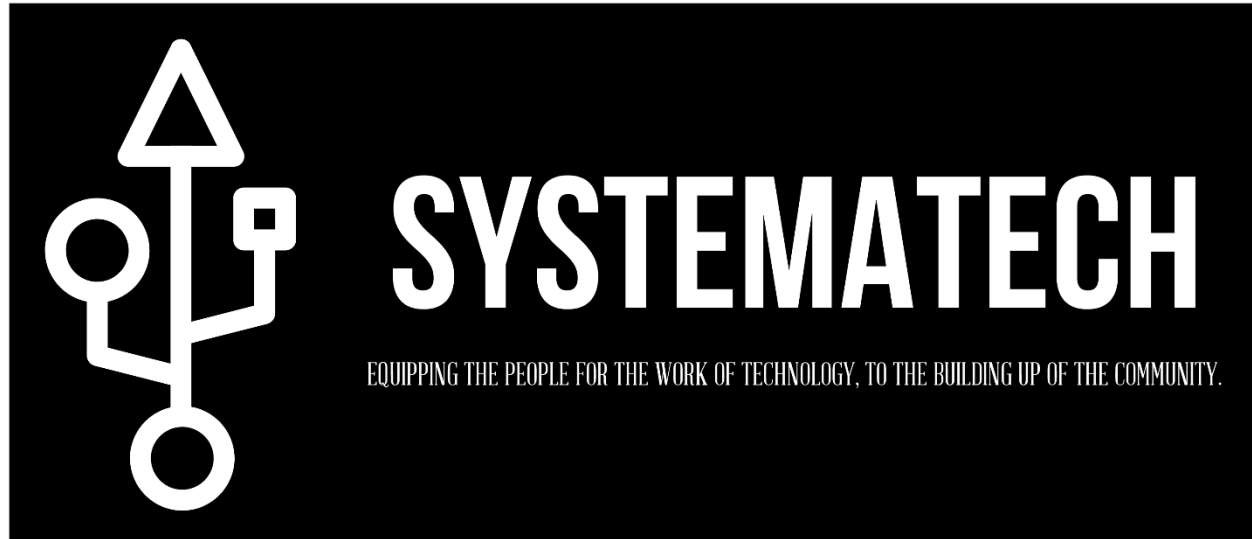


## Catalog



Students are expected to be familiar with the information presented in this school catalog, with any supplements and addenda to the catalog, and with all school policies. By enrolling in SystemATech, students agree to accept and abide by the terms stated in this catalog and all school policies. If there is any conflict between any statement in this catalog and the enrollment agreement signed by the student, the enrollment agreement controls.

SYSTEMATECH

Telephone: (803)474-4407

Publication Date: 12/02/2022

Volume 1, 1<sup>st</sup> Edition

### **Directory**

*Name: President/CEO Ashley S. Felton*

*Name: Officer, Tammy Anthony*

*Name: Officer, Arnold Anthony*

*Name: Faculty, John Wray*

*Name: Faculty, Shereen Reeves*

*Name: Faculty, Steven Murray Jr*

*Name: Faculty, Malcolm Doe*

### **Mission Statement**

Our mission at SystemATECH Co. is to help our students develop the skills necessary to change their lives and futures permanently and positively by attaining financially rewarding and personally fulfilling careers in Information Technology.

### **Description of Facilities**

At this time all classes will be held online.

### **Living Quarters**

Systematech will not provide any living quarters or living assistance for current or future students.

### **South Carolina Commission on Higher Education**

Licensed by the South Carolina Commission on Higher Education, 1122 Lady Street, Suite 300, Columbia, SC, 29201, telephone number 803-737-2260, and website address [www.che.sc.gov](http://www.che.sc.gov). Licensure indicates only those minimum standards have been met; it is not an endorsement or guarantee of quality. Licensure is not equivalent to or synonymous with accreditation by an accrediting agency recognized by the US Department of Education.

### **Accrediting Agency**

SystemATech is licensed by the South Carolina Commission on Higher Education to operate in the State of South Carolina. The Credit agencies is:

CompTIA located at 3500 Lacey Road, Suite 100- Downers Grove, IL 60515 (telephone 866-835-8021 / 630-678-8300). [www.comptia.org](http://www.comptia.org).

ANSI located at 1899 L St NW 11 Floor, Washington, DC 20036 (telephone 202-293-8020)  
[www.ansi.gov](http://www.ansi.gov)

### **Class Hours**

Students are required to attend three lecture classes per week online in addition to a scheduled learning Lab each week. Students will be schedule at enrollment to attend a specific lecture class schedule. Breaks will be held as deemed necessary by the instructor with no more than one and half hours break per class day. An instructor is available outside of class hours throughout the day. See hours below.

#### **Lecture Schedule Tuesday – Thursday: EST**

Morning: 8:30am – 4:30pm

Evening: 6:00 pm – 11:00 pm

### **Admission Requirements**

Students must meet with a member of the Admissions Team to be considered for acceptance into our programs. The Admissions Team member will ascertain the prospective students' ability to enroll in a program during the admissions process. SystemATECH will determine acceptance into any offered program. The decision to allow a student to enroll in the program will also be guided by the standards for the State below. Some programs will have prerequisite requirements that are outlined within the program curriculum. Any prospective student who has a special needs request or accommodation must submit the request in writing via email to their Admissions Advisor/Director prior to enrollment to determine if the school can accommodate the request.

#### **State of South Carolina**

- Documentation of one of the following is required for enrollment: High School transcript, copy of the certificate of high school equivalency, transcript showing graduation from a community college or university that operates in compliance with state or local law, completion of secondary education equivalent to high school education in the United States or a signed, notarized attestation of graduation from any of the above. VA benefit enrollment requirements may vary. Please consult with your Admissions team for those requirements.
- There is a minimum age requirement of 16 for enrollment into any program at SystemATECH. Applicants under the age of 18 need a parent or guardian's signature in addition to their own signature on the Enrollment agreement.

### **Policy on Non-Discrimination**

SystemATECH does not discriminate nor condone discrimination on the basis of sex, religion, nationality, color, race, age, disability, sexual orientation, or any other legally protected characteristic. Testing facilities are handicap accessible. Students with special needs may need to meet minimum mobility requirements for testing of the companies issuing the certification.

Students with special educational needs should notify their Admissions Representative before scheduling with testing to verify the accommodation.

### **Transfer Credit**

SystemATech Co. will not accept transfer credits or credit hours for courses taken at other institutions.

### **Standards of Progress**

#### **Grading Scale**

The chart to the right is the grading scale based on the percentage of points earned over the length of a program or course.

The final grade will be comprised of multiple components, each critical to the success of the student. Refer to the course syllabus for each course breakdown. The table to the right shows the common breakdown of the final grade for programs: (Note: Courses will only consist of tests as the criteria for the total grade

% of Total Points Earned	Letter Grade	GPA
90-100	A	4.0
80-89	B	3.0
70-79	C	2.0
60-69	D	1.0
59 or below	F	0.0
Temporary Leave of Absence	L	n/a

Criteria	% of Total Grade
Final Exam	40%
Post Assessments	30%
Graded Labs	20%
Homework Assignments	10%

A student must achieve the following to graduate from a program at SystemATECH Co:

1. Completion of all credit hours in the program
2. Cumulative grade percentage of 70% or higher (2.0 GPA)
3. Minimum GPA of 60% is required for individual courses.
4. Completion of 80% of the scheduled clock hours in each course.
5. Completion of the graduation requirements within the maximum program length, which is 143% of the published length of the program. (Not applicable for Avocational courses)

All graduates will receive a Certificate of Completion.

### **Attendance Policy & Conduct**

Unsatisfactory attendance, including absence of three (3) consecutive days, will result to a possible termination of Enrollment Certifications.

Students must also meet all academic standards of progress for SystemATECH including but not limited to the Satisfactory Academic Progress policy. At the end of each course students must meet the following non-cumulative standards:

- GPA of 70% or higher for that course.

- Attendance of 80% of scheduled clock-hours or higher for that course.

Students not meeting this requirement at the end of any course will be placed on Academic Probation. Students on Academic Probation will have until the end of the course to meet these standards. When the above standards are met the student will be removed from Academic Probation. Failure to meet these standards by the end of the probationary period will result in an Academic Termination. Students wishing to appeal this action due to mitigating circumstances must do so in writing within 10 days. Please refer to the appeals process.

### **Dismissal from a Program**

Students are expected to conduct themselves in a professional manner and to act, speak, and show respect to others as in a business environment and online. SystemATECH reserves the right to dismiss students for activities detrimental to themselves, other students, and the school. Reasons for dismissal include, but are not limited to, the following:

- Any Behavior that negatively affects the learning environment.
- Unlawful possession, use, or distribution of illicit drugs and alcohol.
- Providing false information required during the admissions process.
- Violation of the terms and conditions of the Enrollment Agreement.
- Violating the Copyright Infringement Policy
- Falsifying student records.
- Not meeting Satisfactory Academic Progress.
- Failure to attend for three (3) consecutive calendar days.
- Nonpayment of any student loan/arrangement.

If a student is dismissed from the program and wants to re-enter the same program where they left off, they must go through the enrollment process within 90 days of withdraw date. After 90 days would be considered a new enrollment. Approval for reenrollment is at the sole discretion of SystemATECH.

### **Tuition of Charges**

Programs can be combined. (1 These items are non-refundable once the students starts and issued to the student) (2 These items are optional and will be removed from the total cost if opted out or only one charge is needed due to combining courses)

Program Cost	\$8400.00
Tuition	\$4995.00
Curriculum (1)	\$2726.00
Registration Fee (1)	\$100.00
Computer (1,2)	\$579.00

### **Cancellation & Refund Policy**

#### **Policies**

- a. If an applicant is rejected for enrollment or the program is canceled prior to the start of the program a full refund will be made. If an applicant cancels prior to the start of scheduled classes or never attends class (no-show), the institution will issue a full refund of tuition and fees.
- b. Refund amounts must be based on a student's last date of attendance (LDA). When determining the number of weeks completed by the student, the institution may consider a partial week the same as if a whole week were completed, provided the student was present at least one day during the scheduled week.
- c. During the first week of classes, tuition charges withheld must not exceed 10 percent (10%) of the stated tuition up to a maximum of \$1,000.
- d. After the first week and through fifty percent (50%) of the period of financial obligation, tuition charges retained must  
  
not exceed a pro rata portion of tuition for the training period completed, plus ten percent (10%) of the unearned  
  
tuition for the period of training that was not completed, up to a maximum of \$1,000.
- e. After fifty percent (50%) of the period of financial obligation is completed, the institution may retain the full tuition

#### **State of South Carolina**

Refund policy shall provide for a pro rata refund calculation, except that this paragraph will not apply for any student whose date of withdrawal is after the sixty percent point (in time) in the period of enrollment for which the student has been charged.

(1) Pro rata refund is a refund for a student attending the institution for the first time of not less than that portion of the tuition, fees, room and board, and other charges assessed the student equal to the portion of the period of enrollment for which the student has been charged that remains on the last day of attendance by the student, rounded downward to the nearest ten

percent of that period, less any unpaid charges owed for the period of enrollment for which the student has been charged, and less an administrative fee not to exceed one hundred dollars.

(2) The portion of the period of enrollment for which the institution charged that remains shall be determined for credit hour programs, by dividing the total number of weeks comprising the period of enrollment for which the student has been charged into the number of weeks remaining in that period as of the last recorded day of attendance by the student.

(3) After the student's first period of enrollment, a refund as provided in this section, except for room and board, must be made for students who withdraw in subsequent period(s) of enrollment due to mitigating circumstances. Mitigating circumstances are those that directly prohibit pursuit of a program and which are beyond the student's control: serious illness of the student, death in the student's immediate family, or active duty military service, including active duty for training.

(4) After expiration of the seventy-two-hour cancellation privilege, if the student does not attend, not more than one hundred dollars shall be retained by the institution.

(5) All efforts will be made to refund prepaid amounts for books, supplies and other charges unless the student has consumed or used those items and they can no longer be used or sold to new students, or returned by the institution to the supplier as "new" merchandise.

(6) Refunds shall be paid within forty days after the effective date of termination.

### **Career Services and Job Placement Assistance**

SystemATECH provides lifetime career services to students currently enrolled in or graduates of any program at SystemATECH. Career services at SystemATECH consist of but are not limited to:

- (a) Resume preparation assistance
- (b) Cover Letter preparation assistance
- (c) Interview preparation
- (d) Job referrals
- (e) Career counseling
- (f) Application Assistance
- (g) On-site Certification Test Center
- (h) Refresher Courses for Alumni

Students are encouraged to meet with their Career Services Director often to discuss the status of their career search and their training stage and certification level. The Career Services Director will serve as a liaison between the student and employer and continually works to build and improve relationships with local employers in the area. SystemATECH cannot by law guarantee a job upon completion of the

student's program. Background checks are a standard part of the hiring process for many employers. If you have a criminal history, it will impact your job search. SystemATech cannot define that impact for you.

### **Agreement to Arbitrate**

As a condition of enrollment, Student and SystemATECH (the "Parties") agree to resolve through binding and mandatory arbitration any dispute, claim, controversy, cause of action, lawsuit, or proceeding (including, but not limited to, any statutory, tort, contract or equity claim) between Student and SystemATECH or any current or former employee(s) of SystemATECH that arises, arose, or has arisen out of, or is or was in any way related to, this Enrollment Agreement, the subject matter of this Enrollment Agreement, or Student's enrollment, attendance, or educational experience at SystemATECH (individually and collectively, a "Dispute"). The Parties are encouraged to make an initial attempt, in good faith, to resolve the Dispute through SystemATECH's student complaint process or other informal means. If the Dispute is not resolved pursuant to SystemATECH's student complaint process or other informal means, then the Dispute will be resolved by binding arbitration between the Parties.

1. Explanation of Arbitration. Arbitration is the referral of a Dispute to an impartial person (an arbitrator) for a final and binding determination of the Dispute. In agreeing to binding and mandatory arbitration, the Parties voluntarily give up certain rights, including the right to pursue a Dispute in court, the right to a trial by a judge or jury, rights to appeal, and other rights that may be available in a court, such as broader discovery rights. As provided by this arbitration provision, the Parties also give up the right to bring or participate in any class action, collective action, private attorney general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others. If you have any questions about this arbitration provision or the arbitration process, please contact the school.

#### **2. Arbitration Procedures.**

a. The arbitration will be administered by the American Arbitration Association ("AAA") or, in the event the AAA declines or is unable to administer the arbitration, by an arbitration forum or arbitrator that the Parties mutually agree upon. If, after making a reasonable effort, the Parties are unable to agree upon an arbitration forum or arbitrator, a court having proper jurisdiction will appoint an arbitration forum or arbitrator. The arbitration will be conducted in accordance with the AAA's Consumer Arbitration Rules, or the appropriate rules of any alternative arbitration forum selected by the Parties or appointed by a court, except as modified by this arbitration provision. The AAA's Consumer Arbitration Rules and other information regarding the AAA's arbitration procedures are available from the AAA, which can be contacted by mail at 120 Broadway, Floor 21, New York, New York 10271, by telephone at 212-716-5800, or through its website at [www.adr.org](http://www.adr.org).

b. Any Dispute shall be heard by a single arbitrator who is an attorney. As a condition of appointment, the arbitrator shall follow all applicable substantive laws (except as otherwise provided in this arbitration provision), shall agree to the terms of this arbitration provision, and shall lack authority not to enforce the terms of this arbitration provision. The arbitrator shall have



the exclusive authority to determine and adjudicate any issue relating to the existence, formation, validity, enforceability, applicability, or interpretation of this Enrollment Agreement and this arbitration provision, provided, however, that a court shall have exclusive authority to enforce the Class Action Prohibition. The arbitrator's decision shall be accompanied by a reasoned opinion from which there shall be no appeal.

c. The place of arbitration shall be the location (city and state) of the campus where the Dispute arose ("Campus"). Judgment on the arbitral award may be entered exclusively in the location of the Campus. The law of the state of the Campus shall apply.

d. The Parties shall each bear their own attorney's fees, costs, and expenses, except that the costs of arbitration, as set forth in the AAA Consumer Arbitration Rules, shall be determined by the AAA Consumer Arbitration Rules.

e. This arbitration provision governs if there is a conflict with the rules of the arbitral forum.

3. Class Action Prohibition. The scope of the arbitration shall be limited to the Dispute between the Parties. The Parties expressly waive all rights to bring any class action, collective action, private attorney general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others. The arbitrator shall have no authority or jurisdiction to compel, hear, or permit any class action, collective action, private attorney general action, or any other type of action or proceeding in which anyone acts or proposes to act in a representative capacity on behalf of others. By way of illustration and not limitation, neither Student nor SystemATECH can bring a class action against each other or participate in a class action against the other, whether as a named class representative or an absent or putative class member.

4. Federal Arbitration Act. The Parties agree that this Arbitration Agreement involves interstate commerce, and that the enforceability of this Arbitration Agreement shall be governed, both procedurally and substantively, by the Federal

Arbitration Act, 9 U.S.C. §§ 1-9.

5. Severability. If the Class Action Prohibition is found to be illegal or unenforceable as to all or some parts of a Dispute, then those parts will not be arbitrated but will be resolved in court, with the balance of the Dispute resolved through arbitration. If any other part of this arbitration provision is found to be illegal or unenforceable, then that part will be severed; however, the remaining parts shall still apply and shall be interpreted to as nearly as possible achieve the original intent of this arbitration provision.

6. Small Claims Lawsuits Permitted. Notwithstanding anything to the contrary, this arbitration provision does not prevent the Parties from filing a lawsuit in any small claims court of competent jurisdiction.

7. Inapplicability to Borrower Defense to Repayment Applications to U.S. Department of Education. SystemATECH cannot require Student to participate in arbitration or any internal dispute resolution process offered by SystemATECH prior to filing a borrower defense to

repayment application with the U.S. Department of Education pursuant to 34 C.F.R. § 685.206(e); SystemATECH cannot, in any way, require Student to limit, relinquish, or waive his or her ability to pursue filing a borrower defense claim, pursuant to § 685.206(e) at any time; and any arbitration required by this pre-dispute arbitration agreement tolls the limitations period for filing a borrower defense to repayment application pursuant to § 685.206(e)(6)(ii).

### **Software Piracy, Copyright Laws, and Internet Use**

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject those in violation to civil and criminal liabilities.

#### **Potential Civil and Criminal Sanctions for Copyright Infringement:**

- In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or

“statutory” damages affixed at not less than \$750 and not more than \$30,000 per work infringed.

- For “willful” infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also

assess costs and attorneys’ fees. For details, see Title 17, United States Code, Sections 504, 505.

- Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense. For more information, please see the website of the U.S. Copyright Office at [www.copyright.gov](http://www.copyright.gov).

SystemATECH strictly prohibits the piracy of software, and the violation of piracy and copyright laws and reserves the right to dismiss students from the program who are found to be using the equipment to illegally copy software or other copyrighted materials for their own gain. No student should attempt to copy, make available, or distribute copies of copyrighted material. Inappropriate conduct and violations for willfully violating this policy will be reviewed and addressed by Site Coordinator based on the campus in which the student is enrolled. Academic consequences for willfully violating copyright laws include but are not limited to: 1. Receiving a grade of 0 for a test or assignment where the violation took place. 2. Receiving a grade of 0 in the course where the violation took place. 3. Dismissed from the Program.

Students will have access to the Internet for educational purposes only. Surfing the Internet or using any Internet based application during class is strictly prohibited, including all social networking sites and all web-based messenger services, unless specifically required by labs and the instructor. Student recording of classroom lectures, discussions, and/or activities is not

permitted unless a student has an approved accommodation prior to starting their full program. It is expected that all students regularly and actively participate in their scheduled classroom sessions to best engage with the learning material, openly explore with their co-student key concepts, and have their questions answered for understanding in real-time.

### **Confidentiality of Student Records**

The policy of SystemATECH is to comply with the Family Educational Rights and Privacy Act (FERPA) and, in so doing, protect the confidentiality of personally identifiable educational records of students and former students. The student has the following rights: the right to inspect and review his/her education records within 45 days of the day the school receives a request for access; the right to request an amendment of his/her education records that the student believes are inaccurate or misleading; the right to consent to disclosures of personal identifiable information (pii) contained in his/her education records except to the extent that FERPA authorizes disclosure without consent; and the right to file a complaint with the U.S. Department of Education concerning alleged failures by SystemATECH to comply with the requirements of FERPA. A health and safety exception permits the disclosure of pii from a student's record to appropriate parties if knowledge of the information is necessary to protect the health or safety of the student or other individuals from an immediate threat.

### **Holidays Observed**

- New Year's Day
- Martin Luther King Jr. Day
- President's Day
- Juneteenth
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas Eve

Christmas Day

### **Program(s) Offered**



## **CompTIA A+ Certification - Core 1 Course Outline**

---

## Overview

The course shown here was designed for the new exam. CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is the only industry recognized credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment. It is trusted by employers around the world to identify the go-to person in end point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

The Official CompTIA® A+® Core 1 (course provides the background knowledge and skills you will require to be a successful A+ technician. It will help you prepare to take the CompTIA A+ Core Series certification examination, in order to become a CompTIA A+ Certified Professional.

## Already have some IT experience?

Individuals with previous IT experience, should consider taking our Boot Camp A+ class that covers the content from both our A+ Hardware class and our A+ Operating System/Security class. That 10 days of material is delivered in a 5-day format and is supplemented with after-hours exam prep sessions that help fill in any gaps that you have. For more information on this classes schedule an appointment with us here:

### \*\*\* NOTE: This class also available in eLearning Format \*\*\*

Too busy at work to miss 5 days out of the office to take this class? Consider the CompTIA On-Demand version of this course. Watch videos, take the same hands-on labs, access an online expert, and study at on your own time, at your own pace. For details on this alternative format, go to [CompTIA On-Demand A+ Certification Training](#) CompTIA A+ Core 1 and Core 2 Includes live/online instruction from a certified CompTIA instructor, course materials, practice exams, 2 certification exams and complimentary lunch and refreshments.

Tuition \$4995.00

8 weeks course

Hours: 198

### \*\*\* Note Regarding Exam Preparation \*\*\*

#### Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SYSTEMATECH Training Department.

## Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many addition hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA

or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

### **Course Objectives**

In this course, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers and digital devices. You will:

Install and configure PC system unit components and peripheral devices.

Install, configure, and troubleshoot display and multimedia devices.

Install, configure, and troubleshoot storage devices.

Install, configure, and troubleshoot internal system components.

Explain network infrastructure concepts.

Configure and troubleshoot network connections.

Implement client virtualization and cloud computing.

Support and troubleshoot laptops.

Support and troubleshoot mobile devices.

Install, configure, and troubleshoot print devices.

### **Students**

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 1 220-1101 Certification Exam.

### **Prerequisites**

To ensure your success in this course, you should have experience with basic computer user skills, be able to complete tasks in a Microsoft® Windows® environment, be able to search for, browse, and access information on the Internet, and have basic knowledge of computing concepts. You can obtain this level of skills and knowledge by taking the following official CompTIA courses:

The Official CompTIA® IT Fundamentals+ (Exam FC0-U61)

Note: The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: <https://certification.comptia.org/training/exam-objectives>

### **Course Outline**

#### **Lesson 1: Installing and Configuring PC Components**

Topic A: Use Appropriate Safety Procedures

Topic B: PC Components

Topic C: Common Connection Interfaces

Topic D: Install Peripheral Devices

Topic E: Troubleshooting Methodology

#### **Lesson 2: Installing, Configuring, and Troubleshooting Display and Multimedia Devices**

Topic A: Install and Configure Display Devices

Topic B: Troubleshoot Display Devices

Topic C: Install and Configure Multimedia Devices

### **Lesson 3: Installing, Configuring, and Troubleshooting Storage Devices**

Topic A: Install System Memory

Topic B: Install and Configure Mass Storage Devices

Topic C: Install and Configure Removable Storage

Topic D: Configure RAID

Topic E: Troubleshoot Storage Devices

### **Lesson 4: Installing, Configuring, and Troubleshooting Internal System Components**

Topic A: Install and Upgrade CPUs

Topic B: Configure and Update BIOS/UEFI

Topic C: Install Power Supplies

Topic D: Troubleshoot Internal System Components

Topic E: Configure a Custom PC

### **Lesson 5: Network Infrastructure Concepts**

Topic A: Wired Networks

Topic B: Network Hardware Devices

Topic C: Wireless Networks

Topic D: Internet Connection Types

Topic E: Network Configuration Concepts

Topic F: Network Services

### **Lesson 6: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

Topic F: Install and Configure IoT Devices

### **Lesson 7: Implementing Client Virtualization and Cloud Computing**

Topic A: Configure Client-Side Virtualization

Topic B: Cloud Computing Concepts

### **Lesson 8: Supporting and Troubleshooting Laptops**

Topic A: Use Laptop Features

Topic B: Install and Configure Laptop Hardware

Topic C: Troubleshoot Common Laptop Issues

### **Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Mobile Device Types

Topic B: Connect and Configure Mobile Device Accessories

Topic C: Configure Mobile Device Network Connectivity

Topic D: Support Mobile Apps

## **Lesson 10: Installing, Configuring, and Troubleshooting Print Devices**

Topic A: Maintain Laser Printers

Topic B: Maintain Inkjet Printers

Topic C: Maintain Impact, Thermal, and 3D Printers

Topic D: Install and Configure Printers

Topic E: Troubleshoot Print Device Issues

Topic F: Install and Configure Imaging Devices)

Copyright SystemATech Co. 2020



## CompTIA A+

### CompTIA A+ Certification - Core 2 Course Outline

---

#### Overview

The course shown here was designed for the new exam. CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is the only industry recognized credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment. It is trusted by employers around the world to identify the go-to person in end point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

The Official CompTIA® A+® Core 2 course provides the background knowledge and skills you will require to be a successful A+ technician. It will help you prepare to take the CompTIA A+ Core Series certification examination in order to become a CompTIA A+ Certified Professional.

#### Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many addition hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

#### Course Objectives

In this course, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. You will:

- Support operating systems.
- Install, configure, and maintain operating systems.
- Maintain and troubleshoot Microsoft Windows.
- Configure and troubleshoot network connections.
- Manage users, workstations, and shared resources.
- Implement physical security.
- Secure workstations and data.
- Troubleshoot workstation security issues.
- Support and troubleshoot mobile devices.
- Implement operational procedures.

#### Target Student

This course is designed for individuals who have basic computer user skills and who are interested



in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 2 220-1102 Certification Exam.

### **Prerequisites**

To ensure your success in this course, you should attend the CompTIA A+ Certification - Exam 220-1101 Core 1 class or have equivalent experience :

[CompTIA A+ Certification - Exam 220-1101 Core 1](#)

Note: The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page:

[CompTIA A+ Certification Exam Objectives](#)

### **Course Outline**

#### **Lesson 1: Supporting Operating Systems**

Topic A: Identify Common Operating Systems

Topic B: Use Windows Features and Tools

Topic C: Manage Files in Windows

Topic D: Manage Disks in Windows

Topic E: Manage Devices in Windows

#### **Lesson 2: Installing, Configuring, and Maintaining Operating Systems**

Topic A: Configure and Use Linux

Topic B: Configure and Use macOS

Topic C: Install and Upgrade Operating Systems

Topic D: Maintain OSs

#### **Lesson 3: Maintaining and Troubleshooting Microsoft Windows**

Topic A: Install and Manage Windows Applications

Topic B: Manage Windows Performance

Topic C: Troubleshoot Windows

#### **Lesson 4: Configuring and Troubleshooting Networks**

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

#### **Lesson 5: Managing Users, Workstations, and Shared Resources**

Topic A: Manage Users

Topic B: Configure Shared Resources

Topic C: Configure Active Directory Accounts and Policies

#### **Lesson 6: Security Concepts**

Topic A: Logical Security Concepts

Topic B: Threats and Vulnerabilities  
Topic C: Physical Security Measures

### **Lesson 7: Securing Workstations and Data**

Topic A: Implement Security Best Practices  
Topic B: Implement Data Protection Policies  
Topic C: Protect Data During Incident Response

### **Lesson 8: Troubleshooting Workstation Security Issues**

Topic A: Detect, Remove, and Prevent Malware  
Topic B: Troubleshoot Common Workstation Security Issues

### **Lesson 9: Supporting and Troubleshooting Mobile Devices**

Topic A: Secure Mobile Devices  
Topic B: Troubleshoot Mobile Device Issues

### **Lesson 10: Implementing Operational Procedures**

Topic A: Use Appropriate Safety Procedures  
Topic B: Environmental Impacts and Controls  
Topic C: Create and Maintain Documentation  
Topic D: Use Basic Change Management Best Practices  
Topic E: Implement Disaster Prevention and Recovery Methods  
Topic F: Basic Scripting Concepts  
Topic G: Professionalism and Communication

### **Appendix A: Mapping Course Content to CompTIA® A+® Core 2 (Exam 220-1102)**



## **CompTIA Network+ Certification Training Course Outline**

---

## Overview

The CompTIA® Network+® course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. If you are pursuing a CompTIA technical certification path, the CompTIA® A+® certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

The CompTIA® Network+® course can benefit you in two ways. It can assist you if you are preparing to take the CompTIA Network+ examination (Exam N10-007). Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

### \*\*\* NOTE: This class also available in On-Demand, eLearning Format \*\*\*

Too busy at work to miss 5 days out of the office to take this class? Consider the CompTIA On-Demand version of this course. Watch videos, take the same hands-on labs, access an online expert 24/7, and study at on your own time, at your own pace.

Tuition \$4995.00

8 weeks course

Hours: 198

For details on this alternative format, go to  
[CompTIA On-Demand Network+ Certification Training](#)

## Network+ Exam Objectives

[Click here for Network+ Exam Objectives](#)

## Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SYSTEMATECH Training Centers.

## Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many addition hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

## Course Objectives

In this course, you will describe the major networking technologies and systems of modern networks, and be able to configure, manage, and troubleshoot modern networks.

You will:

- Identify basic network theory concepts and major network communications methods.
- Describe bounded network media.
- Identify unbounded network media.
- Identify the major types of network implementations.
- Identify TCP/IP addressing and data delivery methods.
- Implement routing technologies.
- Identify the major services deployed on TCP/IP networks.
- Identify the infrastructure of a WAN implementation.
- Identify the components used in cloud computing and virtualization.
- Describe basic concepts related to network security.
- Prevent security breaches.
- Respond to security incidents.
- Identify the components of a remote network implementation.
- Identify the tools, methods, and techniques used in managing a network.
- Describe troubleshooting of issues on a network.

### **Target Audience**

CompTIA Network+ is the first certification IT professionals specializing in network administration and support should earn. Network+ is aimed at IT professionals with job roles such as network administrator, network technician, network installer, help desk technician and IT cable installer.

### **Course Prerequisites**

Students should meet the following criteria prior to taking the course:

Taken and passed both CompTIA A+ Certification exams or have 9-12 months knowledge and experience of IT administration

Be able to configure and support PC, laptop, mobile (smartphone / tablet), and print devices

Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers)

Configure and manage users, groups, and shared resources in a simple SOHO network

Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls

### **Course Outline**

#### **Module 1 / Local Area Networks**

Topologies and the OSI Model • Key Features of Networks • Network Topologies • The OSI Model • Physical Layer • Data Link Layer • Network Layer • Transport Layer • Upper Layers • OSI Model Summary • Labs • VM Orientation

Ethernet • Transmission Media • Media Access Control • Broadcast Domains • Ethernet Frames • Ethernet Deployment Standards • MAC Addressing • Address Resolution Protocol (ARP) • Packet Sniffers • Labs • Configuring Ethernet Networking

Hubs, Bridges, and Switches • Hubs and Bridges • Switches • Switch Interface Configuration • Spanning Tree Protocol (STP) • Power over Ethernet (PoE)

Infrastructure and Design • Network Infrastructure Implementations • Planning an Enterprise Campus Network • Network Hierarchy and Distributed Switching • Software Defined Networking • Planning a SOHO Network • TCP/IP Protocol Suite

Policies and Best Practices • Procedures and Standards • Safety Procedures • Incident Response Policies • Security and Data Policies • Password Policy • Employee Policies

## **Module 2 / IP Addressing**

Internet Protocol • IPv4 • IPv4 Address Structure • Subnet Masks • IP Routing Basics • ipconfig / ifconfig • ICMP and ping • Labs • Configuring IPv4 Networking  
IPv4 Addressing • IPv4 Addressing Schemes • Classful Addressing • Public versus Private Addressing • Subnetting and Classless Addressing • Planning an IPv4 Addressing Scheme • Public Internet Addressing • Variable Length Subnet Masks (VLSM) • Labs • Configuring IPv4 Subnets  
IPv6 Addressing • IPv6 Address Format • IPv6 Addressing Schemes • IPv6 Address Autoconfiguration • Migrating to IPv6 • Labs • Configuring IPv6 Networking  
DHCP and APIPA • IPv4 Address Autoconfiguration • Configuring DHCP • DHCPv6 • Labs • Configuring Address Autoconfiguration

## **Module 3 / Internetworking**

Routing • Routing Basics • Routing Algorithms and Metrics • Dynamic Routing Protocols • Administrative Distance and Route Redistribution • IPv4 and IPv6 Internet Routing • High Availability Routing • Installing and Configuring Routers • Routing Troubleshooting Tools • Labs • Configuring Routing  
TCP and UDP • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • TCP and UDP Ports • Port Scanners • Protocol Analyzers • Labs • TCP and Port Scanning  
Name Resolution and IPAM • Host Names and FQDNs • Domain Name System • Configuring DNS Servers • Resource Records • Name Resolution Tools • IP Address Management (IPAM) • Labs • Configuring Name Resolution and IPAM  
Monitoring and Scanning • Performance Monitoring • Network Monitoring Utilities • Logs and Event Management • Simple Network Management Protocol • Analyzing Performance Metrics • Patch Management • Vulnerability Scanning • Labs • Performance Testing and Monitoring  
Network Troubleshooting • Troubleshooting Procedures • Identifying the Problem • Establishing a Probable Cause • Establishing a Plan of Action • Troubleshooting Hardware Failure Issues • Troubleshooting Addressing Issues • Troubleshooting DHCP Issues • Troubleshooting Name Resolution • Troubleshooting Services

## **Module 4 / Applications and Security**

Applications and Services • TCP/IP Services • HTTP and Web Servers • SSL / TLS and HTTPS • Email (SMTP / POP / IMAP) • Voice Services (VoIP and VTC) • Real-time Services Protocols • Quality of Service • Traffic Shaping • Bottlenecks and Load Balancing • Multilayer Switches • Labs • Configuring Application Protocols  
Virtualization, SAN, and Cloud Services • Virtualization Technologies • Network Storage Types • Fibre Channel and InfiniBand • iSCSI • Cloud Computing • Configuring Cloud Connectivity  
Network Security Design • Security Basics • Common Networking Attacks • Network Segmentation and DMZ • Virtual LANs (VLAN) • VLAN Trunks • Network Address Translation (NAT) • Device and Service Hardening • Honeypots and Penetration Tests  
Network Security Appliances • Basic Firewalls • Stateful Firewalls • Deploying a Firewall • Configuring a Firewall • Deploying a Proxy • Intrusion Detection Systems (IDS) • Denial of Service • Labs • Configuring a NAT Firewall  
Authentication and Endpoint Security • Authentication and Access Controls • Social Engineering • Authentication Technologies • PKI and Digital Certificates • Local Authentication • RADIUS and TACACS+ • Directory Services • Endpoint Security • Network Access Control • Labs • Secure Appliance Administration

## **Module 5 / Operations and Infrastructure**

Network Site Management • Network Cabling Solutions • Distribution Frames • Change and

Configuration Management • Network Documentation and Diagrams • Labeling • Physical Security Devices • Business Continuity and Disaster Recovery • Network Link Management • Power Management • Backup Management • Labs • Network Inventory Management  
Installing Cabled Networks • Twisted Pair Cable (UTP / STP / ScTP) • Twisted Pair Connectors • Wiring Tools and Techniques • Cable Testing Tools • Troubleshooting Wired Connectivity • Other Copper Cable Types • Fiber Optic Cable and Connectors • Transceivers and Media Converters  
Installing Wireless Networks • Wireless Standards (IEEE 802.11) • Wireless Network Topologies • Wireless Site Design • Troubleshooting Wireless Connectivity • Wireless Security • Wi-Fi Authentication • Extensible Authentication Protocol • Troubleshooting Wireless Security • Wireless Controllers  
Installing WAN Links • Wide Area Networks (WAN) • Telecommunications Networks • Modern Telecommunications Networks • Local Loop Services • Installing WAN Links • Wireless WAN Services • Internet of Things  
Configuring Remote Access • Remote Access Services (RAS) • MPLS and PPP • SIP Trunks • Virtual Private Networks (VPN) • SSL / TLS / DTLS VPNs • IPsec • Internet Key Exchange / ISAKMP • Remote Access Servers • Remote Administration Tools • Managing Network Appliances • Remote File Access • Labs • Configuring Secure Access Channels • Configuring a Virtual Private Network

Exam Code@ N10-007



# CompTIA Security+ Certification Training Course Outline

---

## Overview

CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator and network administrator.

## Course Prerequisites

Students should meet the following criteria prior to taking the course:

Recommended that students have taken CompTIA Network+ certification course and exam, together with 24 months experience in networking support/IT administration

Know the function and basic features of the components of a PC

Use Windows Server to create and manage files and use basic administrative features (Explorer, Control Panel, Management Consoles, Command Line Tools)

Operate the Linux OS using basic command-line tools

Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers)

Understand TCP/IP addressing, core protocols, and troubleshooting tools

## Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SystemATech Training Centers.

## Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many additional hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

Tuition \$4995.00

8 weeks course

Hours: 198

## Course Outline

### Module 1 / Threats, Attacks, and Vulnerabilities

Indicators of Compromise • Why is Security Important? • Security Policy • Threat Actor Types • The Kill Chain • Social Engineering • Phishing • Malware Types • Trojans and Spyware • Open Source Intelligence • Labs • VM Orientation • Malware Types

Critical Security Controls • Security Control Types • Defense in Depth • Frameworks and Compliance • Vulnerability Scanning and Pen Tests • Security Assessment Techniques • Pen Testing Concepts • Vulnerability Scanning Concepts • Exploit Frameworks • Lab • Using Vulnerability Assessment Tools

Security Posture Assessment Tools • Topology Discovery • Service Discovery • Packet Capture • Packet Capture Tools • Remote Access Trojans • Honeypots and Honeynets • Labs • Using Network Scanning Tools 1 • Using Network Scanning Tools 2 • Using Steganography Tools

Incident Response • Incident Response Procedures • Preparation Phase • Identification Phase • Containment Phase • Eradication and Recovery Phases

## **Module 2 / Identity and Access Management**

Cryptography • Uses of Cryptography • Cryptographic Terminology and Ciphers • Cryptographic Products • Hashing Algorithms • Symmetric Algorithms • Asymmetric Algorithms • Diffie-Hellman and Elliptic Curve • Transport Encryption • Cryptographic Attacks • Lab • Implementing Public Key Infrastructure

Public Key Infrastructure • PKI Standards • Digital Certificates • Certificate Authorities • Types of Certificate • Implementing PKI • Storing and Distributing Keys • Key Status and Revocation • PKI Trust Models • PGP / GPG • Lab • Deploying Certificates and Implementing Key Recovery

Identification and Authentication • Access Control Systems • Identification • Authentication • LAN Manager / NTLM • Kerberos • PAP, CHAP, and MS-CHAP • Password Attacks • Token-based Authentication • Biometric Authentication • Common Access Card • Lab • Using Password Cracking Tools

Identity and Access Services • Authorization • Directory Services • RADIUS and TACACS+ • Federation and Trusts • Federated Identity Protocols

Account Management • Formal Access Control Models • Account Types • Windows Active Directory • Creating and Managing Accounts • Account Policy Enforcement • Credential Management Policies • Account Restrictions • Accounting and Auditing • Lab • Using Account Management Tools

## **Module 3 / Architecture and Design (1)**

Secure Network Design • Network Zones and Segments • Subnetting • Switching Infrastructure • Switching Attacks and Hardening • Endpoint Security • Network Access Control • Routing Infrastructure • Network Address Translation • Software Defined Networking • Lab • Implementing a Secure Network Design

Firewalls and Load Balancers • Basic Firewalls • Stateful Firewalls • Implementing a Firewall or Gateway • Web Application Firewalls • Proxies and Gateways • Denial of Service Attacks • Load Balancers • Lab • Implementing a Firewall

IDS and SIEM • Intrusion Detection Systems • Configuring IDS • Log Review and SIEM • Data Loss Prevention • Malware and Intrusion Response • Lab • Using an Intrusion Detection System

Secure Wireless Access • Wireless LANs • WEP and WPA • Wi-Fi Authentication • Extensible Authentication Protocol • Additional Wi-Fi Security Settings • Wi-Fi Site Security • Personal Area Networks



Physical Security Controls • Site Layout and Access • Gateways and Locks • Alarm Systems • Surveillance • Hardware Security • Environmental Controls

#### **Module 4 / Architecture and Design (2)**

Secure Protocols and Services • DHCP Security • DNS Security • Network Management Protocols • HTTP and Web Servers • SSL / TLS and HTTPS • Web Security Gateways • Email Services • S/MIME • File Transfer • Voice and Video Services • VoIP • Labs • Implementing Secure Network Addressing Services • Configuring a Secure Email Service

Secure Remote Access • Remote Access Architecture • Virtual Private Networks • IPSec • Remote Access Servers • Remote Administration Tools • Hardening Remote Access Infrastructure • Lab • Implementing a Virtual Private Network

Secure Systems Design • Trusted Computing • Hardware / Firmware Security • Peripheral Device Security • Secure Configurations • OS Hardening • Patch Management • Embedded Systems • Security for Embedded Systems

Secure Mobile Device Services • Mobile Device Deployments • Mobile Connection Methods • Mobile Access Control Systems • Enforcement and Monitoring

Secure Virtualization and Cloud Services • Virtualization Technologies • Virtualization Security Best Practices • Cloud Computing • Cloud Security Best Practices

#### **Module 5 / Risk Management**

Forensics • Forensic Procedures • Collecting Evidence • Capturing System Images • Handling and Analyzing Evidence • Lab • Using Forensic Tools

Disaster Recovery and Resiliency • Continuity of Operations Plans • Disaster Recovery Planning • Resiliency Strategies • Recovery Sites • Backup Plans and Policies • Resiliency and Automation Strategies

Risk Management • Business Impact Analysis • Identification of Critical Systems • Risk Assessment • Risk Mitigation

Secure Application Development • Application Vulnerabilities • Application Exploits • Web Browser Exploits • Secure Application Design • Secure Coding Concepts • Auditing Applications • Secure DevOps • Lab • Identifying a Man-in-the-Browser Attack

Organizational Security • Corporate Security Policy • Personnel Management Policies • Interoperability Agreements • Data Roles • Data Sensitivity Labeling and Handling • Data Wiping and Disposal • Privacy and Employee Conduct Policies • Security Policy Training

Exam Code# **(SY0-601)**



---

### Overview

While IT professionals today are expected to understand some basic cloud terminology and concepts, and most have likely worked with public cloud or Software-as-a-Service solutions, the ability to analyze, evaluate, design, and test cloud computing solutions is a difficult skillset to find, and it is currently in high demand. In this course, you will apply the skills required to evaluate and implement standard deployments. You will implement, maintain, and deliver cloud technologies including network, storage, and virtualization technologies to create cloud solutions. You will manage workload migrations, manage cloud vendors to control costs, use automation and orchestration to bring business value from cloud solutions, and ensure security of cloud implementations through the use of cybersecurity best practices. In addition, this course prepares you to pass the CompTIA® Cloud+® exam and earn the corresponding certification.

### Course Objectives

In this course, you will deploy, test, secure, manage, optimize, and troubleshoot a cloud solution. You will:

- Prepare to deploy cloud solutions.
- Deploy a pilot project.
- Test a pilot project deployment.
- Design a secure network for cloud deployment.
- Determine CPU and memory sizing for cloud deployments.
- Determine storage requirements for cloud deployments.
- Plan Identity and Access Management for cloud deployments.
- Analyze workload characteristics to ensure successful migration to the cloud.
- Secure systems to meet access requirements.
- Maintain cloud systems.
- Implement backup, restore, and business continuity measures.
- Analyze cloud systems for required performance.
- Analyze cloud systems for anomalies and growth forecasting.
- Troubleshoot deployment, capacity, automation, and orchestration issues.
- Troubleshoot connectivity issues.
- Troubleshoot security issues.

Tuition \$4995.00                      8 weeks course                      Hours: 198

### Target Student

This course is designed for IT professionals who wish to develop cloud computing skills to enable them to move IT workloads to the cloud and integrate products and services from different providers and industries. The focus is to ensure that cloud deployments are secure, that automation and orchestration are used effectively to bring business value from the cloud, and that costs are controlled through effective management of cloud vendors.

This course is also designed for students who are preparing to take the CompTIA Cloud+ certification exam CV0-002, or who plan to use Cloud+ as the foundation for more advanced cloud certifications or career roles. A criminal record may prevent the student from obtaining employment in the field.

### **Prerequisites**

To ensure your success in this course, you should have 24-36 months' experience with IT networking, network storage, and data center administration. You should also have familiarity with any major hypervisor technologies for server virtualization, basic knowledge of common cloud service models, and common cloud deployment models.

### **Course Content**

#### **Lesson 1: Preparing to Deploy Cloud Solutions**

Topic A: Describe Interaction of Cloud Components and Services

Topic B: Describe Interaction of Non-cloud Components and Services

Topic C: Evaluate Existing Components and Services for Cloud Deployment

Topic D: Evaluate Automation and Orchestration Options

Topic E: Prepare for Cloud Deployment

#### **Lesson 2: Deploying a Pilot Project**

Topic A: Manage Change in a Pilot Project

Topic B: Execute Cloud Deployment Workflow

Topic C: Complete Post-Deployment Configuration

#### **Lesson 3: Testing Pilot Project Deployments**

Topic A: Identify Cloud Service Components for Testing

Topic B: Test for High Availability and Accessibility

Topic C: Perform Deployment Load Testing

Topic D: Analyze Test Results

#### **Lesson 4: Designing a Secure and Compliant Cloud Infrastructure**

Topic A: Design Cloud Infrastructure for Security

Topic B: Determine Organizational Compliance Needs

#### **Lesson 5: Designing and Implementing a Secure Cloud Environment**

Topic A: Design Virtual Network for Cloud Deployment

Topic B: Determine Network Access Requirements

Topic C: Secure Networks for Cloud Interaction

Topic D: Manage Cloud Component Security

Topic E: Implement Security Technologies

#### **Lesson 6: Planning Identity and Access Management for Cloud Deployments**

Topic A: Determine Identity Management and Authentication Technologies

Topic B: Plan Account Management Policies for the Network and Systems

Topic C: Control Access to Cloud Objects

Topic D: Provision Accounts

**Lesson 7: Determining CPU and Memory Sizing for Cloud Deployments**

Topic A: Determine CPU Size for Cloud Deployment

Topic B: Determine Memory Size for Cloud Deployment

**Lesson 8: Determining Storage Requirements for Cloud Deployments**

Topic A: Determine Storage Technology Requirements

Topic B: Select Storage Options for Deployment

Topic C: Determine Storage Access and Provisioning Requirements

Topic D: Determine Storage Security Options

**Lesson 9: Analyzing Workload Characteristics to Ensure Successful Migration**

Topic A: Determine the Type of Cloud Deployment to Perform

Topic B: Manage Virtual Machine and Container Migration

Topic C: Manage Network, Storage, and Data Migration

**Lesson 10: Maintaining Cloud Systems**

Topic A: Patch Cloud Systems

Topic B: Design and Implement Automation and Orchestration for Maintenance

**Lesson 11: Implementing Backup, Restore, Disaster Recovery, and Business Continuity Measures**

Topic A: Back Up and Restore Cloud Data

Topic B: Implement Disaster Recovery Plans

Topic C: Implement Business Continuity Plans

**Lesson 12: Analyzing Cloud Systems for Performance**

Topic A: Monitor Cloud Systems to Measure Performance

Topic B: Optimize Cloud Systems to Meet Performance Criteria

**Lesson 13: Analyzing Cloud Systems for Anomalies and Growth Forecasting**

Topic A: Monitor for Anomalies and Resource Needs

Topic B: Plan for Capacity

Topic C: Create Reports on Cloud System Metrics

**Lesson 14: Troubleshooting Deployment, Capacity, Automation, and Orchestration Issues**

Topic A: Troubleshoot Deployment Issues

Topic B: Troubleshoot Capacity Issues

Topic C: Troubleshoot Automation and Orchestration Issues

**Lesson 15: Troubleshooting Connectivity Issues**

Topic A: Identify Connectivity Issues

Topic B: Troubleshoot Connectivity Issues

**Lesson 16: Troubleshooting Security Issues**

Topic A: Troubleshoot Identity and Access Issues

Topic B: Troubleshoot Attacks Topic C: Troubleshoot Other Security Issues

## **CompTIA CYSA+ Exam Code (CS0-002)**

### **Overview:**

This course is intended for individuals wishing to obtain the qualification of a CompTIA CySA+ Cybersecurity Analyst Certification. CompTIA's CySA+ Certification is an intermediate-level certificate for IT professionals with previous experience working in IT security. The CompTIA CySA+ examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam certifies that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis. In turn, these skills will be used to interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

### **Certification track:**

This courseware bears the seal of CompTIA Approved Quality Content. The seal signifies that this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple elearning tools to help increase coverage of the learning objectives. The contents of this training material were created for the CompTIA CYSA+ Cybersecurity Analyst Certification CS0-002 exam covering the 2020 Edition certification exam objectives.

### **Additional Notes Regarding CompTIA Certification Exams:**

As with most professional IT certifications, many additional hours of study are required before the class and after the class. Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

Tuition \$4995.00

8 weeks course

Hours: 198

### **Target audience and course prerequisites:**

CompTIA CYSA+ certification is aimed at IT professionals with (or seeking) job roles such as IT Security Analyst, Security Operations Center (SOC) Analyst, Vulnerability Analyst, Cybersecurity Specialist, Threat Intelligence Analyst, and Security Engineer.

### **Ideally, you should have successfully completed:**

CompTIA Network+ Certification AND Security+ Certification courses or have equivalent knowledge before attending this training.

Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.
- Identify network attack strategies and defenses.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

### **Course Outline:**

#### Module 1 – Threat Management 1

- Cybersecurity Analysts
- Cybersecurity Roles and Responsibilities
- Frameworks and Security Controls
- Risk Evaluation
- Penetration Testing Processes
- Reconnaissance Techniques
- The Kill Chain
- Open Source Intelligence
- Social Engineering
- Topology Discovery
- Service Discovery
- OS Fingerprinting

#### Module 2 – Threat Management 2

- Security Appliances
- Configuring Firewalls
- Intrusion Detection and Prevention
- Configuring IDS
- Malware Threats
- Configuring Anti-virus Software
- Sysinternals
- Enhanced Mitigation Experience Toolkit
- Logging and Analysis
- Packet Capture
- Packet Capture Tools
- Monitoring Tools
- Log Review and SIEM
- SIEM Data Outputs

- SIEM Data Analysis
- Point-in-Time Data Analysis

### Module 3 – Vulnerability Management

- Managing Vulnerabilities
  - Vulnerability Management Requirements
  - Asset Inventory
  - Data Classification
  - Vulnerability Management Processes
  - Vulnerability Scanners
  - Microsoft Baseline Security Analyzer
  - Vulnerability Feeds and SCAP
  - Configuring Vulnerability Scans
  - Vulnerability Scanning Criteria
  - Exploit Frameworks
- Remediating Vulnerabilities
  - Analyzing Vulnerability Scans
  - Remediation and Change Control
  - Remediating Host Vulnerabilities
  - Remediating Network Vulnerabilities
  - Remediating Virtual Infrastructure Vulnerabilities
- Secure Software Development
  - Software Development Lifecycle
  - Software Vulnerabilities
  - Software Security Testing
  - Interception Proxies
  - Web Application Firewalls
  - Source Authenticity
  - Reverse Engineering

### Module 4 – Cyber Incident Response

- Incident Response
  - Incident Response Processes
  - Threat Classification
  - Incident Severity and Prioritization
  - Types of Data
- Forensics Tools
  - Digital Forensics Investigations
  - Documentation and Forms
  - Digital Forensics Crime Scene
  - Digital Forensics Kits
  - Image Acquisition

- Password Cracking
- Analysis Utilities
- Incident Analysis and Recovery
- Analysis and Recovery Frameworks
- Analyzing Network Symptoms
- Analyzing Host Symptoms
- Analyzing Data Exfiltration
- Analyzing Application Symptoms
- Using Sysinternals
- Containment Techniques
- Eradication Techniques
- Validation Techniques
- Corrective Actions

## Module 5 – Security Architecture

- Secure Network Design
- Network Segmentation
- Blackholes, Sinkholes, and Honeypots
- System Hardening
- Group Policies and MAC
- Endpoint Security
- Managing Identities and Access
- Network Access Control
- Identity Management
- Identity Security Issues
- Identity Repositories
- Context-based Authentication
- Single Sign On and Federations
- Exploiting Identities
- Exploiting Web Browsers and Applications
- Security Frameworks and Policies
- Frameworks and Compliance
- Reviewing Security Architecture
- Procedures and Compensating Controls
- Verifications and Quality Control
- Security Policies and Procedures
- Personnel Policies and Training

**Exam Code (CS0-003)**