

National Business and Industry Leadership Team (BILT) Knowledge Domains - updated May 2019
IT Infrastructure KSAs - Knowledge, Skills, and Abilities (and Tasks)

Knowledge		# votes (4 = most important)				
		4	3	2	1	Avg
K-1	Knowledge of computer networking concepts and protocols, and network security methodologies.	11				4.0
K-2	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).		7	1	2	2.5
K-3	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (e.g., PCI, PII, PHI, GDPR)	8	4	1	0	3.5
K-4	Knowledge of cybersecurity and privacy principles.	7	4	1		3.5
K-5	Knowledge of cyber threats and vulnerabilities.	3	6			3.1
K-6	Knowledge of specific operational impacts of cybersecurity lapses.	4	3	2		3.8
K-7	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	9	1			3.9
K-8	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	10	1			3.9
K-9	Knowledge of how to assess existing infrastructure (e.g., LAN, WAN)	5	5	1		3.4
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	9			3.3
K-11	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	8	5			3.6
K-12	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	5	6	1		3.3
K-13	Knowledge of measures or indicators of system performance and availability.	7	6			3.5
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]).	11		1		3.8
K-15	Knowledge of remote access technology concepts.	6	4	2		3.3
K-16	Knowledge of server administration and systems engineering theories, concepts, and methods.	6	5	1		3.4
K-17	Knowledge of telecommunications concepts (will change all the time).	5	3	3	1	3.0
K-18	Knowledge of Virtual Private Network (VPN) security.	6	6			3.5
K-19	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	7	5			3.6
K-20	Knowledge of network tools (e.g., ping, traceroute, nslookup)	11	2			3.8
K-21	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	11	1			3.9
K-22	Knowledge of web filtering technologies. (e.g., Encapsula)	2	4	6	1	2.5
K-23	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	3	6	3		3.0
K-24	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	5	3	4		3.1
K-25	Knowledge of Wi-Fi.	8	3	1		3.6
K-26	Knowledge of Voice over IP (VoIP).	7	4	2		3.4
K-27	Knowledge of the common attack vectors on the network layer.	4	7	1		3.3
K-28	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	10	2			3.8
K-29	Knowledge of network and systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools (NOC and SOC).	8	5			3.6
K-30	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1	7	5		2.7
K-31	Knowledge of concepts of certificates, key management and usage.	7	2	1		3.6
K-32	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	1	2	6	3	2.1
K-33	OMITTED					
K-34	OMITTED					

National Business and Industry Leadership Team (BILT) Knowledge Domains - updated May 2019
IT Infrastructure KSAs - Knowledge, Skills, and Abilities (and Tasks)

K-35	OMITTED					
K-36	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 interference techniques.		9	4		2.7
K-37	Knowledge of an information classification program and procedures for information compromise.	3	5	4		2.9
K-38	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	10	2			3.8
K-39	Knowledge of controls related to the use, processing, storage, and transmission of data.		13			3.0
K-40	Knowledge of performance tuning tools and techniques.		9	4		2.7
K-41	Knowledge of server and client operating systems. (e.g., Linux/Unix OS, Windows Server OS)	11	1			3.9
K-42	Knowledge of systems administration concepts including network storage and servers.	10	2			3.8
K-43	Knowledge of the enterprise information technology (IT) architecture.	8	4	1		3.5
K-44	Knowledge of the type and frequency of routine hardware maintenance.	4	8			3.3
K-45	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	3	9		1	3.1
K-46	Knowledge of virtualization technologies and virtual machine development and maintenance.	8	5			3.6
K-47	Knowledge of information technology (IT) user security policies (e.g., account creation, password rules, access control).	10	3			3.8
K-48	Knowledge of system administration, network, and operating system hardening techniques.	4	7	1		3.3
K-49	OMITTED					
K-50	Knowledge of systems engineering theories, concepts, and methods.	6	3	3		3.3
K-51	Knowledge of system/server diagnostic tools and fault identification techniques.	7	5			3.6
K-52	Knowledge of operating system command-line tools.	7	5			3.6
K-53	Knowledge of principles and methods for integrating system components including network storage and servers.	4	6	2		3.2
K-54	OMITTED					
K-55	OMITTED					
K-56	Cloud and Cloud Services					
K-57	Script Automation and Application Programming Interfaces	11		1		3.8
K-58	Develop and implement network backup and recovery procedures.		11	2		2.8
K-59	Plan, execute, and verify data redundancy and system recovery procedures.		2	6	2	2.0
K-60	Knowledge of asset management and why it's important to the business	7	3			3.7
K-61	Knowledge of infrastructure data storage capabilities and storage cluster	9	1			3.9

Skills		# votes (4 = most important)				
		4	3	2	1	Avg
S-1	Skill in analyzing network traffic capacity and performance characteristics.	8	4			3.7
S-2	Skill in establishing a routing schema.	4	6	1		3.3
S-3	Skill in implementing, maintaining, and improving established network security practices.	3	9			3.3
S-4	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.	12				4.0
S-5	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	6	6			3.5
S-6	Skill in securing network communications.	6	6			3.5
S-7	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	3	8	1		3.2

National Business and Industry Leadership Team (BILT) Knowledge Domains - updated May 2019
IT Infrastructure KSAs - Knowledge, Skills, and Abilities (and Tasks)

S-8	Skill in basic configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	8	3	1		3.6
S-9	Skill in testing network infrastructure contingency and recovery plans.	6	5			3.5
S-10	Skill in applying various subnet techniques (e.g., CIDR)	8	4			3.7
S-11	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	10	2			3.8
S-12	Skill in configuring and basic optimizing software.	1	10			3.1
S-13	Skill in diagnosing connectivity problems.	10	2			3.8
S-14	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).		12			3.0
S-15	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	9	3			3.8
S-16	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	5	4	3		3.2
S-17	OMITTED					
S-18	Skill in conducting system/server management and maintenance.	3	9			3.3
S-19	Skill in correcting physical and technical problems that impact system/server performance.	8	4			3.7
S-20	Skill in troubleshooting failed system components (i.e., servers)	9	2			3.8
S-21	Skill in identifying system/server performance, availability, capacity, or configuration problems.	3	8			3.3
S-22	Skill in installing system and component upgrades (i.e., servers, appliances, network devices).	9	3			3.8
S-23	Skill in monitoring and optimizing basic system/server performance.	7	4			3.6
S-24	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).	8	2	2		3.5
S-25	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).	10	2			3.8

Abilities		# votes (4 = most important)				
		4	3	2	1	Avg
A-1	Ability to install network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	10	2			3.8
A-2	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	11	1			3.9
A-3	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	10	2			3.8
A-4	Ability to operate the organization's LAN/WAN pathways.	0	9	1		2.9
A-5	Ability to monitor measures or indicators of system performance and availability.	4	8			3.3
A-6	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	8	2	2		3.5
A-7	Ability to monitor traffic flows across the network.	8	4			3.7
A-8	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	9	3			3.8
A-9	Ability to accurately interpret and clarify incidents, problems, and events submitted in the trouble ticketing system.	7	5			3.6
A-10	Ability to apply an organization's goals and objectives and maintain architecture.		11	1		2.9
A-11	Ability to update, and/or maintain standard operating procedures (SOPs).		7	4		2.6
A-12	Ability to collaborate effectively with others.	10	2			3.8
A-13	Ability to function effectively in a dynamic, fast-paced environment.	11	2			3.8
A-14	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	5	6	1		3.3
A-15	Ability to maintain automated security control assessments	5	5		1	3.3

National Business and Industry Leadership Team (BILT) Knowledge Domains - updated May 2019
IT Infrastructure KSAs - Knowledge, Skills, and Abilities (and Tasks)

Tasks		# votes (4 = most important)				Avg
		4	3	2	1	
T-1	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	8	6			3.6
T-2	OMITTED					
T-3	Diagnose network connectivity problem.	13	1	1		3.8
T-4	Implement new system design procedures, test procedures, and quality standards. (Not an entry-level task; needs certification and on-the-job training - but would be nice for curriculum to touch on)			11	3	1.8
T-5	Install and maintain network infrastructure device operating system software which would include patch network vulnerabilities to safeguard information (e.g., IOS, firmware).	7	7			3.5
T-6	Install or replace network hubs, routers, and switches.	10	3			3.8
T-7	Integrate new systems into existing network architecture.	1	6	6		2.6
T-8	Monitor network capacity and performance.	6	6	1		3.4
T-9	OMITTED					
T-10	Provide feedback on network requirements, including network architecture and infrastructure.			6	7	1.5
T-11	Test and maintain network infrastructure including software and hardware devices.		11	1		2.9
T-12	Conduct functional and connectivity testing to ensure continuing operability.	6	6	1		3.4
T-13	Implement group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	10	3			3.8
T-14	Update existing documentation	5	6	1		3.3
T-15	Validate baseline system security according to organizational policies (similar to T-5: software and system updating)	1	5	2		2.9
T-16	Manage accounts, network rights, and access to systems and equipment.	6	3	3		3.3
T-17	OMITTED					
T-18	Provide ongoing optimization and problem-solving support.	4	7	1		3.3
T-19	Install, update, and troubleshoot systems/servers.	7	4			3.6
T-20	Check system hardware availability, functionality, integrity, and efficiency.	7	5			3.6
T-21	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	9	3			3.8
T-22	OMITTED					
T-23	Implement local network usage policies and procedures.	7	5			3.6
T-24	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	8	4			3.7
T-25	Monitor and maintain system/server configuration.	9	2			3.8
T-26	Installation, implementation, configuration, and support of system components.	12	1			3.9
T-27	Troubleshoot faulty system/server hardware.	12				4.0
T-28	Perform repairs on faulty system/server hardware.	7	5			3.6
T-29	Troubleshoot hardware/software interface and interoperability problems.	3	6	1		3.2