INFOSEC INSTITUTE

CATALOG

July 1, 2024 – June 30, 2025

Hampton Inn Cascades | 46331 McClellan Way, Sterling, VA 20165
(804) 439-9990 | support.infosec@cengage.com

Updated August 27, 2024

Table of Contents

General Information

Infosec Institute's Mission

Infosec Institute believes knowledge is power when fighting cybercrime. We empower people to be cyber-safe at work and home and help IT and security professionals achieve their career goals. It's our mission to equip all organizations and individuals with the knowledge, skills and confidence to outsmart cybercrime.

School's Purpose

Infosec Institute's purpose is to empower individuals and organizations with the knowledge and skills needed to securely code, configure and defend critical assets. We fulfill our mission with engaging security awareness training for the general workforce and role-based, hands-on training for cyber professionals from our industry-leading education platforms.

Our training delivery and examination preparation capabilities are developed, tested and maintained by our in-house team of educators, product managers and developers, who work closely with clients and students to ensure our technology platforms meet their specific needs. As a vendor-neutral security education organization, we deliver certification preparation training and practice exams for major IT and security certifying bodies like CompTIA, ISACA and (ISC)2. We have extensive experience developing and delivering engaging and effective content, assessments and exams aligned to established cyber frameworks like the NICE Workforce Framework for Cybersecurity (NICE Framework), while ensuring adherence to certifying body requirements, educational best practices and proven skill validation methodologies.

Guided by the philosophy that knowledge is the best defense against cybercrime, Infosec Institute also provides free cyber education resources to over 1 million readers every month through its Infosec Institute Resources blog, shares career guidance through its Cyber Work Podcast and has awarded over $400,000 in educational opportunities for aspiring cybersecurity professionals through its annual Infosec Institute Accelerate Scholarship Program.

School's Authorizations

Infosec Institute is certified to operate by the State Council of Higher Education for Virginia (SCHEV) 101 N. 14th Street, 10th Floor, James Monroe Building, Richmond, VA 23219; (804) 225-2600

School's Ownership

Infosec Institute is a private post-secondary career school that is owned by Cengage Learning, Inc., a Delaware corporation. Cengage Learning's principal office is located at 5191 Natorp Blvd, Mason, OH 45040. Infosec Institute's Virginia location is at 13800 Coppermine Road, Suite 304, Herndon, VA.

The history and development of the postsecondary school

- 2004: Infosec was founded by CEO Jack Koziol.
- March 2022: Infosec was purchased by Cengage Group.
- March 2023: Cengage Learning, Inc. filed a fictitious name dba with the Virginia State Corporation Commission for Infosec Institute.
- April 2023: Infosec Institute received a Certificate to Operate from the State Council of Higher Education for Virginia (SCHEV).

Description of School's Facilities and Equipment

Infosec Institute programs are conducted in person at hospitality industry meeting rooms utilizing facility audio-visual equipment supplemented with shipments of Infosec Institute equipment including laptops, switches, projectors, microphones, digital whiteboards and internet mobile hotspots, to back up the facility's internet solution.

Information about Infosec Institute's Additional Academic Resources and Library

In addition to the material provided through the designated program enrollment, all Infosec Institute students will have access to the entire program information upon enrollment through 90 days after the program end date. This includes access to a program preparation course to help them get a jumpstart on their certification goals in advance of their program start date.

Additional program resources are available through Infosec Institute's online learning platform featuring hands-on, role-based cybersecurity training resources. It includes:

- Custom certification practice exams
- Skill assessments
- Infosec Institute peer community networking and support

Description of School's Telecommunications Activities

In addition to the in-person program learning experience, the full course information is available through Infosec Institute's online learning platform, accessible through a basic web browser with a login granted upon registration in the course.

Locations

Program Classroom Locations:

Hampton Inn Cascades

46331 McClellan Way
Sterling, VA 20165

Hampton Inn & Suites Washington-Dulles International Airport

22700 Holiday Park Drive
Sterling, VA 20166

Holiday Inn Washington Dulles International Airport

45424 Holiday Drive,
Sterling, VA 20166

Hampton Inn Washington Dulles Airport South

4050 Westfax Drive
Chantilly, VA 20151

School Hours of Operation

8:30am-5:30pm on the days noted per program

Program Schedule: Monday through Friday Programs:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- CompTIA CySA+
- CompTIA CASP+
- EC Council Certified Ethical Hacker
- ISACA CISA
- ISACA CISM
- (ISC)2 CCSP

Program Schedule: Monday - Thursday Programs:

- PMI PMP Exam Prep

Program Schedule: Sunday - Friday Programs:

- ISC(2) CISSP

Program Schedule: Monday - Sunday Programs:

- Microsoft Azure Admin and Security Technologies
- Cisco CCNA Associate and Cyber Ops Associate

School Calendar

Programs are scheduled throughout the calendar year on a rolling 12-month basis. No programs are scheduled the last two weeks of December.

School Holidays

New Year's Day
Martin Luther King Jr. Day
Memorial Day
Independence Day
Labor Day
Thanksgiving Day and the Friday following
Christmas Day

Admission and Entrance Requirements

Admission and Entrance Requirements

Admission to the program is contingent upon being 18 years of age or older, and paying the course enrollment tuition. While there are no hard prerequisites needed in order to take the course, there are recommended actions and prerequisites to take prior to each course that will help ensure student success. Please refer to our course list section for additional information on each course offered.

Admission and enrollment in a course is achieved once the student:

1. provides the school with the needed information to enroll, and
2. successfully processes a full, up-front payment for the course.

The student must adhere to steps 1 and 2 from above by the end of business day, on the day prior to the course start date to ensure adequate time for the student to be enrolled and set up in the class. A student is notified of enrollment through an automated email that allows them to set up their online account for access to the course material and additional library resources.

Since the school is not an accredited institution, and does not offer credit for completion of the course, there is no situation in which Infosec Institute would transfer any documentation of the student's course progress to another education institution for credit transfer. This is fully disclosed in the Infosec Institute Terms and Conditions.

Upon completion of the course, the student will receive a certificate of completion. Completion of the course is documented on the student's file in Infosec Institute's database.

Financial Aid

Infosec Institute does not provide financial aid/assistance.

Student Disclosure Information

Infosec Institute Grading Program and Policy

Infosec Institute's professional training programs are designed for skill and knowledge enhancement for attendees to pursue initial exposure to and advancement within the information security industry, often with professional certification goals.

As such, the grading and progress categories for our programs are defined as “Pass” and “Incomplete” as defined below:

> **PASS:** Attended 100% of the program’s live delivery sessions and participated in all elements of the course including topic discussions and hands-on exercises, where applicable. This is determined by the instructor, in addition to achieving a 90% or greater score on the final program practice exam.
>
> **INCOMPLETE:** Did not reach pass status above. Mitigation can occur through completion of additional associated training material, including but not limited to, review of the class recordings for any missed time and completion of program learning paths. A final practice exam will be made available to the student via Infosec Institute's online tool, at which point their final exam score will denote whether they officially receive a PASS or INCOMPLETE standing.

Standards and Requirements for Satisfactory Progress

Students learn through lecture, practical exercise, and review on pertinent topics to the training program. The program design is to teach industry standards and/or certification entity standards for each applicable domain or topic area. Reinforcement and review is scheduled throughout the duration of the course program to solidify learning objectives. Satisfactory progress is defined as fully attending the live session and participating in topic discussions and hands-on exercises.

The following are actions taken when satisfactory progress is not met:

- Students not in attendance on any program day are contacted via email and phone to determine their status for that day and are advised of their program incomplete status and the steps to mitigate the incomplete status including review of the day’s class recordings and completion of the Infosec Institute Skills associated learning path.
- Students not participating in class or not fully completing hands-on exercises as reported by the instructor are contacted and advised of their pending incomplete status and encouraged to complete any missed

hands-on exercises and engage appropriately in class discussions. A second report by the instructor will place the student in Incomplete status and require completion of the Infosec Institute online associated learning path to mitigate the status.

Required Criteria for Satisfactory Completion of the Program

PASS status is the defined criteria for satisfactory completion of any Infosec Institute program and is achieved through achieving a 90% or greater on the final practice exam held at the last portion of the program. Achieving a 90% on Infosec Institute's final practice exam affirms that the student understands the program material comparable to passing the actual Certification Exam in said program.

Course Completion Status and Certificate

Students are informed during the active course program should they be approaching any element of incomplete status and the steps mitigate.

Students are informed at the end of the course program via email of their status of Pass or Incomplete. Incomplete status attendees are provided with the mitigation steps of reviewing recordings and completing Infosec Institute online learning paths to achieve Pass status through retaking the Practice Exam virtually. Students have complimentary access to the Infosec Institute online learning platform for 90 days after program ends to mitigate any Incomplete status categories.

Course Completion Pass and Graduation: Students are considered to have met program graduation requirements through the achievement of 90% score on the program final practice exam. This metric validates learning objectives and skills necessary to perform at the required standard.

Students' Rights, Privileges and Responsibilities

Students have the right to learn in a professional and inviting adult learning environment, free of distractions and full of encouragement. Students are responsible to fully participate in the course program, complete all hands-on activities and prepare for each day as determined by their instructor.

Student Complaints/Grievances Procedure

Complaint and grievance procedures are as follows. Students are encouraged to submit support cases for any necessary support question, concern, complaint or grievance. Support cases are managed and escalated according to the severity of the concern and resolved by support. For cases not resolved at the support level, escalation occurs to the Client Experience Management team for resolution. A phone discussion with the student by a member of the management/executive team would occur to resolve the concern. Review of course learning objectives, prerequisites, enrollment agreements and other pertinent policy documentation would be reviewed to mitigate the situation.

A student who is unsatisfied with the resolution to his complaint after following the procedure described above, may contact the State Council of Higher Education for Virginia (SCHEV) as a last resort. Contact information for the agency is:

State Council of Higher Education for Virginia (SCHEV)
101 North 14 Street 10th Floor
Richmond, VA 23219
Phone: 804-225-2600
Website: www.schev.edu

A student complaint form can be completed and submitted electronically at:
https://www.schev.edu/students/resources/student-complaints

Non-Retaliation

No retaliation will be permitted against any student who registers a complaint or makes a report of discrimination or harassment, or against anyone who provides testimony as a witness or who otherwise provides assistance to any complaining or reporting employee, or who provides assistance to Infosec Institute in connection with the investigation of any complaint or report. If a student believes they have been retaliated against, they should provide a written or oral complaint to the Infosec Institute Client Experience Management team as soon as possible. The complaint should be as detailed as possible, including the names of individuals involved, the names of any witnesses and any documentary evidence. All complaints of prohibited retaliation that are reported to management will be investigated. Infosec Institute will immediately undertake and direct an effective, thorough and objective investigation of the retaliation allegations. The investigation will be completed and a determination regarding the alleged retaliation will be made. If Infosec Institute determines that an individual has been retaliated against, Infosec Institute shall take effective remedial action appropriate to the circumstances. Infosec Institute shall also take action to deter any future retaliation. If a complaint of retaliation is substantiated, appropriate disciplinary action, up to and including termination, will be taken and Infosec Institute will communicate to the complainant that action has been taken to prevent further retaliation.

Probation, Dismissal and Readmission

Policy on Probationary Period

Infosec Institute has no probation program for its professional training and certification programs.

See Student Disclosure Information documentation on grading and the “incomplete” status, which allows students many options to accomplish their training and certification goals.

Policy on Dismissal from Course

Students are expected to interact in a professional manner that encourages participation with all classmates.

Within the information security industry, one is expected to have the highest level of integrity and will often be required to acknowledge such when applying for roles and certifications. As such, Infosec Institute expects the same within the learning environment offered throughout our courses.

Infosec Institute holds to extremely high standards of honesty, integrity, performance and conduct. We expect our students to exemplify these characteristics as they are essential for professional success. Infosec Institute expects its students to have careful regard for our standards and avoid even the appearance of dishonesty or misconduct.

If the student does not hold to these standards, as determined by the instructor, administrators or written complaints from other students, the student will be dismissed from the course and refunded in accordance with the Infosec Institute Refund Policy.

See Student Conduct for information regarding appeals to the conduct policy.

Student Records

Length of Record Maintenance

Infosec Institute will keep the student enrollment records permanently in a digital format and the financial transactions between the student and Infosec Institute for a minimum of 3 years after the last day of attendance.

Maintaining Student Information Confidentiality

We aim to protect student personal information through a system of organizational and technical security measures.

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the internet itself is 100% secure. Although we will do our best to protect student personal information, transmission of personal information to and from our services is at the user's own risk. Students should only access the services within a secure environment.

We may process or share data based on the following legal basis:

- **Consent:** We may process student data if the student provides written and specific consent to use their

personal information for a specific purpose.

- **Legitimate Interests:** We may process student data when it is reasonably necessary to achieve our legitimate business interests.
- **Performance of a Contract:** Where we have entered into a contract with the student, we may process student personal information to fulfill the terms of our contract.
- **Legal Obligations:** We may disclose student information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).
- **Vital Interests:** We may disclose student information where we believe it is necessary to investigate, prevent or take action regarding potential violations of our policies, suspected fraud, situations involving threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

Our full Data Protection Agreement can be provided upon request.

Obtaining Student Record Information

Students may download program completion certificates and financial records for each program enrolled from their personal Infosec Institute online account.

Release of Student Record Information

Infosec Institute will not release student confidential information under any circumstance, unless it falls within any of the legal basis as noted in subsection Maintaining Student Information Confidentiality above.

Student Conduct

Expected Student Conduct

Students are expected to interact in a professional manner that encourages participation with all classmates. Interactions are provided via one-on-one student exercises, as well as one-on-many group exercises incorporating the instructor.

Within the information security industry, one is expected to have the highest level of integrity and will often be required to acknowledge such when applying for roles and certifications. As such, Infosec Institute expects the same within the learning environment.

The maintenance of extremely high standards of honesty, integrity, performance and conduct is essential to the professional success of our students. Infosec Institute expects its students to have careful regard for our standards and avoid even the appearance of dishonesty or misconduct.

Although it is not possible to provide students with a complete list of every possible offense that will lead to expulsion, in order to provide some guidance, examples of unacceptable conduct are listed below. You should be aware that conduct that is not listed may also result in disciplinary action, up to and including immediate expulsion.

- Malicious or willful destruction or damage to Company property or supplies, or the property of another student or venue assets.
- Theft or unauthorized removal of property from venue premises, including the property of Infosec Institute, the venue, the instructor or another student.
- Inappropriate, malicious, disparaging or derogatory oral or written statements concerning program participants
- Falsifying personal records, including any application or other information, or any other records or documents related to the Infosec Institute training program, employees or representatives, including time records.
- Excessive tardiness, absenteeism or like abuse of the student's dedicated training program period.
- Failure to give proper notice of an expected absence.
- Dishonesty of any kind.
- Except as permitted by law, possession, use or display of any weapon, on Infosec Institute's venue premises.
- Possession, use or being under the influence of drugs or alcohol while participating in the Infosec Institute training program, or while on Infosec Institute venue premises.
- Fighting on Infosec Institute venue property, or any conduct endangering, or any verbal or nonverbal threat to endanger, property, life, safety or health.
- Obscene or abusive language or behavior.
- Any form of unlawful or unethical conduct, harassment or discrimination.

These examples are not all-inclusive, but merely illustrate the kind of conduct that may be detrimental to Infosec Institute and its student population.

Infosec Institute Actions if Violations Occur

Any initial violation of student conduct policy will be documented with a written email warning to the student indicating the program expulsion may occur should the behavior continue.

Following any initial violation of conduct that Infosec Institute deems egregious, for example endangering fellow students or Infosec Institute personnel or deemed high probability for liability, the student will be immediately expelled from the program as notified either verbally or in writing via email.
Student communications should be directed to:

Student Conduct Committee
Infosec Institute
13800 Coppermine Road, Suite 304
Herndon, VA 20170

The committee will meet monthly to review any correspondence and respond accordingly, always looking for an opportunity to meet student learning needs while maintaining the integrity of Infosec Institute.

Appeal Process and Readmission

Expelled students may submit a written appeal with any appropriate supporting documentation to:
Student Conduct Committee
Infosec Institute
13800 Coppermine Road, Suite 304
Herndon, VA 20170

The committee will meet monthly to review any correspondence and respond accordingly, always looking for an opportunity to meet student learning needs while maintaining the integrity of Infosec Institute.

Dress Code

Casual dress is not only accepted, it is highly recommended. Infosec Institute's programs typically run all day, multiple days in a row, so the more comfortable you are, the more focused the experience.

Additional Ethical Standards Statement

Within the information security industry, one is expected to employ an extremely high standard of honesty, integrity, performance and conduct, and will often be required to acknowledge such when applying for roles and certifications, often signing industry standard conduct agreements through the professional certification entity.

Attendance – Leave of Absence – Information

Types of Absences

Infosec Institute programs are condensed, focused programs covering 3 to 7 consecutive days in length, thus the traditional absence policies are not applicable to our programs.

Students desiring to participate in our programs are advised to schedule their session at a time where they can dedicate themselves to full participation. Therefore, any absence is typically an unscheduled/emergency type of situation where Infosec Institute has mitigation options for the student to consider.

If a student misses a day or less, the mitigation occurs through completion of associated Skills platform access to include review of the class recordings for any missed time and completion of Skills Learning Paths.

If a student misses more than 1 day of course instruction, discussions occur with the student to determine if the student should sit for the program again rather than reviewing class recordings and viewing Infosec Institute Skills learning paths. A decision on the mitigation option is agreed upon and pursued.

Tardiness

Tardiness is defined as not in class at the daily class start time.

Tardiness of 15 minutes or more will affect attendance for the day and require the student to view the class recording of the missed time.

Making up Missed Work Due to Absences

Make-up work is completed through the student's personal Infosec Institute Skills account and includes access to class recordings for any missed time, as well as through completion of Infosec Institute Skills learning paths.

Consequences of Unsatisfactory Attendance and Readmittance

If a student misses more than 1 day of course instruction, discussions occur with the student to determine if a resit of the program is a better option than the mitigation through reviewing class recordings and viewing Infosec Institute Skills learning paths. A decision on the mitigation option is agreed upon and pursued.

Leave of Absence Policy

Because Infosec Institute programs are condensed, focused programs covering 3 to 7 consecutive days in length, the traditional Leave of Absence policies are not applicable to our programs.

We do provide no-charge program resit options where circumstances warrant.

Inability to Make Up Missed Time Policy

Students are sent program start date reminders and new enrollment confirmations for program resits. The final reminder is sent one week prior to the program start date.

Students who do not show for their program resit are considered to have a program status of incomplete.

A student may submit a written exception to their program incomplete status with detailed circumstances and documentation for consideration. Exceptions must be received within 1 year of the initial program enrollment start date. Exception requests should be submitted to:

Student Exception Committee
Infosec Institute
13800 Coppermine Road, Suite 304
Herndon, VA 20170

Tuition, Fees, and Refunds

Program Tuition Costs

There is solely a tuition cost, with no other fees or charges. Additional material is available for purchase via third party sources.

Assigned Course Number	Program Offered	Tuition Cost
TIA-101	CompTIA A+	$2,499
TIA-103	CompTIA Security+	$2,799
TIA-102	CompTIA Network+	$1,499
TIA-201	CompTIA CASP+	$2,995
TIA-105	CompTIA CySA+	$2,999
IA-200	$(ISC)^2$ CISSP	$4,299
AUD-205	ISACA CISM	$3,595
AUD-204	ISACA CISA	$3,595
PM-100	PMI PMP Exam Prep	$2,699
SEC-200	EC-Council Certified Ethical Hacker	$4,599
CSC-301	Cisco CCNA Associate and Cyber Ops Associate	$3,999
MS-AZ-104	Microsoft Azure Admin and Security Technologies	$4,399
IA-205	$(ISC)^2$ CCSP	$4,399
CF-100	Cyber Foundations Immersive Bootcamp	$15,000

Refund Policy

All tuition and payments remitted to the school by a prospective student shall be refunded if the student is not admitted, does not enroll in the school, does not begin the program or course, withdraws prior to the start of the program, or is dismissed prior to the start of the program.

Upon payment and enrollment into the program, the student applicant may cancel, by written notice, their enrollment at any time prior to the first class day of the session for which application was made. When cancellation is requested under these circumstances, the school is required to refund all tuition paid by the student.

A student who enters the school but withdraws or is terminated during the first quartile (25%) of the program shall be entitled to a minimum refund amounting to 75% of the cost of the program.

A student who withdraws or is terminated during the second quartile (more than 25% but less than 50%) of the program shall be entitled to a minimum refund amounting to 50% of the cost of the program.

A student who withdraws or is terminated during the third quartile (more than 50% but less than 75%) of the program shall be entitled to a minimum refund amounting to 25% of the cost of the program.

A student who withdraws after completing more than three quartiles (75%) of the program shall not be entitled to a refund.

Expenses incurred by students for instructional supplies, tools, activities, library, rentals, service charges, deposits and all other charges are not required to be considered in tuition refund process when these expenses have been represented separately to the student in the enrollment contract and catalog, or other documents, prior to enrollment in the course or program. The school shall adopt and adhere to reasonable policies regarding the handling of these expenses when calculating the refund.

Programs Offered

Assigned Course Number	Program Offered	Clock Hours
TIA-101	CompTIA A+	40
TIA-103	CompTIA Security+	40
TIA-102	CompTIA Network+	40
TIA-201	CompTIA CASP+	40
TIA-105	CompTIA CySA+	40
IA-200	$(ISC)^2$ CISSP	48
AUD-205	ISACA CISM	40
AUD-204	ISACA CISA	40
PM-100	PMI PMP Exam Prep	32
SEC-200	EC-Council Certified Ethical Hacker	40
CSC-301	Cisco CCNA Associate and Cyber Ops Associate	56
MS-AZ-104	Microsoft Azure Admin and Security Technologies	56
IA-205	$(ISC)^2$ CCSP	40

CF-100	Cyber Foundations Immersive Bootcamp	720

Internships, Externships, and Production Work

Infosec Institute's education programs do not include internships, externships, or production work.

CompTIA A+

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's authorized CompTIA A+ Program is an accelerated, in-depth single-course program designed to teach the skills required to become a successful computer technician. This training focuses on teaching students basic software and hardware knowledge like installation and configuration, as well as the fundamentals of networking, security, virtualization, desktop imaging and deployment. Students will learn a wide range of entry-level computer technician skills and leave fully prepared to pass their CompTIA A+ certification exam.

Educational objectives

In this course, students will learn how to:

- Assemble components based on customer requirements
- Install, configure and maintain devices, PCs and software for end users
- Understand the basics of networking and security/forensics
- Properly and safely diagnose, resolve and document common hardware and software issues
- Apply troubleshooting skills
- Provide appropriate customer support
- Understand the basics of virtualization, desktop imaging and deployment

Prerequisites

- General understanding of Windows OS
- Experience with Microsoft products and technologies

Program Outline

Day	Course Number: TIA-101 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Peripheral Devices	
Day 1 PM	System Components	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Troubleshooting and Mobile Devices	
Day 2 PM	Printers and Network Hardware	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Networks	

Day	Course Number: TIA-101 Course Topic	Clock Hours
	Exam Review	
	Exam 220-1001	
Day 3 PM	Supporting Windows (I)	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Supporting Windows (II)	
Day 4 PM	Supporting Windows (III)	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Supporting Windows Networks	
	Linux, iOS X and Mobile OS	
Day 5 PM	Exam Review	
	Exam 220-1002	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

CompTIA Security+

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's authorized CompTIA Security+ single-course program teaches students information security theory and reinforces that theory with hands-on exercises to help them learn by doing. Students will learn how to configure and operate many different technical security controls, identify potential security risks and respond to incidents faster — and leave prepared to pass their CompTIA Security+ exam.

Educational objectives

In this course, students will learn how to:

- Assess the cybersecurity posture of an enterprise environment
- Recommend and implement appropriate cybersecurity solutions
- Monitor and secure hybrid environments
- Operate with an awareness of applicable laws and policies
- Identify, analyze and respond to cybersecurity events and incidents

Prerequisites

- 12-24 months of experience working with information systems and networking

Program Outline

Day	Course Number TIA-103 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Threats, Attacks and Vulnerabilities	
Day 1 PM	Threats, Attacks and Vulnerabilities cont'd	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Architecture and Design	
Day 2 PM	Architecture and Design cont'd	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Implementation	
Day 3 PM	Implementation cont'd	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Operations and Incident Response	
Day 4 PM	Governance, Risk, and Compliance	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Topic Review	
	Exam review	
Day 5 PM	Exam: SYO-601	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

CompTIA Network+

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's authorized CompTIA Network+ single-course program is comprehensive training that teaches students important networking administration and support skills. This program helps students master important information technology concepts, including the design and implementation of networks, using routers and switches to segment traffic, troubleshooting network problems and more. Students will leave with the skills needed to take the next step in their IT career and the knowledge required to pass their CompTIA Network+ certification exam.

Educational objectives

In this course, students will gain proficiency in:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Prerequisites

- General understanding of Windows client operating systems
- Experience with Microsoft products and technologies

Program Outline

Day	Course Number TIA-102 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Comparing OSI Model Network Functions	
	Deploying Cabling	
Day 1 PM	Deploying Ethernet Switching	
	Troubleshooting Ethernet Networks	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Explaining IPv4 Addressing	
	Supporting IPv4 and IPv6 Networks	
	Configuring and Troubleshooting Routers	
Day 2 PM	Explaining Network Topologies and Types	
	Explaining Transport Layer Protocols	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Explaining Network Services	
	Explaining Network Applications	
	Ensuring Network Availability	
Day 3 PM	Explaining Common Security Concepts	
	Supporting and Troubleshooting Secure Networks	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Deploying and Troubleshooting Wireless Networks	
	Comparing WAN Links and Remote Access Methods	
	Explaining Organizational and Physical Security Concepts	

Day	Course Number TIA-102 Course Topic	Clock Hours
Day 4 PM	Explaining Disaster Recovery and High Availability Concepts	
	Applying Network Hardening Techniques	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Summarizing Cloud and Datacenter Architecture	
	Course Topic Review	
Day 5 PM	Exam Review	
	Exam: N10-008	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

CompTIA CASP+

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description
Infosec Institute's CompTIA CASP+ single-course program teaches students the skills required to conceptualize, design and engineer secure solutions across complex enterprise environments. Students will apply critical thinking across a spectrum of security disciplines to propose and implement solutions that map to enterprise drivers. In addition to learning how to implement cybersecurity solutions, students will leave with the knowledge and skills needed to pass the CompTIA CASP+ certification exam.

Educational objectives
In this course, students will learn how to:

- Analyze security requirements in hybrid networks
- Implementing enterprise-wide, zero-trust security architecture
- Implementing secure cloud and virtualization solutions
- Integrating risk mitigation, threat and vulnerability management procedures.
- Conducting incident response tactics and digital forensics analysis
- Configure endpoint security controls, enterprise mobility and cloud/hybrid environments
- Implementing enterprise-wide PKI and cryptographic solutions
- Comparing overall cybersecurity compliance to regulations, such as CMMC, PCI-DSS, SOX, HIPPA, FISMA, NIST and CCPA

Prerequisites

- Ten years of experience in IT administration, with at least five of those years including hands-on technical security experience.

Program Outline

Day	Course Number TIA-102 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Performing Risk Management Activities	
Day 1 PM	Summarizing Governance & Compliance Strategies	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Implementing Business Continuity & Disaster Recovery	
	Identifying Infrastructure Services	
Day 2 PM	Performing Software Integration	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Explain Virtualization, Cloud and Emerging Technology	
	Exploring Secure Configurations & System Hardening	
Day 3 PM	Understanding Security Considerations of Cloud and Specialized Platforms	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM		
Day 4 PM	Implementing Cryptography	
	Implementing Public Key Infrastructure	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Architecting Secure Endpoints IIoT & IoT Concepts	
	Summarizing	
Day 5 PM	Exam Review	
	Exam: CAS-004	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

CompTIA CySA+

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's CompTIA CySA+ Program teaches students the knowledge and skills required to configure and use the latest industry-standard threat detection tools. Students will learn how to perform data analysis to identify vulnerabilities and expose cyber threats — with the ultimate goal of helping organizations protect and secure their applications and systems. In addition to learning the behavioral analytics skills needed to provide increased visibility into cyber threats, students will gain the knowledge required to pass their CompTIA CySA+ certification exam.

Educational objectives

In this course, students will gain proficiency in:

- Threat and vulnerability management
- Software and systems security
- Security operations and monitoring
- Incident response
- Compliance and assessment

Prerequisites

- Three to four years of hands-on information security experience, as well as a Security+ certification or equivalent knowledge.

Program Outline

Day	Course Number TIA-105 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Threat and Vulnerability Management	
Day 1 PM	Threat and Vulnerability Management (cont'd)	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Software and Systems Security	
Day 2 PM	Software and Systems Security cont'd	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Security Operations and Monitoring	
Day 3 PM	Security Operations and Monitoring cont'd	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Incident Response	
Day 4 PM	Incident Response cont'd	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**

Day	Course Number TIA-105 Course Topic	Clock Hours
Day 5 AM	Compliance and Assessment	
Day 5 PM	Exam Review	
	Exam: CS0-002	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

(ISC)^2 CISSP

Program Length: 48 hours (Sunday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's (ISC)^2 single-course program teaches students a broad range of cybersecurity skills, from developing security policies to managing risk to understanding technical security controls. Students will leave with the necessary skills and knowledge to effectively create and execute enterprise-wide information security strategies — and successfully pass their (ISC)^2 CISSP certification exam.

Educational objectives

In this course, students will gain proficiency in:

- Security and risk management
- Asset security
- Security engineering
- Communication and network security
- Identity and access management
- Security assessment and testing
- Security operations
- Software development security

Prerequisites

In order to obtain the CISSP certification, you must have:

- At least five years of professional experience in the information security field
- A work history reflecting direct experience in at least two of the eight domains listed in the (ISC)^2 CISSP Common Body of Knowledge (CBK)

However, you can become an Associate of (ISC)^2 by passing the exam without the required work experience.

Program Outline

Day	Course Number IA-200 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Security & Risk Management (I)	
Day 1 PM	Security & Risk Management (I)	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Asset Security	
	Security Engineering (I)	
Day 2 PM	Security Engineering (II)	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Communications & Network Security	
Day 3 PM	Identity & Access Management	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Security Assessment & Testing	
Day 4 PM	Security Operations (I)	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Security Operations (II)	
Day 5 PM	Software Development Security	
	Exam Readiness/Preparation	
	Day 5 Clock Hours	**8**
Day 6 AM	Review of all Eight Domains	
Day 6 PM	Exam Review	
	Day 6 Clock Hours	**8**
	Total Clock Hours	**48**

ISACA CISM

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's ISACA CISM single-course program equips students with in-depth knowledge of security governance, risk management, security program development and management, and security incident management best practices. In addition to gaining knowledge and experience around effective security management, students will leave fully prepared to earn their ISACA CISM certification.

Educational objectives

In this course, students will gain proficiency in:

- Information security governance
- The role of an information security steering group
- Legal and regulatory issues associated with internet businesses, global transmissions and transborder data flows
- Common insurance policies and imposed conditions
- Information security process improvement
- Recovery time objectives (RTO) for information resources
- Cost-benefit analysis techniques for mitigating risks to acceptable levels
- Security metrics design, development and implementation
- Information security management due to diligence activities and reviews of the infrastructure
- Events affecting security baselines that may require risk reassessments
- Changes to information security requirements in security plans, test plans and reperformance
- Disaster recovery testing for infrastructure and critical business applications
- External vulnerability reporting sources
- CISM information classification methods
- Life-cycle-based risk management principles and practices
- Security baselines and configuration management in the design and management of business applications and infrastructure
- Acquisition management methods and techniques
- Evaluation of vendor service level agreements and preparation of contracts

Prerequisites

- Five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas. The work experience must be gained within the ten-year period preceding the application date for certification or within five years from exam pass date.

Program Outline

Day	Course Number AUD-205 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Information Security Governance (I)	
Day 1 PM	Information Security Governance (I)	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Risk Management (I)	
Day 2 PM	Risk Management (II)	

Day	Course Number AUD-205 Course Topic	Clock Hours
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Information Security Program Development and Management (I)	
Day 3 PM	Information Security Program Development and Management(II)	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Information Security Program Development and Management (III)	
Day 4 PM	Information Security Program Development and Management (IV)	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Information Security Incident Management (I)	
Day 5 PM	Information Security Incident Management (II)	
	Exam Review	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

ISACA CISA

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's ISACA CISA single-course program teaches students the skills necessary to develop, manage and supervise programs to defend against unauthorized admittance to information. Students will gain in-depth knowledge of auditing information systems and how it applies to real-world scenarios — and leave fully prepared to pass their ISACA CISA exam.

Educational objectives

In this course, students will gain proficiency in:

- The process of auditing information systems
- Governance of IT and management
- Information systems acquisition, development and implementation
- Information systems operations, maintenance and services management
- Protection of information assets

Prerequisites

- Five years of professional information systems auditing, control or security work experience is required for certification; however, up to three years can be waived if other requirements are met. Students have five years after passing the exam to gain the necessary work experience and apply for certification.

Program Outline

Day	Course Number AUD-204 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	The Process of Auditing Information Systems	
Day 1 PM	Governance of IT and Management	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Information Systems Acquisition, Development and Implementation (I)	
Day 2 PM	Information Systems Acquisition, Development and Implementation (II)	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Information Systems Operations, Maintenance and Service Management (I)	
Day 3 PM	Information Systems Operations, Maintenance and Service Management (II)	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Protection of Information Assets (I)	
Day 4 PM	Protection of Information Assets (I)	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Content review	
	Exam Readiness/Preparation	
Day 5 PM	Exam Review	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

PMI PMP Exam Prep

Program Length: 32 hours (Monday through Thursday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's PMP Exam Prep single-course program teaches critical project management concepts, principles and techniques needed to become an effective project manager. Students will learn to master the knowledge, skills, tools and techniques used in project management through days of live instruction and 35 additional hours of PMP exam preparation materials — and leave fully prepared to pass the PMI PMP certification exam.

Educational objectives

In this course, students will learn how to:

- Initiate a project, including performing project assessments and stakeholder analysis
- Plan a project, including scope, cost, schedule, human resources, communications, procurement, quality control and change management
- Execute a project, including managing project resources, implementing approved changes and maintaining stakeholder relations
- Monitor and control a project, including verifying deliverables and project objectives, and measuring performance, changes and risk
- Close a project, including financial and legal closure, collating lessons and obtaining feedback from stakeholders

Prerequisites

This program is intended for professionals that are preparing to take the PMP exam:

- Applicants must have 35 hours of specific project management education (included with this program)
- With a Bachelor's Degree (or the global equivalent), applicants must have three years of professional project management experience, during which 4,500 hours are spent leading and directing project tasks, up to eight years from the time of application.
- Without a Bachelor's Degree (or the global equivalent), applicants must have five years of professional project management experience, during which at least 7,500 hours are spent leading and directing project tasks, up to eight years from the time of application.

Program Outline

Day	Course Number PM-100 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	What is Project Management	
Day 1 PM	Initiating Planning (I)	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Planning (II)	
Day 2 PM	Planning (III)	
	Exam Readiness/Preparation	

Day	Course Number PM-100 Course Topic	Clock Hours
	Day 2 Clock Hours	**8**
Day 3 AM	Planning (IV)	
Day 3 PM	Executing (I)	
	Executing (II)	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Monitoring/Controlling (I)	
Day 4 PM	Monitoring/Controlling (II)	
	Exam Review	
	Day 4 Clock Hours	**8**
	Total Clock Hours	**32**

EC-Council Certified Ethical Hacker

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's EC-Council Certified Ethical Hacking single-course program teaches students the skills, tools and techniques needed to effectively pentest an organization's infrastructure. Students learn ethical hacking methodologies and gain hands-on hacking experience in cloud-hosted cyber ranges, including reconnaissance, gaining access to systems, exploiting vulnerabilities and exfiltrating data. Students will leave with the ability to quantitatively assess and measure threats to information assets. This program also prepares students to earn the in-demand EC-Council Certified Ethical Hacker (CEH) certification.

Educational objectives

In this course, students will gain proficiency in:

- Passive reconnaissance and OSINT
- Target system, identification, service enumeration and vulnerability scanning
- Password security, social engineering and physical security
- Deep target penetration and covering tracks
- Network scanning
- Data exfiltration
- Scripting
- Vulnerability exploitation
- Web application attacks

Prerequisites

- Firm understanding of the Windows Operating System
- Exposure to the Linux Operating System or other Unix-based operating system
- Grasp of the TCP/IP protocols

Program Outline

Day	Course Number SEC-200 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Pentesting Process	
Day 1 PM	Passive REconnaissance and OSINT	
	Capture The Flag Exercises	
	Day 1 Clock Hours	**8**
Day 2 AM	Network Scanning	
Day 2 PM	Target System Identification, Service Enumeration and Vulnerability Scanning	
	Capture The Flag Exercises	
	Day 2 Clock Hours	**8**
Day 3 AM	Exploitation	
Day 3 PM	Password Security, Social Engineering, and Physical Security	
	Capture The Flag Exercises	
	Day 3 Clock Hours	**8**
Day 4 AM	Deep Target Penetration and covering tracks	
Day 4 PM	Web Application Attacks	
	Capture The Flag Exercises	
	Day 4 Clock Hours	**8**
Day 5 AM	Scripting	
	Post-Engagement Activities	
	Exam Review	
Day 5 PM	Exam review	
	Exam: EC Council Certified Ethical Hacker	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

Cisco CCNA Associate and Cyber Ops Associate

Program Length: 56 hours (Monday through Sunday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's Cisco CCNA Associate and Cyber Ops Associate single-course program equips students with hands-on networking experience inside the Infosec Institute Networking Cyber Range. Program topics include network access, IP connectivity, IP services, automation and programmability for Cisco networks and more. In addition to gaining practical experience in a networking and switching environment, students will leave prepared for the simulation-based questions found within the CCNA Associate certification exam and the Cisco Cybersecurity Operations Fundamentals exam.

Educational objectives

In the CCNA Associate portion of this course, students will learn how to:

- Make appropriate decisions concerning implementation of hardware and configuration, based on ISR routers and switches running the Cisco iOS
- Proficiently administer Cisco routers
- Install, configure and maintain dependable, functional networks
- Properly identify protocols involving Cisco networking devices
- Troubleshoot general network and security issues
- Successfully operate routers and switched LAN networks

In the Cyber Ops Associate portion of this course, students will gain proficiency in the topics covered by the Cisco Cybersecurity Operations Fundamentals exams including:

- Security concepts
- Security monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedures

Prerequisites

- Familiarity with networking topics such as TCP/IP, IP configuration, peer-to-peer networking, subnetting, building a routing table and other network protocols, standards and architecture.

Program Outline

Day	Course Number CSC-301 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Network Fundamentals	
Day 1 PM	Network Fundamentals cont'd	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Network Access	
Day 2 PM	Network Access cont'd	
	Exam Readiness/Preparation	

	Day 2 Clock Hours	**8**
Day 3 AM	IP Connectivity	
Day 3 PM	IP Connectivity cont'd	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	IP Services	
Day 4 PM	Security Fundamentals	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Automation & Programmability	
Day 5 PM	Exam review	
	Exam: CCNA 200-301 CCNA Associate Exam	
	Day 5 Clock Hours	**8**
Day 6 AM	Security Concepts	
	Security Monitoring	
Day 6 PM	Host-Based Analysis	
	Network Intrusion Analysis	
	Exam Readiness/Preparation	
	Day 6 Clock Hours	**8**
Day 7 AM	Network Intrusion Analysis cont'd	
	Security Policies & Procedures	
Day 7 PM	Exam Review	
	Exam: CCNA 200-201 Cisco Cybersecurity Operations Fundamentals Exam	
	Day 7 Clock Hours	**8**
	Total Clock Hours	**56**

Microsoft Azure Admin and Security Technologies

Program Length: 56 hours (Monday through Sunday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's Microsoft Azure Admin and Security Technologies single-course program teaches students vital Microsoft Azure administration and security skills through hands-on labs and expert instruction. The combination of practical labs and expert instruction ensures students leave the program with skills that directly transfer to the workplace — and the knowledge needed to pass the two certification exams: Azure Administrator Associate and Microsoft Certified: Azure Security Engineer Associate.

Educational objectives

In this course, students will learn how to:

- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Configure and manage virtual networking
- Monitor and back up Azure resources
- Manage identity and access
- Implement platform protection
- Manage security operations
- Secure data and applications

Prerequisites

- A basic understanding of cloud computing is recommended but not required.

Program Outline

Day	Course Number MS-AZ-104 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Identity	
Day 1 PM	Governance & Compliance	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Azure Administration	
	Virtual Networking	
Day 2 PM	Intersite Connectivity	
	Network Traffic Management	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Azure Storage	
	Azure Virtual Machines	
Day 3 PM	Serverless Computing	
	Data Protection	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Monitoring	
	Azure Admin Exam Review	
Day 4 PM	Exam AZ-104: Microsoft Azure Administrator	
	Day 4 Clock Hours	**8**
Day 5 AM	Identity and Access	
Day 5 PM	Identity & Access con't	
	Exam Readiness/Preparation	

Day	Course Number MS-AZ-104 Course Topic	Clock Hours
	Day 5 Clock Hours	**8**
Day 6 AM	Platform Protection	
Day 6 PM	Security Operations	
	Exam Readiness/Preparation	
	Day 6 Clock Hours	**8**
Day 7 AM	Data and Applications	
	Exam Review	
Day 7 PM	Exam AZ-500 Microsoft Azure Security Technologies	
	Day 7 Clock Hours	**8**
	Total Clock Hours	**56**

$(ISC)^2$ CCSP

Program Length: 40 hours (Monday through Friday 8:30 am – 5:30 pm) / 1 Week
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description

Infosec Institute's $(ISC)^2$ CCSP single-course program is a comprehensive course designed to teach students how to secure cloud-based environments. Topics include cloud architecture and design requirements, operational and compliance issues, and the security of cloud data, applications and infrastructure. Students will leave the program fully prepared to earn their $(ISC)^2$ CCSP certification, one of the most in-demand certifications focused on cloud security.

Educational objectives

In this course, students will gain proficiency in:

- Cloud concepts, architecture and design
- Cloud data security
- Cloud platform and infrastructure security
- Cloud application security
- Cloud security operations
- Legal, risk and compliance
- Cloud computing concepts and principles
- Securing virtual environments
- Cloud design requirements
- Protecting sensitive cloud assets
- Data classification and categorization
- Digital rights management

- Cloud storage architectures
- Cloud-specific risks
- Testing, architecture and auditing of cloud services
- Standards for achieving high availability
- Legal issues unique to the cloud

Prerequisites

In order to obtain the CCSP certification, you must have:

- At least five years of professional experience in the information technology field
- Three of those years must be in information security, and one year must include experience in one of the six CCSP domains

However, you can become an Associate of $(ISC)^2$ by passing the exam without the required work experience.

Program Outline

Day	Course Number IA-205 Course Topic	Clock Hours
Day 1 AM	Course Introduction	
	Cyber Security Basics	
Day 1 PM	Cloud Concepts, Architecture & Design	
	Exam Readiness/Preparation	
	Day 1 Clock Hours	**8**
Day 2 AM	Cloud Concepts, Architecture & Design cont'd	
Day 2 PM	Cloud Data Security	
	Exam Readiness/Preparation	
	Day 2 Clock Hours	**8**
Day 3 AM	Cloud Platform & Infrastructure Security	
Day 3 PM	Cloud Platform & Infrastructure Security cont'd	
	Exam Readiness/Preparation	
	Day 3 Clock Hours	**8**
Day 4 AM	Cloud Application Security	
Day 4 PM	Cloud Security Operations	
	Exam Readiness/Preparation	
	Day 4 Clock Hours	**8**
Day 5 AM	Legal, Risk, and Compliance	
Day 5 PM	CCSP Test Essential Knowledge areas	
	Day 5 Clock Hours	**8**
	Total Clock Hours	**40**

Cyber Foundations Immersive Bootcamp

Program Length: 720 hours (Includes Live Instructor led session each Tuesday and Thursday 6 PM – 10 pm, Saturday 9 AM – 4 PM) 26 Weeks total
Delivery: Face-to-face or Online
Graduation Document: Certificate of Completion

Program Description
This intensive 26-week program covers a wide array of critical topics designed to provide students with a deep understanding of information security's role in technology today.

This program is an intensive course that covers a wide range of critical topics about information security and its role in today's technology. The program is designed to provide students with a deep understanding of information security, and they will learn to identify and protect vulnerable systems through hands-on research and guidance from instructors.

The curriculum focuses on foundational Windows troubleshooting, where students will navigate complex scenario-based labs to develop critical skills such as effective communication, documentation, terminal operations, performance monitoring and software application management. They will also learn to resolve and document tech issues and incidents using the CompTIA troubleshooting methodology alongside the ITIL service management framework.

Students will get the opportunity to experience real-world scenarios by becoming the systems administrator for the fictional GlobeX Corporation. They will learn about network design, troubleshooting, VPN tunneling, firewall configuration and server deployment, alongside user identity management, scripting, automation, and system health monitoring.

The program concludes with a deep dive into cybersecurity operations (SecOps Foundations), where students will explore cyber frameworks, data encryption, cloud security, network security, threat modeling and incident response. They will also acquire ethical hacker skills in penetration testing, culminating in two major projects to showcase their newfound skills.

Educational Objectives
In this program, students will gain proficiency in:

- Windows troubleshooting
- CompTIA troubleshooting methodology
- ITIL service management
- Network Design
- Troubleshooting
- VPN tunneling
- Firewall Configuration
- Server Deployment

- Cyber Frameworks
- Data Encryption
- Cloud Security
- Network Security
- Threat Modeling
- Incident Response

Prerequisites

This program has been designed for beginners, whether you are at the beginning of your career or switching into the cybersecurity industry. We do recommend that you have a general understanding of Windows client operating system as well as experience with Microsoft products and technologies.

Program Outline

Code	Course Name	Clock Hours
101	Cybersecurity Foundations 101: Introduction to Modern Computing Technologies	40
102	Cybersecurity Foundations 102: Introduction to Cybersecurity	40
201	Supporting Technology and Troubleshooting Systems	160
301	Networking & System Administration	160
401	Security Engineering	320
	TOTAL PROGRAM HOURS	720

Course Descriptions

Participants will gain firsthand experience with the Infosec Institute Cyber Foundations program, enhancing their understanding of system vulnerabilities and the necessary measures to safeguard against them.

Cyber Foundations 101- Introduction to Modern Computing Technologies
48 Clock Hours

Session	Course Topic	Clock Hours
1	Overview of Modern Technologies • Introduction to Modern Computing Technologies • Evolution of Computing Technologies • Key Components of Modern Computing Systems	4

	• Trends and Future Directions in Computing	
2	Computing Architectures and Systems • Types of Computing Architectures: Centralized, Distributed, and Cloud Computing • Overview of High-Performance Computing (HPC) and Grid Computing • Introduction to Quantum Computing • Set up a virtualized environment using a hypervisor	4
3	Basics of Operating Systems • Introduction to Operating Systems • Operating System Structures and Components • Process Management and Scheduling • Memory Management	4
4	Advanced OS Concepts • File Systems and Storage Management • Security and Protection Mechanisms in OS • Network and Distributed Operating Systems • Install and configure a Linux operating system	4
5	Windows and Linux Operating Systems • Overview of Windows Operating System • Overview of Linux Operating System • Comparison between Windows and Linux OS • Basic commands and scripting in Linux	4
6	Mobile and Embedded Operating Systems • Introduction to Mobile Operating Systems (Android, iOS) • Embedded Operating Systems and Real-time Operating Systems (RTOS) • Use Cases and Applications • Develop a simple application for a mobile OS	4
7	Cloud Computing • Introduction to Cloud Computing • Cloud Service Models: IaaS, PaaS, SaaS • Cloud Deployment Models: Public, Private, Hybrid • Create and manage a virtual machine on a cloud platform	4
8	Virtualization Technologies • Introduction to Virtualization • Types of Virtualization: Server, Desktop, Network, and Storage	4

	• Benefits and Challenges of Virtualization • Set up and configure virtual machines using a virtualization tool	
9	Internet of Things (IoT) and Edge Computing • Introduction to IoT and Edge Computing • Architectures and Protocols for IoT • Use Cases and Applications of IoT • Set up a basic IoT device and collect data	4
10	Artificial Intelligence and Machine Learning • Introduction to AI and Machine Learning • AI and ML in Modern Computing 4 • Tools and Frameworks for AI and ML • Build a simple machine learning model using Python	4
11	Review and Case Studies • Review of Key Concepts • Discussion of Real-world Case Studies	4
12	Final Project and Assessment • Complete a final project that integrates multiple aspects of modern computing technologies and operating systems • Presentation and demonstration of the final project	4
	Total Clock Hours	**48**

Cyber Foundations 102 - Introduction to Cybersecurity
40 Clock Hours

If you're stepping into the world of computer configuration for the first time, Cyber Foundations 102 offers the perfect introduction to understanding the inner workings of computers.

This course is designed to familiarize you with system interfaces, help you identify and install hardware components, and guide you through the process of setting up Windows and Linux operating systems.

Through hands-on practice and expert instruction, you'll build the foundational skills necessary to launch a successful career in technical operations, minus the complexities of deploying systems. Join Cyber Foundations 102 to begin your journey into the technical realm with confidence and competence.

Session	Course Topic	Clock Hours

1	Introduction to Cybersecurity • Overview of Cybersecurity • Importance and Impact of Cybersecurity • Setting up a secure virtual lab environment	5
2	Cybersecurity Frameworks and Standards • Overview of Cybersecurity Frameworks • Introduction to NIST, ISO, and other Standards • Implementing basic security policies in the virtual lab	5
3	Network Security • Fundamentals of Network Security • Network Security Devices and Technologies • Configuring firewalls and intrusion detection systems	5
4	Advanced Network Security • Virtual Private Networks (VPNs) and Secure Communication • Wireless Network Security (1 hour) • Setting up and securing a VPN	5
5	Securing Web Applications • Common Web Application Vulnerabilities • Secure Coding Praticies • Performing vulnerability assessments on web applications	5
6	Endpoint Security and Cryptography • Endpoint Protection and Management • Malware and Antivirus Solutions • Setting up endpoint protection solutions • Introduction to Cryptography-- • Basics of Cryptography • Symmetric and Asymmetric Encryption • Implementing encryption and decryption methods	5
7	Incident Response and Management • Incident Response Lifecycle • Types of Incidents and Responses • Conducting a simulated incident response • Advanced Incident Management • Forensic Investigation Techniques (1 hour) • Developing Security Policies (1 hour)	5

	• Performing a forensic investigation on a compromised system • Creating and implementing security policies in the lab environment	
8	Final Project and Assessment • Complete a comprehensive final project that integrates all aspects of the course • Presentation and demonstration of the final project	5
	Total Clock Hours	**40**

Cyber Foundations 201 - Supporting Technology and Troubleshooting Systems
160 Clock Hours

This six-week course is designed for individuals aiming to enhance their skills in supporting technology operations, specifically focusing on troubleshooting, and resolving issues related to hardware, software, and virtual or cloud-based systems.

Participants will engage in practical, scenario-based labs to develop foundational troubleshooting skills for Windows environments. The curriculum emphasizes critical skills such as effective communication, thorough documentation of knowledge and processes, basic terminal operations, monitoring system performance, managing system processes, handling various issues, and utilizing backup, imaging, and recovery tools, alongside software application management.

The instructional approach is hands-on, centering on practical systems support and problem-solving. Students will apply the CompTIA troubleshooting methodology and the ITIL service management framework to efficiently communicate, solve, and document technological issues and incidents. Furthermore, the course delves into the integration of endpoints within the broader IT infrastructure, covering topics like network ports and protocols, Wi-Fi connectivity, and server-based user identity support.

It spans a total of 160 hours, encompassing lectures, laboratory work, coworking sessions, and collaborative projects, aiming to equip students with both the technical and some soft skills necessary for a successful career in technology support and operations.

Session	Course Topic	Clock Hours
1	Introduction to Computer Operations • Course Overview and Expectations • Introduction to Windows Troubleshooting • Setting Up the Virtual Lab Environment	20

	• Customer Service and Technical Support • ITIL Service Management Framework • Using an Issue Tracking System • CompTIA Troubleshooting Methodology • Knowledge Management and Documentation • Developing Standard Operating Procedures • Remote Desktop Support and Diagnostics	
2	Windows 10 Troubleshooting and Configuration • Windows 10 Configuration Basics • Performance Monitoring and Tuning • Configuring Windows 10 Settings • Endpoint Imaging, Backup, and Recovery • Software Application Deployment and Updates • Creating and Restoring System Images • Troubleshooting Windows 10 Issues • System Process Management • Performing Startup Repair and Data Restoration • Monitoring and Managing System Processes	20
3	Technical Service and Support • Service Level Agreements (SLA) • Technical Project Support • Managing SLAs and Project Support Tasks • Technical Reporting and Communication • Remote IT Service and Support • Writing Technical Reports • Endpoint Technical Support • Troubleshooting Methodology • Providing Remote IT Support • Applying Troubleshooting Methodologies	20
4	Hardware and Software Management • Software Application Deployment, Updating, and Removal • Performance Monitoring and Tuning • Deploying and Updating Software Applications • Backup and Recovery Tools • Data Restoration and Secure Disposal • Using Backup and Recovery Tools • Windows 10 OS Deployment and Configuration	20

	• Linux and Windows Terminal Commands • Deploying and Configuring Windows 10 OS • Practicing Terminal Commands	
5	Infrastructure Connectivity • Network Protocols and Concepts (TCP/IP, DHCP, DNS • Network Ports and Ethernet • Configuring Network Adapter Settings • Network Troubleshooting • Network Routers • Troubleshooting Network Connectivity • Active Directory User Support • Cloud Instance Deployment • Managing Active Directory Users • Deploying Cloud Instances Using AWS Lightsail	20
6	Scripting and Automation • Introduction to Bash Scripting • OS Task Automation Concepts • Writing Basic Bash Scripts • Using GitHub for Version Control • Practical Applications of Scripting • Performing Basic GitHub Operations • Advanced Bash Scripting • Introduction to GitHub • Automating Tasks with Bash Scripts • Scripting for System Administration Tasks	20
7	Advanced Troubleshooting and Connectivity • Advanced Windows 10 Troubleshooting • Network Security Basics • Troubleshooting Complex Windows 10 Issues • Virtualization Using VirtualBox • pfSense Firewall Configuration • Setting Up and Configuring Virtual Machines • Integrating Virtual and Physical Networks • Case Studies in Troubleshooting • Deploying and Configuring pfSense Firewall • Troubleshooting Network Issues in Virtual Environments	20

8	Capstone Project • Capstone Project Introduction and Requirements • Project Planning and Group Discussion • Starting the Capstone Project • Working on the Capstone Project • Finalizing the Capstone Project	10
9	Capstone Project Presentations and Final Review • Preparing Capstone Project Presentations • Capstone Project Presentations • Group Presentations • Course Review and Final Q&A • Final Assessment and Feedback	10
	Total Clock Hours	**160**

Cyber Foundations 301 - Networking & System Administration
160 Clock Hours

This six-week course offers comprehensive experience in server and networking skills through the context of the GlobeX Corporation, a fictional company evolving from a startup to an international organization. As the appointed administrator within this narrative, you will engage in a range of technical tasks that reflect the real-life duties of a cybersecurity professional.

The curriculum is structured around hands-on activities that simulate actual job responsibilities. These include designing and troubleshooting networks, configuring VPNs and firewalls, implementing network security measures, deploying, and managing servers, managing user identities, and automating routine tasks through scripting. You will also monitor system health and conduct professional exercises in change management and project planning.

It encompasses 160 hours of instruction, including lectures, practical lab sessions, coworking opportunities, and group projects, all aimed at equipping you with the necessary skills in network and systems administration to prepare for the follow-on Cybersecurity skills in pursuit of core Cybersecurity roles.

Session	Course Topic	Clock Hours
1	Introduction and Fundamentals • Course Overview and Expectations • Introduction to Networking and Systems Administration • Setting Up the Virtual Lab Environment	20

	• Overview of Network Components and Topologies • Basics of Network Design • Designing a Simple Network • Introduction to Agile Project Management • Basics of Microsoft Windows Server 2019 • Installing and Configuring Windows Server 2019	
2	Network Design and Configuration • LAN Connectivity to Cloud Resources on AWS • Network Access Controls • Configuring AWS VPC and Subnets • Router and Firewall Administration with pfSense • VPN Tunneling Concepts • Setting Up pfSense and Creating VPN Tunnels • - Network Service Administration (TCP/IP, DHCP, DNS) • Network Traffic Analysis Tools • Configuring DHCP and DNS Services • Using Network Traffic Analysis Tools	20
3	Systems Administration • Identity Management with Active Directory (AD) and LDAP • User Identity Management Concepts • Setting Up and Managing AD/LDAP • IT Infrastructure and Systems Design • Patch Management Strategies • Implementing Patch Management Solutions • Virtual Machine Administration • Overview of Software Administration • Setting Up and Managing Virtual Machines • Administering Software on Virtual Machines	20
4	Advanced Networking • Advanced Network Design • Network Infrastructure Troubleshooting • Designing a Complex Network • Network Service Administration Continued • Virtual Private Network (VPN) Client and Tunnel	20

	• Configuring Advanced Network Services • Network Security Fundamentals • Firewall Configuration and Management • Implementing and Managing Firewalls • Network Security Best Practices	
5	Scripting and Automation • Introduction to Bash Scripting • OS Task Automation Concepts • Writing and Executing Basic Bash Scripts • Introduction to Powershell • Automating Tasks with Powershell • Writing and Executing Powershell Scripts • Introduction to Python for Automation • Scripting Best Practices • Writing and Executing Python Scripts for Automation	20
6	Integration and Cloud Computing • Integrating Cloud Systems with On-Premise Systems • Overview of Cloud Security • Configuring Hybrid Cloud Solutions • Extending pfSense Capabilities with Packages • Monitoring System Health • Installing and Configuring pfSense Packages • Change Management and Project Planning • Planning and Implementing a Change Management Project	20
7	Capstone Project Capstone Project Introduction and Requirements • Project Planning and Group Discussion • Starting the Capstone Project • Working on the Capstone Project • Finalizing the Capstone Project	20
8	Capstone Project Presentations and Final Review • Preparing Capstone Project Presentations • Capstone Project Presentations • Group Presentations • Course Review and Final Q&A • Final Assessment and Feedback	20

	Total Clock Hours	160

Cyber Foundations 401 - Cybersecurity Engineering
320 Clock Hours

The 12-week Cyber Foundations 401-level courses are advanced offerings aimed at equipping individuals with comprehensive cybersecurity skills. These courses are tailored for students who already possess a foundational understanding of IT operations, gained through previous courses, self-directed study, or professional experience.

This cybersecurity engineering-focused course first delves into information assurance principles, safeguarding data, securing cloud-based platforms and familiarizing participants with essential SecOps tools and techniques. As the course progresses, students will shift focus towards constructing threat models, evaluating the security of web applications, devising custom defenses against malware and executing fundamental penetration testing.

It is during the 401 components that our career services solution is introduced which includes:

- One 2-page Resume re-write
- One 30-minute interview prep session
- One LinkedIn makeover
- 30-days of premium access to Career.io.

This curriculum is designed to provide practical, hands-on experience with contemporary cybersecurity tools and methodologies, preparing students for the demands of the current cybersecurity landscape. Students will also learn about the various tools, tactics, and methods cyber attackers use and how these can be leveraged to bolster and guide organizational security efforts

Session	Course Topic	Clock Hours
1	Cybersecurity and Governance • Course Overview and Expectations • Introduction to Cybersecurity • Setting Up the Virtual Lab Environment • Cybersecurity Frameworks (e.g., SOC2 • CIA Triad • Systems Hardening Practices • Risk Analysis, Assessment, and Reporting • Security Compliance and Auditing • Conducting a Security Compliance Audit • Implementing Risk Mitigation Strategies	25

2	Data Security and Encryption • Data Classification and Data Loss Prevention • Data Privacy Concepts and Regulations (GDPR, CCPA) • Implementing Data Loss Prevention (DLP) Strategies • Encryption Standards and Password Security • Protecting Data at Rest and in Transit • Setting Up Encryption for Data at Rest and in Transit • Public Key Infrastructure (PKI) and SSL/TLS • Practical Applications of Encryption • Configuring SSL/TLS for Web Servers • Implementing PKI Solutions	25
3	SecOps Foundations • Threat Detection with IDS and SIEM • Incident Response Lifecycle • Setting Up and Configuring an IDS • Indicators of Compromise (IOC) and SIEM Deployment • SIEM Log and Event Analysis • Deploying and Configuring a SIEM System • Threat Hunting Techniques • SIEM Troubleshooting and Data Ingestion • Writing and Running SIEM Queries • Threat Hunting Using SIEM Data	25
4	Cloud Security • Cloud Identity and Access Management • Cloud Security in AWS • Setting Up IAM in AWS • Data Loss Prevention in Cloud Environments • Intrusion Detection & Prevention Systems (IDS/IPS) in the Cloud • Configuring IDS/IPS in AWS • Virtual Private Cloud (VPC) and AWS Native Tooling • Network Traffic Analysis in the Cloud • Configuring and Managing VPCs • Using AWS CloudTrail for Security Monitoring	25
5	Threat Modeling and Analysis • Tactics, Techniques, and Procedures • Cyber Kill-Chain and MITRE ATT&CK	25

	• Creating Threat Models Using MITRE ATT&CK • OWASP and STRIDE • Threat Modeling and Data Flow Diagrams • Conducting OWASP-Based Threat Assessments • Practical Applications of Threat Modeling • Case Studies in Threat Modeling • Developing Threat Models for Real-World Scenarios	
6	Threat Hunting • Malware Detection with YARA Rules and VirusTotal API • Malware Traffic Analysis • Creating and Using YARA Rules • Forensic Investigation Techniques • Threat Hunting with Zeek and RITA • Conducting Forensic Investigations • Advanced Threat Hunting Techniques • Case Studies in Threat Hunting • Threat Hunting in Complex Environments	25
7	Application Security and Vulnerability Analysis • Web Application Scanning and Exploitation (Burp Suite, OWASP ZAP) • Common Vulnerability Scoring System (CVSS) • Conducting Web Application Scans • Network and Application Vulnerability Scanning • Vulnerability Risk Rating • Using Nessus for Vulnerability Scanning • Handling Scanner Output and False Positives • Prioritizing Vulnerabilities • Analyzing and Prioritizing Vulnerability Scan Results	25
8	Penetration Testing • Enumeration and Exploitation Techniques • Legal Considerations in Penetration Testing • Performing Network Enumeration • Penetration Test Lifecycle • Planning and Scoping a Penetration Test • Conducting Penetration Test Planning and Scoping • Target Profiling and Evaluation • OSINT for Penetration Testing	25

	• Executing a Penetration Test	
9	Incident Response and SIEM • Incident Response Operations • SIEM Event Monitoring • Setting Up Incident Response Procedures • Advanced SIEM Configuration • Configuring and Querying a SIEM System • Writing SIEM Queries • Practical Applications of Incident Response • Case Studies in Incident Response • Performing Incident Response Simulations	25
10	Cloud Security Advanced • Advanced Cloud Security Techniques • Securing Cloud Infrastructure • Implementing Advanced Cloud Security Measures • Cloud Security Incident Response • Cloud Compliance and Auditing • Conducting Cloud Security Audits • Integrating Cloud Security with On-Premise Systems • Case Studies in Cloud Security • Configuring Hybrid Cloud Security Solutions	25
11	Capstone Project Preparation • Capstone Project Introduction and Requirements • Group Discussion and Project Planning • Starting the Capstone Project • Working on the Capstone Project • Developing and Implementing Capstone Project Components	10
12	Capstone Project Completion • Finalizing the Capstone Project	10
	Total Clock Hours	**320**

Cyber Foundations 501
Post Course Optional (free 6 week access**)**
Hands on Skills validation and Badging within the Infosec Skills Cyber Range tool

Additional Curriculum Information

Evaluating and Improving Offered Courses

End of Course Surveys. Infosec Institute solicits feedback from students at the end of every course. Students are asked to rate the following areas on a 1-10 point scale, with 10 being "exceptional":

- Overall Course Rating Instructor
- Rating Overall
- Instructor Rating Instruction Skills Instructor
- Rating Subject Matter Course Materials
- Rating
- Training Environment Rating

Survey feedback is:

- Reviewed weekly at the Client Experience department level
- Used to drive action plans where required and tracked to completion
- Shared with individual instructors in a monthly feedback session focused on class performance and quality
- Shared with fulfillment and support staff for opportunities to fine tune processes, procedures and responses
- Shared with Infosec Institute's content team as needed to address content-related issues
- Reviewed weekly at executive staff meetings
- Reviewed quarterly at company-wide meetings

Infosec Institute coordinates with technology and certification providers on content specific to their programs to ensure Infosec Institute students receive the highest quality material in the industry.

Feedback on supplemental content delivered through the Infosec Institute online platform is also reviewed regularly for application and content development improvements.

Faculty Accessibility

In-course support is available through email access to the instructor during class or through submission of a support ticket through the student's personal Infosec Institute online account.

Post-class support is available through submission of a support ticket through the student's personal Infosec Institute online account.

Availability of Academic Support Services

Infosec Institute does not offer official tutoring. Added support is offered through the supplemental Infosec Institute online platform learning path and associated components.

Updated August 27, 2024

Program advising is submission of a support ticket through the student's personal Infosec Institute online account.

Graduation Requirements

Infosec Institute's professional training and certification programs provide a Certificate of Completion upon the student achieving a 90% or greater on the practice exam taken at the culmination of the course. Students receive a Pass or Incomplete status as noted in the Student Disclosure Information section.

Career Advising and Placement Services

Each training and certification program aligns with industry and certification entity recommended job roles as well as defined government cyber security code regulations.

Infosec Institute does not provide career advising or placement services.

Distance Education

Minimum technology specifications required:

An internet connection (wired or wireless):

- Recommended bandwidth:
  - 600kbps/1.2Mbps (up/down) for high quality video
  - For gallery view: 1.5Mbps/1.5Mbps (up/down)
- Speakers and a microphone (built-in, USB plug-in or wireless Bluetooth)

Supported operating systems:

- Microsoft Windows 7 or later
- Mac OS X with MacOS 10.7 or later
- Linux: recent Linux distros

Supported tablet and mobile devices:

- iOS and Android devices
- Blackberry devices

Available Student Support Services

All the same support services noted above for students attending the program in person.

Available Navigation Training

The Infosec Institute learning platform has an online tutorial for on-site navigation. In addition, individual support is available through submission of a support ticket through the student's personal account.

Methods for Timely Interaction

Remote students have the same level access to the instructor and support faculty as in person students, with all the same access and support functionality.

Library Resources

All students have access to the full digital library of course materials, information, practice tests, lesson plans, class recordings via the school log in portal.

Information Exchange Privacy and Safety Policy

Reference Infosec Institute's privacy policy on the website at https://www.infosecinstitute.com/privacy-policy/

Ownership and Faculty Information

Powers, Duties, and Responsibilities

Senior Vice President - General Manager (Bret Fund)

- Communicating, on behalf of the company, with employees, government entities, and the public
- Leading the development of the company's short- and long-term strategy
- Creating and implementing the company or organization's vision and mission
- Maintaining awareness of the competitive market landscape, expansion opportunities, industry developments, etc.
- Ensuring that the company maintains high social responsibility wherever it does business

Director of Client Experience (Scott Frederickson)

- Focuses on executing the company's business plan, according to the established business model.
- Oversees the day-to-day administrative and operational functions of a business.
- Establishing policies that promote company culture and vision.
- Set comprehensive goals for performance and growth
- Manage relationships with partners/vendors

Students

- Students do not participate in institutional governance.

Staff and Faculty

Please refer to the Staff and Faculty Addenda for the current listing of administrative personnel and instructors.

INFOSEC INSTITUTE

CATALOG ADDENDA

Staff and Faculty

July 1, 2024 – June 30, 2025

Hampton Inn Cascades | 46331 McClellan Way, Sterling, VA 20165
(804) 439-9990 | registrar.infosec@cengage.com

Staff and Faculty

Administrative Management

Senior Vice President – General Manager - Bret Fund
Director of Customer Experience - Scott Fredrickson

Faculty

1. **Steve Allen**: (MS Cybersecurity, MBA IT Management, BS IT).
   Certificates: ISC2, ISACA CISA, CISM.

2. **Henry Alonzo**: (MS Telecommunications & Network Administration, BS Electronics Engineering Technology)
   Certificates: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional Enterprise (CCNP), Cisco Certified Specialist Enterprise Advance Infrastructure Implementation, Cisco Certified Specialist Enterprise Core, Cisco Certified Specialist Enterprise Design, Cisco Certified System Instructor.

3. **James Beamon**: (BS Mathematics, MS Information Assurance / Cybersecurity, MBA Business Administration)
   Certifications: (ISC)2: CISSP, CGRC, ISSEP - ISACA: CISM, CRISC, CGEIT, CISA.

4. **Matthew Brussel**: (BS IT – Economic) Employed Plaza Systems, Information Security Advisor 2/2018 - Present.
   Certifications: CISSP CEH CASP – Security + - CCNA Security – Cyber Ops Associate – VMware VCP VCTA VCA – MCSE.

5. **Grace Buckler**: (MS Cybersecurity & Privacy, BA Technical Communications)
   Certifications: CISSP, CISA, CIPP/E, CIPP/US, CIPP/G, CIPM, PMP, CRISC, CDPE.

6. **Ross Casanova**: Employed: GDIT - Cyber Security Analyst 11/2018 – Present (held multiple roles in field)
   Certifications: Certified Information Systems Professional (CISSP), Security+ CE, Comp TIA. Certified Ethical Hacker, EC Counsel - Certificate of Cloud Security Knowledge (CCSK) - CSA - Certified Identity Risk Manager (CIRM), IMI – Social Media Security Professional (SMSP), CompTia – GIAC Security Essentials Certification (GSEC), SANs – Information Security Assessment Methodology (IAM), NSA – Ultimate Knowledge Institute Certified Instructor – ITIL Foundation Certificate in IT Service Management (ITILv3-F) – IACRB Certified Security Awareness Practitioner - Certified Cloud Security Professional (CCSP).

7. **Christian Espinosa**: (MBA Computing & Information Management, BS General Engineering)
   Certifications: CCISO: Certified CISO – CEI: Certified EC Council Instructor – CISSP: Certified Information Systems Security Professional – PMP: Project Management Professional - CRISC: Certified in Risk & Information Systems Control – CHFI: Computer Hacking Forensic Investigator – CySA+: Cybersecurity Analyst – CHPC: Certified High Performance Coach – CWAPT: Certified Web App Penetration Tester – Master Neuro Linguistic Programming (NLP) Practitioner – Network + - ECSA: EC Council Certified Security Analyst – CEH: Certified Ethical Hacker – Security + - CISA: Certified Information Systems Auditor – CEPT: Certified

Expert Penetration Tester – CSSA: Certified SCADA Security Architect – LPT: Licensed Penetration Tester.

8. **Rod Evans**: Employed: Youth Opportunity Center – Cybersecurity Specialist 2003 – 2006, Intense School – Cybersecurity Instructor 2006 – 2010 - Infosec 2006 – Present

9. **Scott Fass**: (MPA Public Administration, BA Geology, ROTC USA Army Commission). Employed Fass Advisory Group, CEO / Founder – Project management Certification, Strategic Planning, Emotional Intelligence. Certifications: PMI PMP Exp. Date 3/2025, PMI ATP.

10. **Tommy Gober**: (MS Instructional Technology, BS Computer Science Education, AS Computer Science) Certifications: CISSP from ISC2 – CompTIA Security+ - CompTIA Linux+ - CompTIA Network+ - CompTIA CASP+ (Certified Advanced Security Practitioner) – CompTIA CySA+ (Cybersecurity Analyst) – CompTIA PenTest+ - CompTIA A+ - CompTIA IT Fundamentals+ - CompTIA CTT+ (Certified Technology Trainer) – TX State Board of Educator Certification (certified teacher) – Google Apps for Education Certified Individual – Microsoft Office Specialist (Word, Excel, PowerPoint, Outlook).

11. **West Goewey**: Employed: Netwest Consulting LLC – Owner / Trainer – contractor for Security & IT Bootcamps 1/1/1996 – Present Certifications: ISC2 Certification CISSP, EC Council Certification: Certified Ethical Hacker (C|EH) v6-11, EC Council Certification: Computer Hacking Forensics Investigator (C|HFI), EC Council Certification: Certified Network Defender (C|ND), CIAC Certified Incident Handler (GCIH), CompTIA CySA+, CompTIA Security+, CompTIA Security Analytics Professional CSAP+, CompTIA Cloud+, CompTIA PenTest+, EC Council Certification: Certified EC Council Instructor (C|EI) - CompTIA Security Analytics Professional CSAP Security+, CYSA+ - CompTIA Secure Infrastructure Specialist CSIS A+, Network+, Security+ - CompTIA Secure Infrastructure Expert CSIE Security+, CySA+, PenTest+, CASP – CompTIA Security Analytics Expert CSAE Security+, CySA+, CASP – CompTia Network Security Professional CNSP – CompTIA Network Vulnerability Assessment Professional CNVP - CompTIA IT Operations Specialist CIOS Net+ A+ - CompTIA Net+ A+ - CompTIA Cloud Admin Professional (CCAP) – CompTIA Secure Cloud Professional (SCCP) Security+ Cloud+ - Infosec Institute: Certified Red Team Operations Professional (CRTOP) – Infosce Institute: Certified Cyber Threat Hunting Professional (CCTHP) – Infosec Institute: Incident Response & Network Forensics Training Bootcamp – Infosec Institute: Certified Penetration Testing (CPT) – Infosec Institute: Certified Expert Penetration Tester (CEPT) – Core Impact Certified – Microsoft Certified Professional – Microsoft Certified Solutions Associate: Windows Server 2008 – Microsoft Certified IT Professional Enterprise Administrator on Windows Server 2008 Charter Member – Microsoft Certified Technology Specialist Windows Server 2008 Applications Infrastructure, Configuration Charter Member – Microsoft Certified Technology Specialist Windows Server 2008 Network Infrastructure Charter Member – Microsoft Certified Technology Specialist Windows Server 2008 Active Directory, Configuration Charter Member.

12. **Dave Gray**: (BBA Management, MS Government, MBA Business). Employed: University of CA, SanDiego, Faculty Instructor CMMC & CCP from 12/2022 to Present and Austin Community College, Faculty Instructor ISC2 CISSP, CompTIA Security+ ce from 11/2012 to Present. Certifications: CCA / CMMC Authorized Provisional, CCP / CMMC Authorized Provisional Instructor, CISSP / Certified Information Systems Security, CGRC / Certified in Governance, Risk & Compliance, PMP / Project Management Professional, CompTIA Security+, C|EH / Certified Ethical Hacker, CAICO / Provisional Instructor (PI) – CAICO / Certified CMMC

Professional (CCP) – CAICO / Certified CMMC Assessor (CCA) – CAP / Certified Authorization Professional aka CGRC – ITIL / Information Technology Infrastructure Library.

13. **AJ Holt**: Employed TechInternal, LLC, Cybersecurity Trainer from 8/2003 to Present.
    Certifications: Microsoft Certified Trainer – Certified EC Council Instructor – Windows Hybrid Administrator (AZ-800 / AZ-801) – Azure Fundamentals (AZ-900) – Certified Ethical Hacker V.10 – CompTIA Security Analytics Expert (CSAE) - CompTIA Security Analytics Professional (CSAP) - CompTIA CASP+ - CompTIA CYSA+ - CompTIA Security+ - CompTIA Network+ - Microsoft Certified Solution Expert: Cloud and Server Infrastructure – Microsoft Certified Solution Expert: Windows Server 2012 Server Infrastructure – Microsoft Certified Solution Associate: Windows Server 2016 – Microsoft Certified Solution Associate: Windows 8 – Microsoft Certified Solution Associate: Windows 7 – Microsoft Certified Solution Associate: Windows Server 2008 – Microsoft Certified IT Professional: Server 2008 Enterprise Administrator – Microsoft Certified IT Professional: Server 2008 Server Administrator – Microsoft Certified IT Professional: Windows 7 Desktop Administrator – Microsoft Certified Technology Specialist: Windows Server 2008 – Microsoft Certified Technology Specialist: Windows Vista – Microsoft Certified Technology Specialist: Sharepoint Server 2007 Configuration - Microsoft Certified Systems Engineer: Security (Windows Server 2003) – Microsoft Certified Systems Administrator: Security (Windows Server 2003) – Microsoft Certified Systems Engineer: Messaging (Windows Server 2003) – Microsoft Certified Systems Administrator: Messaging (Windows Server 2003) – Microsoft Certified Systems Engineer: Security (Windows 2000 Charter Member) – Microsoft Certified Systems Administrator: Security (Windows 2000 Charter Member) – Microsoft Certified Systems Engineer + Internet (NT 4.0) – Microsoft Certified Desktop Technician – Certified Cisco Network Associate.

14. **Barbara Johnson**: (BS Industrial Systems Engineering and MBA Business).
    Certifications: Certified Information Systems Security Professional (CISSP), ISC^2– Certified Information Systems Security Management Professional (ISSMP), ISC^2– - Certified Information Systems Auditor (CISA), ISACA – Certified Information Security Manager (CISM), ISACA - Certified Risk & Information Systems Control (CRISC), ISACA – Certified Data Privacy Solutions Engineer (CDPSE), ISACA – Certified Business Continuity Professional (CBCP), DRll – Certificate of the Business Continuity Institute (CBCl) & Member Business Continuity Institute (MBCl), BCl – Cloud Essential+, CompTIA.

15. **Cliff Jones**: LaunchPad Training (owner) 5/1/2020 to present.
    Certifications: Microsoft Certified Solutions Expert (includes Server Infrastructure, Private Cloud, Desktop Infrastructure, Messaging). Microsoft Certified IT Professional (includes Enterprise Messaging Exchange 2007, Enterprise Administrator 2008, Enterprise Support Technician Vista). Microsoft Certified Technology Specialist (includes System Center 2011 Configuration Manager, Microsoft Exchange Server 2007 Configuration, 2008 R2 Server Virtualization, Windows Server 2008 Active Directory Configuration, Windows Server 2008 Application Infrastructure, Windows Server 2008 Network Infrastructure, Microsoft System Center Configuration Manager, Microsoft Windows Vista, Microsoft SQL Server 2000, Microsoft Windows Sharepoint Services 3.0, Microsoft Office Sharepoint 2007). Microsoft Certified Solutions Associate (includes Windows 8, Windows Server 2012, Windows Server 2008). Microsoft Certified Systems Engineer (includes Microsoft Windows Server 2003, Microsoft Windows 2000, Microsoft Windows NT 4.0). Microsoft Certified Trainer CompTIA (includes A+, Networking+, CNIP, Security+, Cyber Security Analyst+, CSAP, Server+, Cloud+, CCAP).

16. **Ted Jordon**: (MS Mechanical Engineering, MC Mechanical Engineering). Employed Learning Tree International, Sr. Technical Trainer. Certifications: CompTIA Security+ - CompTIA Exp Date 7/2029 – CompTIA Cybersecurity Analyst (CySA+) – CompTIA, Certified Cloud Security Professional (CCSP) – ISC^2, Certified Information Systems Security Professional (CISSP) – ISC^2, Certified Secure Software Lifecycle Professional (CSSLP) - ISC^2, Computing Hacking Forensic Investigator Certification – Infosec.

17. **Wilfredo Lanz**: (BS Economics). Employed CA State University, Fullerton, Instructor – Extended Education: Networks for Industrial Applications. Certifications Microsoft Certified Trainer, MCT – Microsoft Azure Solutions Architect Expert – Microsoft Azure Administrative Associate – Microsoft Certified Systems Engineer, MCSE/MCSA Windows Server 2016/ Windows 10 – Microsoft Certified Software Expert (MCSE): Server Infrastructure (Windows Server 2012) – Cisco Certified Network Associate, CCNA Security, Cisco Certified Design Associate (CCDA) – CompTIA Advanced Security Practitioner (CASP), Network+, Security+, A+ Certified.

18. **Bill Lipiczky**: (BA Political Science). Employed Managed By Design, Inc., Sr. Cyber Security Practitioner, 2006 – Present.
    Certifications: ITIL 4 Managing Professionals – CISSP – SSCP – ITIL Expert – Service Manager – CISA – CISM – COBIT – GSLC – Security+ - ABCP – CompTIA CTT+ - TIPA Assessor – Prince2 – Certified Cloud Security Officer C(CSO – Information Systems Security Officer C(ISSO – Scrum Fundamentals – MCNI – CI – MCSE – MCSA – CCNA.

19. **Albert Lyngzeidetson**: (PhD Cognitive Science, MA Philosophy, BA Psychology & Philosophy). Employed Theseus Digital Security, Cybersecurity Consultant 9/2018 to Present.

20. **Ken Magee**: (MBA / Management - Management Theory, BS / Management Computer Science). Employed Data Security Consultation & Training, LLC – President / Owner 2001 to Present.
    Certifications: CMMC Certified Professional - CMMC Provisional Instructor – CMMS Provisional Assessor – ISACA Certified Instructor, ISACA – COBIT 2019 Framework Certification, ISACA – CAC (Cybersecurity Audit Certificate), ISACA – ISSAP, ISC^2 – ISSEP, ISC^2 – CASP, CompTIA – CySA, CompTIA – CCSP, ISC^2 – SSCP, ISC^2 – CTT+, CompTIA – CEH, EC-Council – CPT, IACRB – ISSMP, ISC^2– CISM, ISACA – GIAC GSEC, SANS – Security+ - CGAP – CFE – CIA – ISO 27001 Provisional Auditor – GIAC GSNA, SANS.

21. **Jeremy Martin**: Employed CyberVance/NDI/ATA.gov, Sr. Instructor / Cybersecurity Analyst 4/2015 – Present and Information Warfare Center, Sr. Instructor 10/2010 to Present.
    Certifications: ACE AccessData Certified Examiner (FTK) – ACSA ArcSight Certified Security Analyst – AME AccessData Mobile Examiner (MPE+) – CCFE Certified Computer Forensics Examiner – CCTHP Certified Cyber Threat Hunting Professional – CDRP Certified Data Recovery Professional – CHFI Computer Hacking Forensic Investigator – CMFE Certified Mobile Forensic Examiner – CySA+ CompTIA Cybersecurity Analyst – CASS Certified Applications Security Specialist – CCPT Certified Cloud Penetration Tester – CEH Certified Ethical Hacker – CEPT Certified Expert Penetration Tester – CNDA Certified Network Defense Architect – CRTOP Certified Red Team Operations Professional – CREA Certified Reverse Engineering Analyst – CEREA

Certified Reverse Engineering Analyst - CSSA Certified SCADA Security Analyst – CWAPT Certified Web Application Penetration Tester – CMWAPT Certified Mobile & Web Application Penetration Tester – I-PTE ISSAF Penetration Testing Expert / OISSG – LPT – ECSA Licensed Penetration Tester – NSA-IEM NSA's Infosec Evaluation Methodology – Pentest+ CompTIA Pentest+ - CHS-III Certification in Homeland Security / Level 3 – CISSP Certified Information Systems Security Professional ISC^2 – CISSP-ISSAP CISSP Information Systems Security Architecture Professional ISC^2 – CISSP-ISSMP CISSP Information Systems Security Management Professional (ISC)^2 – CEI Certified EC-Council Instructor – Certified Oxygen Forensics Trainer – NSA-IAM – MCTS – A+ - Network+ - Security+ - CPT – I-PTQ – CIW Professional – CIW DSS – NCSA: Computer Hardware Tech – Retina (DISA.mil).

22. **Kristina Nairn**: (BS / Biology). Employed Learning Tree International, Instructor / Cybersecurity & Programming 4/2001 – Present. Certifications: ISACA CISA Certified Information Systems Auditor – ISACA/CSA CCAK Certificate of Cloud Auditing Knowledge - ISC^2 CCSP Certified Cloud Security Professional - ISC^2 HCISPP Healthcare Information Security Privacy Practitioner - ISC^2 CAP Certified Authorization Professional - ISC^2– CSSLP Certified Secure Software Lifecycle Professional - ISC^2 SSCP Systems Security Certified Practitioner – EC Council CEI Certified EC-Council Instructor – EC Council CEH Certified Ethical Hacker – CompTIA CASP+ CompTIA Advanced Security Practitioner – CompTIA Security+ - CompTIA CySA+ - CompTIA Network+ - CompTIA Server+ - CompTIA A+ - ITIL Foundations – CertNexus CFR Cybersecurity First Responder.

23. **Ralph O'Brien**: (Professional University Certificate / European Centre on Privacy & CyberSecurity DPO). Certifications: (2022) CIPP/US Certified Information Privacy Professional / US, International Association of Privacy Professionals – (2020) CDPSE, Certified Data Privacy Solutions Engineer, ISACA – (2006) Information Security Management Principles, British Computer Society, ISEB (Distinction Level) & Lead Tutor for ISEB CISMP course, British Computer Society – (2014) HIPAA Privacy for Bas; trustarc – (2023) ISO/IEC 27001 Lead Implementor (Firebrand) training course - (2023) ISO/IEC 27001 Lead Auditor (Firebrand) training course – (2005) BS7799 (AD066), BSI Management Systems – (2021) Global Privacy & Data Protection, trustarc – (2016) Fellow of Information Privacy (FIP) – (2005) BSi Registered Lead Auditor ISO 9001 & ISO/IEC 27001, British Standards Institution – (2004) Diversity Training, Advisory Conciliation & Arbitration Service (ACAS) – (2003) CRAMM IS Risk Management, Mentis Consultancy – (2003) Data Protection Audit Manual Techniques & Methodology, Privacy Laws & Business International – (2002) Project Management Skills, Design Basics, Human Rights Act for Supervisors – (2006) Planning & Documenting DBsy Risk Assessment, QinetiQ – (2015) CIPT Certificate in Privacy Technologist, International Association of Privacy Professionals - (2014) CIPM Certificate in Privacy Management, International Association of Privacy Professionals - (2013) CIPP Europe, Certified Privacy Professional, International Association of Privacy Professionals – (2011) ISO 27002 Implementation Exin course & ISO 27001 Lead Implementer IT Governance – (2010) BS 25999-2 Implementer, IT Governance (now ISO 22301) & ISO 27001 Lead Audit, IT Governance.

24. **Elias Papatestas**: (BA Psychology, MS Information Systems). Independent Contractor 2003 – Present. Certifications: CCSI #33597 – CCNA - CCNA Security - CCNP Routing & Switching – Network+ - Security+ - A+ - Linux+ - CWNT – CWNA – CTT+ - ACA – CTP – Convergence+.

25. **Akyl Phillips**: (Certificate Computer Science). Employed Hulu / Lead Security Operations Center Consultant 8/2020 – 9/2021) and Hireright / Senior Security Engineer 2/2019 – 8/2020.

Certifications CompTIA Security + - CompTIA Pentest+ - EC Council CEH – GIAC GPEN – GIAC GCIH.

26. **Jeff Recor**: (BS IT /Cyber Security).
    Certifications: CompTIA A+ - Network+ & Security+ - Microsoft SCCM – Certified Cisco Systems Instructor (CCSI) – Microsoft Certified Trainer (MCT) – CompTIA Certified Training Instructor (CCTI).

27. **Carlton Simmons**: (PhD Information Systems & Science Specialization IS Security, MBA / MS Management Information Systems, BA Political Science).
    Certifications: Cisco Certified Network Associate - Microsoft Certified Trainer – Microsoft Certified Systems Engineer – Microsoft Certified Systems Administrator – Microsoft Certified Information Technical Professional – Master CIW Certified Instructor (PROSOFTTRAINING.COM) – Master CIW Designer (PROSOFTTRAINING.COM) – CIW Professional (PROSOFTTRAINING.COM) – ITIL Service Management Foundation (EXIN) – Project Management Professional – Certified Information Systems Professional, ISC^2 – Certified Ethical Hacker, EC Council – Certified Hacking Forensic Investigator, EC Council, Citrix Certified Enterprise Administrator, Citrix Systems, Inc. – Citrix Certified Instructor, Citrix Systems, Inc. – Citrix Certified Sales Professional, Citrix Systems Inc. – Certified e-Training Facilitator, The Training Clinic, Inc. – Certified Technical Trainer+, CompTIA – CASP, CompTIA – Project+, CompTIA – Security+, CompTIA – iNetwork+, CompTIA – Network+, CompTIA – A+, CompTIA.

28. **Steve Spearman**: (BA History). Employed: Patronus Security LLC, Lead Security Consultant & vCISO 11/2020 – 9/2023.
    Certifications: HealthCare Information Security & Privacy Practitioner (HCISPP) - CISSP

29. **Victoria Thomas**: (MS Integrated Marketing Communications). Employed: Salesforce, Sr. Manager Security Awareness Campaigns 9/2021 – 3/2023, Charles Schwab Corp., Sr. Manager, Security Awareness & IT Risk Culture.
    Certifications: SANS Security Awareness Professional (SSAP Credential), SANS Institute Certified Security Awareness – Practitioner (CSAP Certification), IACRB Security Awareness & Culture Professional (SACP Certification) – H Layer Credentialing Prosci Certified Change Practitioner (ADKAR), Prosci.

30. **Nick Valenteen**: (MS Information Assurance, BS Marketing). Employed: Valenteen Associates, Info Assurance Instructor 2002 – Present.
    Certification: Certificate of Cloud Security Knowledge – Cloud Security Alliance.

31. **Paula Woodall**: Employed University of Alabama, Birmingham – Instructor: Window Server, C#, SQL Server, Sharepoint.
    Certifications: CompTIA Data+ - Microsoft Certified: Power RB Data Analyst Associate – Microsoft Certified: Azure Database Administrator Associate – Microsoft Certified: Azure Data Engineer Associate – MCSE: Data Management & Analytics.