Cybersecurity Technical Support Specialist

Study Guide

Assessment:
0329 Cybersecurity Technical Support Specialist

OKLAHOMA WORKS

OKLAHOMA CareerTech | CTTC CareerTech Testing Center

Overview

This study guide is designed to help students prepare for the Cybersecurity Technical Support Specialist assessment. It includes information about the assessment, the skills standards upon which the assessment is based, resources that can be used to prepare for the assessment, and test taking strategies.

Each of the four sections in this guide provides useful information for students preparing for the Cybersecurity Technical Support Specialist assessment.

- CareerTech and Competency-Based Education: A Winning Combination
- Cybersecurity Technical Support Specialist Assessment
  - Assessment Information
  - Standards and Test Content
  - Sample Questions
  - Abbreviations, Symbols, and Acronyms
- Strategies for Test Taking Success
- Notes

Disclaimer

The Oklahoma Department of Career and Technology Education cannot vouch for the accuracy of the information contained in any linked site. Our intent is to simply provide a list of sites that we feel may be useful to you. Some of the links presented here are commercial sites. We do not endorse these sites or their products, and we do not request or accept any fee for inclusion on this list. The department makes no representations or warranties, express or implied, with respect to the document, or any part thereof, including any warrantees of title, noninfringement of copyright or patent rights of others, merchantability, or fitness or suitability for any purpose.

Equal Opportunity/Nondiscrimination Statement

The Oklahoma Department of Career and Technology Education does not discriminate on the basis of race, color, national origin, sex/gender, age, disability or veteran status. Inquiries concerning application of this policy may be referred to the ODCTE Compliance Coordinator, 1500 W. Seventh Ave., Stillwater, OK 74074-4364, or call 1-800-522-5810 or 405-377-2000.

CareerTech and Competency-Based Education: A Winning Combination

Competency-based education uses learning outcomes that emphasize both the application and creation of knowledge and the mastery of skills critical for success. In a competency-based education system, students advance upon mastery of competencies, which are measurable, transferable outcomes that empower students.

Career and technology education uses industry professionals and certification standards to identify the knowledge and skills needed to master an occupation. This input provides the foundation for development of curriculum, assessments and other instructional materials needed to prepare students for wealth-generating occupations and produce comprehensively trained, highly skilled employees demanded by the work force.

Tools for Success

CareerTech education relies on three basic instructional components to deliver competency-based instruction: skills standards, curriculum materials, and competency assessments.

Skills standards provide the foundation for competency-based instruction and outline the knowledge and skills that must be mastered in order to perform related jobs within an industry. Skills standards are aligned with national skills standards and/or industry certification requirements; therefore, a student trained to the skills standards is equally employable in local, state and national job markets.

Curriculum materials and textbooks contain information and activities that teach students the knowledge and skills outlined in the skills standards. In addition to complementing classroom instruction, curriculum resources include supplemental activities that enhance learning by providing opportunities to apply knowledge and demonstrate skills.

Certification Assessments test the student over material outlined in the skills standards and taught using the curriculum materials and textbooks. When used with classroom performance evaluations, certification assessments provide a means of measuring occupational readiness.

Each of these components satisfies a unique purpose in competency-based education and reinforces the knowledge and skills students need to gain employment and succeed on the job.

Measuring Success

Evaluation is an important component of competency-based education. Pre-training assessments measure the student's existing knowledge prior to receiving instruction and ensure the student's training builds upon this knowledge base. Formative assessments administered throughout the training process provide a means of continuously monitoring the student's progress towards mastery.

Certification assessments provide a means of evaluating the student's mastery of knowledge and skills. Coaching reports communicate assessment scores to students and provide a breakdown of assessment results by standard area. The coaching report also shows how well the student has mastered skills needed to perform major job functions and identifies areas of job responsibility that may require additional instruction and/or training.

Cybersecurity Technical Support Specialist Assessment Information

What is the Cybersecurity Technical Support Specialist assessment?

The Cybersecurity Technical Support Specialist assessment is an end-of-program assessment for students in Cybersecurity Technical Support Specialist programs. The assessment provides an indication of student mastery of knowledge and concepts necessary for success in careers in this area.

How was the assessment developed?

The assessment was developed by the CareerTech Testing Center. Items were developed and reviewed by a committee of subject matter experts.

The committee assigned frequency and criticality ratings to each skill, which determines the significance of each task for test development:

Frequency: represents how often the task is performed on the job. Frequency rating scales vary for different occupations. The rating scale used in this publication is presented below:

1 = less than once a week 2 = at least once a week 3 = once or more a day

Criticality: denotes the level of consequence associated with performing a task incorrectly. The rating scale used in this publication is presented below:

1 = slight 2 = moderate 3 = extreme

What does the assessment cover?

Specifically, the test includes multiple-choice test items over the following areas:

Cybersecurity Technical Support Specialist (55 questions)

Demonstrate Knowledge of Principles and Practices within Cybersecurity Professions 11%
Understand Defense-in-Depth Principles and Practices in Cybersecurity Professions. 15%
Demonstrate Knowledge of Privacy Principles and Practices in Cybersecurity Professions. 13%
Demonstrate Knowledge of Laws, Policies and Regulations Related to Cybersecurity Professions . . 5%
Demonstrate Knowledge of Threats and Vulnerabilities in Cybersecurity 4%
Demonstrate Knowledge of Enterprise Cybersecurity Architecture Principles and Practices. . . . 18%
Demonstrate Knowledge of Risk Management Principles and Practices in Cybersecurity Professions 5%
Demonstrate Knowledge of Operating Systems and Virtual Machines in Cybersecurity Professions 5%
Demonstrate Knowledge of Computer Networking Principles and Practices in Cybersecurity Professions 9%
Demonstrate Knowledge of Cryptology Principles and Practices 5%
Demonstrate Knowledge of System Administration 2%
Demonstrate Employability Skills. 8%

What are the benefits of using this assessment?

Students receive a competency certificate for each assessment they pass. This certificate should be included in the student's portfolio and used to communicate their mastery of the subject matter to potential employers. Oklahoma students can also receive a digital badge that can be added to the students' digital resume or social media accounts. For more information on digital badges, please visit the badging section of the website at **https://oklahoma.gov/careertech/educators/certifications-and-badging/badging.html**.

When should the assessment be taken?

The CareerTech Testing Center recommends that students take this assessment as soon as possible after receiving all standards-related instruction, rather than waiting until the end of the school year.

Is the assessment timed?

No. However, most students finish the assessment within one hour.

What resources can students use on these assessments?

Students are allowed to use calculators and scratch paper on CTTC assessments; however, these items must be provided by the testing proctor and returned to the proctor before the student's exam is submitted for scoring. Calculator apps on cell phones and other devices may not be used on these assessments.

What accommodations can be made for students with Individualized Education Plans (IEPs)?

Accommodations are allowed for students with an Individualized Education Plan. Examples of allowable accommodations include:

- **Extended time** — This assessment is not timed; therefore, students may take as much time as needed to finish. The assessment must be completed in one testing session.
- **Readers** — A reader may be used to read the assessment to a student who has been identified as needing this accommodation.
- **Enlarged text** — Students needing this accommodation can activate this feature by clicking the AA icon in the upper right corner of the screen.

What can students expect on Test Day?

All CTTC assessments are web-based and delivered exclusively by a proctor in the school's assessment center. The proctor **cannot** be an instructor or anyone who was involved with the student during instruction.

Assessments are delivered in a question-by-question format. When a question is presented, the student can select a response or leave the question unanswered and advance to the next question. Students may also flag questions to revisit before the test is scored. All questions must be answered before the test can be submitted for scoring.

After the assessment is scored, the student will receive a score report that shows the student's score on the assessment and how the student performed in each standard area.

Can students retake the test?

Students may retake the test unless their school or state testing policies prohibit retesting. Students who retest must wait at least three days between attempts.

Standards and Test Content

Duty A: Demonstrate Knowledge of Principles and Practices within Cybersecurity Professions (6 questions)

CODE	TASK	F	C
A.01	Demonstrate knowledge of cybersecurity-specific principles and practices	3	3
A.02	Demonstrate knowledge of the CIA (Confidentiality, Integrity, and Availability) Triad	3	3
A.03	Demonstrate knowledge of the IAAA (Identification, Authentication, Authorization, Accountability) framework	3	3
A.04	Identify the differences between Threats, Vulnerabilities, and Harms	2	2

Duty B: Understand Defense-in-Depth Principles and Practices in Cybersecurity Professions (8 questions)

CODE	TASK	F	C
B.01	Understand the principle of physical security	2	2
B.02	Understand the principle of network security	2	3
B.03	Understand the principle of endpoint security	2	3
B.04	Understand the principle of application security	2	2
B.05	Demonstrate knowledge and understanding of Identity and Access Management (IAM)	3	3
B.06	Recognize the importance of monitoring and training	2	2
B.07	Understand importance of user awareness and training	2	3

Duty C: Demonstrate Knowledge of Privacy Principles and Practices in Cybersecurity Professions (7 questions)

CODE	TASK	F	C
C.01	Understand the privacy principle of data security	2	2
C.02	Understand the privacy principle of transparency	2	2
C.03	Understand the privacy principle of data minimization	2	2
C.04	Understand the privacy principle of purpose limitation	2	2
C.05	Understand the concept of data integrity	2	3
C.06	Understand retention limitation	1	2
C.07	Understand the principle of consent	2	2

Duty D: Demonstrate Knowledge of Laws, Policies and Regulations Related to Cybersecurity Professions (3 questions)

CODE	TASK	F	C
D.01	Demonstrate knowledge of the laws related to: • Cybersecurity • Exploitation • Targeting	2	2
D.02	Demonstrate knowledge of the policies affecting cybersecurity professions	2	2
D.03	Know the regulations affecting cybersecurity	2	2

Duty E: Demonstrate Knowledge of Threats and Vulnerabilities in Cybersecurity (2 questions)

CODE	TASK	F	C
E.01	Understand the types and characteristics of threats: • Cybersecurity • System • Threat Characteristics	2	2
E.02	Understand the types of vulnerabilities: • Cybersecurity • System • Vulnerability Characteristics	2	2

Duty F: Demonstrate Knowledge of Enterprise Cybersecurity Architecture Principles and Practices (10 questions)

CODE	TASK	F	C
F.01	Understand the operational and safety impact of cybersecurity lapses	2	2
F.02	Understand the importance of separation of duties	2	2
F.03	Demonstrate knowledge of asset management	3	2
F.04	Demonstrate knowledge of patch management	3	2
F.05	Demonstrate knowledge of backup management	2	3
F.06	Understand the principles of Zero Trust and Least Privilege	2	3
F.07	Understand the importance of an Incident Response Plan	2	3
F.08	Demonstrate knowledge of regulatory compliance	2	2
F.09	Understand the importance of logging, monitoring, and vulnerability scanning	2	3

Duty G: Demonstrate Knowledge of Risk Management Principles and Practices in Cybersecurity Professions (3 questions)

CODE	TASK	F	C
G.01	Understand the concept of risk management	3	2
G.02	Demonstrate knowledge of the risk management process	2	2
G.03	Understand the key components of a risk management framework	1	2

Duty H: Demonstrate Knowledge of Operating Systems and Virtual Machines in Cybersecurity Professions (3 questions)

CODE	TASK	F	C
H.01	Identify and understand operating system structures	2	2
H.02	Demonstrate an understanding of an operating system's "internals"	2	2
H.03	Develop an understanding of machine virtualization • Virtual machine development and maintenance • Detection of virtual machines • Virtual machine tools	2	2

Duty I: Demonstrate Knowledge of Computer Networking Principles and Practices in Cybersecurity Professions (5 questions)

CODE	TASK	F	C
I.01	Demonstrate an understanding of network communications: • Digital • Telecommunication • Wireless	2	2
I.02	Demonstrate knowledge of network protocols, architecture, and configurations: • Client and Server Architecture • Host Access Control • Network Access Control • Open Systems Interconnect (OSI) Reference Model	3	3
I.03	Understand the concept of network security	3	3
I.04	Identify and understand signal jamming tools and techniques	1	1

Duty J: Demonstrate Knowledge of Cryptology Principles and Practices (3 questions)

CODE	TASK	F	C
J.01	Identify and understand algorithms and types of encryption: • Asymmetric • Symmetric • Developing Algorithms	2	2
J.02	Understand cryptographic key management	2	3
J.03	Understand encryption algorithms	1	2

Duty K: Demonstrate Knowledge of System Administration (1 question)

CODE	TASK	F	C
K.01	Demonstrate knowledge of System Administration	3	3

Duty L: Demonstrate Employability Skills (4 questions)

CODE	TASK	F	C
L.01	Collaborate effectively with others	3	2
L.02	Prepare and deliver reports and briefings	3	3
L.03	Exhibit effective public speaking and presentation skills	2	2

Sample Questions

_____ 1. Which is the most effective method for recovering data after a ransomware attack?

a. maintaining secure backups
b. installing antivirus software
c. enabling multifactor authentication
d. using network segmentation

_____ 2. Which component of the CIA Triad ensures that information is accessible to authorized users when needed?

a. Confidentiality
b. Integrity
c. Availability
d. Authentication

_____ 3. In the OSI model, which layer is responsible for routing packets between networks?

a. data link
b. network
c. transport
d. session

_____ 4. Which skills type includes body language, eye contact, good email etiquette, active listening, and asking questions?

a. communication
b. technical
c. academic
d. language

_____ 5. The primary purpose of an Incident Response Plan is to _____.

a. eliminate all cybersecurity risks across an organization
b. provide a structured process for responding to security incidents
c. replace employee security training with automated response tools
d. increase network bandwidth and system processing performance

Sample Questions — Key

1. Which is the most effective method for recovering data after a ransomware attack?

a.	maintaining secure backups	Correct
b.	installing antivirus software	Incorrect
c.	enabling multifactor authentication	Incorrect
d.	using network segmentation	Incorrect

2. Which component of the CIA Triad ensures that information is accessible to authorized users when needed?

a.	Confidentiality	Incorrect
b.	Integrity	Incorrect
c.	Availability	Correct
d.	Authentication	Incorrect

3. In the OSI model, which layer is responsible for routing packets between networks?

a.	data link	Incorrect
b.	network	Correct
c.	transport	Incorrect
d.	session	Incorrect

4. Which skills type includes body language, eye contact, good email etiquette, active listening, and asking questions?

a.	communication	Correct
b.	technical	Incorrect
c.	academic	Incorrect
d.	language	Incorrect

5. The primary purpose of an Incident Response Plan is to _____.

a.	eliminate all cybersecurity risks across an organization	Incorrect
b.	provide a structured process for responding to security incidents	Correct
c.	replace employee security training with automated response tools	Incorrect
d.	increase network bandwidth and system processing performance	Incorrect

Abbreviations, Symbols and Acronyms

The following is a list of abbreviations, symbols, and acronyms used in the Cybersecurity Technical Support Specialist study guide and on the Cybersecurity Technical Support Specialist assessment.

CIA	Confidentiality, Integrity, and Availability
IAAA	Identification, Authentication, Authorization, Accountability
IAM	Identity and Access Management
OSI	Open Systems Interconnect

Test Taking Strategies

This section of the study guide contains valuable information for testing success and provides a common-sense approach for preparing for and performing well on any test.

General Testing Advice

1. Get a good night's rest the night before the test — eight hours of sleep is recommended.
2. Avoid junk food and "eat right" several days before the test.
3. Do not drink a lot or eat a large meal prior to testing.
4. Be confident in your knowledge and skills!
5. Relax and try to ignore distractions during the test.
6. Focus on the task at hand — taking the test and doing your best!
7. Listen carefully to the instructions provided by the exam proctor. If the instructions are not clear, ask for clarification.

Testing Tips

1. Read the entire question before attempting to answer it.
2. Try to answer the question before reading the choices. Then, read the choices to determine if one matches, or is similar, to your answer.
3. Do not change your answer unless you misread the question or are certain that your first answer is incorrect.
4. Answer questions you know first, so you can spend additional time on the more difficult questions.
5. Check to make sure you have answered every question before you submit the assessment for scoring — unanswered questions are marked incorrect.

NOTES

NOTES

NOTES

NOTES