.e., servers).	3.4
S-23	Skill in identifying system/server performance, availability, capacity, or configuration problems.	3.3
S-24	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).	3.4
S-25	Skill in monitoring and optimizing basic system/server performance.	3.3
S-26	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).	3.1
S-27	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	3.3
Cloud S-1	Skill in identifying and distinguishing private, public, and hybrid cloud implementations.	3.3
Cloud S-2	Skill in identifying and distinguishing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.	3.1
Cloud S-3	Skill in executing test cases for identified functional or non-functional requirements.	2.8
Cloud S-4	Skill in documenting results of executed test cases showing whether according to developed success criteria the test case passes, fails, or partially passes.	3.1
Cloud S-5	Skill in documenting and determining root cause failure(s) for items that failed or partially passed.	3.1
Cloud S-6	Skill in preparing written reports.	3.4
Cloud S-7	Skill in preparing presentations.	3.4
Cloud S-8	Skill in producing virtual machines from a cloud image.	3.3
Cloud S-9	Skill in producing virtual machines within a cloud region.	3.1

Cloud S-10	Skill in demonstrating how to customize virtual networks with IP address range, subnets, routing tables and gateways.	3.3
Cloud S-11	Skill in analyzing and troubleshooting cloud virtual networks.	3.0
Cloud S-12	Skill in preparing and deploying virtual machines in a virtual network (private or public subnet).	3.1
Cloud S-13	Skill in deploying cloud storage technologies with the assistance of a senior technician.	2.9
Cloud S-14	Skill in analyzing and troubleshooting different cloud storage technologies.	2.8
Cloud S-15	Skill in applying permissions from the IAM (Identity and Access Management).	3.0
Cloud S-16	Skill in applying permissions for IAM (Identity and Access Management) Group(s).	2.9
Cloud S-17	Skill in applying permissions for IAM (Identity and Access Management) user(s).	2.9
Cloud S-18	Skill in preparing and deploying a cloud high availability and business continuity solution.	2.6
Cloud S-19	Skill in deploying a containerized application.	2.6
Cloud S-20	Skill in analyzing and troubleshooting containers.	2.9
Cloud S-21	Skill in implementing auto scaling and load balancing.	3.1
Cloud S-22	Skill in using management tools like Chef, Puppet, etc.	2.9
	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.	3.6
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	3.7
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	3.6

A-4	Ability to operate the organization's LAN/WAN pathways.	3.5
A-5	Ability to monitor measures or indicators of system performance and availability.	3.4
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	3.1
A-7	Ability to monitor traffic flows across the network.	3.5
A-8	Ability to recognize and escalate the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	3.7
A-9	Ability to interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	3.7
A-10	Ability to apply an organization's goals and objectives to maintain architecture.	3.3
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).	3.1
A-12	Ability to collaborate effectively with others.	3.8
A-13	Ability to function effectively in a dynamic, fast-paced environment.	3.6
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.3
A-15	Ability to maintain automated security control assessments.	3.4
Cloud A-1	Ability to work within a project team.	3.8
Cloud A-2	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.	3.7
Cloud A-3	Ability to work under stress.	3.6
Cloud A-4	Ability to problem solve.	3.8
Cloud A-5	Ability to analyze and interpret customer input for expressed and implied requirements.	3.6

Cloud A-6	Ability to translate technical language into lay terminology when needed.	3.5
Cloud A-7	Ability to read and interpret technical documents, diagrams, and decision trees.	3.7
Cloud A-8	Ability to listen and understand what people say.	3.9
Cloud A-9	Ability to recognize and understand details.	3.8
Cloud A-10	Ability to order and arrange items.	3.4
Cloud A-11	Ability to create appropriate presentation visuals for technical material.	3.5