2015

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

ARE WE PREPARING STUDENTS FOR THE FUTURE? AN EVALUATION OF INFORMATION SECURITY EDUCATION IN COMPUTER DEGREES AT NC UNIVERSITIES

Mark Jonathan Grover

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2015

Approved by

Advisory Committee

_____	_____
Dr. Jeffery Cummings	Dr. Laurie Patterson

_____
Dr. Bryan Reinicke, Chair

Accepted By

_____
Dean, Graduate School

ABSTRACT

Are we preparing students for the future? An evaluation of Information Security education in computer degrees at NC Universities. Grover, Mark Jonathan, 2015. Capstone Paper, University of North Carolina Wilmington.

The purpose of this paper is to determine what elements of Information Security should be taught in Computer Science and Information Technology programs. The need for professionals that are security aware is at an all-time high, yet there is no readily available research outlining specific education required to prepare students. This research is a result of an analysis of the current state of computer security jobs available to North Carolina graduates, and currently taught coursework collected from the University of North Carolina System. This capstone project will help educators reduce the gap between what is taught in a classroom and what is needed to fulfill job requirements.

ACKNOWLEDGEMENTS

I have invested a lot of hard work and effort into completing this research. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them.

I am highly indebted to my capstone committee for their guidance and constant supervision, as well as providing necessary feedback to ensure successful completion of this research.

I would like to express my gratitude towards my wife, Rosemary, and my children, Caleb and Lauren, for enduring long nights and missed activities as I was approaching completion. To my mom and mother-in-law for giving of their time to watch the kids, and give me quiet time to work. Their support and encouragement helped me stay focused towards completion.

I would like to express my special gratitude and thanks to Melissa Watson and Mike Orr, two wonderful people who supported me in this endeavor while I was working full-time. My thanks and appreciation go to my colleagues for encouraging words when I needed them most. A special thanks goes out to Sohail Sukhera, Sean Piotrowski, and Mike Hervey, for pushing me when I was feeling overwhelmed. Thank you.

Table of Contents

Chapter 1: Introduction

The demand for Information Security professionals is at an all-time high, yet there is no readily available research outlining specific education deliverables within a Computer Science or Information Technology curricula to prepare students. According to a recent *Computerworld* article, the demand for cybersecurity professionals over the past five years grew 3.5 times faster than the demand for other IT jobs (Vijayan, 2013). The Bureau of Labor and Statistics predict information security analyst jobs to grow 22% from 2010 to 2020 (U.S. Department of Labor, 2013). Salaries for security professionals are typically higher than others in IT. Robert Half Technology's 2014 Salary Survey shows a network security administrator can expect to earn between $95,000 and $131,500 and a data security analyst can expect to earn between $100,500 and $137,250 (Robert Half Technology, 2013).

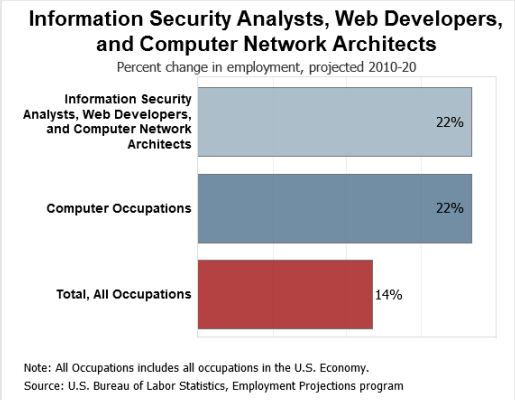

Figure 1- 2013 Projected Change in employment for Security Analysts

In May 2009, President Barack Obama identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation" (Obama, 2009). Since then many schools and universities have begun to offer varying degree programs that focus in Information Security; however, the education delivered at each is quite different. Unlike a math or accounting degree, where there is an acceptable standard by which to measure one school to another, the same does not exist for information security.

Since starting this research in 2013, multiple groups have met to discuss the learning outcomes for Cyber-related educational offerings. One provider of curricula

recommendations is The Association for Computing Machinery (ACM). ACM regularly publishes curricula recommendations for Computer Science and Information Technology programs. As of this writing, the most recent Computer Science curriculum guideline for undergraduate programs was published in December 2013, and the Information Technology guideline was published in November 2008 (Association for Computing Machinery, 2015). Other groups such as the Cyber Education Project (CEP) have formed to develop curriculum guidelines for a "Cyber Science" degree track (Cyber Education Project, 2015). What these groups have in common is the desire to create curricula that meets accreditation standards.

One popular Computer Science accrediting body is ABET, formerly known as the Accreditation Board for Engineering and Technology. ABET consists of "over 3,400 applied science, computing, engineering, and engineering technology programs at nearly 700 colleges and universities in 28 countries worldwide" (ABET, 2015). Ultimately the recommendations made in this research must adhere to ABET standards.

This research attempts to answer two questions. Are North Carolina Computer Science and Information Technology graduates prepared to begin working in the security field? Are security certifications required of new graduates? By answering these questions, this research will help educators ensure baseline information security education is being taught to ensure a quality, employable, cybersecurity workforce.

This capstone has the following objectives:

- Map North Carolina area cybersecurity jobs to educational requirements.
- Define acceptable cybersecurity curriculum core standards that should be taught in Computer Science and Information Technology programs.

Chapter 2: Review of Literature Review and Analysis

It is clear that education is key to obtaining a job as a security professional. The 2013 IT Salary Survey on Security performed by *InformationWeek* shows that 99% of participants indicated they had completed at least some higher education or tech school classes (Lemos, 2013). According to the Bureau of Labor and Statistics, "Information security analysts usually need at least a bachelor's degree in computer science, programming, or a related field" (U.S. Department of Labor, 2013). This is supported by a survey of 682 IT Security professionals who were polled. Of those who responded, between 77% - 78% of respondents have a Bachelor's degree or higher (See Figure 2). Higher education can also serve as a substitute for experience, as some job postings mention that education can be utilized in lieu of experience.

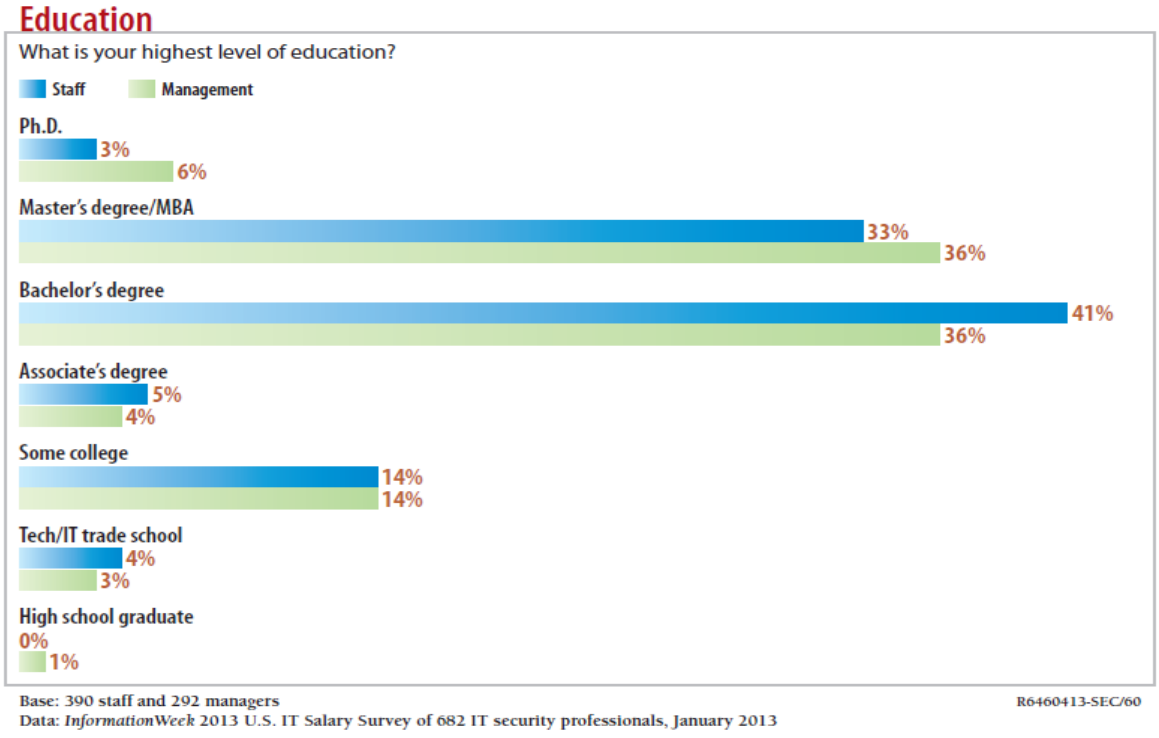

Figure 2- InformationWeek 2013 Salary Survey: Security, Education held by participants

The same report goes on to ask the question, "What type of training would you find most valuable to you in developing your career?" (Lemos, 2013). The answers given

to this question provides an honest assessment of where the participants feel they need to improve (See Figure 3). Note that certification courses rate as one of the top two considered most valuable in further developing a security career, only slightly behind the need for technology-specific training. A Nextgov.com article dated April, 2013 states "staff members holding certifications make $12,000 more and managers make $10,000 more in base salary than their noncertified counterparts" (Ballenstedt, 2013).

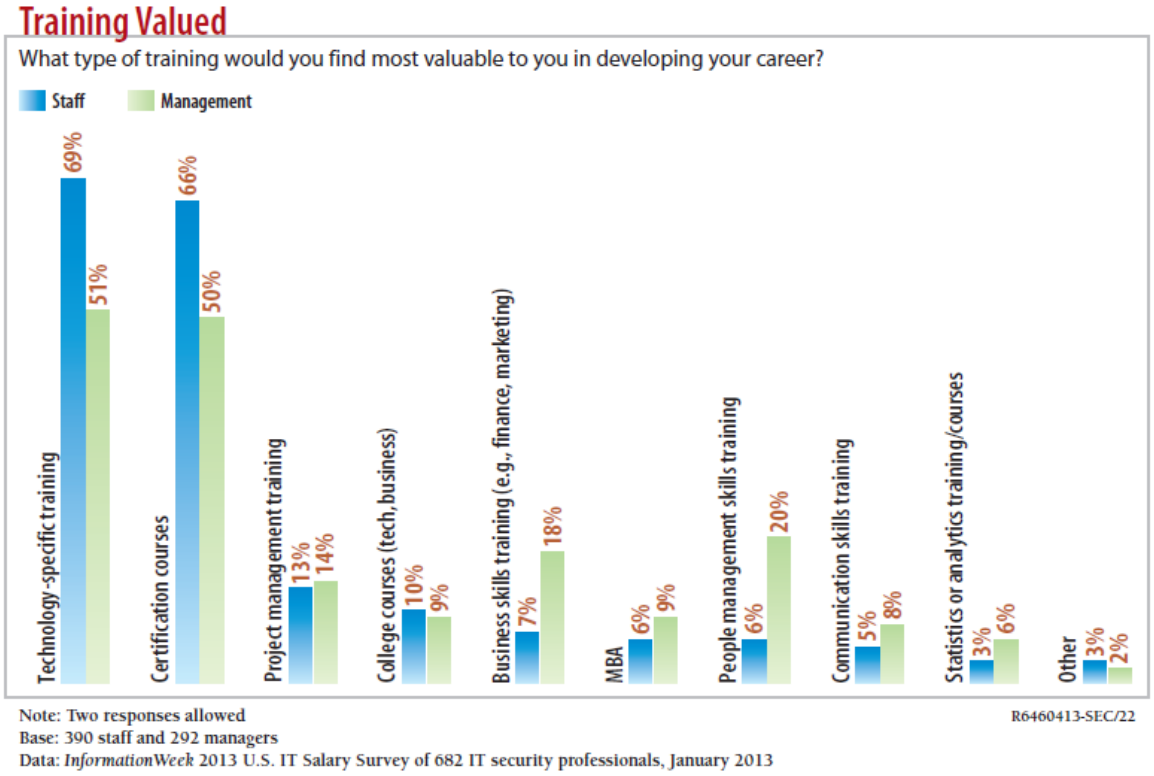

Figure 3- InformationWeek 2013 Salary Survey: Security, Most Valuable Training

According to the 2013 and 2014 US IT Salary Surveys of IT security staff and management professionals performed by *InformationWeek*, more than 60% of those surveyed have at least one security certification (See Figure 4). The same surveys also provided statistics about the effect security certifications have on compensation. Certification attributes to an average increase in total compensation of $9,000 to $14,000 annually (See Figure 5). A 2008 *NetworkWorld* article by Jon Brodkin states that "a

$21,000 boost in salary can be yours if you obtain Certified Information Systems Security Professional (CISSP) or two other major security certifications" (Brodkin, 2008). The article cited research by Foote Partners, an IT research and advisory firm that continuously monitors compensation of IT professionals. Foote Partners has been collecting IT skills and certification data since 1999 and publishes them quarterly for a fee. As of this writing, the 2015 IT Skills and Certifications Pay Index™ could be purchased for $4,600 per single quarterly edition (Foote Partners, LLC, 2015). A February 3, 2014 search of PayScale.com revealed a salary range for jobs that utilize a given certification, but do not include data that shows the salary before or after achieving a given certification. Additional searches were performed in an effort to find data that shows a monetary value for successfully achieving a given certification; however, that information could not be acquired without a fee.

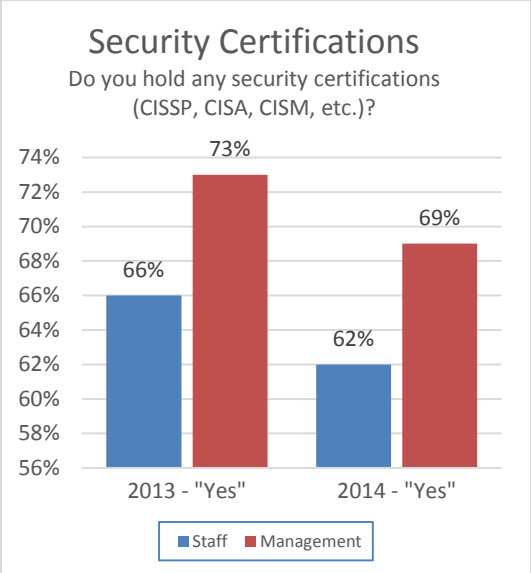

Figure 4- Security Certifications: InformationWeek 2013 & 2014 US IT Salary Survey of IT security professionals. 2013 Base: 390 staff/292 managers. 2014 Base: 369 staff/252 managers.

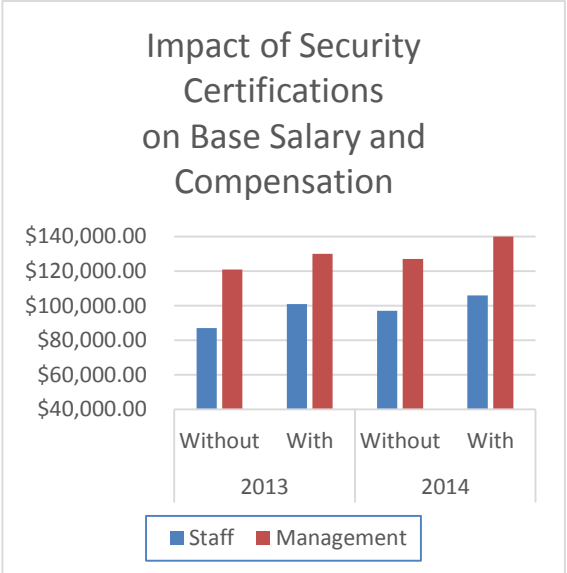

Figure 5- Certification Compensation: InformationWeek 2013 & 2014 US IT Salary Survey of IT security professionals. 2013 Base: 390 staff/292 managers. 2014 Base: 369 staff/252 managers.

A February 2014 *InformationWeek* commentary by Mark Aiello listed four reasons why security certifications matter (Aiello, 2014). Since most people getting certifications do not receive reimbursement, certifications "show your commitment to the security field." By taking initiative to complete certification on your own, certification also "makes you more attractive to potential employers." With the modern automation utilized by Human Resource departments in performing keyword searches on job applications, certification has the added benefit of "jumping out when resumes are reviewed by electronic search." Certification also provides a sense of community amongst peers with the same certification. Based on this research, the body of knowledge security certifications cover should be included as an integrated part of an education deliverable.

What the *InformationWeek* salary survey does not address is job titles. While a job title is just a name, it is important when looking for a job. A research project by Lenny Zeltser and John Hoyt revealed that according to a 2011 Bing.com search there are 821 variations of job tiles that refer to "Information Security" (Lenny Zeltser, 2011). As seen in Appendix A, Zeltser's research found Chief Information Security Officer (CISO) placed number one, and the following 41 variations were found with a frequency of at least 200 hits per query. Because a recent college graduate typically does not have the necessary number of years' experience to be a CISO, this research focuses on entry-level Analyst job positions. These jobs come in varying titles beginning with Information Assurance, Cybersecurity, and Security.

Job postings are written detailing what duties are required to fulfill specific job roles. A November 7, 2013 search of the Dice.com employment database for the term "security analyst" limited to include only Georgia, South Carolina, North Carolina, and

Virginia yielded fifty results (Dice, 2013). Thirty six of them were applicable to this research. The results show that each security position has varying job, education, certification and experience requirements (See Appendix B). Twenty-five of the 36 jobs, or 69%, had a Bachelor's degree listed as either preferred or required. Ten jobs listed a Bachelor's degree as a requirement. Thirty of the jobs had either a required or suggested minimum experience listed. Of those with a required minimum, nineteen required five years or less experience.

Interestingly, fifty percent of the jobs had some kind of certification listed as preferred or required. The most popular certification requested was Certified Information Systems Security Professional (CISSP), followed by Security+ (See Figure 6). There were a total of 25 unique certifications being listed as preferred or required, with CISSP being listed as preferred or required 31% of the time.

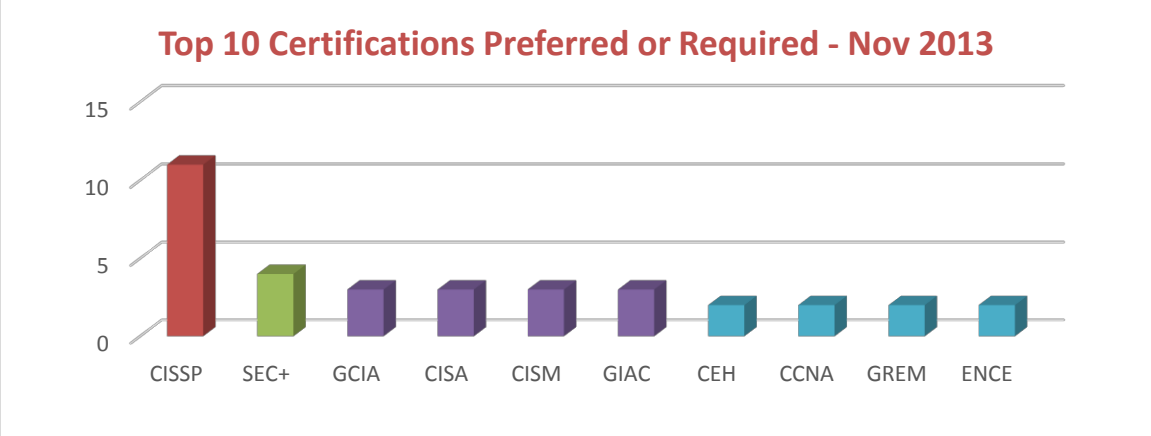

Figure 6- Certifications preferred or required based on November 2013 Job Listings in Appendix B

The same search was performed a year later, on November 28, 2014 (See Appendix B). Forty-four of the 60 jobs returned, or 73%, had a Bachelor's degree listed as either preferred or required. Forty-one of the 60 jobs had either a required or suggested minimum experience listed. Of those with a required minimum, 32 of them required five years or less experience. The search also revealed 60% had some form of

certification requirement or recommendation. The most popular certification requested was once again CISSP; followed by Security+, Certified Information Systems Auditor (CISA), and Certified Ethical Hacker (CEH), all tied for second (See Figure 7). There were a total of 33 unique certifications listed as preferred or required, with CISSP listed as preferred or required 40% of the time.

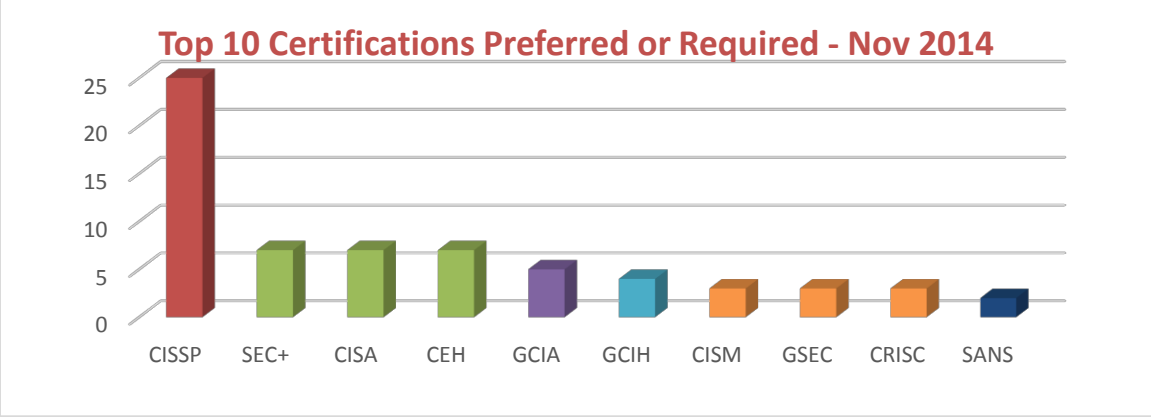

Figure 7- Certifications preferred or required based on November 2014 Job Listings in Appendix B

After evaluating the 2013 and 2014 Dice.com job results, only one result named what degree was required; namely, a BS in Computer Science. All other education results listed Bachelor of Science, Bachelor of Arts, or Bachelor's preferred or required. Based on both job result data sets, the data suggests that a Bachelor's degree should be considered a requirement for securing a job as a security analyst.

To address the need for some common understanding about cybersecurity, the National Institute of Standards and Technology (NIST) was tasked with creating a cybersecurity framework. The result was the National Initiative for Cybersecurity Education (NICE). "The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security" (National Institute of Standards and Technology, 2011). The NICE framework was designed to help map work to a

predefined set of knowledge, skills, and abilities (KSAs). The framework addresses what skills are needed for various types of jobs; however, it does not provide specifics on what education and certifications are required to obtain the necessary skills.

On November 19th and 20th, 2013, the inaugural Cyber Education Symposium was hosted in Arlington, VA. The event featured key representatives from industry, government, and education in a panel format to discuss how to better prepare a cybersecurity workforce. The various panels met to discuss challenges and spoke in very abstract terms about educational requirements. The last plenary panel consisted of Robert Hutchinson, Sandia National Labs; Albert Palacios, the Department of Education; Evan Wolff, Crowell & Moring; and Tom Baughan, Monster.com. The entire panel was asked to give their opinions as to what specific education they wanted to see out of two- and four-year graduates. The answers given were still very abstract. At the conclusion of the last session, Ms. Phyllis Bailey, Assessments and Training Division, Army Office of Information Assurance & Compliance, volunteered a more specific answer by providing a list of certifications that she is currently training army personnel to achieve. The Department of Defense and others have specific requirements for Information Assurance workers, and what those specific requirements are for education is the answer this paper endeavors to find.

It is clear that there needs to be a set of standards that properly equips a cybersecurity workforce. There is consensus that certain jobs require specific certifications. This document intends to show the educational requirements of various security workers to help higher education institutions make better decisions on what should be taught. This capstone project will help educators reduce the gap between what is taught in a classroom and what is needed to fulfill job requirements.

Definition of Terms

ACM. Abbreviation for Association for Computing Machinery.

CEH. Abbreviation for Certified Ethical Hacker.

CIP. Abbreviation for Classification of Instruction Programs.

CISA. Abbreviation for Certified Information Systems Auditor.

CISO. Abbreviation for Chief Information Security Officer.

CISSP. Abbreviation for Certified Information Systems Security Professional.

CS. Abbreviation for Computer Science.

Cybersecurity. For this paper, the definition as defined by the National Initiative for Cybersecurity Careers and Studies will be used. It defines cybersecurity as "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." (NICCS, 2013)

DHS. Abbreviation for Department of Homeland Security.

DOD. Abbreviation for Department of Defense.

IAS. Abbreviation for Information Assurance and Security. This term is used to reference a specific section of the ACM Computer Science Curricula 2013 and ACM

Information Curricula 2008: the Information Assurance and Security knowledge area.

Information Assurance. For this paper, the definition as defined by NICCS will be used. The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.

Information Security. See Information Assurance

$(ISC)^2$. Abbreviation for International Information System Security Certification Consortium, Inc. Can also be represented as ISC2.

IT. Abbreviation for Information Technology.

KA. Abbreviation for Knowledge Area.

NICCS. Abbreviation for the National Initiative for Cybersecurity Careers and Studies. NICCS is a part of NICE and serves as a national resource for cybersecurity awareness, education, careers, and training.

NICE. Abbreviation for the National Initiative for Cyber Education.

NIST. Abbreviation for the National Institute of Standards and Technology.

SACS. Abbreviation for Southern Association of College and Schools.

UNC System. Abbreviation for the University of North Carolina System. Used to reference the public institutions that make up the North Carolina higher educational system.

Chapter 3: Methodology

This research attempts to evaluate the Computer Science and Information Technology degree programs within the University of North Carolina education system with established curriculum and accreditation guidelines. The University of North Carolina education system (UNC System) consists of "16 university campuses across the state" (University of North Carolina, 2015). To ensure similar programs are evaluated, Classification of Instruction Programs (CIP) is utilized. CIP was "developed by the US Department of Education's National Center for Education Statistics in 1980 for the accurate tracking and reporting of fields of study and program completions activity" (US Department of Education: Institute of Education Sciences, 2015). For this research Computer Science programs with a CIP code of 11.0701 and Information Technology programs with a CIP code of 11.0103 were evaluated. All the schools within the UNC System are accredited by the Southern Association of College and Schools (SACSCOC, 2014).

Table 1 is a list of all the UNC System schools, and whether a Computer Science program is offered or not. Since the majority of schools in the table offer multiple Computer Science degree programs, columns have been added to reflect the different degree offerings. The final column identifies any additional accreditation that a Computer Science program may have. The accreditation is broken down by the accrediting body, program, and what years that accreditation has been in place. Table 2 is similar, except it lists only the schools that offer an Information Technology degree.

Table 1- UNC System Schools with CS degree program

	CIP	Computer Science				Accreditation (ABET, 2015)
		BA	BS	MS	PhD	
Appalachian State University	11.0701		X	X		ABET: CS,BS 1986-Present
East Carolina University	11.0701	X	X	X		
Elizabeth City State University	11.0701		X			
Fayetteville State University	11.0701		X			ABET: CS,BS 2009-Present
NC A&T State University	11.0701		X	X	X	ABET: CS,BS 1995-Present
NC Central University	No Computer Science Program					
NC State University	11.0701		X	X	X	ABET: CS,BS 1987-Present
UNC Asheville	11.0701		X			
UNC-Chapel Hill	11.0701	X	X	X		
UNC Charlotte	11.0701	X	X	X		
UNC Greensboro	11.0701		X	X		ABET: CS,BS 1995-Present
UNC Pembroke	11.0701		X			
UNC Wilmington	11.0701		X			ABET: CS-Systems Option,BS 2009-Present
UNC School of the Arts	No Computer Science Program					
Western Carolina University	11.0701		X			Seeking ABET Accreditation in 2017[1]
Winston-Salem State University	11.0701		X			ABET: CS,BS 1995-Present

Table 2- UNC System Schools with IT degree program

	CIP	Information Technology			Accreditation (ABET, 2015)
		BS	MS	PhD	
East Carolina University	11.0103	X			
NC A&T State University	11.0103	BS in Information Technology program starting Fall 2015[2]			
UNC Charlotte	11.0103		X		
UNC Pembroke	11.0103	X			
UNC Wilmington	11.0103	X			
Winston-Salem State University	11.0103	X			ABET: IT,BS 2011-Present

Many universities are already offering very good information security programs, and those programs directly target students looking for those degrees. However, the job

[1] http://www.wcu.edu/academics/departments-schools-colleges/cas/casdepts/mathcsdept/mathcsacadprogs/, January 30, 2014

[2] http://www.ncat.edu/academics/schools-colleges1/sot/index.html, January 30, 2014

data set for this research did not have any postings requiring an information security degree. An evaluation of typical computer science and information technology programs is made to determine if general security awareness is effectively delivered.

Existing information security education delivered is compared to existing job openings to determine if job needs are being met. Considering how different many of the business major programs are, all business majors are excluded, which includes most Management Information Systems programs. Minors have also been excluded, as the depth of instruction can make it difficult to perform direct comparisons. The primary research method employed in this paper is qualitative in nature. Where possible, quantitative assessments have been performed for the purposes of more clearly making comparisons.

Once each school with a qualifying program are identified, required core classes will be evaluated. This research is not comparing a given program to another, but placing focus on only the required core classes that include security, and any security related electives offered. In order to identify classes that include security, the search terms of "security", "secure", "crypto", "assurance", "intrusion", and "protect" are used. These terms were selected after a pre-evaluation of the course catalogs of the schools evaluated. Each university's course catalog was searched and classes that matched these keywords were added to the appendix for reference, with the respective matching keyword underlined. Utilizing the keywords resulted in a reduced chance of overlooking a course that delivers security related content; however, each catalog was reviewed fully for any additional security class offerings. A table of schools with required and optional security classes is generated, to make comparison easier.

An October 2014 article by Ed Tittle titled "Best Information Security Certifications for 2015" listed Security+, Certified Ethical Hacker, GIAC Security Essentials, CISSP, and Certified Information Security Manager as the top five information security certifications for 2015 (Tittel, 2015). Based on the November 2014 job data, the top four certifications identified were CISSP, Security+, CISA and CEH (See Figure 7). Further evaluation of these four certifications revealed that the CISA certification concentrates on auditing, and has a five year minimum experience requirement (See Appendix C), so it will not be evaluated as part of this research. The CISSP has a five year work experience requirement, but a four year degree can be used to substitute for one year's experience. Considering its popularity, it will still be evaluated; however, new graduates would not normally be qualified for this certification. Both the Security+ and CEH certifications prefer two years' experience and are targeted at IT professionals working with security.

An analysis of the CISSP, Security+, and CEH certifications are performed, breaking each body of knowledge into its component parts. Common elements from each certification are identified, and used to evaluate the classes being taught. The goal is to create a list of required elements of security that should be taught, yet be certification neutral. This is referred to as the recommended body of knowledge. To further validate results, they are evaluated against ABET's accreditation requirements.

With the recommended body of knowledge in hand, a comparison is made with each class that contains a security element. Each class content is compared to the recommended body of knowledge to see how many elements are being fulfilled. Once each class has been evaluated, each University program is evaluated, and ranked, based on its fulfillment of the recommended body of knowledge.

Chapter 4: Outline of Completed Project

I. Evaluation of security courses currently being delivered

The current course offerings from the different institutions utilize very different naming and numbering schemes which present a challenge when examining what educational value is being delivered. Table 3 is a summary of Appendix D: an evaluation of each UNC System school with a Computer Science program, and security classes offered. To ensure similar programs are evaluated, CIP codes are utilized.

Table 3- Computer Science classes with a security element

CIP Code	UNC School	Degree	Required Classes with a Security Element	Additional Classes with a Security Element
11.0701	Appalachian State University	BS	CS 3430	CS 3760, 3770, 4435, 4520
11.0701	Appalachian State University	MS	CS 5520	
11.0701	East Carolina University	BA	CSCI 4000, 4300	CSCI 4540
11.0701	East Carolina University	MS		SENG 6247
11.0701	East Carolina University	BS	CSCI 4000	CSCI 4300, 4540
11.0701	Elizabeth City State University	BS	CSC 260, 410, BMIS 410	CSC 420
11.0701	Fayetteville State University	BS	CSC 403, 490	CSC 323, 380
11.0701	NC A&T State University	BS	COMP 450, 476	COMP 120, 170, 320, 321, 420, 421
11.0701	NC A&T State University	PhD	COMP 821, 823	COMP 620, 621, 627, 722, 723, 724, 725, 726, 727, 750, 755, 829, 875, 876
11.0701	NC A&T State University	MS	COMP 620, 621, 726	COMP 627, 722, 723, 724, 725, 727, 750, 755
11.0701	NC State University	M	CSC 540, 570	CSC 513, 515, 522, 547, 574, 575
11.0701	NC State University	BS	CSC 246	CSC 200, 340, 405, 413, 422, 440, 453, 474
11.0701	NC State University	PhD	CSC 540, 570	CSC 513, 515, 522, 547, 574, 575, 705, 712, 743, 774
11.0701	NC State University	MS	CSC 540, 570	CSC 513, 515, 522, 547, 574, 575
11.0701	UNC Asheville	BS	CSCI 331	CSCI 444
11.0701	UNC-Chapel Hill	PhD		
11.0701	UNC-Chapel Hill	BA		COMP 380, 382, 535
11.0701	UNC-Chapel Hill	BS		COMP 380, 382, 535
11.0701	UNC-Chapel Hill	MS		COMP 721, 722, 734

CIP Code	UNC School	Degree	Required Classes with a Security Element	Additional Classes with a Security Element
11.0701	UNC Charlotte	MS	ITIS 6200	ITCS 5146, 6144, 6164, ITIS 5220, 5221, 6120, 6130, 6150, 6164, 6167, 6177, 6201, 6210, 6230, 6240, 6320, 6362, 6420
11.0701	UNC Charlotte	BA		ITCS 1203, 4131, 4146
11.0701	UNC Charlotte	BS	ITCS 4146, ITIS 3200	ITCS 1203, 4131
11.0701	UNC Greensboro	BS	CSC 562	CSC 580, 583
11.0701	UNC Greensboro	MS		CSC 680, 676
11.0701	UNC Pembroke	BS		CSC 3350, 3380, 4020, 4350
11.0701	UNC Wilmington	BS	CSC 385	CSC 105, 446
11.0701	Western Carolina University	BS		CS 210, 430, 431
11.0701	Winston-Salem State University (Security Option)	BS	CSC 3325, 4330, 4360, 4370	CSC 1307, 3323, 3332, 3355, 4323,

On average, 68% of UNC System Computer Science programs have a required course that included a published security element. Table 4 provides a breakdown of the distribution of results.

Table 4- Computer Science Programs Evaluated

	Programs evaluated	Programs with a required class containing a Security Element	% Schools with a required class containing a Security Element
Bachelor's Degree	17	12	71%
Master's Degree	8	5	62%
Doctoral Degree	3	2	67%
Total	**28**	**19**	**68%**

Although Table 4 shows greater than 60% of schools have a required class with a security element, the material delivered can be quite different. Table 5 shows an unequal distribution of required security elements taught. An equal distribution would show all schools teaching the same elements throughout. The first column contains a list of key security elements taught. This list was created by evaluating the required security classes and finding the primary topic taught. As unique security elements were identified it

would then be added to the list, and the corresponding class added to the distribution column with a parenthetical reference to the school. The list is not based on a given set of criteria, but rather an attempt to combine dissimilar course names into a cohesive unit for ease of comparison. For example, the first row states "Database" as a key security element being taught. Appalachian State University teaches CS 3440 – Database and NC State teaches CS 540 – Database Management concepts and Systems (See Appendix D). Both classes have a focus on Databases, but the course titles and numbers are different and the classes do not cover the same exact material. Although other UNC System schools may also require a Database class, if course catalog for each respective school did not list security as an element of the class, it was not evaluated. According to Table 5, the only schools with a published required security element in a Database class is Appalachian State and NC State.

Table 5- Distribution of Computer Science Required Classes with a Security Element

Key Security Element Being Taught	**Distribution**		
Database	CS 3430 (App State)	CSC 540 (NC State)	
Operating Systems	CS 5520 (App State)	COMP 450 (NCA&T)	CSC 246 (NC State)
	CSCI 331 (Asheville)	CSC 562 (Greensboro)	
Ethics	CSCI 4000 (ECU)	CSC403 (Fay State)	CSC 385 (UNCW)
Systems Programming	CSCI 4300 (ECU)		
Seminar in Computer Science	CSC 260 (Eliz State)	CSC 490 (Fay State)	
Networks	BMIS 410 (Eliz State)	COMP 476 (NCA&T)	COMP 726 (NCA&T)
	CSC 570 (NC State)	CSC 410 (Eliz State)	
Cloud Computing	COMP 821 (NCA&T)		
Social Computing	COMP 823 (NCA&T)		
Information, Privacy & Security	COMP 620 (NCA&T)	ITIS 6200 (Charlotte)	ITIS 3200 (Charlotte)
	CSC 3325 (Winston)		
Web Security	COMP 621 (NCA&T)	CSC 4370 (Winston)	
Grid Computing	ITCS 4146 (Charlotte)		
Cryptography	CSC 4330 (Winston)		
Hardware & Media	CSC 4360 (Winston)		

The same research that was performed on Computer Science curriculum was performed on Information Technology programs. Table 6 is an evaluation of each school, program offering, and security classes offered.

Table 6- Information Technology classes with a security element

CIP Code	UNC School	Degree	Required Security Classes	Security Electives
11.0103	East Carolina University	BS IT	ICTN 4200, 4201, 4800, 4801	
11.0103	UNC Charlotte	MS IT	ITIS 6200	ITIS 5220, 5221, 5250, 6150, 6167, 6210, 6220, 6230, 6240, 6362, 6420
11.0103	UNC Pembroke	BS IT	ITC 2080	ITC 3250
11.0103	UNC Wilmington	BS IT	CIT 204, 324, 410, 213	
11.0103	Winston-Salem State University	BS IT	CSC 3325	

Unlike the Computer Science programs, all the UNC System Information Technology programs have required classes with a security element. However, there is still no agreement with what elements of security should be required. Table 7 is an evaluation of Information Technology required classes with a security element, similar to the Computer Science evaluation in Table 5.

Table 7- Distribution of Information Technology Required Classes with a Security Element

Key Security Element	Distribution		
Database	CIT 213 (UNCW)		
Information, Privacy & Security	ITIS 6200 (Charlotte)	CSC 3325 (Winston)	
Intrusion Detection	ICTN 4200 (ECU)	ICTN 4201 (ECU)	
Information Assurance	ICTN 4800 (ECU)	ICTN 4801 (ECU)	
Systems Administration	ITC 2080 (Pembroke)		
Digital Media	CIT 204 (UNCW)		
Info. Sec. Management	CIT 324 (UNCW)		
Web App. Development	CIT 410 (UNCW)		

While evaluating the curriculum at each UNC System school, an effort was made to determine if certification is currently a deliverable. Of the classes evaluated, there was no mention of any requirement for a certification as a class prerequisite, or requiring certification for class completion.

II. Guidelines compared against security certifications

Table 8 is mapping the ACM 2013 Computer Science (CS) curricula recommendations to the top three information security certifications requested for area jobs. The ACM CS Guideline consists of eighteen knowledge areas (KA). This research focuses on the Information Assurance and Security (IAS) portion of the curricula guideline, so all references to the ACM guidelines refer to the IAS KA. Some elements of the ACM IAS guidelines follow closely to the NICE framework. When the ACM Guidelines were being assembled, the workshop participants considered NICE as "a good starting point from which to build a cybersecurity curriculum" (McGettrick, 2013). However, others cautioned that "a simpler categorization scheme would better guide curriculum development." The result is a simpler curricular framework.

Note that no individual certification in Table 8 covers all the recommended areas. Many of the most important elements of a comprehensive security education can be found by looking at commonalities in all three certifications. The first column of the table is the ACM 2013 Computer Science IAS curricula guideline. A numbering system has been added to allow cross-reference from certification knowledge areas. The remaining columns is a cross-reference to the location where the knowledge areas from the ACM guideline can be found in the respective certification. The dotted decimal numeric values represent the domain or module followed by the subsection that covers that material. Appendix C contains a breakdown of each certification's exam objective based on exam outlines. For example, in Table 8 row 1.1 is CIA (Confidentiality, Integrity, and Availability). CIA is covered in CISSP Domain 1 [Security & Risk Management] subsection A [Confidentiality, Integrity, & Availability] as well as Domain 3 [Security Engineering] subsection A [Implement & Manage Secure Engineering

Processes]. CIA can be found in the Security+ exam objectives under Domain 2 [Compliance and Operation Security] subsection 9 [Select Appropriate Control to Meet the Goals of Security]. Finally, the CEH covers CIA in Module 1 [Introduction to Ethical Hacking] subsection 1 [Information Security Overview].

Table 8- ACM 2013 Computer Science Curricula Guidelines and security certification mapping

ACM IAS Guideline for Computer Science	CISSP	Security+ SY0-401	CEH 312-50
1. IAS/Foundational Concepts in Security [1 Core- Tier1 hour]			
1.1 CIA (Confidentiality, Integrity, Availability)	1.A / 3.A	2.9	1.1
1.2 Concepts of risk, threats, vulnerabilities, and attack vectors	1.I-K	2.1	1.2
1.3 Authentication and authorization, access control	5.A-B, E	5.2	1.6 / 5.4
1.4 Concept of trust and trustworthiness	1.E	5.2	9.1
1.5 Ethics	1.E	2.3	1.3 / 1.6
2. IAS/Principles of Secure Design [1 Core- Tier1 hour, 1 Core- Tier2 hour]			
2.1 Least privilege and isolation	7.E	5.2	-
2.2 Fail-safe defaults	7.K	2.9	-
2.3 Open design	3.A	-	-
2.4 End-to-end security	3.C	2.1	-
2.5 Defense in depth	3.A-E	1.3	1.6
2.6 Security by design	3.A	1.3	-
2.7 Tensions between security and other design goals	3.D	-	-
2.8 Complete mediation	5.F	-	-
2.9 Use of vetted security components	3.D	-	-
2.10 Economy of mechanism	3.D	-	-
2.11 Usable security	5.E	-	1.1
2.12 Security composability	5.D	-	-
2.13 Prevention, detection, and deterrence	1.I / 4.D / 5.F / 7.C,H	1.2	9.2 / 11.4 / 15.8 / 18.5
3. IAS/Defensive Programming [1 Core- Tier1 hour, 1 Core- Tier2 hour]			
3.1 Input validation and data sanitation	8.B	4.1	13.2-3
3.2 Choice of programming language and type-safe languages	8.B	4.1	-
3.3 Examples of input validation and data sanitization errors (Buffer Overflow/SQL injection/XSS vulnerability)	8.B	3.5	13.2 / 13.5 / 14.1-9 / 18.1-7
3.4 Race conditions (time-of-check-to-time-of-use)	8.B	4.1	-

ACM IAS Guideline for Computer Science	CISSP	Security+ SY0-401	CEH 312-50
3.5 Correct handling of exceptions and unexpected behaviors	8.A-C	4.1	-
3.6 Correct usage of 3rd party components	5.D / 7.H	2.2	-
3.7 Effectively deploying security updates (patch management)	7.I	4.3	12.5-6
4. IAS/Threats and Attacks [1 Core- Tier2 hour]			
4.1 Attacker goals, capabilities, and motivations	1.J	2.1	1.3
4.2 Examples of malware	7.H	3.1	6.1-7 / 7.1-6
4.3 Denial of Service (DoS and Distributed Denial of Service (DDoS)	7.H	3.2	10.1-8
4.4 Social engineering (e.g., phishing)	1.J	3.3	9.1-6 / 2.3
4.5 Attacks on privacy and anonymity	1.J	2.2	3.2
4.6 Malware/unwanted communication such as covert channels and steganography	7.C	2.9	5.4
5. IAS/Network Security [2 Core- Tier2 hours]			
5.1 Network specific threats and attack types	4.D	1.1-5 / 3.6	3.1-2 / 2.3 / 11.2
5.2 Use of cryptography for data and network security	4.A	6.1-3	19.1-8
5.3 Architectures for secure networks	4.A	4.5	3.1 / 17.1-2 / 20.5
5.4 Defense mechanisms and countermeasures	4.B	1.3	6.5 / 7.5 / 8.8 / 10.6 / 11.4 / 12.5 / 13.5 / 14.9 / 15.7 / 17.7 / 18.5
5.5 Security for wireless, cellular networks	3.G / 4.B	1.5 / 3.4	15.1-9
5.6 Other non-wired networks	3.E	3.4 / 4.5	16.1-8
5.7 Censorship resistance	-	-	3.2
5.8 Operational network security management	7.C	3.6	-
6. IAS/Cryptography [1 Core- Tier2 hour]			
6.1 Basic Cryptography Terminology	2.E / 3.E,I / 4.A	6.1	19.1
6.2 Cipher types together with typical attack methods such as frequency analysis	3.E	6.2	19.2
6.3 Public Key Infrastructure support for digital signature and encryption and its challenges	3.I	6.3	19.4
6.4 Mathematical Preliminaries essential for cryptography	3.I	6.1	19.1-2
6.5 Cryptographic primitives	3.I	6.1-3	19.1-2
6.6 Symmetric key cryptography	3.I	6.1-3	19.1
6.7 Public Key cryptography	3.I	6.3	19.4

ACM IAS Guideline for Computer Science	CISSP	Security+ SY0-401	CEH 312-50
6.8 Authenticated key exchange protocols (e.g., TLS)	4.C	1.4 / 6.2	19.5
6.9 Cryptographic protocols	3.I	6.2	19.2
6.10 Motivate concepts using real-world applications	3.I	6.1-3	19.1-8
6.11 Security definitions and attacks on cryptographic primitives	3.I	6.1	19.7
6.12 Cryptographic standards and references implementations	3.I	6.1	19.1-8
6.13 Quantum cryptography	3.I	6.1	-
7. IAS/Web Security [Elective]			
7.1 Web security model	3.F	6.3	13.1
7.2 Session management, authentication	5.B	4.2 / 5.2	11.1
7.3 Application vulnerabilities and defenses	7.D	3.5-6 / 4.1-3	13.2
7.4 Client-side security	3.E	3.2 / 4.1	-
7.5 Server-side security tools	3.E	-	13.6
8. IAS/Platform Security [Elective]			
8.1 Code integrity and code signing	6.B / 8.A-D	3.7	-
8.2 Secure boot, measured boot, and root of trust	3.I	6.3	-
8.3 Attestation	3.K	4.4	-
8.4 TPM and secure co-processors	3.D	4.4	-
8.5 Security threats from peripherals	3.H	4.4	5.4
8.6 Physical attacks	3.J-K / 5.A / 7.O	2.7 / 4.3	-
8.7 Security of embedded devices	3.H	4.5	16.1-8
8.8 Trusted path	7.E	4.3	6.1
9. IAS/Security Policy and Governance [Elective]			
9.1 Privacy policy	1.C-D, H / 2.C	2.1	1.6 / 5.4
9.2 Inference controls/statistical disclosure limitation (infer secrets from a database)	3.E	-	-
9.3 Backup policy, password refresh policy	1.F	2.1-2 / 5.3	1.6
9.4 Breach disclosure policy	1.D	2.5	1.1
9.5 Data collection and retention policies	2.D	2.1 / 2.3	-
9.6 Supply chain policy	1.H	-	-
9.7 Cloud security tradeoffs	3.E / 7.D	2.1	-
10. IAS/Digital Forensics [Elective]			
10.1 Basic Principles and methodologies for digital forensics	7.A	2.4	-
10.2 Design systems with forensic needs in mind	-	-	-
10.3 Rules of Evidence - general concepts & differences between jurisdictions and Chain of Custody	2.B / 7.A	2.4	-

ACM IAS Guideline for Computer Science	CISSP	Security+ SY0-401	CEH 312-50
10.4 Search and Seizure of evidence: legal and procedural requirements	2.F / 7.B	2.4	-
10.5 Digital Evidence methods and standards	7.A	2.4	-
10.6 Techniques and standards for Preservation of Data	2.A / 7.A / 7.F	2.4	-
10.7 Legal and Reporting Issues including working as an expert witness	-	2.4	-
10.8 OS/File system Forensics	-	2.4	-
10.9 Application Forensics	-	2.4	-
10.10 Web Forensics	-	-	-
10.11 Network Forensics	-	2.4	-
10.12 Mobile Device Forensics	-	4.2	-
10.13 Computer/network/system attacks	1.J	2.4	-
10.14 Attack detection and investigation	7.B	2.4	-
10.15 Anti-forensics	-	-	-
11. IAS/Secure Software Engineering [Elective]			
11.1 Building security into the software development lifecycle	8.A	4.1	-
11.2 Secure design principles and patterns	8.B	3.7	-
11.3 Secure software specifications and requirements	8.A-D	3.7	-
11.4 Secure software development practices	8.B	4.1	-
11.5 Secure testing	8.C	4.1	-
11.6 Software quality assurance and benchmarking measurements	8.C-D	3.7	-

Similar to Table 8, Table 9 maps the ACM 2008 Information Technology curricula recommendations to the top three information security certifications requested for area jobs. The ACM IT Guideline consists of eleven knowledge areas (KA). Table 9 focuses on the Information Assurance and Security (IAS) portion of the IT curricula guideline, and follows the same format as Table 8.

Table 9- ACM 2008 Information Technology Curricula Guidelines and security certification mapping

ACM IAS Guideline for Information Technology	CISSP	Security+ SY0-401	CEH 312-50
1. IAS/Fundamental Aspects [3 hours]			
1.1 History and terminology	Throughout	Throughout	Throughout
1.2 Security mindset	Throughout	Throughout	Throughout
1.3 Design principles	3.A-E	1.3	1.6
1.4 System/security life-cycle	7.E	4.1	-
1.5 Security implementation mechanisms	3.A-E	2.9	1.2
1.6 Information assurance analysis model	3.B	3.6	1.1
1.7 Disaster recovery	6.C	2.8	-
1.8 Forensics	7.A	2.4	-
2. IAS/Security Mechanisms			
2.1 Cryptography	2.E / 3.E,I / 4.A	6.1-3	19.1-8
2.2 Authentication	5.A-B, E	5.1-3	1.6 / 5.4
2.3 Redundancy	7.K	2.8	-
2.4 Intrusion detection	7.C,H	3.6 / 4.3	17.1-2
3. IAS/Operational Issues			
3.1 Trends	-	2.6	1.1
3.2 Auditing	6.E	2.3	20.1
3.3 Cost/benefit analysis	1.G	2.8	1.3
3.4 Asset management	7.D	2.7 / 4.2-3	-
3.5 Standards	1.F / 2.E	2.1-2	-
3.6 Enforcement	8.B	2.3 / 2.5	-
3.7 Legal issues	1.D	4.2	-
3.8 Disaster recovery	6.C	2.8	-
4. IAS/Policy			
4.1 Creation of policies	1.F	2.1	1.6
4.2 Maintenance of policies	1.F	2.1	1.6
4.3 Prevention	1.J	2.7	1.6
4.4 Avoidance	1.J	2.7	1.6
4.5 Incident response (forensics)	7.G	2.4	1.6
4.6 Domain integration	7.D	1.1-2 / 2.7	1.6
5. IAS/Attacks			
5.1 Social engineering	1.J	3.3	9.1-6 / 2.3
5.2 Denial of Service	7.H	3.2	10.1-8
5.3 Protocol attacks	4.A	3.2	8.1 / 8.4
5.4 Active attacks	-	3.7	5.4 / 8.1
5.5 Passive attacks	-	3.7	5.4 / 8.1

ACM IAS Guideline for Information Technology	CISSP	Security+ SY0-401	CEH 312-50
5.6 Buffer overflow attacks	8.B	3.5	13.2 / 13.5 / 14.1-9 / 18.1-7
5.7 Malware	7.H	3.1	6.1-7 / 7.1-6
6. IAS/Security Domains			
6.1 Security awareness	1.L	1.4 / 2.2	1.1 / 13.1-2
7. IAS/Forensics			
7.1 Legal systems	2.F / 7.B	2.4	-
7.2 Digital forensics and its relationship to other forensic disciplines	7.A	2.4	-
7.3 Rules of evidence	7.A	2.4	-
7.4 Search and seizure	2.F / 7.B	2.4	-
7.5 Digital evidence	7.A	2.4	-
7.6 Media analysis	2.A / 7.A / 7.F	2.4	-
8. IAS/Information States			
8.1 Transmission	4.B	4.4	-
8.2 Storage	4.B	4.4	-
8.3 Processing	4.B	4.4	-
9. IAS/Security Services			
9.1 Confidentiality, Integrity, Availability	1.A / 3.A	2.9	1.1
9.2 Authentication	5.A-B, E	5.2	1.6 / 5.4
9.3 Non-repudiation	3.I	2.9 / 6.1	1.1
10. IAS/Threat Analysis Model			
10.1 Risk assessment	1.I	2.1 / 4.5	-
10.2 Cost benefit	1.I	2.1	-
11. IAS/Vulnerabilities			
11.1 Perpetrators	1.J	3.2-5	1.3
11.2 Inside attacks	1.J	3.2-5	9.2
11.3 External attacks	1.J	3.2-5	1.3
11.4 Black hat	-	3.8	1.3
11.5 White hat	-	3.8	1.3
11.6 Ignorance	-	3.8	-
11.7 Carelessness	-	3.8	-
11.8 Network	4.D	1.5 / 3.4,6	3.1-2
11.9 Hardware	7.D	4.3	5.4
11.10 Software	8.B	4.1	5.4
11.11 Physical access	7.O	2.7,9	-

In an effort to validate the mapping in Table 8 and Table 9, a request was sent to each certifying body asking for their review (See Appendix C). EC-Council, certifying body for the CEH, was very quick to respond and provided additional resources assisting in this research. Their final response came from their instructional design department: "EC-Council monitors all of our public endorsements, findings and communications and are unable to fulfill your request at this time outside of the information already referenced on the EC-Council web site. Information you present in your thesis is based on your particular research and opinions. Please consider comparing all our certification courses as many items in your chart reference content in several of our other offerings." $(ISC)^2$, certifying body for the CISSP, utilized an online request form that made it difficult to submit the review request with proper table formatting, prompting a reply: "Unfortunately, the format of your below email does not allow us to accurately review the contents of the message. $(ISC)^2$ does not have the resources to provide an accurate review of our CISSP domains in conjunction with the standards of another IT body. I apologize for any inconvenience this may cause." As of this writing no response has been received from CompTIA, certifying body for the Security+, regarding the request.

Although this research focused on three specific certifications, it is important to note that these certifying bodies offer additional certifications that would fill many of the gaps or shortcomings of the certifications evaluated. For example, $(ISC)^2$ offers a Certified Cyber Forensic Professional (CCFP) certification which would fill in the gaps found in the Digital Forensics portion of the ACM CS IAS guideline not covered by the CISSP. Likewise, EC-Council offers certifications in Computer Hacking Forensic Investigator (CHFI), and EC-Council Certified Secure Programmer (ECSP) which would

address the shortcomings in the CEH relative to the Digital Forensics and Secure Software Engineering portions of the ACM CS IAS guideline.

III. Recommended body of knowledge compared with existing Computer Science course delivery.

The ACM CS IAS curricula guideline is broken down into groups of related information not only to convey the information easier, but to help define what domains should be considered core elements within a computer science program. In Table 10, note the use of the terms Core Tier-x and Elective associated with the various Knowledge Areas. The 2013 ACM CS curricula guideline explains Core Tier-1 as a topic that "should be a required part of every Computer Science curriculum" and are typically covered in introductory courses (ACM and IEEE, 2013, p. 30). Core Tier-2 topics are "generally essential in an undergraduate computer-science degree" (ACM and IEEE, 2013, p. 30). The guideline stresses the importance of the Core materials, in bold, by stating, "A computer-science curriculum should aim to cover 90-100% of the Core Tier-2 topics, with 90% considered a minimum" (ACM and IEEE, 2013, p. 30). Not all the materials within the electives are expected to be covered; however, "A program covering only core material would provide insufficient breadth and depth in computer science" (ACM and IEEE, 2013, p. 31). The Core hours represent the number of lecture hours for a given knowledge area. For example, IAS/Foundational Concepts in Security has one Core-Tier 1 hour, and IAS/Network Security has two Core-Tier 2 hours. To simplify the evaluation of the course offerings, IAS Foundation Concepts in Security, Principles of Secure Design, and Defensive Programming are all considered Core 1. IAS/Threats and Attacks, Network Security, and Cryptography are all Core 2, and the electives remain the same.

Table 10- ACM IAS CS Guideline Core hour distribution

ACM IAS Guideline KA's	Core-Tier hours	
1. IAS/Foundational Concepts in Security	(1) Core- Tier1 hour	Core 1
2. IAS/Principles of Secure Design	(1) Core- Tier1 hour, (1) Core- Tier2 hour	
3. IAS/Defensive Programming	(1) Core- Tier1 hour, (1) Core- Tier2 hour	
4. IAS/Threats and Attacks	(1) Core- Tier2 hour	Core 2
5. IAS/Network Security	(2) Core- Tier2 hours	
6. IAS/Cryptography	(1) Core- Tier2 hour	
7. IAS/Web Security	Elective	
8. IAS/Platform Security	Elective	
9. IAS/Security Policy and Governance	Elective	
10. IAS/Digital Forensics	Elective	
11. IAS/Secure Software Engineering	Elective	
Totals:	**(3) Core-Tier1 hours, (6) Core-Tier2 hours**	

What Table 10 does not include are additional Knowledge Areas that include security elements. Other KA's such as IM/Information Management Concepts, OS/Overview of OS, SDF/Development Methods, and others exist within the ACM CS guideline, and support the security topics from a fundamental perspective. An additional 32 Core-Tier1 hours and an additional 31.5 Core-Tier2 hours of security related material is distributed in other KA's (ACM and IEEE, 2013, pp. 98-102).

In order to accurately evaluate if Computer Science classes currently deliver an appropriate amount of security related curricula, required computer science classes that include a security element needed to be mapped to the ACM CS IAS Guideline. Table 11 maps the data from Table 5- Distribution of Computer Science Required Classes with a Security Element to the ACM CS IAS Guideline. Although most of the classes in this table are not dedicated security classes, the mapping attempts to most closely associate the KA's being delivered within the guideline.

Table 11- Computer Science security elements being taught mapped to ACM CS IAS Guideline

Key Security Element Being Taught	Most Closely Maps to ACM IAS Guideline
Database	IAS/Defensive Programming
Operating Systems	IAS/Platform Security
Ethics	IAS/ Foundational Concepts in Security
Systems Programming	IAS/Defensive Programming & IAS/Secure Software Engineering
Seminar in Computer Science	IAS/Foundational Concepts in Security
Networks	IAS/Network Security
Cloud Computing	IAS/Platform Security
Social Computing	IAS/Threats and Attacks
Information, Privacy & Security	IAS/Foundational Concepts in Security, IAS/Principles of Secure Design, IAS/Security Policy and Governance
Web Security	IAS/Web Security
Grid Computing	IAS/Network Security
Cryptography	IAS/Cryptography
Hardware & Media	IAS/Platform Security

With the exception of Digital Forensics, all the elements of the ACM CS IAS guideline KA's are being taught in some form or another in required courses offered at the various schools within the UNC System (See Table 11). However, what is the exact distribution? An accurate assessment of these findings require an evaluation of each degree offering, including required and elective course offerings.

Table 12, Table 13, and Table 14 are summaries of the detailed evaluation of each required and elective class offered in Computer Science curriculum programs within the UNC System (See Appendix E for details). Table 12 is an evaluation of Bachelor Degrees in Computer Science. The data is broken down into Core1, Core2, and Electives followed by the percentage of the guideline being fulfilled. Each Core or Elective column contains the total number of classes being offered, whether required or elective, that meet the given criteria. Note that Core 1 and Core 2 each consist of three KA's, and Electives consist of 5 KA's (See Table 10 for detailed breakdown). The rightmost column is a percentage of the ACM CS IAS Guideline currently being met. This is

calculated by the sum of Core 1, Core 2, and Electives, and dividing by the total number of KA's, which is eleven.

Table 12- Evaluation of Computer Science Bachelor's Degrees with required and elective courses that include security elements compared to ACM CS IAS Guideline

UNC School	Degree	Core 1 Fulfilled (max 3)	Core 2 Fulfilled (max 3)	Electives Fulfilled (max 5)	% ACM CS IAS Guideline being delivered. (KA's offered / 11 KA's)
Appalachian State University	BS	1	1	3	45%
East Carolina University	BA	2	1	1	36%
East Carolina University	BS	2	1	1	36%
Elizabeth City State University	BS	1	1	1	27%
Fayetteville State University	BS	1	1	1	27%
NC A&T State University	BS	2	1	3	55%
NC State University	BS	3	1	2	55%
UNC Asheville	BS	0	0	2	18%
UNC-Chapel Hill	BA	1	2	0	27%
UNC-Chapel Hill	BS	1	2	0	27%
UNC Charlotte	BA	1	1	0	18%
UNC Charlotte	BS	2	1	1	36%
UNC Greensboro	BS	0	2	1	27%
UNC Pembroke	BS	1	2	2	45%
UNC Wilmington	BS	2	1	0	27%
Western Carolina University	BS	3	2	1	55%
Winston-Salem State University (Security Option)	BS	3	1	3	64%

Table 12 reveals that an average of 50.98% of Core 1 KA's, 41.18% of Core 2 KA's, and 25.88% of Elective KA's are currently being delivered in Bachelors of Computer Science programs. One possible outlier is the Winston-Salem State University Computer Science program, given that it has a Security Option. Winston-Salem State's program currently adheres to 64% of the ACM CS IAS recommendation. There is a three

way tie between NC A&T State University, NC State University, and Western Carolina University with each adhering to 55% of the ACM IAS recommendation.

Table 13 is a similar evaluation of the Master's degree programs.

Table 13- Evaluation of Computer Science Master's Degrees with required and elective courses that include security elements compared to ACM CS IAS Guideline

UNC School	Degree	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM CS IAS Guideline being delivered. (KA's offered / 11 KA's)
Appalachian State University	MS	0	0	1	9%
East Carolina University	MS	0	0	1	9%
NC A&T State University	MS	3	2	4	82%
NC State University	M	1	1	3	45%
NC State University	MS	1	2	3	55%
UNC-Chapel Hill	MS	1	1	1	27%
UNC Charlotte	MS	3	3	4	91%
UNC Greensboro	MS	0	1	2	27%

Table 13 reveals that an average of 37.5% of Core 1 KA's, 41.67% of Core 2 KA's, and 47.50% of Elective KA's are currently being delivered in Masters of Computer Science programs. Of interest is that the number of Core 1 KA's are down 13.48% as compared to Bachelor's degree programs. One reason for the decrease could be that a given Master's degree program assumes its students have most of the foundational elements presented in Core 1. Also compared to Bachelor's degrees, Core 2 values are almost identical and Electives are up 21.62%

Table 14 is a similar evaluation of Doctoral degree programs. NC A&T State University's PhD program includes a concentration in Security, hence the high percentage of guidelines being met. UNC-Chapel Hill's program is very broad, as is reflected in the lack of security KA's required.

Table 14- Evaluation of Computer Science Doctoral Degrees with required and elective courses that include security elements compared to ACM IAS Guideline

UNC School	Degree	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (KA's offered / 11 KA's)
NC A&T State University	PhD	3	2	4	82%
NC State University	PhD	1	2	4	64%
UNC-Chapel Hill	PhD	0	0	0	0%

It is difficult to make an accurate statistical evaluation of the PhD programs as a whole, as each program is unique.

IV. Recommended body of knowledge compared with existing Information Technology course delivery.

Similar to the evaluation of computer science curricula, the ACM IT IAS curricula guideline was broken down into groups of related information. Table 15 maps the data from Table 7- Distribution of Information Technology Required Classes with a Security Element to the ACM IT ISA Guideline. This mapping attempts to most closely associate the KA's being delivered within the guideline.

Table 15- Information Technology security elements being taught mapped to ACM IT IAS Guideline

Key Security Element Being Taught	Most Closely Maps to ACM IT Guideline
Database	IAS/Security Domains
Information, Privacy & Security	IAS/Fundamental Aspects, IAS/Security Mechanisms, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities
Intrusion Detection	IAS/Attacks, IAS/Vulnerabilities
Information Assurance	IAS/Fundamental Aspects, IAS/Security Domains, IAS/Information States, IAS/Security Services
Systems Administration	IAS/Information States
Digital Media	IAS/Security Mechanisms, IAS/Forensics, IAS/Information States
Info. Sec. Management	IAS/Fundamental Aspects, IAS/Operational Issues, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities
Web App. Development	IAS/Attacks, IAS/Vulnerabilities

Table 15 reveals that all the elements of the ACM IT IAS guideline KA's are being taught in required courses offered at the various schools within the UNC System.

Table 16 is a summary of a detailed evaluation of each required and elective classes offered in Information Technology curriculum programs within the UNC System (See Appendix E for details).

Table 16- Evaluation of Information Technology Degrees with required and elective courses that include security elements compared to ACM IT IAS Guideline

UNC School	Degree	KA's Fulfilled (max 11)	% ACM IT IAS Guideline being delivered. (KA's offered / 11 KA's)
East Carolina University	BS	6	55%
UNC Pembroke	BS	5	45%
UNC Wilmington	BS	11	100%
Winston-Salem State University	BS	7	64%
UNC Charlotte	MS	11	100%

V. Statistical analysis of results.

An evaluation of each certification was made to find any gaps between the ACM CS IAS and ACM IT IAS guidelines and the Knowledge Areas (KA's) of each certification. Appendix C includes detailed breakdown of each certification outline knowledge area back to the respective ACM IAS guideline. Table 17, Table 18, and Table 19 are summarizations of findings.

Table 17- Percent of CISSP Domain KA's linked to ACM IAS Guideline

CISSP Domains	% KA's Linked to ACM CS IAS Guideline	% KA's Linked to ACM IT IAS Guideline
Security & Risk Management (CISSP Domain 1) – 12 KA's	75%	58%
Asset Security (CISSP Domain 2) – 6 KA's	100%	50%
Security Engineering (CISSP Domain 3) – 11 KA's	100%	54%
Communication & Network Security (CISSP Domain 4) – 4 KA's	100%	75%
Identity and Access Management (CISSP Domain 5) – 7 KA's	71%	43%
Security Assessment and Testing (CISSP Domain 6) – 5 KA's	20%	40%
Security Operations (CISSP Domain 7) – 16 KA's	63%	63%
Software Development Security (CISSP Domain 8) – 4 KA's	100%	25%

Table 18- Percent of Security+ Domain KA's linked to ACM IAS Guideline

Security+ Domains	% KA's Linked to ACM CS IAS Guideline	% KA's Linked to ACM IT IAS Guideline
Network Security (Security+ Domain 1) – 5 KA's	100%	100%
Compliance and Operational Security (Security+ Domain 2) – 9 KA's	78%	100%
Threats and Vulnerabilities (Securtiy+ Domain 3) – 8 KA's	88%	100%
Application, Data, and Host Security (Security+ Domain 4) – 5 KA's	100%	100%
Access Control and Identity Management (Security+ Domain 5) – 3 KA's	67%	100%
Cryptography (Security+ Domain 6) – 3 KA's	100%	100%

Table 19- Percent of CEH Module KA's linked to ACM IAS Guideline

Certified Ethical Hacker Modules	% KA's Linked to ACM CS IAS Guideline	% KA's Linked to ACM IT IAS Guideline
Introduction to Ethical Hacking (CEH Module 1) – 6 KA's	67%	67%
Footprinting and Reconnaissance (CEH Module 2) – 6 KA's	17%	17%
Scanning Networks (CEH Module 3) – 2 KA's	100%	100%
Enumeration (CEH Module 4) – 11 KA's	0%	0%
System Hacking (CEH Module 5) – 4 KA's	25%	25%
Trojans and Backdoors (CEH Module 6) – 7 KA's	100%	100%
Viruses and Worms (CEH Module 7) – 6 KA's	100%	100%
Sniffers (CEH Module 8) – 9 KA's	11%	22%
Social Engineering (CEH Module 9) – 6 KA's	100%	100%
Denial of Service (CEH Module 10) – 8 KA's	100%	100%
Session Hijacking (CEH Module 11) – 5 KA's	60%	0%
Hacking Webservers (CEH Module 12) – 8 KA's	25%	0%
Hacking Web Applications (CEH Module 13) – 7 KA's	71%	43%
SQL Injection (CEH Module 14) – 9 KA's	100%	100%
Hacking Wireless Networks (CEH Module 15) – 9 KA's	100%	0%
Hacking Mobile Platforms (CEH Module 16) – 8 KA's	100%	0%
Evading IDS, Firewalls and Honeypots (CEH Module 17) – 8 KA's	38%	25%
Buffer Overflows (CEH Module 18) – 7 KA's	100%	100%
Cryptography (CEH Module 19) – 8 KA's	100%	100%
Penetration Testing (CEH Module 20) – 6 KA's	17%	17%

An evaluation of the data in Table 17, Table 18, and Table 19 suggests that both ACM IAS Guidelines most closely align with the Security+ certification. A student completing a Computer Science or Information Technology program that delivered all the knowledge areas suggested in either ACM IAS Guideline should have a good foundation to prepare them for Security+ certification. Even though shortcomings may exist, a well-rounded student should be able to quickly fill any gaps through personal study. Although the typical graduate will not have the necessary work experience to sit for the CISSP, the majority of knowledge domains should be covered.

Table 20 and Table 21 are collapsed versions of Table 8 and Table 9 respectively, showing the IAS knowledge areas and what percentage of those areas are tested in the certifications evaluated.

Table 20- Percent of ACM CS Guideline covered by popular certification

ACM CS IAS Guideline	% of ACM CS KA's Tested		
	CISSP	Security+ SY0-401	CEH 312-50
IAS/Foundational Concepts in Security	100%	100%	100%
IAS/Principles of Secure Design	100%	46%	23%
IAS/Defensive Programming	100%	100%	43%
IAS/Threats and Attacks	100%	100%	100%
IAS/Network Security	88%	88%	88%
IAS/Cryptography	100%	100%	92%
IAS/Web Security	100%	80%	80%
IAS/Platform Security	100%	100%	38%
IAS/Security Policy and Governance	100%	71%	43%
IAS/Digital Forensics	47%	80%	0%
IAS/Secure Software Engineering	100%	100%	0%

Table 21- Percent of ACM IT Guideline covered by popular certification

ACM IT IAS Guideline	% of ACM IT KA's Tested		
	CISSP	Security+ SY0-401	CEH 312-50
IAS/Fundamental Aspects	100%	100%	63%
IAS/Security Mechanisms	100%	100%	75%
IAS/Operational Issues	88%	100%	38%
IAS/Policy	100%	100%	100%
IAS/Attacks	71%	100%	100%
IAS/Security Domains	100%	100%	100%
IAS/Forensics	100%	100%	0%
IAS/Information States	100%	100%	0%
IAS/Security Services	100%	100%	100%
IAS/Threat Analysis Model	100%	100%	0%
IAS/Vulnerabilities	64%	100%	73%

The results show the majority KA's of both the CISSP and Security+ exam are covered as part of the ACM CS ISA guideline. The CEH exam is focused on a specific knowledge area, namely penetration testing, hence why the noticeable shortcomings in comparison to the ACM CS IAS guideline.

VI. Alignment with Accrediting Bodies and Recommended Guidelines

A lot of statistics have been provided supporting the existing ACM Guidelines. Core instructional areas have been identified, but how do they align with ABET certification criteria? ABET accreditation criteria is broken into two sections. General criteria apply to all programs and "must satisfy every Criterion" for accreditation (ABET, 2015, p. 2). Program Criteria are discipline-specific, and must satisfy "all the specific Program Criteria implied by the program title" (ABET, 2015, p. 2). ABET general criteria is broken into eight criterion ranging from student performance to institutional support. Criterion 3 addresses nine student outcomes that must be documented and periodically reviewed. Of particular relevance to this research, subsection (e) states "An

understanding of professional, ethical, legal, security and social issues and responsibilities" must be attained by the time of graduation (ABET, 2015, p. 3).

Beyond the general criteria, ABET has no program criteria requiring any additional security element for computer science degrees. However, ABET lists an additional security element as part of its curriculum requirements for an Information Technology program. Criterion 5 states that IT programs must "have course work or an equivalent educational experience..." in "information assurance and security" (ABET, 2015, p. 7). ABET does not provide a list of KA's detailing how that should be done, other than listing it as a requirement.

Chapter 5: Conclusions and Future Work

Conclusions

This research does not attempt to settle the debate of whether certifications should or should not be a deliverable in an educational setting. However, it is clear that a properly delivered security minded curricula does provide a solid foundation for at least two of the top three certifications identified in this research, namely Security+ and CISSP. Although the 2013 ACM CS Curricula Guideline was published in December 2013, adoption rates are lagging within the UNC System. The ACM CS Curricula Guideline leadership group acknowledged the difficulties associated with adopting any change to existing curricula stating, "Adding knowledge areas at the baccalaureate level is a zero-sum game. The curriculum for any computing major already has tight time allotments, and 'elbowing in' cybersecurity knowledge areas must be done carefully so as not to 'elbow out' topics deemed essential in the curriculum" (McGettrick, 2013, p. 3). Although challenges exist, the ACM CS Curricula Guideline leadership group "felt that all computing graduates should have at least one technical course in cybersecurity" (McGettrick, 2013, p. 24).

Both ACM CS and IT Curricula Guidelines used in this research are just that, guidelines. It was not intended to be a mandatory implementation list. This research has provided additional evidence to assist UNC System schools determine what elements of the guideline should be applied by including job data, in the form of certification data, to support the needs of local job opportunities. An effective implementation of these guidelines will fulfill both the educational and employment skills required by graduates.

Future Work

In the future, it would be interesting to see the data from expanding this research to include other school systems in other states. Considering available jobs, and education being delivered within other geographic areas, how closely are other school systems fulfilling the educational needs of their students?

Other majors, such as Information Systems, could be evaluated against curriculum guidelines to see how closely those programs are following recommended curricula. Those results could be compared against this research.

Examining if ACM guideline elements can be woven into existing classes. Recommendations could be made to improve the educational shortcomings found in this research.

It would also be interesting to learn why the ACM Information Assurance and Security guidelines for Computer Science and Information Technology programs are different. Should the differences between the two guidelines be normalized into a single cohesive Information Assurance and Security guideline for all computer majors?

This research could be repeated in a few years to see what changes, if any, are applied to existing programs to address the educational shortcomings found in this research.

Evaluating if any four year universities include certification as a course deliverable. Given how closely the ACM IAS guideline aligns itself with security certifications, evaluating if certifications should be a deliverable in any four year education institution.

References

ABET. (2015, January 30). *Accreditation Criteria and Supporting Documents.* Retrieved January 30, 2015, from ABET: http://abet.org/cac-criteria-2015-2016/

ABET. (2015, January 30). *Accredited Program Search*. Retrieved January 30, 2015, from ABET: http://main.abet.org/aps/Accreditedprogramsearch.aspx

ABET. (2015, January 12). *Why Accreditation Matters*. Retrieved January 12, 2015, from ABET: http://www.abet.org/why-accreditation-matters/

ACM and IEEE. (2013). *Computer Science Curricula 2013.* New York: Assoociation for Computing Machinery. Retrieved January 5, 2015, from http://www.acm.org/education/CS2013-final-report.pdf

Aiello, M. (2014, January 26). *5 Reasons Security Certifications Matter*. Retrieved January 11, 2015, from InformationWeek Government: Cybersecurity: http://www.informationweek.com/careers/5-reasons-security-certifications-matter/d/d-id/1114017

Association for Computing Machinery. (2015, January 12). *Curricula Recommendations*. Retrieved January 12, 2015, from Association for Computing Machinery: Advancing Computing as a Science & Profession: http://www.acm.org/education/curricula-recommendations

Ballenstedt, B. (2013, April). *Cybersecurity Jobs Continue to Pay Better Than Others*. Retrieved November 30, 2013, from Nextgov: http://www.nextgov.com/cio-briefing/wired-workplace/2013/04/cybersecurity-jobs-continue-pay-premium/62485/

Brodkin, J. (2008, June 11). *Salary boost for getting CISSP, related certs.* Retrieved from NetworkWorld: http://www.networkworld.com/article/2280774/lan-wan/salary-boost-for-getting-cissp--related-certs.html

Computing Technology Industry Association. (2015, January 20). *CompTIA: Get IT Certified.* Retrieved January 20, 2015, from CompTIA: Exam Objectives - Select Security+ SY0-401 Exam: http://certification.comptia.org/Training/testingcenters/examobjectives.aspx

Cyber Education Project. (2015, February 4). *The Cyber Education Project*. Retrieved February 4, 2015, from About the CEP: http://www.cybereducationproject.org/

Dice. (2013, November 7). *Technology and Engineering Professionals Careers*. Retrieved November 7, 2013, from Dice.com: http://www.dice.com

East Carolina University Department of Political Science. (2014, December 10). *Master of Science in Security Studies*. Retrieved December 10, 2014, from East Carolina University - Department of Political Science: http://www.ecu.edu/polsci/sec/msss.html

EC-Council. (2015, January 20). *CEH: Certified Ethical Hacking course from EC-Council*. Retrieved January 20, 2015, from EC-Council: Hackers are here. Where are you?: http://www.eccouncil.org/Certification/certified-ethical-hacker

Foote Partners, LLC. (2015, January 30). *2015 IT Skills and Certifications Pay Index*. Retrieved January 30, 2015, from Foote Partners, LLC: Foote Research Group: http://www.footepartners.com/htscpi_latest.htm

International Information Systems Security Certification Consortium, Inc. (2015, January 20). *Candidate Information Bulletin (CIB): CISSP, Exam Outline Request.*

Retrieved January 20, 2015, from (ISC)2 Certification Programs: About our credentials & process: https://www.isc2.org/exam-outline/default.aspx

Lemos, R. (2013, January). *Research: 2013 Salary Survey: Security*. Retrieved from InformationWeek Reports: http://reports.informationweek.com/abstract/166/10337/Professional-Development-and-Salary-Data/Research:-2013-Salary-Survey:-Security.html

Lenny Zeltser, J. H. (2011, April 21). *Which Information Security Job Titles Are Least and Most Common?* Retrieved November 30, 2013, from Lenny Zeltser on Information Security: http://blog.zeltser.com/post/4832658181/information-security-job-titles-popularity

McGettrick, A. (2013, August 30). Toward Curricular Guidelines for Cybersecurity. *Association for Computing Machinery*, pp. 1-33. Retrieved February 4, 2015, from http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

National Institute of Standards and Technology. (2011, September 19). *National Initiative for Cybersecurity Education (NICE)*. Retrieved November 30, 2013, from http://csrc.nist.gov/nice/aboutUs.htm

NICCS. (2013, December 1). *Cyber Dictionary*. Retrieved December 1, 2013, from National Initiative for Cybersecurity Careers and Studies: http://niccs.us-cert.gov/glossary

Obama, B. (2009, May). *The Comprehensive National Cybersecurity Initiative*. Retrieved November 30, 2013, from The White House: Foreign Policy: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Robert Half Technology. (2013, October 14). *Robert Half Technology 2014 Salary Guide*. Retrieved November 30, 2013, from Salary Guide and Salary Center: http://www.roberthalf.com/salary-guides

SACSCOC. (2014, December 20). *Commission on Colleges: Search Results*. Retrieved December 20, 2014, from Southern Association of Colleges and Schools Commission on Colleges: http://www.sacscoc.org/search.asp

Tittel, E. (2015, Feburary 5). *Best Information Security Certifications for 2015*. Retrieved Feburary 5, 2015, from Tom's IT PRO: Real-World Business & Technology: http://www.tomsitpro.com/articles/information-security-certifications,2-205.html

U.S. Department of Labor. (2013, November 30). *Occupational Outlook Handbook, 2012-13 Edition, Information Security Analysts, Web Developers, and Computer Network Architects,*. Retrieved from Bureau of Labor Statistics: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm

University of North Carolina. (2014, November 24). *Program and Degree Finder*. Retrieved November 24, 2014, from University of North Carolina System: http://www.northcarolina.edu/apps/programs/index.php

University of North Carolina. (2015, January 30). *About Our System*. Retrieved January 30, 2015, from University of North Carolina: A System of Higher Learning: http://www.northcarolina.edu/?q=content/about-our-system

US Department of Education: Institute of Education Sciences. (2015, January 12). *What is CIP?* Retrieved January 12, 2015, from Classification of Instructional Programs (CIP): http://nces.ed.gov/ipeds/cipcode/Default.aspx?y=55

Vijayan, J. (2013, March 7). *Demand for IT security experts outstrips supply*. Retrieved November 30, 2013, from Computerworld:

http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply

Appendix A

Security Job Titles with Frequencies Greater than 200

Appendix A

Title	Frequency
Chief Information Security Officer	250
Chief Security Advisor	250
Cyber Security Advisor	250
Cyber Security Specialist	250
Data Auditor	250
Data Investigator	250
Data Security Administrator	250
Information Assurance Analyst	250
Information Security Architect	250
Information Security Auditor	250
IT Investigator	250
IT Security Administrator	250
IT Security Analyst	250
IT Security Engineer	250
IT Security Specialist	250
Network Security Analyst	250
Network Security Architect	250
Network Security Engineer	250
Network Security Manager	250
Network Security Strategist	250
Regional Security Manager	250
Security Advisor	250
Security Director	250
Security Investigator	250
Security Strategist	250
Security Systems Administrator	250
Security Systems Analyst	250
Security Systems Engineer	250
Security Systems Specialist	250
Senior Security Architect	250
Senior Security Specialist	250
Senior Security Strategist	250
Cyber Investigator	245
Chief Enterprise Risk Officer	242
Cyber Security Engineer	240
Senior Information Security Analyst	237
Information Security Advisor	231
Application Security Analyst	224
IT Security Strategist	220
Data Security Analyst	219
Senior IT Security Consultant	213
Security Lead	200

Appendix B

November 2013 Security Analyst Job Openings

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Abingdon	VA	29-Oct	IT Security Analyst	Highlands Union Bank	Bachelor's	N	GSEC or CISSP	7+
		Skills:	Knowledge is expected in the following disciplines: Access Control Tools, Management and Administration Application Security Audit and Control principles Encryption Processes, Management and Administration Firewall Management and Administration Hardware/software Security Testing and Evaluation Information Security Awareness Programs and Communications Intrusion Detection/Prevention Incident Handling Practices and Procedures Computer Forensic Practices and Procedures Information Security Policy and Standards Information Security Risk Assessment VOIP Technology Security VPN's (Virtual Private Networks) and SSL Vulnerability Assessment Practices/Technology (i.e. Operating Systems, Network, Application, Database, and Web)					
Alexandria	VA	16-Oct	Lead Cyber Security Analyst	Evolver, Inc.	Bachelor's	Y	CEH, CISSP	10+
		Skills:	Technical Experience you will need: Qradar SIEM Juniper Firewalls and IDP's CIRT Team planning and initiatives Encryption technologies Understanding of network security architecture best practices. Excellent analytic, problem solving and troubleshooting skills. Able to define, document and support systems, policies and procedures. CEH -CISSP -Other applicable certifications					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Alpharetta	GA	29-Oct	Sr. Information Security Analyst	Relay Health	Bachelor's	N	PCI DSS	6+
		Skills:	Critical Skills * Minimum of 4+ years in IT, Information Security Services, IT audit, and/or IT Risk Management Experience * Strong Project and Time Management skills * Capable of anticipating needs and driving clarity on expectations. * Experience in Risk Assessment, audit, and IT security assessments * Familiar with compliance regulations, IT, security frameworks and standards. * Experience working with PCI DSS					
Arlington	VA	6-Nov	Sr. Security Analyst	SRA International		N		4+
		Skills:	Malware reverse Engineer					
Arlington	VA	22-Oct	Sr. Security Solutions Engineer	Software Engineering Institute	Bachelor's	Y		10+
		Skills:	**Skills/Abilities**: Ability to function in the role of a consultant; planning and organizational skills; strong problem solving skills; excellent oral and written communication skills; ability to work both independently and with teams ; proven ability to research, compare, test and evaluate alternative technical solutions, and communicate the results; broad understanding of network, host and application security issues; expertise in one major network security or network engineering areas: incident handling, network traffic analysis, forensics, vulnerability assessment, network auditing, capacity planning, network architecture, etc; theoretical knowledge of and practical experience with various Internet protocols (e.g., TCP/IP, DNS, SMTP, BGP, TLS); user or implementation level experience with a subset of the following classes of technologies: IDS (e.g., Snort, RealSecure), Networking Monitoring, IPS, SIM/SEM (e.g, ArcSight, eSecurity), network mapping, vulnerability scanners (e.g., Nessus), firewalls, and routers (Cisco).					
Arlington	VA	7-Nov	Network Security Analyst - Secret	Cydecor	Bachelor's	Y	CCNA or CCNP, MCITP or MCTS	5+
		Skills:	Skills: Possess IAT Level III Information Assurance (IA) in accordance with DoD 8570.01M "Information					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Assurance Workforce Improvement Program"					
			CCNA – Cisco Certified Network Associate or CCNP – Cisco Certified Network Professional is desired					
			MCITP – Microsoft Certified IT Professional or MCTS – Microsoft Certified Technology Specialist is desired					
Arlington	VA	4-Nov	Sr. Information Assurance Security Analyst	Advanced Systems Development	Bachelor's	N	CISSP REQ	8+
		Skills:	Preferred Skills & Certifications:					
			Knowledge of IT security principles and practices and the ability to evaluate the effectiveness and efficiency of existing security control measures					
			Familiar with network security, network troubleshooting, security architectures, and TCP/IP					
			Knowledge of DoD IA regulations					
			Experience with C&A and DIACAP					
			Experience with of DISA STIGs					
			Experience with Scanning/Vulnerability Management tools (VMS, Retina, Nessus, SRRs and SCAP)					
Ashburn	VA	7-Nov	Computer Security Analyst	Strategic Enterprise Solutions, Inc.	Bachelor's	Y		3+
		Skills:	REQUIRED SKILLS					
			** SIEM Analytics.					
			** Incident Response Experience.					
Atlanta	GA	7-Nov	Network Security Analyst	ICF	Bachelor's	N		3+
		Skills:	Preferred Skills/Experience:					
			Initiative and a personal interest in Information Technology Security.					
			People skills and the ability to communicate effectively with various clients with the ability to explain and elaborate on technical details.					
			Prior experience with data correlation tools such as LogRhythm, ArcSight, QRadar, Splunk, etc.					
			Prior experience with Sourcefire security solutions.					
			Prior experience with DLP solutions such as Fidelis, Symantec DLP, and Interguard.					
			Have used network security analysis tools such as Snort, TCPDUMP, WireShark, and other Host or Network based Intrusion Detection Systems.					
			Experience with system vulnerability assessment.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Familiar with computer forensic tools Netwitness, FTK, EnCase or other network forensic applications. Knowledge of Linux/UNIX and Windows OS security. Knowledge of computer programming languages and scripting languages. An understanding of DOD information assurance policy and regulations. Security Operations Center (SOC) experience. Understanding of network hardware devices and experience configuring Access Control Lists or other Firewall or Router configuration experience.					
Atlanta	GA	30-Oct	Sr. IT Security Analyst	Grep staff, llc	Bachelor's	Y	At least 2 of: SANS GCIA, GCIH, CREM, ENCE	8+
		Skills:	Ability to conduct detailed security event analysis from network traffic attributes and host-based attributes (memory analysis, binary analysis, etc.) Ability to operate effectively with minimal supervision Ability to prioritize activities to support program execution Familiarity with malware reverse engineering concepts Prior scripting experience to enhance intrusion analysis efficiency Two of the following certifications: SANS GCIA, SANS GCIH, SANS GREM, ENCE					
Atlanta	GA	5-Nov	Information Security Vulnerability Management Analyst	Visionaire Partners	Bachelor's	Y	GPEN, CISSP, or CISM	3+
		Skills:	Vulnerability Scans. Penetration Tests. Excellent Communication Skills / Ability to interface with leaders on the business-side. GPEN, CISSP, or CISM Certifications would be a huge plus.					
Atlanta	GA	1-Nov	Senior Network & Host Security Analyst	Visionaire Partners	Bachelor's	Y	Two of the following:	6+

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
							SANS GCIA, SANS GREM, ENCE, SANS GCIH	
		Skills:	Network Traffic Security Analysis Host-based Analysis (Memory Analysis Binary Analysis) Two of the following certifications: SANS GCIA, SANS GREM, ENCE, SANS GCIH					
Atlanta	GA	4-Nov	IT Security Analyst - H2618 Security Engineer	Hunter Technical Resources, LLC	Bachelor's	N	Security +, GCIA	2+
		Skills:	Prior experience leveraging intrusion detection tools to identify security events Possess a basic understanding of scripting languages					
Charlotte	NC	7-Nov	Security Analyst - Technical Support	Matrix Resources				
		Skills:	• Demonstrated working technical knowledge and application of concepts, practices and procedures in the architecture and use of the malware protection and security analytics systems • Demonstrated working technical knowledge and application of concepts, practices and procedures with multiple security, network, network security, forensics applications and/or a component family; including solid familiarity with products from leading vendors • Experience providing production support for multiple critical systems and the ability to be on-call on a rotational basis within a Team • Experience creating and maintaining engineering, deployment, and operational documentation • Experience in vendor case management including issues identification and resolution • Experience with troubleshooting issues • Strong Knowledge and experience with system administration processes and practices on both Linux and Windows platforms • Strong knowledge and experience in the use of TCP/IP-based network protocols and applications					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Charlotte	NC	7-Nov	IT Security Analyst	Robert Half Technology			CISSP or CISA	1+
		Skills:	1. Knowledge of IT audit concepts 2. Knowledge of leading security practices, procedures and policies pertaining to data access and information systems 3. Understanding of risk and risk analysis relating to IT systems 4. Working knowledge of network security and IT infrastructure of both hardware and software, such as firewall, IDS/IPS, anti-virus, system monitoring, encryption technologies, WAN/LAN, operating systems, authentication, authorization, vulnerability scanning and monitoring tools					
Charlotte	NC	7-Nov	Oracle IT Security Analyst	Jack Richman & Associates / JRA Consulting	Bachelor's	N	Orcle Cert Pro, MCDBA	4+
		Skills:	•Security oriented professional with experience in financial services. •Minimum - Securing Oracle database environments. •Administering Guardium database monitoring and Vormetric infrastructure. •Familiarity with best practices surrounding security incident response. •Demonstrated ability to identify, analyze, quantify and report on database security issues. •Experience developing and implementing policies and procedures.					
Charlotte	NC	7-Nov	Info Security Analyst	Kforce Inc.				
		Skills:	Demonstrated working technical knowledge and application of concepts, practices and procedures in the architecture and use of the malware protection and security analytics systems * Demonstrated working technical knowledge and application of concepts, practices and procedures with multiple security, network, network security, forensics applications and/or a component family; including solid familiarity with products from leading vendors * Experience providing production support for multiple critical systems and the ability to be on-call on a rotational basis within a Team * Experience creating and maintaining engineering, deployment, and operational documentation * Experience in vendor case management including issues identification and resolution * Experience with troubleshooting issues * Strong Knowledge and experience with system administration processes and practices on both Linux					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			and Windows platforms * Strong knowledge and experience in the use of TCP/IP-based network protocols and applications					
Charlotte	NC	7-Nov	Senior AD Security Analyst	CCCi				6+
		Skills:	Proven knowledge of Active Directory support and group policy implementation is desired. - Works effectively with defined direction and supervisory review. - Ability to handle multiple tasks and projects concurrently. - Good understanding of IT policy, standards and processes. - Performs complex project oriented tasks.					
Charlotte	NC	6-Nov	IT Security Analyst - Oracle Database	Citco Technology Management				
		Skills:	SAME AS ORACLE IT SECURITY ANALYST POSTED BY JACK RICHMAN & ASSOCIATES POSTING					
Charlotte	NC	7-Nov	Info Security Analyst	Randstad Technologies	Bachelor's	Y	CISSP, GIAC, OR CISM	3+
		Skills:	Advanced knowledge of Windows, Unix, Linux operating systems Strong knowledge of networking fundamentals, common protocols services and related security issues (SMTP, DNS, TCP/IP 801.1x, SSL) Knowledgeable in programming or scripting languages (C, VB, Perl, Python, shell scripting) Experience with vulnerability assessments and penetration testing					
Charlotte	NC	14-Oct	Information Security Analyst	Signature Consultants				4+
		Skills:	4+ years of experience with UNIX, Pearl, or Korn Scripting within a Large Enterprise environment (500+ servers).					
Charlotte	NC	31-Oct	IT Security Analyst	Staffor Consulting LLC	Bachelor's	N		6+
		Skills:	•Possesses and applies a broad knowledge of operating systems, networks, application development, and databases. PKI and ADFS (AD Federations Services)					
Columbia	SC	28-Oct	Security Analyst	Systemtec, Inc	Bachelor's	N		4+

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
		Skills:	Network Security experience - at least 4 years SIEM (Security Information Event Management) – at least 1 years Practical experience supporting desktops, windows servers, Unix servers - 4 years ArcSight Application support is preferred - 1 year Bachelor's Degree is preferred					
Duluth	GA	16-Oct	Sr. Security Analyst	Illuminate360	Bachelor's	N	Some Combination of CISSP, CISA, CISM, CRISC, CGEIT	5+
		Skills:	Extensive Security experience developing security plans, processes, strategic road maps, etc., either internally for an organization and/or as a consultant. Knowledge of ISO 27002, COBIT, or other information security models. Understanding of security elements of Microsoft Windows, AIX, Linux, NFS, CIFS, and other common platforms and protocols.					
Duluth	GA	16-Oct	Penetration Tester / Information Security Analyst	PossibleNOW, Inc.			Security+ or Higher	5+
		Skills:	Skill Requirements: Hands on knowledge and experience with The Metasploit Framework Knowledgeable in common cyber threat terminology, methodologies, possess basic understanding of cyber incident and response, and related current events Windows and Linux Operating System knowledge Layer 2 and 3 Security Be able to understand and piece together multiple complex logs Experience with: Splunk, Icinga, Nessus, Nexpose, Metasploit, Firewalls and IPS, F5 LTM and ASM					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Excellent verbal and written communication skills and the ability to interact professionally with a diverse group					
Durham	NC	5-Nov	Network Security Engineer	ASAP Staffing	Bachelor's	N	CISSP, GIAC, Security+	4+
		Skills:	Skills Inventory Skill, Experience, Need 1)TCP/IP Knowledge, Expert, Required 2)Intrusion Detection / Prevention (IDS/IPS), Intermediate, Required 3)IP Packet Analysis, Intermediate, Required 4)Attack Recognition, Intermediate, Required 5)Anomaly Detection, Intermediate, Desired 6)System/Network Administration, Intermediate, Desired 7)Firewall Knowledge, Intermediate, Desired 8)Routing/Switching, Intermediate, Desired 9)Unix/Linux Knowledge, Intermediate, Desired					
Durham	NC	7-Nov	Network Security Engineer	United information Technologies				
		Skills:	SAME AS NETWORK SECURITY ENGINEER POSTED BY ASAP STAFFING					
Fairfax	VA	6-Nov	Vulnerability Assessment & Security testing Team Lead	Northrop Grumman	Bachelor's	Y		9+
		Skills:	Current active TS with ability to obtain SCI or active within the past 2 years. Additional clearances may also be required for the government access. Bachelor's Degree in Information Systems, Computer Science, or related degree: or 7 years with Master; or 14 with HS (years of experience may be traded in lieu of degree) 7 years of experience in Information Systems Security. 2+ years experience either executing or defending against complex, targeted cyber threats to high-value systems and data. 2 + years experience using scan/attack/assess tools and techniques, including proficiency in at least one of the following frameworks: Metasploit, Core Impact, Immunity Canvas, etc. 2 + years experience conducting full-scope assessments and penetration tests on known adversary techniques including: social engineering, server and client-side attacks, protocol subversion, physical access restrictions, web					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			application exploitation Experience configuring, running, and validating the findings of vulnerability discovery tools such as Nessus, SAINT, NeXpose, LanGuard.					
Greensboro	NC	15-Oct	Security Analyst	Modis	Bachelor's	N		
		Skills:	Requires knowledge of security issues, techniques and implications across all existing computer platforms. Formal training or work experience in a variety of security tools (including network/host vulnerability assessment, intrusion detection and security analysis). Formal training or work experience in architecting / implementing at least 2 of the following technical security areas (Firewall/VPN, Active Directory, UNIX). Working knowledge of UNIX and Microsoft operating systems and technologies, including an understanding of security and user administration in these environments. Strong familiarity with security issues surrounding network computing (malware, DLP, intrusion detection etc); experience in implementation of security systems and controls. Strong understanding of TCP/IP networking, firewalls and Remote Access VPN solutions. Strong understanding of network security vulnerabilities and remediation.					
Herndon	VA	7-Nov	Security Analyst	TEKsystems				
		Skills:	Provide support of security infrastructure including SIEM, network and system forensics solutions, malware detection, IDS/IPS and other detection and monitoring solutions. -Provide day-to-day operations support for IDS/IPS systems. -Work with teams in other locations to ensure ongoing, reliable performance of integrated security solutions across operating companies. -Participate in the development and improvement of process/procedure manuals and documentation.					
Herndon	VA	7-Nov	Security Analyst	Softthink Solutions, Inc.				5+
		Skills:	5+ years hands-on technical experience with Windows 3+ years hands-on technical experience with Security Software Management (McAfee EPO preferred) Working knowledge of networking and security fundamentals, Advanced troubleshooting skills, Quick learner and prioritization skills Thorough with a strong ability to pay close attention to details Excellent written and verbal communications skills					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Morrisville	NC	31-Oct	Security Analyst, Level II	SilverSky	Bachelor's	N	CISSP, CIAC, CCSP, CISA, or CEH	5+
		Skills:	Qualifications: Bachelor's degree in Information Systems, Telecommunications, or equivalent IT field experience. Minimum 5 years of experience in Information Technology and/or Networking. Minimum 3 years of Windows Server administration experience within an Active Directory environment. Minimum 2 years of experience in IT Security. Experience with PCI ASV scanning and the PCI Security Standards Council. Experience analyzing windows/linux/network device logs. Experience with system and network administration. Experience with vulnerability scanners (Nessus, SAINT, Rapid7, OpenVAS) Strong troubleshooting ability; able to look at a situation from multiple perspectives to determine the problem and solution. Knowledge of TCP/IP protocols and capable of analyzing firewall logs to determine what is occurring. CISSP, GIAC, CCSP, CISA, or CEH certification. Experience with Shell scripting (Bash, Perl, WSH, PowerShell, etc.) preferred. Experience with Syslog (rsyslog, syslog-ng, nxlog) preferred.					
RTP	NC	7-Nov	Information Security Analyst	Modis	Bachelor's	Y	CCNA, RHCE, MCSE, CISSP	5+
		Skills:	• Familiarity with SourceFire NGIPS products required • Network administration, TCP/IP knowledge and application in securing systems, investigating security incidents. • Demonstrate clear experience with Mac/UNIX/Windows operating systems. • IT security with a focus on computer incident response, malicious code/exploits, anti-virus, etc.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			• Knowledge of Qradar product group and tools. • Scripting skills (BASH, Python, PERL). • Familiar with Windows & Mac exploits, malware and malicious code trends . • Demonstrate good customer service, communications using English, and troubleshooting skills. • Demonstrate interest and knowledge in learning of security trends and malware analysis. • Fluent in English. Good communication and presentation skills.					
Reston	VA	22-Oct	SIEM Security Analyst	Mandiant	Bachelor's	N		
		Skills:	Experience working on a mission critical security operations team, preferably 24x7 Experience reviewing raw log files, data correlation, and analysis (i.e. firewall, network flow, IDS, system logs) Experience with enterprise information security data management tools such as ArcSight or Splunk is preferred Experience with well-known security tools such as NMAP, Nessus, TCPDump, Wireshark, Netcat, and Backtrack Knowledge of attack vectors, threat tactics, and attacker techniques Understanding of Windows operating systems and command line tools A solid foundation in networking fundamentals, with a deep understanding of TCP/IP and other core protocols Knowledge of network based services and client/server applications Exemplary communication and interpersonal skills					
Reston	VA	4-Nov	IT Security Analyst	Triple Canopy, Inc	Bachelor's	N	GIAC, Security+, CISSP	5+
		Skills:	Demonstrated experience conducting internal and external Vulnerability Assessments, (VA), and Penetration Tests Aptitude with analysis of log files Experience auditing Windows/Active Directory and Linux/Web Applications Proficiency deploying, configuring and managing IDPS Hands on experience with security appliances					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Experience conducting incident response and after action reviews Willing and able to obtain and maintain a Secret Clearance and be eligible for Top Secret					
Reston	VA	4-Nov	Cyber Security Analyst	The Matrixx Group				3+
		Skills:	3+ years of direct experience in cyber security and risk management 5 years Information Security experience Ability to apply NIST 800-53 Rev 3 and migration to Rev 4 compliance requirements to the customer's environment. Experience using Agiliance RickVision/Open GRC and other information assurance tools US Citizenship with an active DoD Security Clearance of Secret or higher or a Dept. of Veterans' Affairs BI-Moderate clearance					
Savannah	GA	7-Nov	Security analyst - Level III	CESUSA, Inc.				
		Skills:	.Supervise the maintenance and administration of information security core systems, including Firewalls, Intrusion Prevention Systems, Web/Mail Filters and Vulnerability Scanners 4.Serves as technical expert in one or more information security solution spaces.					
Savannah	GA	7-Nov	Information Security Analyst	Cynet Systems	Bachelor's	N		8+
		Skills:	Must have understanding of information systems security; network architecture; general database concepts; electronic mail systems; Microsoft Office applications; intrusion tools. Experience conducting security assessments, penetration testing, and ethical hacking are desirable. Must be trained and have experience in formal incident response procedures and practices. Must have excellent written and oral communication skills may be called upon to testify as an expert witness in support of litigation and human resources issues to validate forensics lab practices and procedures and well as evidentiary handling practices. Expert in one or more security solution spaces (Firewalls, IPS, Filtering, Vulnerability Scanning, Penetration Testing, Code Testing) with experience in others. IT Infrastructure Library (ITIL) exposure is desired.					
Savannah	GA	7-Nov	Security Analyst, Level III	Vdart, Inc.				
		Skills:	SAME AS SECURITY ANALYST POSTED BY CYNET SYSTEMS					

November 2014 Security Analyst Job Openings

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Charlotte	NC	26-Nov	Lead Info Security Analyst--Banking & Trust	TIAA-CREF	Bachelor's	N	CISA, CISSP, CRISC certs. a plus	5+
		Skills:	**Minimum 3 years** experience in the financial services industry in a role specific to risk management, audit or information security * Working knowledge of Federal Financial Institutions Examination Council (FFIEC) guidance, GLBA, Sarbanes-Oxley and other relevant laws and regulations * Excellent verbal and written communication skills enabling candidate to prepare and present to all areas of the business, including senior management * Knowledge of industry-recognized information security-related standards such as ISO2700x, COBIT, PCI-DSS * Basic understanding of application, network, operating system, and core infrastructure security concepts and concerns "					
Charlotte	NC	26-Nov	Sr. Info Security Analyst--Incident Response	TIAA-CREF	Bachelors of Science	Y		5+
		Skills:	* Network intrusion methods, network containment, and segregation techniques and technologies experience. * Firewall configuration and features experience. * Network and platform based security techniques experience. * Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS), both host and network based systems experience. * IP Protocol Suite; knowledge of TCP/IP protocols. * Proficiency with Windows & UNIX * Coding (scripting) experience e.g. Perl, VB Script, Python etc. * Knowledge of incident response and crisis management. * Ability to assess security incidents quickly and effectively and communicate a course of action to respond to the security incident while mitigating risk and limiting the operational and reputational impact to TIAA-CREF					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Columbia	SC	10-Nov	SECURITY ANALYST-COMPLIANCE DATA	Symantec, Inc.				4
		Skills:	- Programming Background - Extensive experience comparing large data sets utilizing SQL and/or Microsoft Excel and/or Microsoft Access - SQL Experience - C/C++ and/or Java and/or Python and/or PHP (any combination of the listed scripting languages) - Experience with UNIX and/or Windows system commands and settings - Experience working in an Enterprise Environment					
Charlotte	NC	28-Nov	Security Analyst	TEKsystems			CISSP, CISA	
		Skills:	- CISSP or CISA Certifications Ideal - Advanced Microsoft Excel Skills - Proven experience identifying security risks and threats - Strong communication skills and the ability to advise other's on findings					
Richmond	VA	24-Nov	Sr Intelligence Security Analyst	Atlantic Resource Group	Bachelor’s		Security certs are a plus	5+
		Skills:	-Experience in SIEM tools and processes, Active Directory, network protocols, Linux, firewalls -5+ years in IS analyst/engineer position -SME on incident analysis and problem resolution -Excellent analytical and problem solving skills					
Alexandria	VA	19-Nov	CYBER SECURITY ANALYST	Dynamics Research Corporation	Bachelor's	Y	Security + IAW DoD 8570 Directive	5+
		Skills:	Perform independent IT security assessments on a regular basis Prepare documentation to enhance system security Prepare and submit documentation supporting system approval to operate (ATO)					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
North Wilkesboro	NC	14-Nov	Cyber Security Analyst	InfusionPoints	BS/BA	Pref	CISSP, CISM, CEH, CISA, Security+, GSEC, CIPP	1-3
		Skills:	-Support Program Managers, Project and Application leads in ensuring the required C&A documentation is prepared, reviewed, and maintained in accordance with FISMA guidance -Ensure Risk Management is provided throughout the life cycle of the systems and networks -Stay abreast of, implement, maintain and monitor industry-best-practice in information technology, compliance, security, and configuration management methodologies such as Capability Maturity Model (CMM), CMMI, Committee of Sponsoring Organizations (COSO)/ Sarbanes-Oxley (SOX), and the Federal Information Security Management Act (FISMA). -Ability to assess and develop security architecture -Understanding of security engineering concepts and requirements -Design and implement system control mechanisms that serve to control -Possible conduct and comprehend vulnerability scans and assist with developing mitigation strategies -Triage all incoming security packages (e.g. check for accuracy, validation of content and prioritization) -Develop and maintain security metrics					
Columbia	SC	21-Nov	System Security Analyst	ASK Staffing Inc.	BS	Y	Industry certs a plus	3-5
		Skills:	-Requires technical expertise in systems administration of security tools (e.g. antivirus, patching, , web content filtering, data loss prevention) combined with an understanding of security best-practices and procedures. -Ability to use detailed knowledge of Microsoft systems to effectively troubleshoot system level issues. -Ability to work in an enterprise environment and function as a technical contributor among a large team of peers and subject matter experts. -Ability to communicate and work with customers without supervision and minimal guidance.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			-Ability to express to our users technical information in a non-technical manner. -Ability to write logical and comprehensible procedures and forms. -Excellent oral and written communications skills for communicating to management,* Internal Audit, user community, and security violators. *** * -Organizational skills for planning and prioritizing work. -Excellent analytical and problem-solving skills. * -Ability to multi-task -Related industry certifications a plus					
Herndon	VA	28-Nov	Senior Cyber Security Analyst	HP	BS/BA		Security+, CEH, GCIA, GCIH, CISSP or similar	5+
		Skills:	-Perform advanced network security event analysis -Work closely with key clients on potential (or active) threats, intrusions, and/or compromises. -Responsible for understanding the global threat landscape and tracking changes in this area, as well as understanding the direct or indirect impact to the HP MSS customer base. -Conducts research on and maps out response to emerging threats, including understanding the level of impact and exposure to our customers, proactively communicating to internal business unit staff and customers on a regular basis updates on emerging threats, and ensuring HP MSS has thorough detection capabilities in place for emerging threats.					
Cary	NC	28-Nov	Lead Security Analyst and Engineer	Verizon	Bachelor's	Pref.		2-5
		Skills:	2 to 5 years of experience in a dedicated security position as a security analyst/incident responder OR security/firewall engineer Experience identifying, documenting, mitigating, and consulting on enterprise security threats Experience in Linux, ArcSight, RSA enVision, or a proprietary SIEM Experience with Symantec CSP highly preferred Experience with Infoblox DNS, Cisco Ironport, and/or Juniper Infranet highly preferred					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Strong communication skills and ability to engage with customers to understand their requirements Clear and concise written and oral English Proactive in following up on customer issues Ability to work a variety of shifts within a 24/7 Security Operations Center environment Ability to excel in high pressure environments Must pass Customer background check					
Ashburn	VA	28-Nov	Lead Network Security Analyst	Verizon	Bachelor's	Pref.	ITIL, CISSP, GSEC, CEH, CCSP, JNCIS-FWV, GCIA, GCIH, Security +	4+
		Skills:	The Qualified candidate must have 4+ years network security analyst experience, responding to and investigating network incidents and threats preferably within the US Government space The person hired for this position must have, or must meet the requirements necessary to obtain, a US DOD Secret clearance They must have excellent customer services skills, proven technical expertise in Information and Network Security, and well-rounded understanding and command of the fundamentals of network routing, TCP/IP and Network Security Preferred Certifications: ITIL, CISSP, GSEC, CEH, CCSP, JNCIS-FWV, GCIA, GCIH, Security + Preferred Technologies: Remedy, WireShark, ArcSight, Juniper, Cisco, Bluecoat, SourceFire, FireEye, McAfee Must be able to work a variety of schedules within a 24/7 Security Operations Center, including evenings, weekends, and holidays					
Merrifield	VA	28-Nov	Sr. Information Security Analyst (RISK HUNTER)	Navy Federal Credit Union	Bachelor's		GCIH, CCNA-	

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
							Security, and/or GREM	
		Skills:	* Bachelor's degree (or 7-9 years of equivalent working experience) * Basic understanding of Information Security with relevant work experience and/or relevant education/certifications. * Familiarity with creating detection signatures and alerts for enterprise monitoring tools. * Exposure to common threats, penetration/intrusion techniques and attack vectors. * Working knowledge of a broad range of current IT Security platforms and technologies such as Encase, Blue Coat AVs/SGs, McAfee IPS, Redseal Networks, Tripwire, Symantec DLP, RSA Security Analytics and AirTight Wireless IPS. * Strong analytical and problem-solving skills. * Ability to perform basic scripting tasks with Splunk to automate repeatable processes using Python 2.0 Ruby, PowerShell and Perl. * Experience working in or supporting a Computer Security Incident Response Team (CSIRT, Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT).					
Atlanta	GA	18-Nov	Sr. Security Analyst II	Randstad Technologies			CISSP	3+
		Skills:	- Candidate must have experience designing and implementing CA Control Minder and CA Governance Minder products. - Candidate will have extensive experience with Windows and UNIX systems. Extensive experience in Unix/Linux Privilege Delegation, Active Directory Bridging, and Privileged Identity Management - Software installation, configuration and integration on one or more of the following platforms/technologies: Active Directory, LDAP, NIS, Kerberos, Unix/Linux, OS X, AS/400, Oracle, SQL Server - Experience with Unix/Linux security, specifically sudo and privilege delegation. - Understanding and designing solutions for heterogeneous environments and systems are essential. - Familiarity with Governance and Compliance issues and solutions as it relates to Privilege Management.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			- Single Sign On, password synchronization and system integration to consolidate user accounts/identities a plus - Software installation, configuration and integration on one or more of the following platforms/technologies: Active Directory, LDAP, NIS, Kerberos, Unix/Linux, OS X, AS/400, Oracle, SQL Server - Good analytical skills and 3 + years of IT experience is a desired. Candidate must be able to perform work independently and collaborate with various teams on projects in a large and complex IT environment. Excellent organizational and communication skills are required. CISSP certification is a plus.					
Charlotte	NC	10-Nov	Information Security Analyst Engineer	Carlisle and Gallagher Consulting Group	Bachelor's		CISSP, SANS, other InfoSec related	
		Skills:	Bachelor’s degree in Information Security or equivalent years of experience required; plus Certified Information Systems Security Professional (CISSP) certification, SANS and other InfoSec related certification a plus Demonstrated experience with Information Security /Risk Management activities required Knowledge and experience with common information security management frameworks, such as International Standards Organization (ISO) 17799/27001 and the IT Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (CobiT) and National Institute of Standards and Technology (NIST) frameworks Excellent troubleshooting and analytical thinking skills Self-directed, self-starter, and motivated with the ability to work with minimal supervision					
Greensboro	NC	28-Nov	Security Analyst	TEKsystems			CISSP or CISA	
		Skills:	Necessary Experience Includes: - CISSP or CISA Certifications Ideal - Advanced Microsft Excel Skills - Proven experience identifying security risks and threats					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			- Strong communication skills and the ability to advise other's on findings					
Durham	NC	7-Nov	Technology Risk Security Analyst	Cedent Consulting Inc	BA/BS or MS	Y	CISSP, CIA, CISA, CRISC	5+
		Skills:	Technology Risk and Information Security domain expertise Hands-on knowledge of various technologies and platforms Knowledge of audit practices, tools, techniques, concepts, and trends Understanding of data processing general controls including physical security, network security and architecture, platform controls including desktops, servers, database security, application controls, change management, disaster recovery, and contingency planning. Prior experience in reviewing applications, systems and general controls review. Strong problem solving and analytical skills Ability to work on multiple tasks and manage priorities and workload Excellent communication skills, written and verbal, and ability to work within a team environment Ability to conduct interviews with technologists and to communicate deficiencies to both business and IT leaders Strong interpersonal and collaboration skills Self-directed pro-active personality requiring minimal supervision Willingness to travel up to 50% of time, inclusive of international travel					
Fairfax	VA	21-Nov	Sr Security Analyst	ELEVI Associates, LLC	BS/BA		GCIA, GCIH, CISSP	6-8
		Skills:	Subject Matter Expert for advanced technology, system/network architecture, threat-related subjects, data analytics, and other areas.• Excellent oral and written communication skills• Proven technical writing experience• Detail-Oriented, proven attention to detail in past projects• Candidate should have a firm grasp on SQL technologies and database architectures.• Product Lifecycle and Project Management experience experience is a plus					
Columbia	SC	18-Nov	Systems Security Analyst	Systemtec, Inc.	BS CS	Y		3-5

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
		Skills:	• Technical expertise in systems administration of security tools (e.g. antivirus, patching, web content filtering, data loss prevention) combined with an understanding of security best-practices and procedures. • Ability to use detailed knowledge of Microsoft systems to effectively troubleshoot system level issues. • Ability to work in an enterprise environment and function as a technical contributor among a large team of peers and subject matter experts.					
McLean	VA	18-Nov	Information Security Analyst/Engineer (Analytics)	Randstad Technologies				
		Skills:	Analyst, Configuration Management, Database, Data Mining, Genetic, Management, Security, Unix, Windows					
Mt. Weather	VA	18-Nov	Senior Security Analyst	Randstad Technologies			CISSP and one of: GCIA, GCED, GCIH, CEH	3
		Skills:	**Must possess Top Secret Security/SCI ** -Candidate must have demonstrated expertise in some of the following skills: Intrusion Detection & Incident Response, Vulnerability Assessment, Intrusion Detection Systems Support, RSA SecureID and PIV and/or Common Access Card (CAC), Secure and Monitor Critical Applications and network assets, Remote Access Support VPN and redundant trusted internet RTIC, Penetration testing, maintenance, training and Vendor product upgrades -Must be able to work independently as well as in a team environment -Must have familiarity with Federal, DoD, and industry information security requirements, standards, and best practices working knowledge of incident response, network architectures, current networking technologies, security requirements and features of networks and applications, and other security issues. -Excellent oral and written communication skills required.					
Richmond	VA	28-Nov	Senior Information Security Analyst	Leading Edge Systems Richmond	BS	Y		5+
		Skills:	-Knowledge and experience in Enterprise Log Management and SIEM tools and processes.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			-Familiarity with the following technologies: SIEM, Active Directory, Microsoft Windows, Linux, firewalls, network protocols, IDS/IPS. -5+ years experience in an information security analyst/engineer role. -Experience and expertise in hands-on utilization of forensics and analysis tools. -Extensive information security knowledge and experience. -Must be highly motivated and able to work effectively under minimal supervision in a fast-paced environment. -Must be team-oriented, placing priority on quality and the successful completion of team goals.					
Fort Lee	VA	27-Nov	Information Security Analyst - PBUSE	NORTHROP GRUMMAN	Bachelor's	Y		5+
		Skills:	1. Must have a Bachelor's Degree in Computer Science, Information Technology / Security or other Engineering / Technical discipline. 2. Must have a minimum of five (5) years' experience working on computer systems with two (2) years PBUSE Information Assurance experience. 3. Must be Information Assurance (IA) Trained and Certified per the Defense Federal Acquisition Regulation Supplement (IAW DoD 8570.1-M, Change2). 4. Must have experience with Oracle SPARC SuperCluster system, Citrix NetScaller, Solaris 11, Exadata Storage Cells, Infiniband networks, Sun-7420 Storage Appliances, Ops Center 12c, ZFS File Systems, Oracle 11gR2 RACs, Oracle Exadata Database Machine. 5. Must be Information Assurance Technical (IAT) Level I certified. 6. Must be Information Assurance System Architect and Engineer (IASAE) Level II certified. 7. Must be IT-II Sensitivity Level certified. 8. Must have an active DoD Secret Clearance to be considered. 9. Must be a US citizen. 10. Must possess or be able to obtain a valid US passport.					
Arlington	VA	10-Nov	Desktop Security Analyst	Tetra Tech AMT	BA/BS	Y	Security+	6+
		Skills:	Experience: 6 years technical experience as computer desktop technician; with 3 years in the security field desired; contractor experience a plus Experience with Siebel CRM is preferred Skills Desired: Security+ Certification Expert level in MS Excel, Word and PowerPoint Hardware skills in PC repair and diagnosis Proven ability to learn new applications and recognize areas for improvement Key skills and experience required are knowledge and experience with Windows XP-based systems & Windows 7, knowledge and experience managing automated data processing systems, knowledge and					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			experience installing and debugging standard operating systems, and knowledge and experience with security monitoring tools. Familiarity with Linux, UNIX, and Macintosh operating systems is also desirable					
Atlanta	GA	28-Nov	Information Security Analyst	Modis				
		Skills:	• Passionate about security • Motivated self-starter • Demonstrated experience in an enterprise security group • Knowledge of SIEM console, alerting, and reporting procedures • Demonstrated hands-on experience analyzing high volumes of logs, packets, network data and other attack artifacts in support of incident investigations • Experience and proficiency with any of the above: Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-based Forensics, Network Forensics					
Columbia	SC	17-Nov	Security Analyst	Modulant	BS			4
		Skills:	-Bachelor Degree in Computer Science, Information Technology or other job related degree OR extra 4 years of combined education and job related IT work experience (a total of 8 years combined education and work experience). -4 years of security and/or server experience -Programming background -4 years of experience comparing large data sets utilizing SQL -Any combination of the following scripting languages: C/C++, Java, Python, PHP -Experience with UNIX and/or Windows system commands and settings. -Large environment experience is required. -Nessus experience is highly desired					
Columbia	SC	20-Nov	Unix Security Analyst	Modulant	BS			6
		Skills:	Bachelor's Degree in Computer Science, IS, or job related degree OR an extra 4 years job related experience (A total 10 years of combined related work and education experience) -6 years of server or other job related experience -MUST have previous experience reading/interpreting/implementing DISA STIG recommendations on Unix (AIX/Solaris/RHEL) servers.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			-Scripting Experience to include previous experience with Unix scripting languages such has KSH or Bash. Candidate must have the ability to automate manual remediation activities on Unix (AIX/Solaris/RHEL servers). -AIX or RHEL or Solaris past experience with Server administration on these operating systems with a focus on security.					
Atlanta	GA	28-Nov	Security Analyst - Courion IAM	Modis	BS	Y		1
		Skills:	• Strong level of analytical and problem-solving abilities. • Strong attention to detail, strong mathematical and reasoning skills required. • Broad understanding of encryption (types of encryption, encryption strength, and best practices for key/certificate management.)• 1 year of experience on at least 2 of the following: Courion IAM, Bit9 Parity, PhoneFactor, ArcSight ESM, Tripwire, Symantec Endpoint Security, WebSense WebFilter, Microsoft Certificate Authority, IT Security System Hardening, Courion Identity Management, Microsoft GPO Management					
Richmond	VA	24-Nov	Senior Information Security Analyst	SPECTRAFORCE TECHNOLOGIES Inc.	BS		Related industry certs a plus	5+
		Skills:	Knowledge and experience in Enterprise Log Management and SIEM tools and processes Familiarity with the following technologies: SIEM, Active Directory, Microsoft Windows, Linux, firewalls, network protocols, IDS/IPS 5+ years' experience in an information security analyst/engineer role Experience and expertise in hands-on utilization of forensics and analysis tools Extensive information security knowledge and experience Must be highly motivated and able to work effectively under minimal supervision in a fast-paced environment Must be team-oriented, placing priority on quality and the successful completion of team goals Excellent analytical and problem solving skills					
Richmond	VA	26-Nov	Security Analyst / Engineer	National Computing Group				
		Skills:	SAME AS SPECTRAFORCE TECH POSTING					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Columbia	SC	21-Nov	System Security Analyst	DP Professionals Inc	BS	Y	Related industry certs a plus	3-5
		Skills:	Technical expertise in systems administration of security tools (e.g. antivirus, patching, web content filtering, data loss prevention) combined with an understanding of security best-practices and procedures Ability to use detailed knowledge of Microsoft systems to effectively troubleshoot system level issues Ability to work in an enterprise environment and function as a technical contributor among a large team of peers and subject matter experts					
Alexandria	VA	24-Nov	IT Security Analyst	Squires Group, Inc	Bachelor's	Y	CISSP, CISM, or GSLC	4
		Skills:	4 years of experience with Cyber Security requirements (IA Controls) 1 year of experience working within DoD Services or Agencies 3 years of experience with writing SSPs or other security related policy documentation 3 years of direct experience with DoD 8500.1, DoD 8500.2, DoD 8510.01, or NIST SP 800-37 & 53 5 years of experience working with computer network devices and operating systems 1 years of experience resolving security findings discovered on network devices and OS 1 year C&A package review for CA/DAA making risk-based recommendations CISSP, CISM, or GSLC certification (DoD 8570 IAM Level III) Knowledge of DoD acquisition policy Understanding of Cloud Computing and FedRamp Prior experience with Defense Agency or DoD Component (DTRA, DSS, DLA, MSC, etc), officials FISMA reporting Per our Federal Government Contract, candidates must have an active Secret clearance					
Atlanta	GA	25-Nov	Information Security Analyst	Visionaire Partners	BS	Y		
		Skills:	Bachelor's degree in CS or comparable experience Experience with several current enterprise level security software and tools.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
Arlington	GA	5-Nov	SOC Cyber Security Analyst II	Blue Canopy Group LLC	BS	Y		6
		Skills:	6 years of security experience with at least a total of 8 years total IT background. Solid working experience with any of the following tools is required: Arcsight, Splunk, Sourcefire IDS, McAfee EPO, Symantec Endpoint, Cisco ASA, NIKSUN, or other packet capturing solutions. The ability to take lead on incident research when appropriate and be able to mentor junior analysts. Excellent written and oral communication skills. Self-motivated and able to work in an independent manner. Bachelor's degree in an IT related field or equivalent education or work experience. Must be able to obtain Public Trust level clearance. (SF-85 and SF-86 submission required). Must have at least one (1) certification in the field of information security from a respectable security organization. Candidates must be willing to work a determined shift in a 15/5 shift schedules working Mon-Fri, either starting at 6:00am or finishing at 9:00pm in an SOC operational support environment. Once candidate is selected, their shift will be determined based on the business need and current shift opening and may include a requirement to rotate shifts on a periodic basis (e.g. every three months).				
Fairfax	VA	24-Nov	Application Security Analyst-TW	Dunhill Professional Search	BS	Y		4+
		Skills:	4+ years of general IT experience 3+ years of information security experience 2+ years of experience related to Application security, code security, vulnerability and risk assessments, security policy development and review, general IT and security controls development, compliance readiness (i.e. NIST 800- Series, DIACAP, FISMA, FedRAMP, FIPS) and technical security architecture/ design/ development/ implementation. Bachelor's Degree (4 Year) from an accredited institution Experience with Burp Suite and HP Fortify. Candidates must be permanent residents of the US and have resided in the US for the last 3 consecutive years				

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
McLean	VA	24-Nov	INFORMATION SYSTEMS SECURITY ANALYST	Dogwood Management Partners, LLC			CISSP, Security+	
		Skills:	CISSP, Security +, or other related security certification Experience with log information, packet captures, security alerts and artifacts to identify malicious activity. Familiarity with log aggregation solutions and RegEx Understanding of technology from the application layer down through network Familiarity with Symantec CCS Incident Management experience Experience and ability to build a data analytics program as well as ability to identify malicious patterns (APTs). Relational database experience or data mining experience is a plus					
Arlington	VA	28-Nov	Security Analyst Consultant	Deloitte	BA/BS	Y	CISSP, CEH or CISA	1+
		Skills:	1+ years of experience in one or more of the following information security domains, including: Security Risk Management, Regulations, Standards Policies and Procedures, Privacy and Data Protection, Network Security Operations, Security Architectures, Disaster Recovery & Business Continuity, Risk Management System Development Life Cycle (design and development experience) Familiarity with leading security industry standards (NIST800 series, etc.) Experience with internal controls, risk assessments, business process and internal IT control testing or operational auditing. Demonstrated ability to write business and technical reports and to participate in presentations Experience in capturing business requirements and converting business requirements into functional and technical specifications.					
Newport News	VA	13-Nov	Computer Cyber Security Analyst	Huntington Ingalls Industries, Inc.	BS	Y	CISSP	
		Skills:	CISSP, Malware, Cybersecurity					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Industry Certifications: - CISSP - FOR572: Advanced Network Forensics and Analysis, 2014 - FOR508: Advanced Computer Forensic Analysis and Incident Response - SEC575: Mobile Device Security and Ethical Hacking - SEC504: Hacker Techniques, Exploits & Incident Handling - SEC503: Intrusion Detection Indepth - FOR610: ReverseEngineering Malware: Malware Analysis Tools and Techniques - SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses - SEC401: Security Essentials Bootcamp					
Burlington	NC	26-Nov	Lead Security Analyst	TeamSoft			CISSP	
		Skills:	User Identity; Security Architecture and Design Broad knowledge of firewalls, intrusion protection, penetration detection, and data encryption Experience with SIEM and QRadar preferred Indepth knowledge of cross-platform OS environments CISSP a plus Knowledge of HIPAA or FDA regulated environemtns a plus.					
Merrifield	VA	28-Nov	Sr. Information Security Analyst	Navy Federal Credit Union	BS		Info. Sec. Certs.	
		Skills:	* Expertise in web applications assessment using tools such as Nessus, Foundstone, and WebInspect open source tool. * Ability to conduct penetration testing with a skill in creating new exploits for pen testing tools. * Understanding of application architectures * Experience in security assessment against OWASP, PCI, GLBA, and other standards * Expert knowledge of current and emerging threats and industry frameworks for vulnerability analysis and reporting * Strong verbal, written, and interpersonal skills * Demonstrate ethical behaviors, the ability to recognize and deal appropriately with confidential and sensitive information, and maintain the highest levels of confidentiality					
Ashburn	VA	28-Nov	Network Information Security Analyst	Verizon	Bachelor's		CISSP, SSCP, CCFP, CEH	10+

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
		Skills:	Bachelor's in a related field Preferred and 10+ years of hands-on experience in Network Security, Security Analysis and Incident Response. 4+ Years using ArcSight ESM.A strong candidate will have multiple security related certifications like CISSP, SSCP, CCFP and CEH. Other relevant certifications such as CCNP, CCNA, SANS, etc. Candidate should have hands on experience in installing, deploying, documenting, and troubleshooting network perimeter security technologies such as firewalls, proxy servers, intrusion prevention/detection (IDS/IPS); knowledge of security compliance policy, programs, processes, and metrics; knowledge of Cyber Security and Information Protection and Privacy; strong networking background combined with strong security operations; in-Depth knowledge of Linux; Ability to automate tasks through the use of scripting tools in multiple languages such as Perl, Java, Vbasic and Python. Candidate must undergo an extensive background investigation as a condition of hire and continued employment.				
Atlanta	GA	28-Nov	Information Security Analyst	TAD PGS, Inc				
		Skills:						
	VA	28-Nov	Senior Cyber Security Analyst	SRA International	Bachelor's	Y		6-9
		Skills:	*Provide support in the information assurance operations include but are not limited to: firewalls, intrusion detection systems, proxy servers, anti-virus operations, security configuration management, vulnerability assessments, accreditations, incident response and auditing. * Perform SRR Scan for UNIX systems, RETINA and GOLD DISK scans. * Provide IAVA's and patches for engineers to complete testing before applying updates to operational systems. * Perform security scans and audits with the Assured Compliance Assessment Solution (ACAS) and Retina, mitigate issues and write associated POAMs. * Ability to obtain related DoD 8570 Certification * Provided configuration Management for all servers. * Monitor and audit Intrusion Detection systems Required: Degree Bachelors Required: Education BACH Required: Work Experience 6-9 Years Required: Responsibilities Prepares reports, briefings, or other media to support necessary tasks as well as to document daily activities.				

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
McLean	VA	18-Nov	Information Security Analyst/Engineer (Incident Response)	Randstad Technologies			CISSP, Security+, SANS or CERT Incident Handler	3-5
		Skills:	-3-5 years experience with Information Security, especially forensics, analysis, monitoring, and Incident response -Strong experience with SIEM systems, IDS, firewalls, proxies, endpoint protection, advanced threat detection, and network forensics tools -Knowledge of security frameworks such as NIST 800-series, ISO 27001 -Experience with Windows, UNIX, and Linux administration -Experience with networking and database administration -Strong oral and written communication skills -Calm under pressure and able to work with others in stressful situations					
Columbia	SC	14-Nov	Security Analyst	Ask It Consulting Inc	BS	Y		
		Skills:	• Bachelor's degree in computer science or related discipline, Master's degree preferred. • 5+ years of professional software development experience. More is better. • Strong knowledge and skills in Windows databases, optimizing queries, SQL Injection attacks, OWASP Top 10 remediation techniques, and ensuring sensitive data is secure in use, transit and at rest. • Strong knowledge and skills in Windows internals, debugging and reverse engineering. • Strong knowledge of Windows Security such as Token / Privileges /SID /ACLs /Group Policy /Active Directory. • Demonstrated ability to design software and systems solutions, securely. • Ability to work collaboratively in a small close-knit team and have good communication skills. • Security expertise. Experience building secure code, penetration testing, and reverse engineering malware. • Experience with Windbg, ollydbg, metaspoilt, wireshark, burp suite, and other security tools. • MS Visual Studio, XML, XHTML, ASP.NET, C++, J#, etc.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			• Experience building and securing Enterprise software products. • Have worked in an Agile development environment with Scrum. • Solid understanding of industry best practices for securing systems, secure systems design, security testing, and implementation.					
Fairfax	VA	28-Nov	FSG Info Security Analyst (Remote)	CGI				
		Skills:	Security Architecture					
Herndon	VA	25-Nov	Cyber Security Analyst	Computer Technologies Consultants, Inc. (CTC)				
		Skills:	Snort based intrusion detection systems including reading, writing and tuning signatures. The candidate will monitor network traffic, identify malicious activity and coordinate incident response activities. Global enterprise incident response, intrusion detection, analysis, reporting Develop security recommendations based on incidents, develop IDS signatures and SIEM detection methodology Host based forensic analysis in the context of incident response Writing technical analysis reports in support of incident response Write IDS and SIEM signatures The number of Snort signatures created The number of Snort signatures tuned The number of incidents detected					
Richmond	VA	27-Nov	GCSS-Army Technical Integration SAP Security Analyst 2 GARMY	NORTHROP GRUMMAN	BS	Y	SAP Security	2
		Skills:	* Strong team skills (respect, consistency, decisiveness, accountability, conviction, cooperation, communication). * Good listening skills * Ability to innovate and brainstorm around business ideas and needs. * Must have strong oral and written English communication skills. * Ability to manage conflict.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			* Must be able to work in a diverse team and be a participating member of a team supporting a large implementation. * An adaptable and flexible approach to problem solving. * A proven track record on working collaboratively with customers and internal teams and external consultants. * Must be able to perform a variety of duties and multi-task. * Ability to be resourceful, creative and maintain flexibility. * Excellent time management and problem solving skills. * Solid analytical skills and a strong vendor/customer focus. * SAP Security certification a major plus.					
Herndon	VA	25-Nov	Cyber Security Analyst	Prism, Inc.				
		Skills:	SAME AS COMPUTER TECHNOLOGIES CONSULTANTS (CTC) POST					
Atlanta	GA	28-Nov	Information Security ISE Analyst/Engineer	Intercontinental Exchange	BS			
		Skills:	Customer Service – Monitors the ISE ticket queue and provides superior customer service for any end-user Information Security need Access Control – Vets, routes, and/or implements permission changes TVM Hardware Deployment –Deploys and maintains advanced SIEM, IDS, WAF, and antivirus solutions Architecture Consulting – Assists developers and architects with network and system design Firewall – Deploys and maintains advanced high-performance firewall environments VPN – Designs and maintains SSL VPN hardware and 2-factor authentication Load Balancer Administration – Designs and maintains a mission-critical high-performance traffic management solution Content Filtering and Advanced Threat Protection – Designs and maintains content filtering technology including proxy servers and cloud-based services Hands-on experience with Systems Administration and/or IP Networking Experience supporting an advanced software development organization					
Richmond	VA	21-Nov	Principal Technical Analyst	Altria	BS	Y	CISSP	8+
		Skills:	Bachelor's degree in Computer Science, Information Systems, Engineering or related discipline					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			8+ years IT experience with 2+ years in an information security role General understanding of IT security fundamentals and Defense-in-Depth practices Broad knowledge of IT technologies, Operating Systems and Applications platforms Detailed understanding of modern networking technologies and network security controls CISSP (Certified Information System Security Professional) certification preferred Excellent verbal and written communication and interpersonal skills					
Norfolk	VA	28-Nov	Risk Assessment/Incident Analyst	Healthcare IT Leaders			CISSP, CRISC	
		Skills:	- CISSP or CRISC certification - Knowledgeable in HIPAA, Hitech, Omnibus, and Nist-800 series (especially 30 and 53) - Demonstrable incident handling experience is a plus					
Atlanta	GA	28-Nov	Information Security TVM Analyst/Engineer	Intercontinental Exchange	BS	Y		
		Skills:	Incident Management – Ensures Information Security incidents are properly documented, categorized, and responded to Systems Compliance – Uses automated and manual processes to assess Windows, UNIX, and network device hosts for adherence with security standards Advanced Threat Protection – Uses automated tools and manual processes to detect, analyze, and mitigate potential malware attacks Intelligence – Ensures TVM dependably processes available threat intelligence Activity Monitoring – Uses automated and manual processes to detect and alert on suspicious network behavior Investigations – Conducts forensic investigations to confirm the extent and intention of suspicious network activity Vulnerability Scanning – Assesses systems and hosts for vulnerabilities and ensures they are remediated Hands-on experience with Systems Administration and/or IP Networking Experience with Regulatory Compliance					
Richmond	VA	28-Nov	Security Specialist	Vaco – Richmond				
		Skills:						
Herndon	VA	28-Nov	Jr. Policy Analyst	Softworld, Inc.	BA/BS	Y		

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
		Skills:	-Experience with information security or IT -2+ years of experience with writing policies, standards, procedures, and guidance -Experience with Microsoft Office, including Word, PowerPoint, and Excel -Knowledge of general information security concepts and methods, including enterprise security programs and governance strategy -Ability to obtain a security clearance					
Raleigh	NC	28-Nov	Security Risk and Compliance Analyst	Citrix	BS	Y	CISA, CISSP, GSEC, CRISC, CGEIT, GSNA, CIPT, CCSK or willingnes s to pursue training and certs.	
		Skills:	* Bachelor's degree in information systems or business or equivalent experience * Strong problem solving, analytical skills, organizational, and project management skills * Outstanding oral and written communication skills * Self-motivation and the ability to work under minimal supervision are a must * Deep experiential understanding of compliance frameworks and security control objectives					
Quantico	VA	17-Nov	Information Assurance Engineer	NCI Information Systems, Inc.	Bachelor's		8570.01M IAT Level III certified.	5+
		Skills:	Active DoD Secret clearance. 5+ years of related experience. MCEN-validated and Marine Corps Blue Team certified.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Ability to travel up to 25% if needed both CONUS and OCONUS. Experience using assessment methods and tools such as: eEye Retina, Defense Information Systems Agency (DISA) Gold Disk DISA Systems Requirements Review (SRR) Scripts DISA STIGs and checklists Secure Configuration Compliance Validation Initiative (SCCVI) Tenable Nessus Enterprise LanSweeper Splunk Enterprise, and Security Compliance Automation Protocol Compliance Checker (SCAP) Familiarity with software assurance tools such as: Portswigger Burp Suite Professional Hewlett Packard WebInspect Jet-Brains IntellJ IDEA Integrated Development Environment (IDE) for application assessments Experience with C&A management tool Telos Xacta IA Manager, DoD ST&E process and monitoring tools such as USMC HBSS, eEye Retina.					
Atlanta	GA	28-Nov	Sr. Security Engineer - Security Engineering & Operations	Modis	BS		CISSP	5
		Skills:	• At least five years working in Information Security with at least one years as a web application developer a plus. • Designed and implemented enterprise network firewalls in the Retail or E-Commerce industries. • Strong understanding of firewall topology and zone based methodology. • Strong understanding of JUNOS and ScreenOS firewall code along with tools like NSM and Space with Juniper Firewall Certifications a plus • Good understanding of dynamic routing protocols such as OSPF, iBGP, and IS-IS • Designed and Implemented a WAF solution within the Retail or E-Commerce industry • Strong understanding of the OSI model with emphasis on Internet application and transport protocols • Strong knowledge of the SDLC process and Information Security Architecture Frameworks • Understanding of Web Programming languages such as HTML, JavaScript, and PHP • Strong knowledge of scripting and regular expressions such as Bash and Perl					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			• Understanding of Apache and Database Administration • Bachelors of Science or equivalent experience with a CISSP certification a plus • Strong written, verbal, and communication skills with emphasis on coordinating third party contracted resources • Able to read and understand network and data-flow diagrams					
Chantilly	VA	7-Nov	Java Security Engineer	Dunhill Professional Search				7+
		Skills:	7+ years of Java/Enterprise Java/J2EE development experience Strong programming skills using JavaScript and NodeJS Expertise with application server technologies Spring Framework, Spring Security, Web Services (JAX-RS/JAX-WS), REST and Hibernate In-depth knowledge of and experience with Java security technologies, single-sign-on and identity management technologies Expertise with web system security concepts, including authentication, authorization (RBAC), encryption/hashing, SAML, and LDAP Knowledge of cross-site scripting (XSS), session hijacking, SQL injection, CSRF (Cross-Site Request Forgery), OWASP Top 10, and other attack vectors Hands-on experience with encryption, hashing, secure random number generation, key derivation, digital signatures, etc. Knowledge of TCP/IP, HTTP/S, and related protocols Knowledge of network-based, system-level and application layer attacks and mitigation methods Experience with static code analysis tools including HP Fortify and Find Bugs Knowledge and experience with agile software development methodologies Minimum 7 years previous experience as an Application Security Developer, Application Security Analyst or equivalent					
Atlanta	GA	24-Nov	Sr. Security Engineer	Metasys Technologies	BS		CISSP, CISM, CISA, PCI QSA, CCFE,	

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
							GIAC, CCIE, CCSP, CBCP, ABCP, MBCP	
		Skills:	Working knowledge of one or more of the following InfoSec solutions: Anti-Virus, intrusion detection, firewalls, content filtering, rick assessment. PREFERRED QUALIFICATIONS - Industry certifications - CISSP, CISM, CISA, PCI QSA, CCFE, GIAC, CCIE, CCSP, CBCP, ABCP, MBCP. Experience performing audits/assessments against controls frameworks experience in network, system or application security design, implementation or support. BS Computer Science, Information Assurance or related field, MS a plus.					
Alexandria	VA	28-Nov	Intrusion Detection Analyst	CGI	BS			2
		Skills:	* At least two (2) years of experience with IDS and IPS technologies. * Knowledge of the TCP and IP protocol suite, security architecture, and remote access security techniques and products. * Knowledge of networking technologies and protocols, including Ethernet, TCP and IP and IP routing. * Experience with security technologies including Intrusion Detection & Prevention Systems (IDS/IPS), Firewalls & Log Analysis, SEIM, Network Behavior Analysis tools, Antivirus, and Network Packet Analyzers, Security Systems Manager, malware analysis and forensics tools. * Ability to perform on call functions and respond to emergency calls during non-business hours. * Candidate must have at least a Top Secret clearance. * Demonstrates knowledge in information technologies to include computer hardware and software, operating systems, and networking protocols. * BS degree in Engineering, CS, Information Security, or Information Systems and two (2) years of related experience. Four (4) years of experience can be substituted in lieu of degree. * Experience in analyzing audit logs, router logs, firewall logs, IDS logs and IPS logs. * Relevant recent IDS/IPS work * Working understanding of IDS and IPS (and their similarities and differences) * Regular expression experience					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			* Scripting experience * Intrusion monitoring, analysis, and escalation experience * Able to recognize the common attack traffic * SIM experience					
Atlanta	GA	28-Nov	SIRT Security Engineer/Analyst	Modis			CEH, GCIA, CISSP or other relevant security related certs.	3+
		Skills:	• Experience working with and manipulating data within logging/SIEM/NIDS technol0gies such as ArcSight ESM, Splunk ES, Sourcefire IDS • Familiarity with one or more scripting languages such as Perl, Python, and PowerShell • Knowledge of multiple operating systems such as Windows, Linux/Unix, and iOS • Solid understanding of PCI-DSS • Excellent written and verbal communication skills • The ability to work both independently and as part of a team					
Arlington	VA	25-Nov	Sr. Firewall Engineer	Knowledge Consulting Group	BS		CISSP	5
		Skills:	Must possess 5 years related firewall experience; BS degree is preferred but not required. Senior-level experience with the installation/administration/troubleshooting/engineering of network firewalls. Experience installing and managing CISCO ASA firewalls a plus. Also, experience with other network security technologies to include enterprise anti-virus, intrusion detection and intrusion prevention systems (IDSs/IPSs), web-proxy/internet monitoring and filtering solutions, security information event manager (SIEM) solutions, network/OS/application/database vulnerability scanners, virtual private networks (VPNs), packet-capture, netflow analysis, and/or load balancing technologies. CCNA and/or CISSP are preferred but not mandatory.					

City	State	Posted	Job Title	Company	Education	Req.?	Certs.	Exp.
			Required strong experience installing, troubleshooting, and managing firewall technology; and performing detailed network traffic analysis. Preferred experience with CISCO ASA, McAfee solutions (Web Gateway, Sidewinders, ePO), but not mandatory. Also, experience with the following a plus, but not required: ArcSight, Nessus, AppDetective, and NIKSUN Senior level position…must be immediately able to lead project converting existing McAfee sidewinder firewalls to CISCO ASAs, and lead a team of security professionals (1 Security Administrator and 1 Security Analyst) , develop/maintain standard operating procedures, and communicate (verbally and written) with senior Gov't IT OPS and IT Security professionals.					

Appendix C

Certification Course Outlines

Certification Summary

	CISSP (April 2015 version)	Security+	CISA	CEH
Eligibility / Recommended Experience	5 years full-time work experience in 2 or more of the 8 domains. 4 year baccalaureate may be substituted for 1 year experience.	2 years in IT administration with a focus on security	Minimum 5 years of IS audit, control, assurance or security work experience is required. A bachelor's or master's degree from a university that enforces the ISACA-sponsored Model Curriculum can be substituted for 1 year experience.	2 years of information security related experience OR attend official instructor-led training
Knowledge Domains	8 domains	6 domains	5 domains	20 domains
Weighted Domain Knowledge	Unequal weighting	Network Security 20% Compliance and Operational Security 18% Threats and Vulnerabilities 20% Application, Data and Host Security 15% Access Control and Identity Management 15% Cryptography 12%	The Process of Auditing IS 14% Governance and Management of IT 14% IS Acquisition, Development and Implementation 19% IS Operations, Maintenance and Support 23% Protection of Information Assets 30%	Background 4% Analysis / Assessment 13% Security 25% Tools/Systems/Programs 32% Procedures/Methodology 20% Regulation/Policy 4% Ethics 2%
Passing Score	700 / 1000	750 / 900	450 / 800	70%
Target Audience*	IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers	IT professionals	Audit, control and/or security responsibility	Security officers, auditors, security professionals, site administrators, network/technology security professionals

* http://www.netlearning.com/certifications/, February 5, 2015

(ISC)^2 Certified Information Systems Security Professional (CISSP)

The CISSP consists of eight domains that "provide a vendor neutral and internationally understood common framework upon which the practice of information security can be discussed, taught and otherwise advanced across geographic and geopolitical boundaries" (International Information Systems Security Certification Consortium, Inc., 2015)

Table 22- CISSP Domains and cross reference to ACM IAS guideline

CISSP	ACM CS	ACM IT
Security & Risk Management (CISSP Domain 1)		
A. Confidentiality, Integrity & Availability	1.1	9.1
B. Security Governanace Principles	-	-
C. Compliance	9.1	-
D. Legal & Regulatory issues to security in a global context	9.1, 9.4	3.7
E. Professional Ethics	1.4-5	-
F. Documented security policy, standards, procedures & guidelines	9.3	3.5, 4.1-2
G. Business continuity	-	3.3
H. Personnel security policies	9.1, 9.6	-
I. Risk management	1.2, 2.13	10.1-2
J. Threat modeling	1.2, 4.1, 4.4-5, 10.13	4.3-4, 5.1, 11.1-3
K. Security risk considerations into acquisition strategy & practice	1.2	-
L. Security education, training & awareness	-	6.1
Asset Security (CISSP Domain 2)		
A. Classify information & supporting assets	10.6	7.6
B. Determine & maintain ownership	10.3	-
C. Protect privacy	9.1	-
D. Ensure appropriate retention	9.5	-
E. Determine data security controls	6.1	2.1, 3.5
F. Establish handling requirements	10.4	7.1,4
Security Engineering (CISSP Domain 3)		
A. Implement & manage secure engineering processes	1.1, 2.3, 2.5-6	1.3,5, 9.1
B. Understand security models fundamentals	2.5	1.3,5,6
C. Select controls and countermeasures based upon system evaluation models	2.4-5	1.3,5
D. Understand security capabilities of information systems	2.5, 2.7, 2.9-10, 8.4	1.3,5
Assess & mitigate vulnerabilities of/in:		
E. Security architectures, designs, and solution elements	2.5, 5.6, 6.1-2, 7.4-5, 8.8, 9.2, 9.7	1.3,5,2.1

CISSP	ACM CS	ACM IT
F. Web-based systems	7.1	-
G. Mobile systems	5.5	-
H. Embedded devices & cyber-physical systems	8.5, 8.7	-
I. Apply cryptography	6.1, 6.3-7, 6.9-13, 8.2	2.1, 9.3
J. Apply secure principles to site & facility design	8.6	-
K. Design & implement physical security	8.3, 8.6	-
Communication & Network Security (CISSP Domain 4)		
A. Apply secure principles to network architecture	5.2-3, 6.1	2.1, 5.3
B. Secure network components	5.4-5	8.1-3
C. Design & establish secure communication channels	6.8	-
D. Prevent or mitigate network attacks	2.13, 5.1	11.8
Identity and Access Management (CISSP Domain 5)		
A. Control physical and logical access to assets	1.3, 8.6	2.2, 9.2
B. Manage identification and authentication of people and devices	1.3, 7.2	2.2, 9.2
C. Integrate identity as a service	-	-
D. Integrate 3rd party identity services	2.12, 3.6	-
E. Implement & manage authorization mechanisms	1.3, 2.11	2.2, 9.2
F. Prevent or mitigate access control attacks	2.8, 2.13	-
G. Manage the identity and access provisioning lifecycle	-	-
Security Assessment and Testing (CISSP Domain 6)		
A. Design and validate assessment and test strategies	-	-
B. Conduct security control testing	8.1	-
C. Collect security process data	-	1.7, 3.8
D. Analyze and report test outputs	-	-
E. Conduct or facilitate internal and 3rd party audits	-	3.2
Security Operations (CISSP Domain 7)		
A. Understand and support investigations	10.1, 10.3, 10.5-6	1.8, 7.2-3,5-6
B. Understand requirements for investigation types	10.4, 10.14	7.1,4
C. Conduct logging and monitoring activites	2.13, 4.6, 5.8	2.4
D. Secure the provisioning of resources	7.3, 9.7	3.4, 4.6, 11.9
E. Understand and apply foundational security operations concepts	2.1	1.4
F. Employ resource protection techniques	10.6	7.6
G. Conduct incident management	-	4.5
H. Operate and maintain preventative measures	2.13, 3.6, 4.2-3	2.4, 5.2, 5.7

CISSP	ACM CS	ACM IT
I. Implement and support patch and vulnerability management	3.7	-
J. Participate in and understand change management process	-	-
K. Implement recovery strategies	2.2	2.3
L. Implement disaster recovery processes	-	-
M. Test disaster recovery plans	-	-
N. Participate in business continuity planning and exercises	-	-
O. Implement and manage physical security	8.6	11.11
P. Participate in addressing personnel safety concerns	-	-
Software Development Security (CISSP Doamin 8)		
A. Understand and apply security in the software development lifecycle	11.1, 11.3	-
B. Enforce security controls in development environments	3.1-5, 8.1, 11.2-4	3.6, 5.6, 11.10
C. Assess the effectiveness of software security	3.5, 8.1, 11.3, 11.5-6	-
D. Assess security impact of acquired software	3.5, 8.1, 11.3, 11.6	-

CompTIA Security+

The Security+ Certification is vendor neutral and consists of 6 domains. The Security+ exam is "an internationally recognized validation of foundation-level security skills and knowledge, and is used by organizations and security professionals around the globe" (Computing Technology Industry Association, 2015)

Table 23- Security+ Domains and cross reference to ACM IAS guideline

Security+	ACM CS	ACM IT
Network Security (Security+ Domain 1)		
1.1. Implement security configuration parameters on network devices	5.1	4.6
1.2. Use Secure Network Administration Principles	2.13, 5.1	4.6
1.3. Explain network design elements and components	2.5-6, 5.1, 5.4	1.3
1.4. Implement common protocols and services	5.1, 6.8	6.1
1.5. Troubleshoot security issues related to wireless	5.1, 5.5	11.8
Compliance and Operational Security (Security+ Domain 2)		
2.1. Explain the importance of risk related concepts	1.2, 2.4, 4.1, 9.1, 9.3, 9.5, 9.7	3.5, 4.1-2, 10.1-2

Security+	ACM CS	ACM IT
2.2. Summarize security implementations of integrating with 3rd parties	3.6, 4.5, 9.3	3.5, 6.1
2.3. Implement appropriate risk mitigation strategies	1.5, 9.5	3.2, 3.6
2.4. Implement basic forensic procedures	10.1, 10.3-9, 10.11, 10.13-14	1.8, 4.5, 7.1-6
2.5. Summarize common incident response procedures	9.4	3.6
2.6. Explain importance of security related awareness and training	-	3.1
2.7. Compare and contract physical security and environmental controls	8.6	3.4, 4.3-4, 4.6, 11.11
2.8. Summarize risk management best practices	-	1.7, 2.3, 3.3, 3.8
2.9. Select appropriate control to meet the goals of security	1.1, 2.2, 4.6	1.5, 9.1, 9.3, 11.11
Threats and Vulnerabilities (Security+ Domain 3)		
3.1. Explain types of malware	4.2	5.7
3.2. Summarize various types of attacks	4.3, 7.4	5.2-3, 11.1-3
3.3. Summarize social engineering attacks and effectiveness with each attack	4.4	5.1, 11.1-3
3.4. Explain types of wireless attacks	5.5-6	11.1-3,8
3.5. Explain types of application attacks	3.3, 7.3	5.6, 11.1-3
3.6. Select appropriate type of mitigation and deterrent technique	5.1, 5.8, 7.3	1.6, 2.4, 11.8
3.7. Use appropriate tools and techniques to discover threats and vulnerabilities	8.1, 11.2-3, 11.6	5.4-5
3.8. Explain proper use of penetration testing versus vulnerability scanning	-	11.4-7
Application, Data, and Host Security (Security+ Domain 4)		
4.1. Explain importance of application security controls and techniques	3.1-2, 3.4-5, 7.3, 7.4, 11.1, 11.4-5	1.4, 11.10
4.2. Summarize mobile security concepts and technologies	7.2-3, 10.12	3.4, 3.7
4.3. Select appropriate solution to establish host security	3.7, 7.3, 8.6, 8.8	2.4, 3.4, 11.9
4.4. Implement appropriate controls to ensure data security	8.3-5	8.1-3
4.5. Compare and contract alternative methods to mitigate risks in static environments	5.3, 5.6, 8.7	10.1
Access Control and Identity Management (Security+ Domain 5)		
5.1. Compare and contrast function and purpose of authentication services	-	2.2

Security+	ACM CS	ACM IT
5.2. Select appropriate authentication, authorization or access control	1.3-4, 2.1, 7.2	2.2, 9.2
5.3. Install & configure security controls when performing account management, based on best practices	9.3	2.2
Cryptography (Security+ Domain 6)		
6.1. Utilize general cryptography concepts	5.2, 6.1, 6.4-6, 6.10, 6.11-13	2.1, 9.3
6.2. Use appropriate cryptographic methods	5.2, 6.2, 6.5-6, 6.8, 6.9-10	2.1
6.3. Use appropriate PKI, certificate management and associated components	5.2, 6.3, 6.5-6, 6.7, 6.10, 7.1, 8.2	2.1

EC-Council Certified Ethical Hacker (CEH)

The CEH is an internationally recognized advanced ethical hacking certification with 20 of the most current security domains. The goal is to "help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation" (EC-Council, 2015)

Table 24- CEH Modules and cross reference to ACM IAS guideline

Certified Ethical Hacker	ACM CS	ACM IT
Introduction to Ethical Hacking (CEH Module 1)		
1. Information Security Overview	1.1, 2.11, 9.4	1.6, 3.1, 6.1, 9.1,3
2. Information Security Threats and Attack Vectors	1.2	1.5
3. Hacking Concepts	1.5, 4.1, 4.4	3.3, 11.1,3-5
4. Hacking Phases	-	-
5. Types of Attacks	-	-
6. Information Security Controls	1.3, 1.5, 2.5, 9.1, 9.3	1.3, 2.2, 4.1-6, 9.2
Footprinting and Reconnaissance (CEH Module 2)		
1. Footprinting Concepts	-	-
2. Footprinting Threats	-	-
3. Footprinting Methodology	5.1	5.1
4. Footprinting Tools	-	-
5. Footprinting Countermeasures	-	-
6. Footprinting Penetration Testing	-	-
Scanning Networks (CEH Module 3)		

Certified Ethical Hacker	ACM CS	ACM IT
1. Overview of Network Scanning	5.1, 5.3	11.8
2. CEH Scanning Methodology	4.5, 5.1, 5.7	11.8
Enumeration (CEH Module 4)		
1. Enumeration Concepts	-	-
2. NetBIOS Enumeration	-	-
3. SNMP Enumeration	-	-
4. UNIX/Linux Enumeration	-	-
5. LDAP Enumeration	-	-
6. NTP Enumeration	-	-
7. SMTP Enumeration	-	-
8. DNS Enumeration	-	-
9. Enumeration Countermeasures	-	-
10. SMB Enumeration Countermeasures	-	-
11. Enumeration Pen Testing	-	-
System Hacking (CEH Module 5)		
1. Information at Hand Before system Hacking Stage	-	-
2. System Hacking: Goals	-	-
3. CEH Hacking Methodology (CHM)	-	-
4. CEH System Hacking Steps	1.3, 4.6, 8.5, 9.1	2.2, 5.4-5, 9.2, 11.9-10
Trojans and Backdoors (CEH Module 6)		
1. Trojan Concepts	4.2, 8.8	5.7
2. Trojan Infection	4.2	5.7
3. Types of Trojans	4.2	5.7
4. Trojan Detection	4.2	5.7
5. Countermeasures	4.2, 5.4	5.7
6. Anti-Trojan Software	4.2	5.7
7. Pen Testing for Trojans and Backdoors	4.2	5.7
Viruses and Worms (CEH Module 7)		
1. Virus and Worm Concepts	4.2	5.7
2. Types of Viruses	4.2	5.7
3. Computer Worms	4.2	5.7
4. Malware Analysis	4.2	5.7
5. Counter-measures	4.2, 5.4	5.7
6. Penetration Testing for Virus	4.2	5.7
Sniffers (CEH Module 8)		
1. Sniffing Concepts	-	5.3-5
2. MAC Attacks	-	-
3. DHCP Attacks	-	-
4. ARP Poisoning	-	5.3
5. Spoofing Attack	-	-

Certified Ethical Hacker	ACM CS	ACM IT
6. DNS Poisoning	-	-
7. Sniffing Tools	-	-
8. Counter measures	5.4	-
9. Sniffing Pen Testing	-	-
Social Engineering (CEH Module 9)		
1. Social Engineering Concepts	1.4, 4.4	5.1
2. Social Engineering Techniques	2.13, 4.4	5.1, 11.2
3. Imperso-nation on Social Networking Sites	4.4	5.1
4. Identity Theft	4.4	5.1
5. Social Engineering Countermeasures	4.4	5.1
6. Social Engineering Pen Testing	4.4	5.1
Denial of Service (CEH Module 10)		
1. DoS/DDoS Concepts	4.3	5.2
2. DoS Attack Techniques	4.3	5.2
3. Botnet	4.3	5.2
4. DDoS Case Study	4.3	5.2
5. DoS Attack Tools	4.3	5.2
6. Counter-measures	4.3, 5.4	5.2
7. DoS/DDoS Protection Tools	4.3	5.2
8. Denial-of-Service (DoS) Attack Penetration Testing	4.3	5.2
Session Hijacking (CEH Module 11)		
1. Session Hijacking Concepts	7.2	-
2. Network-level Session Hijacking	5.1	-
3. Session Hijacking Tools	-	-
4. Counter-measures	2.13, 5.4	-
5. Session Hijacking Pen Testing	-	-
Hacking Webservers (CEH Module 12)		
1. Webserver Concepts	-	-
2. Webserver Attacks	-	-
3. Attack Methodology	-	-
4. Webserver Attack Tools	-	-
5. Counter-measures	3.7, 5.4	-
6. Patch Management	3.7	-
7. Webserver Security Tools	-	-
8. Webserver Pen Testing	-	-
Hacking Web Applications (CEH Module 13)		
1. Web App Concepts	7.1	6.1
2. Web App Threats	3.1, 3.3, 7.3	5.6, 6.1
3. Web App Hacking Methodology	3.1	-
4. Web Application Hacking Tools	-	-
5. Countermeasures	3.3, 5.4	5.6

Certified Ethical Hacker	ACM CS	ACM IT
6. Security Tools	7.5	-
7. Web App Pen Testing	-	-
SQL Injection (CEH Module 14)		
1. SQL Injection Concepts	3.3	5.6
2. Testing for SQL Injection	3.3	5.6
3. Types of SQL Injection	3.3	5.6
4. Blind SQL Injection	3.3	5.6
5. SQL Injection Methodology	3.3	5.6
6. Advanced SQL Injection	3.3	5.6
7. SQL Injection Tools	3.3	5.6
8. Evasion Techniques	3.3	5.6
9. Counter-measures	3.3, 5.4	5.6
Hacking Wireless Networks (CEH Module 15)		
1. Wireless Concepts	5.5	-
2. Wireless Encryption	5.5	-
3. Wireless Threats	5.5	-
4. Wireless Hacking Methodology	5.5	-
5. Wireless Hacking Tools	5.5	-
6. Bluetooth Hacking	5.5	-
7. Counter-measures	5.4-5	-
8. Wireless Security Tools	2.13, 5.5	-
9. Wi-Fi Pen Testing	5.5	-
Hacking Mobile Platforms (CEH Module 16)		
1. Mobile Platform Attack Vectors	5.6, 8.7	-
2. Hacking Android OS	5.6, 8.7	-
3. Hacking iOS	5.6, 8.7	-
4. Hacking Windows Phone OS	5.6, 8.7	-
5. Hacking BlackBerry	5.6, 8.7	-
6. Mobile Device Management (MDM)	5.6, 8.7	-
7. Mobile Security Guidelines and Tools	5.6, 8.7	-
8. Mobile Pen Testing	5.6, 8.7	-
Evading IDS, Firewalls and Honeypots (CEH Module 17)		
1. IDS, Firewall and Honeypot Concepts	5.3	2.4
2. IDS, Firewall and Honeypot System	5.3	2.4
3. Evading IDS	-	-
4. Evading Firewalls	-	-
5. Detecting Honeypots	-	-
6. Firewall Evading Tools	-	-
7. Countermeasures	5.4	-
8. Penetration Testing	-	-
Buffer Overflows (CEH Module 18)		

Certified Ethical Hacker	ACM CS	ACM IT
1. Buffer Overflow Concepts	3.3	5.6
2. Buffer Overflow Methodology	3.3	5.6
3. Buffer Overflow Examples	3.3	5.6
4. Buffer Overflow Detection	3.3	5.6
5. Buffer Overflow Counter-measures	2.13, 3.3, 5.4	5.6
6. Buffer Overflow Security Tools	3.3	5.6
7. Buffer Overflow Penetration Testing	3.3	5.6
Cryptography (CEH Module 19)		
1. Cryptography Concepts	5.2, 6.1, 6.4-6, 6.10, 6.12	2.1
2. Encryption Algorithms	5.2, 6.2, 6.4-5, 6.9-10, 6.12	2.1
3. Cryptography Tools	5.2, 6.10, 6.12	2.1
4. Public Key Infrastructure (PKI)	5.2, 6.3, 6.7, 6.10, 6.12	2.1
5. Email Encryption	5.2, 6.8, 6.10, 6.12	2.1
6. Disk Encryption	5.2, 6.10, 6.12	2.1
7. Cryptography Attacks	5.2, 6.10-12	2.1
8. Cryptanalysis Tools	5.2, 6.10, 6.12	2.1
Penetration Testing (CEH Module 20)		
1. Pen Testing Concepts	-	3.2
2. Types of Pen Testing	-	-
3. Pen Testing Techniques	-	-
4. Pen Testing Phases	-	-
5. Pen Testing Roadmap	5.3	-
6. Outsourcing Pen Testing Services	-	-

Request for review of ACM guideline map to certification deliverable

The following letter was emailed to CompTIA on Tuesday, February 3. On the same day, the letter was copied and pasted into online request forms to EC-Council and $(ISC)^2$, as no email address was provided on their support pages.

To whom this may concern;

My name is Mark Grover and I am a graduate student at the University of North Carolina Wilmington. I am performing research to fulfill the requirements for a Master's of Science in Computer Science and Information Systems. One of the components of my research includes aligning the <insert certification name here> certification with the Association for Computing Machinery (ACM) Computer Science Curricula standards published in December 2013 (www.acm.org/education/CS2013-final-report.pdf). My research attempts to determine if what is being taught in higher education is properly preparing students for information security jobs. One of the ways I am making my evaluation is by comparing educational guidelines with established recognized certifying bodies.

I have attached a copy of my findings and would appreciate if someone could evaluate my findings for accuracy. The attached table includes the ACM guideline and the corresponding <insert certification name here> certification exam objective. Any entry marked with a "-" indicates that I was unable to locate a correlated exam objective, or that material is not covered. The numeric value indicates the Module followed by dotted decimal notation to indicate what sub bulleted section covers a given topic. I have a deadline of February 6, 2015, so your expeditious review is appreciated.

Respectfully,
Mark J. Grover
MSCSIS Graduate Candidate
University of North Carolina Wilmington

ACM Guideline	<insert certification name here>
IAS/Foundational Concepts in Security [1 Core- Tier1 hour]	
CIA (Confidentiality, Integrity, Availability)	<insert value>
Concepts of risk, threats, vulnerabilities, and attack vectors	<insert value>

<< Table Clipped >>

Table contents sent for evaluation can be found in Table 8- ACM 2013 Computer Science Curricula Guidelines and security certification mapping

Appendix D

University of North Carolina System

UNC System Wide Academic Offerings

DISCLOSURE: This list may not include all curriculum offerings at a given institution. The following tables were created utilizing a given keyword. This list was created to support data within this research. The following research data was obtained from the University of North Carolina Program and Degree Finder utility. (University of North Carolina, 2014) Rows highlighted in dark grey were not evaluated, as they were deemed outside the scope of this research.

Using the program lookup keyword "Security" in the degree finder utility, a total of 3 results were returned (see Table 25). All results were deemed outside the scope of this research. The Security Studies program offered at East Carolina University is "focused on four areas of emphasis: international security, homeland security policy, science and technology security, and environmental health and occupational safety." (East Carolina University Department of Political Science, 2014) The program is offered as a Political Science degree and does not align with the intended research of this paper. The Post-Baccalaureate certificate offered by UNC Charlotte was not evaluated, as graduate certificates typically are specialized and direct comparisons cannot be made.

Table 25- UNC Program Degree Finder Results based on keyword "Security"

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
45.0902	Security Studies	East Carolina University	MS (Master of Science)	Social Sciences
30.0501	Security Studies	East Carolina University	PB (Post-Baccalaureate Certificate)	Multi/Interdisciplinary Studies
11.0103	Information Security and Privacy	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services

Using the program lookup keyword "Computer Science" in the degree finder utility, a total of 72 results were returned (see Table 26). A total of 40 results were considered within scope. Of those

Table 26- UNC Program Degree Finder Results based on keyword "Computer Science"

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0701	Computer Science	Appalachian State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	Appalachian State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	East Carolina University	BA (Bachelor of Arts)	Computer and Info Sciences and Support Services
11.0701	Computer Science	East Carolina University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	East Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information and Computer Technology	East Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer and Information Science	Elizabeth City State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	Fayetteville State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC A&T State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC A&T State University	PhD (Doctor of Philosophy)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC A&T State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0199	Computer Science and Business	NC Central University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0901	Computer Networking	NC State University	MS (Master of Science)	Computer and Info Sciences and Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0701	Computer Science	NC State University	M (Master's Degree)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC State University	PhD (Doctor of Philosophy)	Computer and Info Sciences and Support Services
11.0701	Computer Science	NC State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Asheville	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC-Chapel Hill	PhD (Doctor of Philosophy)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC-Chapel Hill	BA (Bachelor of Arts)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC-Chapel Hill	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC-Chapel Hill	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Charlotte	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Charlotte	BA (Bachelor of Arts)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Charlotte	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Greensboro	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Greensboro	MS (Master of Science)	Computer and Info Sciences and Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0701	Computer Science	UNC Pembroke	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	UNC Wilmington	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0101	Computer Science and Information Systems	UNC Wilmington	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	Western Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0701	Computer Science	Winston-Salem State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0101	Computer Science and Information Technology	Winston-Salem State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0401	Geographic Information Science and Technology	East Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.1099	Network Technology	East Carolina University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	NC A&T State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.1001	Information Technology	NC A&T State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0401	Information Sciences	NC Central University	MIS	Computer and Info Sciences and Support Services
11.0802	Analytics	NC State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0401	Information Science	UNC-Chapel Hill	BSIS	Computer and Info Sciences and Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0401	Information Science	UNC-Chapel Hill	MSIS	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Charlotte	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0901	Information Systems and Supply Chain Management	UNC Greensboro	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0901	Information Technology and Management	UNC Greensboro	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Pembroke	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Wilmington	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	Winston-Salem State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0401	Management Information Systems	Winston-Salem State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0401	Geographic Information Science and Technology	East Carolina University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0401	Information and Library Science	UNC-Chapel Hill	PhD (Doctor of Philosophy)	Computer and Info Sciences and Support Services
11.0802	Business Analytics	Appalachian State University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0199	Computer Game Development	East Carolina University	4C (Certificate within Baccalaureate degree)	Computer and Info Sciences and Support Services
11.0901	Computer Network Professional	East Carolina University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.1003	Information Assurance	East Carolina University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.1004	Website Developer	East Carolina University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
14.0901	Computer Engineering	NC A&T State University	BS (Bachelor of Science)	Engineering
14.0901	Computer Engineering	NC State University	BS (Bachelor of Science)	Engineering
14.0901	Computer Engineering	NC State University	MS (Master of Science)	Engineering
11.0801	New Media	UNC Asheville	BA (Bachelor of Arts)	Computer and Info Sciences and Support Services
11.0103	Advanced Databases Knowledge Discovery	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0701	Computer Architecture	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0701	Computer Programming	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0101	Computing and Information Systems	UNC Charlotte	PhD (Doctor of Philosophy)	Computer and Info Sciences and Support Services
11.0701	Game Design and Development	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0103	Health Informatics	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0103	Information Security and Privacy	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0103	Management of Information Technology	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0701	Undergraduate Certificate in Game Design and Development	UNC Charlotte	4C (Certificate within Baccalaureate degree)	Computer and Info Sciences and Support Services
11.0201	Certificate in Computer Programming	Winston-Salem State University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
52.1201	Computer Information Systems	Appalachian State University	BSBA (Bachelor of Science in Business Administration)	Business, Management, Marketing, and Related Support Services

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
52.1201	Computer Information Systems	Western Carolina University	BSBA (Bachelor of Science in Business Administration)	Business, Management, Marketing, and Related Support Services
15.0303	Electrical and Computer Engineering Technology	Western Carolina University	BS (Bachelor of Science)	Engineering Technologies/Technicians

Using the program lookup keyword “Information Technology” in the degree finder utility, a total of 14 results were returned (see Table 27).

Table 27- UNC Program Degree Finder Results based on keyword "Information Technology"

CIP Code	Program Title	Campus	Degree Awarded	Subject Area
11.0401	Geographic Information Science and Technology	East Carolina University	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0401	Geographic Information Science and Technology	East Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information and Computer Technology	East Carolina University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	NC A&T State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.1001	Information Technology	NC A&T State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Charlotte	MS (Master of Science)	Computer and Info Sciences and Support Services

11.0103	Management of Information Technology	UNC Charlotte	PB (Post-Baccalaureate Certificate)	Computer and Info Sciences and Support Services
11.0901	Information Technology and Management	UNC Greensboro	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Pembroke	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	UNC Wilmington	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
11.0101	Computer Science and Information Technology	Winston-Salem State University	MS (Master of Science)	Computer and Info Sciences and Support Services
11.0103	Information Technology	Winston-Salem State University	BS (Bachelor of Science)	Computer and Info Sciences and Support Services
30.0601	Geospatial Information Science and Technology	NC State University	M (Master's Degree)	Multi/Interdisciplinary Studies
11.1099	Network Technology	East Carolina University	MS (Master of Science)	Computer and Info Sciences and Support Services

Appalachian State University

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

Appalachian State University

	BS in Computer Science
	http://programsofstudy.appstate.edu/sites/programsofstudy.appstate.edu/files/CS%20219A_3.pdf
CS 1440	Computer Science I
CS 2440	Computer Science II
CS 2450	Introduction to Computer Systems
CS 2490	introduction to Theoretical Computer Science
CS 3100	Junior Seminar
CS3430	Database
CS3460	Data Structures
CS 3481	Computer Systems I
CS 3482	Computer Systems II
CS 3490	Programming Languages
CS 3667	Software Engineering
CS4100	Senior Seminar
	Choose one Capstone (3 Hours minimum)
CS 4800	Capstone Project
CS 4510	Senior Honors Thesis
	9 Hours Computer Science Electives- 2 apply to security
CS 3760	Systems Admin & Security
CS 3770	Computational Cryptography
	MS Computer Science
	http://www.graduate.appstate.edu/gradstudies/bulletin14/programs/compsci.html
CS 5100	Seminar in Computer Science
CS 5110	Design and Analysis of Algorithms
CS 5483	Computer Architecture
CS 5520	Operating Systems (security issues)
CS 5666	Software Engineering

Appalachian State University
Course Descriptions

Undergraduate:

Source: Appalachian State University Undergraduate Bulletin 2014-2015, http://www.registrar.appstate.edu/catalogs/14_15_undergrad/11_artsandsciences.pdf, November, 24, 2014.

CS 3430. Database (3).F;S. This course covers the design, organization, representation, and manipulation of databases. Topics include the relational model, data definition, data manipulation, queries (SQL), communication and representation (XML), design concepts, security, and integrity. Prerequisite: CS 2440 with a grade of "C" or higher.
CS 3760. System Administration and Security (3).On Demand.
Addresses local and global security issues with computers using different operating systems in a networked environment. Assignments allow student teams to experience a variety of administration responsibilities including installation, operation, and management. Prerequisite: CS 3460 with a grade of "C" or higher. Unix experience recommended.
CS 3770. Computational Cryptography (3).S. This course explores the theory and implementation of modern cryptographic systems and their application to network security. Topics include: symmetric ciphers, encryption standards, public key encryption, key management, cryptoanalysis, and network security. Programming projects involve the implementation of cryptographic systems. Prerequisite: CS 3460.
CS 4435. Server-side Web Programming (3).S. This course introduces the technologies for implementing secure, high performance, and sophisticated web sites. Topics may include: installation and configuration of a web server, client/server web applications with database backends, web development frameworks, web services, web data formats, and content management systems. Prerequisites: CS 3430 and CS 3440.
CS 4520. Operating Systems (4).S. An in-depth study of the design and implementation of operating systems including device drivers, process management, memory management, and security issues. Lecture three hours, laboratory three hours. Prerequisite: CS 3482. (COMPUTER) [Dual-listed with CS 5520.] Dual-listed courses require senior standing; juniors may enroll with permission of the department.

Graduate:

Source: Appalachian State University Graduate Bulletin 2014-2015, http://www.graduate.appstate.edu/gradstudies/bulletin14/courses/compsci.html, November 24, 2014.

CS 5520. Operating Systems/(4).S. An in-depth study of the design and implementation of operating systems including device drivers, process management, memory management, and security issues. Lecture three hours, laboratory three hours. Prerequisite: CS 3482 (Computer Systems II). [Dual-listed with CS 4520.]

East Carolina University Programs

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

East Carolina University

	BS Computer Science
	http://catalog.ecu.edu/preview_program.php?catoid=7&poid=1625&returnto=443
CSCI 2310	Algorithmic Problem Solving and Programming Laboratory
CSCI 2311	Algorithmic Problem Solving and Programming Laboratory
CSCI 2410	Digital Electronics
CSCI 3300	Introduction to Algorithms and Data Structures
CSCI 3310	Advanced Data Structures and Data Abstraction
CSCI 3650	Analysis of Algorithms
CSCI 3675	Organization of Programming Language
CSCI 3700	Database Management Language
CSCI 4000	Ethical and Professional Issues in Computer Science
CSCI 4200	Software Engineering I
CSCI 4230	Software Engineering II
CSCI 4602	Theory of Automate and Linguistics
CSCI 4630	Operating Systems I
	CSCI electives above 2999 - 9 s.h. required
	BA in Computer Science
	http://catalog.ecu.edu/preview_program.php?catoid=7&poid=1624&returnto=443
CSCI 2310	Algorithmic Problem Solving and Programming Laboratory
CSCI 2311	Algorithmic Problem Solving and Programming Laboratory
CSCI 2410	Digital Electronics
CSCI 3200	Data Structures and Their Applications
CSCI 3700	Database Management Language
CSCI 4000	Ethical and Professional Issues in Computer Science
CSCI 4200	Software Engineering I
CSCI 4300	Systems Programming
CSCI 4530	Computer Networks and the Internet
CSCI 4710	Introduction to Developing e-Business Systems
	Choose 6 s.h. CSCI courses above 2999, excldes CSCI 3584 and CSCI 5774
CSCI 4540	Introduction to Mobile Communications and Wireless Security
	MS Computer Science
	http://catalog.ecu.edu/preview_program.php?catoid=6&poid=1329&returnto=346
CSCI 6120	Computer Systems Architecture
CSCI 6230	Software Engineering Foundations

East Carolina University

CSCI 6420 Computability and Complexity
CSCI 5210 Operating Systems II or
CSCI 5220 Program Translation
Additional 18 s.h. from CSCI courses 5000 or above
SENG 6247 Software Security Engineering

BS in Information and Computer Technology
http://catalog.ecu.edu/preview_program.php?catoid=7&poid=1635&returnto=443
Lower Division Core 24 s.h.
ICTN 1500 Information and Computer Technology Fundamentals
ICTN 1501 Information and Computer Technology Fundamentals Laboratory
ICTN 2150 Network Fundamentals
ICTN 2151 Network Fundamentals Laboratory
ICTN 2154 Digital Communication Systems
ICTN 2155 Digital Communication Systems Laboratory
ICTN 2158 Computer Networking Technology
ICTN 2159 Computer Networking Technology Laboratory
ICTN 2510 Network Environment I
ICTN 2511 Network Environment I Laboratory
ICTN 2530 Network Environment II
ICTN 2531 Network Environment II Laboratory
ICTN 2732 Scripting for Information Technology

Upper - Division Core -- 24 s.h.
ITEC 2000 Industrial Technology Applications of Computer Systems or
ITEC 3000 Internet Tools Technology
ICTN 2900 Fundamental Network Security
ICTN 2901 Fundamental Network Security Laboratory
ICTN 3540 Network Environment III
ICTN 3541 Network Environment III Laboratory
ICTN 4000 Network Internship
ICTN 4020 Senior Information and Computer Technology Capstone Design Project I
ICTN 4022 Senior Information and Computer Technology Capstone Design Project II
ICTN 4040 Enterprise Information Security
IDIS 3790 Technical Presentations
ITEC 3290 Technical Writing
ITEC 3300 Technology Project Management

Concentration area -- 12 s.h. (Computer Networking)
ICTN 3250 Internetwork Routing Technology
ICTN 3251 Internetwork Routing Technology Laboratory
ICTN 4150 Switching Network Technology
ICTN 4151 Switching Network Technology Laboratory

East Carolina University

ICTN 4250	Enterprise Network Security Technology
ICTN 4251	Enterprise Network Security Technology Laboratory
ICTN 4590	Network Maintenance and Troubleshooting
ICTN 4591	Network Maintenance and Troubleshooting Laboratory

Concentration area -- 12 s.h. (Information Security)

ICTN 4064	Regulations and Policies
ICTN 4200	Intrusion Detection Technologies
ICTN 4201	Intrusion Detection Technologies Laboratory
ICTN 4600	Enterprise Information Technology Management
ICTN 4601	Enterprise Information Technology Management Laboratory
ICTN 4800	Information Assurance Technologies
ICTN 4801	Information Assurance Technologies Laboratory

East Carolina University
Course Descriptions

Undergraduate:

Source: East Carolina University 2014-2015 Undergraduate Catalog, http://catalog.ecu.edu/content.php?catoid=7&navoid=450, November, 24, 2014.

CSCI 4000 - Ethical and Professional Issues in Computer Science 1 To be taken by CSCI seniors in final semester. Departmental assessment and professional, ethical, legal, security, and social issues and responsibilities related to the practice of computer science.
CSCI 4300 - Systems Programming 3 P: CSCI 3200 or CSCI 3310. Programming issues related to the functionality and general structure of operating systems, networking, security, and the general architecture of information systems are covered.
CSCI 4540 - Introduction to Mobile Communications and Wireless Security 3 FOY P: CSCI 4530 or consent of instructor. Signals, access protocols, application requirements and security issues. Focus is on digital data transfer.
ICTN 2510 - Network Environment I 3 F 2 lecture hours per week. P: ICTN 1500; C: ICTN 2511. Network management using various NOS products. Topics include NOS setup, network resource management, user and group management, and security model.
ICTN 2511 - Network Environment I Laboratory 0 F 2 lab hours per week. P: ICTN 1500; C: ICTN 2510. Network management using various NOS products. Topics include NOS setup, network resource management, user and group management, and security model.
ICTN 2530 - Network Environment II 3 F,S 2 lecture hours per week. P: ICTN 1500; C: ICTN 2531. Network management using various products such as Linux and Solaris, including NOS setup, network resource management, user and group management, and security model.
ICTN 2531 - Network Environment II Laboratory 0 F,S 2 lab hours per week.

P: ICTN 1500; C: ICTN 2530. Network management using various products such as Linux and Solaris, including NOS setup, network resource management, user and group management, and security model.

ICTN 2900 - Fundamental Network Security 3 F 2 lecture hours per week. P: ICTN 2150; C: ICTN 2901. Computer network and information security principles, devices, and applications.

ICTN 2901 - Fundamental Network Security Laboratory 0 F 2 lab hours per week. P: ICTN 2150; C: ICTN 2900. Computer network and information security principles, devices, and applications.

ICTN 3540 - Network Environment III 3 F 2 lecture hours per week. P: ICTN 2530; C: ICTN 3541. Enterprise system administration using mixed vendor network operating systems, such as Linux and Microsoft. Topics include integrating networking services such as network file systems, enterprise printing administration, remote administration, and host and network security issues.

ICTN 3541 - Network Environment III Laboratory 0 F 2 lab hours per week. P: ICTN 2530; C: ICTN 3540. Enterprise system administration using mixed vendor network operating systems, such as Linux and Microsoft. Topics include integrating networking services such as network file systems, enterprise printing administration, remote administration, and host and network security issues.

ICTN 3900 - Web Services Management 3 F 2 lecture hours per week. P: ICTN 2510 , ICTN 2530 ; C: ICTN 3901. Current technologies that provide web services and management for organizations. Topics include web content development, web server installation and configuration, database integration, and security issues.

ICTN 3901 - Web Services Management Laboratory 0 F 2 lab hours per week. P: ICTN 2510 , ICTN 2530; C: ICTN 3900. Current technologies that provide web services and management for organizations. Topics include web content development, web server installation and configuration, database integration, and security issues.

ICTN 4010 - User Application Management and Emerging Technologies 3 F 2 lecture hours per week. P: ICTN 2530; RP: ICTN 4011. Emerging technologies that provide flexible and secure access to enterprise information resources. Topics include wireless and WLAN technology, broadband Internet connection, storage area networks, data warehousing/mining, application support for enterprise network.

ICTN 4011 - User Application Management and Emerging Technologies Laboratory 0 F 2 lab hours per week. P: ICTN 2530; C: ICTN 4010. Emerging technologies that provide flexible and secure access to enterprise information resources. Topics include wireless and WLAN technology, broadband Internet connection, storage area networks, data warehousing/mining, application support for enterprise network.

ICTN 4040 - Enterprise Information Security 3 S P: ICTN 2530, ICTN 2900. Planning, implementing, and maintain an information security program in an enterprise.

ICTN 4200 - Intrusion Detection Technologies 3 F 2 lecture hours per week. P: ICTN 2530, ICTN 2900; C: ICTN 4201. Computer network intrusion detection principles, devices, and applications.

ICTN 4201 - Intrusion Detection Technologies Laboratory 0 F 2 lab hours per week. P: ICTN 2530, ICTN 2900; C: ICTN 4200. Computer network intrusion detection principles, devices, and applications.

ICTN 4250 - Enterprise Network Security Technology 3 S 2 lecture hours per week. P: Current CCNA certification; C: ICTN 4251. Enterprise network security threats,

vulnerabilities, and mitigation techniques. The installation, troubleshooting, and monitoring of network devices to maintain integrity, confidentiality, and availability of data and devices.
ICTN 4251 - Enterprise Network Security Technology Laboratory 0 S 2 lab hours per week. P: Current CCNA certification; C: ICTN 4250. Enterprise network security threats, vulnerabilities, and mitigation techniques. The installation, troubleshooting, and monitoring of network devices to maintain integrity, confidentiality, and availability of data and devices.
ICTN 4800 - Information Assurance Technologies 3 F 2 lecture hours per week. P: ICTN 2530, ICTN 2900; C: ICTN 4801. Information assurance principles, devices, and applications. Emphasis on problems relating to systems of varied operations system technologies and computer networking technologies.
ICTN 4801 - Information Assurance Technologies Laboratory 0 F 2 lab hours per week. P: ICTN 2530, ICTN 2900; C: ICTN 4800. Information assurance principles, devices, and applications. Emphasis on problems relating to systems of varied operations system technologies and computer networking technologies.

Graduate:

Source: East Carolina University 2014-2015 Graduate Catalog, http://catalog.ecu.edu/content.php?catoid=6&navoid=386, November, 24, 2014.

CSCI 6100 - Cryptography and Information Security 3 P: Consent of instructor. Cryptographic techniques to provide secrecy and authenticity of information communicated over an insecure channel; private-key cryptography, public-key cryptography and deployed cryptography.
CSCI 6140 - Mobile Communications and Wireless Security 3 P: CSCI 6130 or consent of instructor. Signals, access protocols, application requirements, and security issues with a focus on digital data transfer.
CSCI 6300 - Cryptographic Protocols 3 P: CSCI 6100 or consent of instructor. Design and analysis of cryptographic protocols for various tasks; emphasis on applications beyond providing secrecy and authenticity of messages.
ICTN 6823 - Information Security Management 3 P/C: ICTN 6050 or ICTN 6800; ICTN 6810 or consent of instructor; ITEC 6050. Survey of information security terms, concepts, principles, and applications in data networking environment.
ICTN 6830 - Advanced Networking Technology 3 P: ICTN 6810. Advanced topics in computer networking technology used in industry. Problem-solving activities dealing with installation, configuration, and security of internet and intranet services.
ICTN 6835 - Enterprise Web Services 3 P: ICTN 6825. Study of integrated web services to a successful enterprise web presence. Topics include development of web site with multiple integrated services, website performance, and security consideration.
ICTN 6865 - Fundamental Network Security 3 P: ICTN 6800 or ITEC 6050. Survey of security challenge to data communication and computer network. Topics include evaluation of network security threats, fundamental configuration of enterprise network devices, and enterprise network security policy development.
ICTN 6870 - Advanced Network Security 3 P: ICTN 6865. Advanced technology for providing secure access to enterprise information network and resources. Topics include

Virtual Private Network (VPN) implementation, intrusion detection system implementation and configuration, and organizational security models.
ICTN 6873 - Network Intrusion Detection and Incident Response 3 P: ICTN 6865. State-of-art intrusion detection technology for protecting data network from malicious attack.
SENG 6247 - Software Security Engineering 3 P: Consent of instructor. Practical and theoretical knowledge in relation to design of secure software systems.

Elizabeth City State University

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

Elizabeth City State University	
	BS in Computer Science with Information Systems Concentration
	http://www.ecsu.edu/mcs/docs/degrees/informationSystemsConcentration.pdf
CSC 114	Introduction to Computer Science
CSC 115	Programming I
CSC 260	Major Orientation
CSC 215	Programming II
CSC 218	Data Structures
CSC 230	Object-Oriented Programming
CSC 260	Sophomore Seminar in CS
CSC 314	Computer Architecture and Org.
CSC 325	Database Systems
CSC 410	Net-Centric computing
CSC 460	Senior Seminar in CS
	Concentration Requirements
BMIS 380	Management information Systems II
TECH 410	Project Management
CSC 413	System Analysis and Design

Course Descriptions

Source: Elizabeth City State University Computer Science Course Descriptions, http://www.ecsu.edu/academics/catalogs/undergrad/7024.htm, November, 24, 2014.

CSC 260: Sophomore Seminar in Computer Science (1) (S) History of Computing; Social Context; Analytical tools; Professional Ethics; Risks; Security Operations, Intellectual Property, and Privacy and Civil Liberties. This course is now designed to give students an introduction to the major and to provide the basic knowledge, overview and foundation for the curriculum. Prerequisite: CSC 215 or CSC 230
CSC 410: Net-Centric Computing (3) (F) Introduction to Networks, Network Communication, Network Security, Web Organization, Networked Applications,

Network Management, Compression, Multimedia Technologies, and Mobile Computing. Prerequisite: CSC 314

CSC 420: Operating Systems (3) (S) Overview of Operating Systems; Operating Systems Principles; Concurrency; Scheduling and Dispatch; Memory Management; Device Management; Security and Protection; File Systems; Real Time and Embedded Systems; Fault Tolerance; System Performance Evaluation; Scripting; Security Models; and Device Management. Prerequisite: CSC 218.

BMIS 410: Business Networks (3) (F) Identify, differentiate and analyze Network requirements in today's businesses. Local Area Networks (LAN) and all five carrier service infrastructures (CSI) transport and related costs to the businesses. Examine several business network types and Total Cost of Operation (TCO), and on-going maintenance and support. Analyze costs and benefits to the business of e-commerce, network security, Intranet and Virtual Private Networks. Prerequisites: Business Administration or Physical Education major, ACCT 210 and BMIS 380, or permission of department chairperson.

Fayetteville State University

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

Fayetteville State University

	BS in Computer Science
	http://catalog.uncfsu.edu/undergraduate/college-of-arts-and-sciences/math/bs-in-computer-science.htm
CSC 105	Introduction to Computer Science for Technical Majors
CSC 120	Introduction to Programming Methodology
CSC130	Program Design and Implementation
CSC 201	Computer Organization and Architecture I
CSC 207	Symbolic Programming
CSC 220	Data Structure/ Algorithms
CSC 303	Computer Organization and Architecture II
CSC 320	Design and Analysis of Algorithms
CSC 322	Programming Languages
CSC 350	Service Learning
CSC 403	Social, Ethical, and Professional Issues (security)
CSC 431	Operating Systems I
CSC 470	Software Engineering
CSC 490	Senior Project (computer security)
	3 credits from CSC 200 or higher,3 credits from CSC 300 or higher,3 credits from CSC 400 or higher. Select one from the following: CSC 202 Or CSC 204
CSC 323	Principles of Database Design (file security)
CSC 380	Introduction to WAN (Wide Area Network) (WAN security concepts)

Course Descriptions

Source: Fayetteville State University Undergraduate Catalog 2014-2015, http://catalog.uncfsu.edu/undergraduate/college-of-arts-and-sciences/math/course-descriptions.htm, November, 24, 2014.

CSC 323 (3-3-0) Principles of Database Design: This course emphasizes the concepts and structures necessary to design and implement a database management system. It will acquaint the students with current literature on the subject and give them an opportunity to use a database management system. Topics include database concepts, hierarchical, network and relational data models, data normalization, data description languages, query facilities, file organization, file security, data integrity, and reliability. Prerequisite: CSC 220

CSC 380 (3-3-0) Introduction to WAN (Wide Area Network): This course discusses the WAN technologies and network services required by converged applications in enterprise networks. The course uses the Cisco Network Architecture to introduce integrated network services and explains how to select the appropriate devices and technologies to meet network requirements. Students learn how to implement and configure common data link protocols and how to apply WAN security concepts, principals of traffic, access control, and addressing services. Finally, students learn how to detect, troubleshot, and correct common enterprise network implementation issues. Prerequisite: CSC 371 And CSC 372

CSC 403 (1-1-0) Social, Ethical, and Professional Issues: This course discusses the impact of computers on society including people, business, and government. Topics include historical and social issues, security, privacy, professional responsibilities, risks and liability, and intellectual property. Prerequisite: 18 hours of CSC credit

CSC 490 (3-3-0) Senior Project: This course presents a formal approach to state-of-the-art techniques in computer science and provides a means for students to apply the techniques. An integral part of the course is the involvement of students working in teams in the organization, management, and development of a large project. Project topics include software systems and methodology, computer organization and architecture, theory and mathematical background, computer security and social issues. Prerequisite: Senior standing And 9 hours of CSC at the 300 level And 6 hours of CSC at the 400 level

MATH 315 (3-3-0) Applied Cryptography: This course is an introduction to classical and modern cryptography. We apply elementary number theory to the problems of cryptography. Topics include classical cryptosystems, basic number theory, the data encryption standards, the RSA algorithm, discrete logarithms, Hash functions, digital signatures, digital cash, secret sharing schemes, and the zero knowledge techniques. A computer algebra system will be used. Prerequisite: MATH 150

NC A&T State University

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

NC A&T State University

	BS in Computer Science
	http://www.ncat.edu/academics/schools-colleges1/coe/comp/index.html
GEEN 111	College of Engineering Colloquium
GEEN 163	Introduction to Computer programming
GEEN 165	Computer Programming Design
COMP 121	Computer Science Freshmen Colloquium
COMP 200	Computer Science Sophomore Colloquium
COMP 280	Data Structures
COMP 285	Design and Analysis of Algorithms
COMP 300	Computer Science Junior Colloquium
COMP 322	Internet Systems
COMP 360	Principles of Programming Languages
COMP 365	Programming Methodologies & Concepts
COMP 375	Computer Architecture and Organization
COMP 385	Theory of Computing
COMP 390	Social Implications of Computing
COMP 450	Operating Systems
COMP 467	Data Base Design
COMP 476	Networked Computer Systems
COMP 510	Software Engineering
COMP 596	Senior Project II
	9 S.H Computer Science Elective- 4 Courses related to Security found
COMP 320	Fundamentals of Information Assurance
COMP 321	Computer System Security
COMP 420	Applied Network Security
COMP 421	Security Management for Information Systems
	MS in Computer Science
	http://www.ncat.edu/academics/schools-colleges1/coe/comp/index.html
COMP 755	Advanced Operating Systems
COMP 785	Advanced Design and Analysis of Algorithms
	Select from one of the available tracks:
	Information Assurance
COMP 620	Information, Privacy, and Security
COMP 621	Web Security
COMP 726	Network Security
COMP xxx	Information Assurance elective

NC A&T State University

	Secure Software Engineering
COMP 710	Software Specification, Analysis, & Design
COMP 725	Software Security Testing
COMP 727	Secure Software Engineering
COMP xxx	Secure Software Engineering elective
	Electives with security:
COMP 627	Wireless Network Security
COMP 723	Intrusion Detection
COMP 724	Security and Multiagent Systems

PhD in Computer Science with Concentration in Security

http://www.ncat.edu/academics/schools-colleges1/coe/comp/index.html

COMP 755	Advanced Operating Systems
COMP 785	Advanced Design & Analysis of Algorithms
COMP 892	Doctoral Supervised Research, prerequisite: COMP-991
	Security Concentration
COMP 821	Cloud Computing & Security
COMP 823	Secure Social Computing
	Component exams:
COMP 755	Advanced Operating Systems and
COMP 785	Advanced Design & Analysis of Algorithms.
	Select 2 additional component exams from:
COMP 725	Software Security Testing
COMP 727	Secure Software Engineering
COMP 620	Information, Privacy, and Security
COMP 621	Web Security
COMP 726	Network Security
COMP 767	Computer Network Architecture

Course Descriptions
Undergraduate:

Source: North Carolina Agricultural & Technical State University – College of Engineering, Bachelor of Science in Computer Science Undergraduate Student Handbook (Last Handbook Update – May 30, 2012), http://www.ncat.edu/academics/schools-colleges1/coe/comp/pdfs/undergrad, November, 24, 2014.

COMP 120. Computers and Their Use Credits 3(2-2) This Course provides a survey of the basic principles of computer hardware, computer communications, application software, operating systems, security, impact on society, use in organizations and systems

development. Principles of programming are introduced. Information is at a level for the students to become informed users. This course cannot be taken for credit by computer science majors. Prerequisite: None. (F;S;SS)

COMP 170. Introduction to Web Engineering Credits 4(3-2) This course introduces basic web development using HTML and client-side and server-side scripting. Students also learn how to incorporate security features into web sites as well as how to access and manage online databases. This course also covers the role of the web in disseminating knowledge, community formation, training, collaboration, and other social activities. Prerequisite: None (F;S;SS)

COMP 320. Fundamentals of Information Assurance Credits 3(3-0) This course covers concepts in computer network and information security. Topics include: software strategies for exchanging secure data and encryption standards. Strategies for the physical protection of information assets are explored. Issues involving information security management within an enterprise are covered, including suitable organizational policy, plans, and implementation strategies. Ethical issues, such as monitoring employee computer use and proper limitations on the use of customer data, are also discussed. Prerequisite: COMP280 (F;S;SS)

COMP 321. Computer System Security Credits 3(3-0) This course introduces the principles of information systems security and examines security policies, models, mechanisms for secrecy, integrity, availability and access controls. Topics include common system vulnerabilities and countermeasures, data availability and usage control, authentication technologies, design secure systems, operating systems security, network security, programming language security, and distributed systems security. Prerequisite: COMP285 (F;S;SS)

COMP 420. Applied Network Security Credits 3(3-0) This course covers network security concepts and various network security practices and solutions. Topics include cryptography, Public Key Infrastructure (PKI), taxonomy of various attack methods, firewalls, intrusion detection and prevention, Internet Protocol (IP) security, and web security. Prerequisite: COMP285 (F;S;SS)

COMP 421. Security Management for Information Systems Credits 3(3-0)18 This course covers in-depth examination of topics in the management of information systems security including access control systems & methodology, risk management, business continuity and disaster recovery planning, legal and ethical issues in information system security, computer operations security, physical security, and information security maintenance. Prerequisite: COMP285 (F;S;SS)

COMP 450. Operating Systems Credits 3(3-0) This is and introduction to the theory and practice of operating system design and implementation. Algorithmic techniques are presented for implementing process management, storage management, processor management, file systems, security, distributed systems, performance evaluation, and real time systems. Prerequisite: COMP 375 or Corequisite: COMP 375. (F;S)

COMP 476. Networked Computer Systems Credits 3(3-0) This course presents an overview of the technology, architecture and software used by systems of network-connected computers. The course will cover data transmission, local area network architecture, network protocols, internetworking, security, and World Wide Web technology. Students will write programs that run concurrently on multiple computers.

Prerequisite: COMP 280 or ECEN327 (F;S)

Graduate:

Source: North Carolina Agricultural & Technical State University – College of Engineering, Master of Science in Computer Science Graduate Student Handbook (Last Updated July 2011), http://www.ncat.edu/academics/schools-colleges1/coe/comp/pdfs/csghbk.pdf, November, 24, 2014.

COMP-620. Information, Privacy and Security Credit 3 (3-0) This course examines the security and privacy issues associated with information systems. There are cost/risk tradeoffs to be made. Discussed are topics such as technical, physical, and administrative methods of providing security, access control, identification, and authentication. Encryption is examined, including Data Encryption Standards (DES) and public key cryptosystems. Management considerations such as key protection and distribution, orange book requirements, and OSI data security standards are covered. Privacy legislation is covered, as is current cryptographic research.
COMP-621. Web Security Credit 3 (3-0) This course focuses on the technologies that provide security services for the World Wide Web. It introduces a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organizations. We discuss, understand and use various security technologies for the World Wide Web (WWW). How to use these technologies to secure WWW applications will be addressed.
COMP-627. Wireless Network Security Credit 3 (3-0) This course covers the security issues associated with wireless networks. Emerging wireless technologies, standards and protocols are explored. The course will define and demonstrate various threats to wireless security. Topics include security service, security protocol, and security architecture for wireless. Details of wireless encryption techniques are examined.
COMP-722. E-Commerce Credit 3 (3-0) This course covers the computer science and technology that enable e-commerce and the business concepts needed to understand e-commerce. Topics reviewed include HTML and CSS as well as client-side scripting. Topics introduced include e-commerce features, business models, and marketing concepts. Topics emphasized include the HTTP protocol, server-side scripting, the XML family of specifications, web services, the Semantic Web, and security in an e-commerce context.
COMP-723. Intrusion Detection Credit 3 (3-0) This course introduces the concepts, techniques, tools, and the state of the art in the area of network intrusion detection systems. Topics to be covered include: network and computer system security fundamentals, network security models and approaches, attack classification and analysis, intrusions detection techniques and tools (vulnerability scanners, network sniffer, system monitoring and logging, etc), firewall, as well as the tools and techniques for intrusion signature analysis, such as TCPdump and Snort, etc. The course will be a seminar-like, research-oriented class. Students are required to actively participate in the class presentations and discussions. Besides the textbooks, we will read and discuss many recent technical papers from current research in intrusion detection.
COMP-724. Security and Multiagent Systems Credit 3 (3-0) This course addresses agents that communicate and coordinate over the web. The focus is on DARPA Agent

Markup Language (DAML) and similar contributions to the area known broadly as the Semantic Web. Necessary background in XML, RDF, and SOAP is covered. The course also considers specifications of security and trustworthiness properties for systems of such agents both using formal techniques (process algebras and modal logics) and considering social aspects of Web use (as in e-commerce).

COMP-725. Software Security Testing Credit 3 (3-0) This course focuses on software security testing techniques and tools. It covers security testing techniques such as code reviews and static analysis, creating test plans based on risk analysis, black-box, white-box and gray-box security testing, fault injection etc. Security testing tools will be introduced.

COMP-726. Network Security Credit 3 (3-0) The course covers various aspects of securing data during their transmission. It includes the following topics: vulnerabilities in software and hardware systems; cyber attack methods and their defense mechanisms; symmetric ciphers; public key ciphers; hash functions; message authentication and digital signature; public key infrastructure and web of trust; email security; web security; IPSec; firewall; intrusion detection system.

COMP-727. Secure Software Engineering Credit 3 (3-0) This course discusses how to incorporate security throughout the software development lifecycle. The main topics include threats to the software, software vulnerabilities, risk management, security requirements, secure design principles and patterns, an overview of secure programming and security testing.

COMP-750. Distributed Systems Credit 3 (3-0) This course examines the operating system concepts necessary for the design and effective use of networked computer systems. Such concepts include communication models and standards, remote procedure calls, name resolution, distributed file systems, security, mutual exclusion, and distributed databases. Students are required to construct an advanced implementation of distributed operating system facilities or a simulation of same.

COMP-755. Advanced Operating Systems Credit 3 (3-0) This course centers on operating systems for multi-processing environments: concurrent processes, mutual exclusion, job scheduling, memory, storage hierarchy, file systems, security, and distributed processing. Also discussed are virtual resource management strategies. A design project involving the construction of operating facilities is produced.

Source: PhD in Computer Science at North Carolina A&T State University – Admission and Program Requirements (Last Updated December 5, 2013), http://www.ncat.edu/academics/schools-colleges1/coe/comp/pdfs/csphd, November, 24, 2014.

Program Requirements listed required classes, but did not contain a course description. Utilized course list to search within the Catalog to obtain descriptions.

Source: North Carolina A&T State University Course Catalog, https://ssbprod.ncat.edu/pls/NCATPROD/bwckctlg.p_display_courses, November, 24, 2014.

COMP 821. Cloud Computing and Security Credit 3 This class covers the practices and applications of cloud computing and related security issues. The topics include

architectures of cloud computing, models of cloud computing, Infrastructure-as-a-Service (IaaS), Software as a Service (SaaS), Platform-as-a-Service (PaaS), virtualization, parallelization, security/privacy/legal, and other issues in cloud computing. Prerequisite: Graduate Standing. (F;S;SS)

COMP 823. Secure Social Computing Credit 3 Social Computing involves computational facilitation of social studies and human social dynamics as well as design and use of information and communication technologies that consider social context. Social computing is a central themes across a number of information and communication technology fields and attracts interest from researchers in computing and social sciences, software and online game vendors, web entrepreneurs, political analysts and digital government practitioners. This course focuses on the privacy, security, risk, and trust aspects of social computing. Prerequisite: Graduate Standing. (F;S;SS)

COMP 829. Topics in Software Assurance Credit 3 This course introduces topics in software assurance education and research. Software security across the development life cycle that address trustworthiness, predictable execution and conformance will be examined. Best practices and methodologies that promote integrity, security, reliability in software development, including processes and procedures that diminish the possibilities of vulnerabilities that could be introduced during development, will be discussed. Students will gain hands-on experience in various techniques and tools. Prerequisites: COMP 710, COMP 727, or Permission of the Instructor. (F;S;SS)

COMP 875. Security Enhanced Operating Systems Credit 3 This course examines operating systems that are designed explicitly to enhance security. The course will cover mandatory access control systems as well as computers intended for home use. Prerequisite: Comp 755. (F;S;SS)

COMP 876. Secure Architectures Credit 3 Hardware and virtual machine enhancements to improve security are explored in this course. The course will cover mandatory access control systems as well as computers intended for home use. Prerequisite: Graduate Standing. (F;S;SS)

NC State University

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

NC State University

	BS in Computer Science
	http://www.csc.ncsu.edu/academics/undergrad/coursework.php
	http://www.csc.ncsu.edu/academics/undergrad/semester.php
E 101	Intro. to Engineering & Prob. Solving
E 115	Intro. to Computing Environments
CSC 116	Introduction to Computing - Java
CSC 216	Programming Concepts – Java
CSC 226	Discrete Mathematics for CSC
CSC 230	C and Software Tools
CSC 236	Comp. Org. & Assembly Lang. for CSC
CSC 246	Operating Systems for CSC

NC State University

302 or 333	Automata, Grammars, and Computability
CSC 316	Data Structures for CSC
CSC 326	Software Engineering
CSC 379	Ethics in Computing
CSC 492	Senior Design Project
	CSC Restricted Electives (total: 12 credit hrs) Security related
CSC 405	Introduction to Computer Security
CSC 474	Network Security

MS in Computer Science

http://www.csc.ncsu.edu/academics/graduate/degrees/ms.php

At least 2 courses taken from each category

Category 1: Theory

CSC 503	Computational Applied Logic
CSC 505	Algorithms
CSC 512	Compiler Construction
CSC 565	Graph Theory
CSC 579	Performance Evaluation
CSC 580	Numerical Analysis
CSC 707	Theory of Computation

Category 2: Systems

CSC 501	Operating Systems
CSC 506	Parallel Architectures
CSC 510	Software Engineering
CSC 520	Artificial Intelligence
CSC 540	Database Systems
CSC 561	Graphics
CSC 570	Networks

Master of Computer Science

http://www.csc.ncsu.edu/academics/graduate/degrees/mcs.php

Select 3+ courses, one from one category, two from the other

Category 1: Theory

CSC 503	Computational Applied Logic
CSC 505	Algorithms
CSC 512	Compiler Construction
CSC 565	Graph Theory
CSC 579	Performance Evaluation
CSC 580	Numerical Analysis
CSC 707	Theory of Computation

Category 2: Systems

CSC 501	Operating Systems

NC State University

CSC 506	Parallel Architectures
CSC 510	Software Engineering
CSC 520	Artificial Intelligence
CSC 540	Database Systems
CSC 561	Graphics
CSC 570	Networks

PhD in Computer Science

http://www.csc.ncsu.edu/academics/graduate/degrees/phd.php

Select 2 courses from each of the two categories

Category 1: Theory

CSC 503	Computational Applied Logic
CSC 505	Algorithms
CSC 512	Compiler Construction
CSC 565	Graph Theory
CSC 579	Performance Evaluation
CSC 580	Numerical Analysis
CSC 707	Theory of Computation

Category 2: Systems

CSC 501	Operating Systems
CSC 506	Parallel Architectures
CSC 510	Software Engineering
CSC 520	Artificial Intelligence
CSC 540	Database Systems
CSC 561	Graphics
CSC 570	Networks

Course Descriptions
Undergraduate:

Source: NC State University Registration & Records Course Catalog, https://www.acs.ncsu.edu/php/coursecat/directory.php, November, 24, 2014.

CSC 200: Introduction to Computers and Their Uses Units: 3 Survey of basic principles of computer hardware, communications, operating systems, microcomputer issues, security, impact on society, system development, and use in organizations. Hands-on use of software, including operating system commands, word processing, spreadsheets, and database managers. Demonstration and application of current end-user applications. May not be used by CSC major as a restricted elective. Offered in Fall Spring Summer

CSC 246: Concepts and Facilities of Operating Systems for Computer Scientists Units: 3 Fundamental concepts of computer operating systems for computer scientists, including memory management, file systems, process management, distributed systems,

deadlocks, and basic security and system accounting. Prerequisite: CSC 230; Corequisite: CSC 236; CSC and CSU Majors and Minors. Offered in Fall Spring Summer

CSC 340: Information Systems Management Units: 3 Fundamentals of information systems development and use in organizational setting. Information systems [IS], concepts, hardware, software, telecommunications, database management. IS development, applications and management in telecommunications, database management, various business processes, global issues, security and ethical challenges. Offered in Fall and Spring. Also listed as: BUS340

CSC 405: Introduction to Computer Security Units: 3 Basic concepts and techniques in information security and management such as risks and vulnerabilities, applied cryptography, program security, malicious software, authentication, access control, operating systems security, multilevel security, trusted operating systems, database security, inference control, physical security, and system assurance and evaluation. Coverage of high-level concepts such as confidentiality, integrity, and availability applied to hardware, software, and data. Prerequisite: CSC 246 Offered in Spring Only

CSC 413: Electronic Commerce Technology Units: 3 An introduction to the technologies underlying electronic commerce. Topics include Web protocols and languages, Web mining, product ontologies, security anonymity, privacy, recommendation systems, personalization, auctions, trading agents, and intellectual property. Prerequisite: CSC 316 Offered in Spring Only

CSC 422: Automated Learning and Data Analysis Units: 3 Introduction to the problems and techniques for automated discovery of knowledge in databases. Topics include representation, evaluation, and formalization of knowledge for discovery; classification, prediction, clustering, and association methods. Selected applications in commerce, security, and bioinformatics. Students cannot get credit for both CSC 422 and CSC 522. Prerequisite: ST 370 and MA 305, and a grade of C- or better in either CSC 226 or LOG 201 Offered in Spring Only

CSC 440: Database Management Systems Units: 3 Introduction to database concepts. This course examines the logical organization of databases: the entity-relationship model; the relational data model and its languages. Functional dependencies and normal forms. Design, implementation, and optimization of query languages; security and integrity, concurrency control, transaction processing, and distributed database systems. Prerequisite: CSC 316, CSC Majors. Offered in Fall Only

CSC 453: Software for Wireless Sensor Systems Units: 3 Development of software for wireless computer systems. Software designs for applications and networking in this environment, including algorithms for ad hoc discovery, routing, and secure data transfer. Software interface to related sensors and subsystems including global positioning system. Algorithms for power management. Programming required. Prerequisite: [CSC 246 or ECE 306] and CSC 230 and CSC 316. Offered in Spring and Summer

CSC 474: Network Security Units: 3 Basic concepts and techniques in information security and management such as risks and vulnerabilities, applied cryptography, authentication, access control, multilevel security, multilateral security, network attacks and defense, intrusion detection, physical security, copyright protection, privacy mechanisms, security management, system assurance and evaluation, and information warfare. Coverage of high-level concepts such as confidentiality, integrity, and

availability applied to hardware, software, and data. Credit not allowed for both CSC 474 and CSC 574. Prerequisite: CSC 230. Offered in Spring Only

Graduate:

CSC 513: Electronic Commerce Technology Units: 3 Exploration of technological issues and challenges underlying electronic commerce. Distributed systems; network infrastructures; security, trust, and payment solutions; transaction and database systems; and presentation issues. Project required. No Audits. Prerequisite: CSC 501. Offered in Spring Only.

CSC 515: Software Security Units: 3 Introduces students to the discipline of designing, developing, and testing secure and dependable software-based systems. Students will learn about risks and vulnerabilities, and effective software security techniques. Topics include common vulnerabilities, access control, information leakage, logging, usability, risk analysis, testing, design principles, security policies, and privacy. Project required. Prerequisite: CSC 510. Offered in Fall Only.

CSC 522: Automated Learning and Data Analysis Units: 3 Introduction to the problems and techniques for automated discovery of knowledge in databases. Topics include representation, evaluation, and formalization of knowledge for discovery; classification, prediction, clustering, and association methods. Selected applications in commerce, security, and bioinformatics. Students cannot get credit for both CSC 422 and CSC 522. Prerequisite: CSC 226 or LOG 201, ST 370, MA 305. Offered in Spring Only.

CSC 540: Database Management concepts and Systems Units: 3 Advanced database concepts. Logical organization of databases: the entity-relationship model; the relational data model and its languages. Functional dependencies and normal forms. Design, implementation, and optimization of query languages; security and integrity, consurrency control, transaction processing, and distributed database systems. Prerequisite: CSC 316. Offered in Fall Only.

CSC 547: Cloud Computing Technology Units: 3 Study of cloud computing principles, architectures, and actual implementations. Students will learn how to critically evaluate cloud solutions, how to construct and secure a private cloud computing environment based on open source solutions, and how to federate it with external clouds. Performance, security, cost, usability, and utility of cloud computing solutions will be studied both theoretically and in hands-on exercises. Hardware-, infrastructure-, platform-, software-, security-, and high-performance computing - "as-a-service". Prerequisites: CSC 501 and ECE/CSC 570. Offered in Spring Only. Also listed as: ECE 547.

CSC 570: Computer Networks Units: 3 General introduction to computer networks. Discussion of protocol principles, local area and wide area networking, OSI stack, TCP/IP and quality of service principles. Detailed discussion of topics in medium access control, error control coding, and flow control mechanisms. Introduction to networking simulation, security, wireless and optical networking. Prerequisite: ECE 206 or CSC 312, ST 371, CSC 258 and Senior standing or Graduate standing. Offered in Fall and Spring. Also listed as: ECE 570.

CSC 574: Computer and Network Security Units: 3 Security policies, models, and mechanisms for secrecy, integrity, and availability. Basic cryptography and its applications; operating system models and mechanisms for mandatory and discretionary

controls; introduction to database security; security in distributed systems; network security [firewalls, IPsec, and SSL]; and control and prevention of viruses and other rogue programs. Prerequisite: [CSC 316] and [CSC 401 or CSC/ECE 570]. Offered in Fall and Spring. Also listed as: ECE 574.
CSC 575: Introduction to Wireless Networking Units: 3 Introduction to cellular communications, wireless local area networks, ad-hoc and IP infrastructures. Topics include: cellular networks, mobility management, connection admission control algorithms, mobility models, wireless IP networks, ad-hoc routing, sensor networks, quality of service, and wireless security. Prerequisite: ECE/CSC 570. Offered in Spring Only. Also listed as: ECE 575.
CSC 705: Operating Systems Security Units: 3 Fundamentals and advanced topics in operating system [OS] security. Study OS level mechanisms and policies in investigating and defending against real-world attacks on computer systems, such as self-propagating worms, stealthy rootkits and large-scale botnets. OS security techniques such as authentication, system call monitoring, as well as memory protection. Introduce recent advanced techniques such as system-level randomization and hardware virtualization. Prerequisite: CSC 501. Offered in Fall Only.
CSC 712: Software Testing and Reliability Units: 3 An advanced introduction to software testing and reliability. The course is a balanced mixture of theory, practice, and application. Methods, techniques, and tools for testing software and producing reliable and secure software are used and analyzed. Software reliability growth models and techniques for improving and predicting software reliability are examined, and their practical use is demonstrated. Good knowledge of C++ or Java. Knowledge of the basics of statistics, calculus, and linear algebra. Prerequisite: CSC 510. Offered in Fall Only. YEAR: Offered Alternate Even Years.
CSC 743: Secure Data Management Units: 3 Advanced topics in secure data management with techniques in traditional database management systems as well as in recent advances in emerging areas. Emphasis on new security issues and challenges imposed by the Internet and the Web on cross-organization data sharing and management. Example topics include XML, data management in P2P, trust management, data authorship, and the integration of security and privacy policies with information systems. Prerequisite: CSC/ECE 574 and [CSC 440 or CSC 540]. Background in databases and basic security concepts required. Offered in Fall Only.
CSC 774: Advanced Network Security Units: 3 A study of network security policies, models, and mechanisms. Topics include: network security models; review of cryptographic techniques; internet key management protocols; electronic payments protocols and systems; intrusion detection and correlation; broadcast authentication; group key management; security in mobile ad-hoc networks; security in sensor networks. Prerequisite: CSC/ECE 570, CSC/ECE 574. Offered in Spring Only. Also listed as: ECE 774.

UNC Asheville

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC Asheville

BS in Computer Science: Concentration in Computer Systems
http://catalog.unca.edu/preview_program.php?catoid=8&poid=1396&returnto=403

CSCI 107 Introduction to Computers and Multimedia (3)

CSCI 181 Introductory Programming for Numeric Applications (3) or
CSCI 182 Introductory Programming for Media Applications (3)

CSCI 202 Introduction to Data Structures (3)
CSCI 255 Computer Organization (4)
CSCI 320 Computer Architecture (3)
CSCI 331 Operating Systems (3)
CSCI 333 Data Structures (3)
CSCI 343 Database Management Systems (3)
CSCI 346 Computer Graphics (3)
CSCI 431 Organization of Programming Languages (3)
CSCI 462 Senior Project (1)
and 9 additional hours in CSCI at the 300 level or above

BS in Computer Science: Concentration in Information Systems
http://catalog.unca.edu/preview_program.php?catoid=8&poid=1397&returnto=403

CSCI 107 Introduction to Computers and Multimedia (3)

CSCI 181 Introductory Programming for Numeric Applications (3) or
CSCI 182 Introductory Programming for Media Applications (3)

CSCI 202 Introduction to Data Structures (3)
CSCI 255 Computer Organization (4)
CSCI 343 Database Management Systems (3)
CSCI 344 Web Technology (3)
CSCI 448 Systems Development Management (3)
CSCI 462 Senior Project (1)
15 additional hours in CSCI at the 300 level or above

Course Descriptions

Source: University of North Carolina at Asheville 2014-15 Catalog, http://catalog.unca.edu/content.php?catoid=8&navoid=435, November, 24, 2014.

CSCI 331 - Operating Systems (3) Concepts of operating systems: processes, synchronization, memory management, file systems and security. Prerequisites: CSCI 202, 255. Odd years Spring.
CSCI 444 - Issues in Electronic Commerce (3) Issues surrounding computer networks and their use for electronic commerce. Topics include legal and ethical considerations,

privacy, security, technology tradeoffs, outsourcing, digital signatures, digital watermarking and Web architectures. Prerequisites: Computer Science Majors: Senior Standing; Other Majors: Permission of Instructor. See department chair.

UNC-Chapel Hill

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC-Chapel Hill

	BA in Computer Science
	http://www.unc.edu/ugradbulletin/depts/compsci.html
COMP 401	Foundation of Programming
COMP 410	Data Structures
COMP 411	Computer Organization
COMP 283	Discrete Structures
	Six additional COMP courses numbered 426 or higher
	Electives with security:
COMP 380	Computers and Society (security & privacy)
COMP 382	Introduction to Cyberculture (security & privacy)
COMP 535	Introduction to Computer Security (network security)
	BS in Computer Science
	http://www.unc.edu/ugradbulletin/depts/compsci.html
	ALL Major courses in BA plus the following:
COMP 455	Models of Languages and Computation
COMP 550	Algorithms and Analysis
STOR 435	Introduction to Probability
	Five additional COMP courses numbered 426 or higher
	Electives with security:
	** See electives under BA
	MS in Computer Science
	http://www.unc.edu/gradrecord/programs/computer.html
	Electives with security:
COMP 631	Computer Networks (network security)
COMP 655	Cryptography
	http://cs.unc.edu/academics/graduate/ms-requirements/course-categories/
	PhD in Computer Science
	http://cs.unc.edu/academics/graduate/phd-requirements/
	http://www.unc.edu/gradrecord/programs/computer.html
COMP 915	Technical Communication in Computer Science
COMP 994	Doctoral Research and Dissertation

Course Descriptions
Undergraduate:

Source: The University of North Carolina at Chapel Hill Undergraduate Bulletin, 2014-2015 Record, http://www.unc.edu/ugradbulletin/pdf/2014-15.pdf, November, 24, 2014.

COMP 380 Computers and Society (3). A broad introduction to instructional technology and computer science issues in society: Internet history, privacy, security, usability, graphics, games, computers in the media, development, economics, social media, AI, IP, computer and Internet ethics, global ethics, current legal issues, etc. Frequent guest speakers. Lecture course of 100+ students.
COMP 382 Introduction to Cyberculture (3). Prerequisite, COMP 380. Permission of the instructor for students lacking the prerequisite. Explores cultural and ethical issues arising from individuals' and societies' use of information and computing technologies. Includes computer ethics; Internet history; IP, DRM, social media; gaming, virtual worlds; privacy; security; anonymity; net neutrality; AI, the technological singularity. Lecture and discussion.
COMP 535 Introduction to Computer Security (3). Prerequisites, COMP 410, and COMP 283 or MATH 381. Principles of securing the creation, storage, and transmission of data and ensuring its integrity, confidentiality, and availability. Topics include access control, cryptography and cryptographic protocols, network security, and online privacy.
COMP 631 Computer Networks (3). Required preparation, a first course in operating systems, a first course in networking (e.g., COMP 431 and 530), and knowledge of probability and statistics. Topics in computer networks, including link layer protocols, switching, IP, TCP, and congestion control. Additional topics may include peer-to-peer infrastructures, network security, and multimedia applications.
COMP 655 Cryptography (3). Prerequisites, COMP 455 and STOR 435. Permission of the instructor for students lacking the prerequisites. Introduction to the design and analysis of cryptographic algorithms. Topics include basis of abstract algebra and number theory, symmetric and asymmetric encryption algorithms, cryptographic hash functions, message authentication codes, digital signature schemes, elliptic curve algorithms, side-channel attacks, and selected advanced topics.
INLS 384 Information and Computer Ethics (3). Prerequisite, INLS 201. Overview of ethical reasoning, followed by examination of ethical issues relevant to information science, including access to information and technology, societal impacts of technology, information privacy, surveillance and security, intellectual property, and professional ethics.
INLS 566 Information Security (3). Prerequisite, INLS 161 or 461. Aspects of data integrity, privacy, and security from several perspectives: legal issues, technical tools and methods, social and ethical concerns, and standards.
INLS 576 Distributed Systems and Administration (3). Prerequisite, INLS 161 or 461. Distributed and client/server-based computing. Includes operating system basics, security concerns, and issues and trends in network administration.

Graduate:

Source: Graduate Record of The University of North Carolina at Chapel Hill, 2014-2015, http://www.unc.edu/gradrecord/pdf/2014-2015.pdf, November, 24, 2014.

COMP 721 Database Management Systems (3). Prerequisites, COMP 521 and 550. Database management systems, implementation, and theory. Query languages, query optimization, security, advanced physical storage methods and their analysis.
COMP 722 Data Mining (3). Prerequisites, COMP 550 and STOR 435. Data mining is the process of automatic discovery of patterns, changes, associations, and anomalies in massive databases. This course provides a survey of the main topics (including and not limited to classification, regression, clustering, association rules, feature selection, data cleaning, privacy, and security issues) and a wide spectrum of applications.
COMP 734 Distributed Systems (3). Prerequisite, COMP 431. Permission of the instructor for students lacking the prerequisite. Design and implementation of distributed computing systems and services. Interprocess communication and protocols, naming and name resolution, security and authentication, scalability, high availability, replication, transactions, group communications, distributed storage systems.
INLS 762 Internet Issues and Future Initiatives (3). Prerequisite, INLS 572. Members of this seminar discuss emerging Internet policy issues such as copyright, intellectual property, privacy, and security. Participants will also explore emerging Internet tools and applications.

UNC Charlotte

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC Charlotte

BA in Computer Science
http://cs.uncc.edu/academics/undergraduate-programs/programs

ITCS 1212	Introduction to Computer Science
ITCS 1212L	Programming Lab I
ITCS 1213	Introduction to Computer Science II
ITCS 1213L	Programming Lab II
ITCS 1600	Computing Professionals
ITCS 2175	Logic and Algorithms
ITCS 2214	Data Structures
ITCS 2215	Design and Analysis of Algorithms
ITCS 3146	Operating systems and Networking
ITCS 3155	Software Engineering
ITCS 3160	Data Base Design and Implementation
ITCS 3688	Computers and Their Impact on Society

Course Descriptions: http://cs.uncc.edu/academics/undergraduate-programs/courses

BS in Computer Science

UNC Charlotte

http://cs.uncc.edu/academics/undergraduate-programs/programs

ALL Major courese in BA plus the following:

ITCS 3181	Logic and Computer Systems
ITCS 3181L	Computer Systems Lab and Recitation
ITCS 4102	Programming Languages

Networking and Distributed Computing Focus: (12 hrs)

ITCS 3166	Introduction to Computer Networks
ITCS 4131	Communication Network Design (includes network security)
ITCS 4145	Parallel Computing
ITCS 4146	Grid Computing (includes security mechanisms)
ITIS 3200	Intro to Information Security & Privacy

MS in Computer Science – Concentration in Information Security and Privacy

http://cs.uncc.edu/academics/masters-program/requirements

ITCS 6112	Software System Design and Implementation
ITCS 6114	Algorithms & Data Structures
ITCS 5102	Survey of Programming Languages (choose 1 of 5102/6182)
ITCS 6182	Computer System Architecture (choose 1 of 5102/6182)

Information Security and Privacy, requires:

ITIS 6200	Principles of Information Security and Privacy

Plus two additional approved ITIS security courses from:*

ITIS 5220	Vulnerability Assurance and System Assessment
ITIS 5221	Secure Web Application Development
ITIS 5250	Computer Forensics
ITIS 6140	Software Testing and Quality Assurance
ITIS 6167	Network and Information Security
ITIS 6210	Access Control and Security Architecture
ITIS 6230	Information Infrastructure Protection
ITIS 6240	Applied Cryptography
ITIS 6362	Information Technology Ethics, Policy, and Security
ITIS 6420	Usable Security and Privacy
ITIS 6220	Data Privacy
ITIS 6150	Software Assurance

* http://cs.uncc.edu/academics/itis-security-courses

MS in Information Technology

http://sis.uncc.edu/academics/masters-programs/degree-requirements

ITIS 5166	Network-Based Application Development
ITIS 6112	Software System Design and Implementation
ITIS 6120	Applied Databases (may be substituted with ITCS 6160 Database Systems)
ITIS 6200	Principles of Information Security and Privacy
ITIS 6342	Information Technology Project Management

UNC Charlotte

ITIS 6400	Principles of Human Computer Interaction
	*Information Security and Privacy Focus: (Select 3)**
ITIS 5221	Secure Programming and Penetration Testing
ITIS 5250	Computer Forensics
IS/CS 6010	Topics Course (only if topic applicable, and coordinator approved)
ITIS 6167	Network Security
ITIS 6210	Access Control and Security Architecture
ITIS 6220	Data Privacy
ITIS 6230	Information Infrastructure Protection
ITIS 6240	Applied Cryptography
ITIS 6320	Cloud Data Storage
ITIS 6362	Information Technology Ethics, Policy, and Security
ITIS 6420	Usable Security and Privacy
	Also possible, but less frequently offered
ITIS 5220	Vulnerability Assessment and System Assurance
ITIS 6140	Software Testing and Quality Assurance
ITIS 6150	Software Assurance

*http://sis.uncc.edu/academics/masters-programs/areas-concentration

Course Descriptions
Undergraduate:

Source: The University of North Carolina at Charlotte Undergraduate Catalog 2014-2015, http://catalog.uncc.edu/sites/catalog.uncc.edu/files/media/Undergraduate-Catalogs/2014-2015-UG-Catalog.pdf, November, 24, 2014.

ITCS 1203. Survey of Computing. (3) Cross-listed as ITIS 1203. Introductory course that explores the broad field of computing as it applies to daily life. Topics cover computers of all sizes from handheld devices to super computers; the role of software from operating systems to applications; the software development process; issues of security and privacy on the Internet and the World Wide Web; and possible fields of study within the broad field of information technology. (On demand)
ITCS 4131. Communication Network Design. (3) Prerequisites: ITCS 3166 or permission of department. Emphasis on the design and analysis of communication networks. Application, host, and network requirements analysis; data flow analysis, models and specifications; technology choices; Interconnection mechanisms; network management and security; physical network design; addressing and routing. (On demand)
ITCS 4146. Grid Computing. (3) Prerequisites: ITCS 1213 and ITCS 1213L. Grid computing software components, standards, web services, security mechanisms, schedulers and resource brokers, workflow editors, grid portals, grid computing applications. (Once every three semesters)
ITIS 1203. Survey of Computing. (3) Cross-listed as ITCS 1203. Introductory course that explores the broad field of computing as it applies to daily life. Topics cover

computers of all sizes from handheld devices to super computers; the role of software from operating systems to applications; the software development process; issues of security and privacy on the Internet and the World Wide Web; and possible fields of study within the broad field of information technology. (Fall, Spring)
ITIS 1210. Introduction to Web-Based Information Systems. (3) Introductory course in developing Web pages for both majors and non-majors. Topics include: an introduction to the mechanisms by which the Internet and the World Wide Web operate, general concepts related to Web-based information systems, the design and construction of Web infrastructure including authoring tools, domain registration, legal and ethical considerations, and basic Web security. (Fall, Spring) (Evenings)
ITIS 2300. Web-Based Application Development. (3) Prerequisite: Sophomore standing or permission of department. Basic concepts for developing interactive web based applications; HTML, client side scripting, server side scripting, user interface design considerations, information security and privacy considerations, system integration considerations. Students will be required to develop working prototypes of web-based applications. (Fall, Spring)
ITIS 3105. Server-Side Applications and Data Management. (3) Prerequisites: ITIS 2300 and ITCS 1213, or permission of department. This course covers principles that are important for implementing advanced Web-based applications. Emphasis will be placed on industrial and business applications which require robust and secure implementations. Server side scripting and processing techniques will be exercised in course projects. (Spring)
ITIS 3110. IT Infrastructure II: Design and Practice. (3) Prerequisites: ITIS 2110 and ITIS 2110L or permission of department. Corequisite: ITIS 3110L. The concepts for the design and implementation of robust IT infrastructures. Topics include: system hardening, secured access, penetration testing, file storage services, as well as advanced topics in design and configuration of network based services. Course grade includes the student's performance in ITIS 3110L. (Fall, Spring)
ITIS 3200. Introduction to Information Security and Privacy. (3) Prerequisite: ITCS 1213 or permission of department. This courses provides an introductory overview of key issues and solutions for information security and privacy. Topics include: security concepts and mechanisms; security technologies; authentication mechanisms; mandatory and discretionary controls; basic cryptography and its applications; intrusion detection and prevention; information systems assurance; anonymity and privacy issues for information systems.
ITIS 3300. Software Requirements and Project Management. (3) Prerequisite: ITIS 2300 or permission of department. Introduction to requirement engineering and project management methodologies. Topics include: requirements elicitation, specification, and validation; structural, informational, behavioral, security, privacy, and computer user interface requirements; scenario analysis; application of object oriented methodologies in requirements gathering; spiral development model; risk management models; software engineering maturity model; project planning and milestones; cost estimation; team organizations and behavior. Case studies will be used. (On demand)
ITIS 3320. Introduction to Software Testing and Assurance. (3) Prerequisites: ITIS 3200 and ITIS 3300 or permission of department. Methods of evaluating software for correctness, and reliability including code inspections, program proofs and testing methodologies. Formal and informal proofs of correctness. Code inspections and their

role in software verification. Unit and system testing techniques, testing tools and limitations of testing. Statistical resting, reliability models. (Fall, Spring) (Evenings)
ITIS 4220. Vulnerability Assessment and Systems Assurance. (3) Prerequisite: ITIS 3200 or permission of department. Methodologies, tools, and technologies that are important for vulnerability assessment and systems assurance. Topics include: ethical hacking techniques, vulnerability assessment, risk assessment/management, finding new exploits, discovering vulnerabilities, penetrating network perimeters, bypassing auditing systems, and assured administration of systems as well as evaluating systems assurance levels. Focus placed on: 1) understanding current penetration techniques for networks, operating systems, services and applications; 2) investigating mitigation and defense strategies; and 3) studying legal and ethical considerations. Based on case studies with a strong lab component. (Fall, Spring)
ITIS 4221. Secure Programming and Penetration Testing. (3) Prerequisite: ITIS 4166 or permission of department. Techniques for web application penetration testing, secure software development techniques for network based applications. Automated approaches such as static code analysis and application scanning are also discussed. (On demand)

Graduate:

Source: The University of North Carolina at Charlotte Graduate Catalog 2014-2015, http://catalog.uncc.edu/sites/catalog.uncc.edu/files/media/Graduate-Catalogs/2014-2015-GRAD-Catalog.pdf, November, 24, 2014.

MBAD 6204. Management of Information Security and Privacy. (3) Prerequisite: MBAD 5121 or equivalent. Managing key security and privacy challenges faced by IT managers. Examines computer network concepts, threat environments, security tools, methods, and controls for risk management and the development of IS security management and policy. Also examines various IS security and privacy standards and evaluation criteria. (On demand)
ITCS 5146. Grid Computing. (3) Prerequisite: Graduate standing or permission of instructor. Grid computing software components, standards, web services, security mechanisms, schedulers and resource brokers, workflow editors, grid portals, grid computing applications. (On demand)
ITCS 6144. Operating Systems Design. (3) Prerequisite: ITCS 6114 or permission of instructor. Introduction to features of a large-scale operating system with emphasis on resource-sharing environments. Computer system organization; resource management; multiprogramming; multiprocessing; file systems; virtual machine concepts; protection and efficiency. (On demand)
ITCS 6164. Design and Implementation of Online Management Information Systems. (3) Prerequisite: ITCS 6114 or permission of instructor. The fundamental concepts and philosophy of planning and implementing an online computer system. Characteristics of online systems; hardware requirements; modeling of online systems; performance measurement; language choice for online systems; organization techniques, security requirements; resource allocation. (On demand)
ITCS 8144. Operating Systems Design. (3) Prerequisite: ITCS 8114 or permission of instructor. Introduction to features of a large-scale operating system with emphasis on resource-sharing environments. Computer system organization; resource management;

multiprogramming; multiprocessing; file systems; virtual machine concepts; protection and efficiency. (On demand)

ITCS 8164. Design and Implementation of Online Management Information Systems. (3) Prerequisite: ITCS 8114 or permission of instructor. The fundamental concepts and philosophy of planning and implementing an online computer system. Characteristics of online systems; hardware requirements; modeling of online systems; performance measurement; language choice for online systems; organization techniques, security requirements; resource allocation. (On demand)

ITIS 5220. Vulnerability Assessment and System Assurance. (3) Cross-listed as HCIP 5220. Prerequisite: permission of department. Discusses methodologies, tools, and technologies that are important for vulnerability assessment and systems assurance. Topics covered include: ethical hacking techniques, vulnerability assessment, risk assessment/management, finding new exploits, discovering vulnerabilities, penetrating network perimeters, bypassing auditing systems, and assured administration of systems as well as evaluating systems assurance levels. Focus will be placed on 1) understanding current penetration techniques for networks, operating systems, services and applications; 2) investigating mitigation and defense strategies; and 3) studying legal and ethical considerations. The course is based on case studies with a strong lab component. (On demand)

ITIS 5221. Secure Programming and Penetration Testing. (3) Prerequisite: ITIS 4166 or ITIS 5166, or permission of department. Techniques for web application penetration testing, secure software development techniques for network based applications. Automated approaches such as static code analysis and application scanning are also discussed. (Fall, Spring)

ITIS 5250. Computer Forensics. (3) Cross-listed as HCIP 5250. Prerequisite: Enrollment in the MS in Information Technology program or permission of department. The identification, extraction, documentation, interpretation, and preservation of computer media for evidentiary purposes and/or root cause analysis. Topics include: techniques for discovering digital evidence; responding to electronic incidents; tracking communications through networks; understanding electronic media, crypto-literacy, data hiding, hostile code, and Windows™ and UNIX™ system forensics; and the role of forensics in the digital environment (On demand)

ITIS 6120. Applied Databases. (3) Cross-listed as HCIP 5160 and ITIS 8120. Prerequisite: Full graduate standing or permission of department. Identification of business database needs; requirements specification; relational database model; SQL; E-R modeling; database design, implementation, and verification; distributed databases; databases replication; object-oriented databases; data warehouses; OLAP; data mining; security of databases; vendor selection; DBMS product comparison; database project management; tools for database development, integration, and transaction control. (Fall) (Evening)

ITIS 6130. Software Requirements Engineering for Information Systems. (3) Prerequisite: Full graduate standing, or permission of department. Introduction to requirement engineering methodologies. Topics include: requirements elicitation, specification, and validation; structural, informational, behavioral, security, privacy, and computer user interface requirements; scenario analysis; application of object oriented methodologies in requirements gathering; spiral development models; risk management models; software engineering maturity model. (On demand)

ITIS 6150. Software Assurance. (3) Cross-listed as ITIS 8150. Prerequisite: ITCS 6112, ITCS 8112, ITIS 5221, ITIS 6112, ITIS 8112, or permission of department. An introduction to software assurance education and research. Topics include: the security of software across the development life cycle that addresses trustworthiness, predictable execution and conformance. Various aspects of secure software requirements, design, construction, verification, and validation, process and engineering management are focused on as they relate to secure software development. Students gain hands-on experience in various techniques and tools as part of a semester long project in addition to other assignments. (On demand)
ITIS 6164. Online-Info Systems. (3) Prerequisites: ITCS 6114 or permission of department. The fundamental concepts and philosophy of planning and implementing an online computer system. Characteristics of online systems; hardware requirements; modeling of online systems; performance measurement; language choice for online systems; organization techniques, security requirements; resource allocation. (On demand)
ITIS 6167. Network Security. (3) Cross-listed as HCIP 6167. Prerequisite: ITIS 6200 or equivalent. Examines the issues related to network security. Topics include: network security background and motivation, network centric threats, network authentication and identification, network security protocols, firewall, IDS, security in wireless environments, email security, instant message security, network application security, and network based storage security. There are heavy lab based components in this course. (Fall) (Evening)
ITIS 6177. System Integration. (3) Pre- or corequisite: ITIS 5166 or equivalent, or permission of department. Examines the issues related to system integration. Topics include: data integration, business process integration, integration architecture, middleware, system security, and system management. (Fall) (Evening)
ITIS 6200. Principles of Information Security and Privacy. (3) Cross-listed as HCIP 6200 and ITIS 8200. Prerequisite: Permission of department. Topics include: security concepts and mechanisms; security technologies; authentication mechanisms; mandatory and discretionary controls; basic cryptography and its applications; database security, intrusion detection and prevention; assurance requirement, assurance class, evaluation methods and assurance maintenance; anonymity and privacy issues for information systems. (Fall, Spring) (Evening)
ITIS 6201. Computer Security and Privacy. (3) Crosslisted as HCIP 6201. Prerequisite: full graduate standing or permission of department. Topics include: threats to computer and communication systems and privacy concepts; basic security defense techniques; web and network security issues; portable device security; operating systems security issues; email security; and security issues in major business applications. (Fall, Evenings)
ITIS 6210. Access Control and Security Architecture. (3) Cross-listed as HCIP 6210. Prerequisite: ITIS 6200. Discusses objectives, formal models, and mechanisms for access control; and access control on commercial off-the-shelf (COTS) systems. Examines the issues related to security architectures and technologies for authorization. Topics include: cryptographic infrastructure, distributed systems security architectures, database systems security architectures, Internet security architectures, network security architectures and e-commerce security architectures. (Spring) (Evening)

ITIS 6220. Data Privacy. (3) Pre- or corequisite: ITIS 6200, full graduate standing, or permission of department. Topics include: privacy concepts, policies, and mechanisms; identity, anonymity, and confidentiality; private data analysis and database sanitization; privacy-preserving data mining techniques including k-anonymity, randomization, and secure function evaluation; privacy issues in social networks, RFID, and healthcare applications. (Fall) (Evenings)
ITIS 6230. Information Infrastructure Protection. (3) Cross-listed as HCIP 6230 and ITIS 8230. Prerequisite: ITIS 6200. Methodologies, tools, and technologies that are important for protecting information systems and information infrastructures. Topics include: techniques, processes and methodologies for information security risk assessment and management, systems modeling and analysis using logic programming and formal methods, tools and technologies for critical infrastructure protection, methodologies for continuous operation and recovery from disasters. (On demand)
ITIS 6240. Applied Cryptography. (3) Cross-listed as HCIP 6240. Prerequisite: Full graduate standing or permission of department. Provides students with an understanding of modern cryptographic techniques, algorithms and protocols that are of fundamental importance to the design and implementation of security critical applications. Covers not only standard cryptographic techniques, but also exposes students to the latest advances in applied cryptography. Topics include: secret and public key ciphers, stream ciphers, one-way hashing algorithms, authentication and identification, digital signatures, key establishment and management, secret sharing and data recovery, public key infrastructures, and efficient implementation. (On demand)
ITIS 6320. Cloud Data Storage. (3) Cross-listed as ITIS 8320. Prerequisite: Full graduate standing or permission of department. The design and implementation of cloud storage and big data systems and the architecture and characteristics of components on which cloud storage systems are built. Topics include: storage device hardware, file systems, mirroring and RAID, array coding techniques, storage area networks (SAN), network-attached storage (NAS), cloud storage and big data, DB in clouds, relational storage models, key value stores and other No-SQL mechanisms, data consistency and availability in the cloud, cloud data privacy and security. (On demand)
ITIS 6362. Information Technology Ethics, Policy, and Security. (3) Prerequisite: Permission of department Management of Information technology involves understanding the broader issues of ethics, policy and security. The growth in Internet usage and E-commerce require IT professionals to consider issues pertaining to data protection, regulation, and appropriate use and dissemination of information. The course is designed to be team-taught by professionals in the field. (Fall)
ITIS 6420. Usable Security and Privacy. (3) Crosslisted as ITIS 8420. Prerequisite: ITIS 6200. Much of the work into security and privacy solutions ignore a critical element: the human who must interact with those solutions. In this course, we investigate privacy and security from a user-centered point of view. How do people think about privacy and security? How do they interact with current applications and solutions? What should be considered in designing user-friendly security systems? This course introduces students to a variety of usability and user interface issues related to privacy and security as well as examine potential designs and solutions. (On demand)
ITIS 8120. Applied Databases. (3) Cross-listed as HCIP 5160 and ITIS 6120.
ITIS 8130. Software Requirements Engineering for Information Systems. (3) Prerequisite: Full graduate standing, or permission of department. Introduction to

requirement engineering methodologies. Topics include: requirements elicitation, specification, and validation; structural, informational, behavioral, security, privacy, and computer user interface requirements; scenario analysis; application of object oriented methodologies in requirements gathering; spiral development models; risk management models; software engineering maturity model. (On demand)

ITIS 8150. Software Assurance. (3) Cross-listed as ITIS 6150.

ITIS 8164. Online-Info Systems. (3) Prerequisites: ITCS 6114 or permission of department. The fundamental concepts and philosophy of planning and implementing an online computer system. Characteristics of online systems; hardware requirements; modeling of online systems; performance measurement; language choice for online systems; organization techniques, security requirements; resource allocation. (On demand)

ITIS 8167. Network and Information Security. (3) Prerequisite: ITCS 6166 or equivalent. Examines the issues related network and information security. Topics include: concepts, security attacks and risks, security architectures, security policy management, security mechanisms, cryptographic algorithms, security standards, security system interoperation and case studies of the current major security systems. (Fall) (Evening)

ITIS 8177. System Integration. (3) Prerequisite: Ph.D. student standing, or permission of the department. Examines the issues related to system integration. Topics include: data integration, business process integration, integration architecture, middleware, system security, and system management. (Fall) (Evening)

ITIS 8200. Principles of Information Security and Privacy. (3) Cross-listed as ITIS 6200 and HCIP 6200.

ITIS 8210. Access Control and Security Architecture. (3) Prerequisite: ITIS 8200. Discusses objectives, formal models, and mechanisms for access control; and access control on commercial off-the-shelf (COTS) systems. Examines the issues related to security architectures and technologies for authorization. Topics include: cryptographic infrastructure, distributed systems security architectures, Internet security architectures, network security architectures and e-commerce security architectures. (Spring) (Evening)

ITIS 8230. Information Infrastructure Protection. (3) Cross-listed as HCIP 6230 and ITIS 6230.

ITIS 8240. Applied Cryptography. (3) Prerequisite: Graduate standing or permission of department. Provides students with an understanding of modern cryptographic techniques, algorithms and protocols that are of fundamental importance to the design and implementation of security critical applications. The course not only covers standard cryptographic techniques, but also exposes students to the latest advances in applied cryptography. Topics include: secret and public key ciphers, stream ciphers, one way hashing algorithms, authentication and identification, digital signatures, key establishment and management, secret sharing and data recovery, public key infrastructures, and efficient implementation. (On demand)

ITIS 8320. Cloud Data Storage. (3) Cross-listed as ITIS 6320.

ITIS 8362. Information Technology Ethics, Policy, and Security. (3) Prerequisite: HADM 6152, MBAD 6121, or MPAD 6120. Management of information technology involves understanding the broader issues of ethics, Policy and Security. The growth in Internet usage and E-commerce require IT professionals to consider issues pertaining to data protection, regulation, and appropriate use and dissemination of information. The course is designed to be team-taught by professionals in the field. (Fall)

ITIS 8420. Usable Security and Privacy. (3) Crosslisted as ITIS 6420.

UNC Greensboro

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC Greensboro

	BS in Computer Science
	http://uncg.smartcatalogiq.com/en/2014-2015/Undergraduate-Bulletin/Academic-Departments-Programs-Courses/Computer-Science-Department/Computer-Science-Major-BS
CSC 130	Introduction to Computer Science
CSC 230	Elementary Data Structures and Algorithms
CSC 250	Foundations of Computer Science I
CSC 261	Computer Organization and Assembly Language
CSC 330	Advanced Data Structures
CSC 339	Concepts of Programming Languages
CSC 340	Software Engineering
CSC 350	Foundations of Computer Science II
CSC 490	Senior Project
CSC 553	Theory of Computation
CSC 562	Principles of Operating Systems
	MS in Computer Science
	http://uncg.smartcatalogiq.com/en/2013-2014/Graduate-Bulletin/Departmental-and-Program-Listings/Computer-Science-Department/Computer-Science-MS
CSC 640	Software Engineering
CSC 656	Foundations of Computer Science
	Security related courses available:
	http://uncg.smartcatalogiq.com/en/2013-2014/Graduate-Bulletin/Courses/CSC-Computer-Science
CSC 580	Cryptography and Security in Computing
CSC 583	Firewall Architecture and Computer Security
CSC 680	Advanced Topics in Computer Security

Course Descriptions
Undergraduate:

Source: The University of North Carolina at Greensboro Undergraduate Bulletin, Catalog Issue for the Year 2014-15, Vol.102, http://uncg.smartcatalogiq.com/en/2014-2015/Undergraduate-Bulletin, November, 24, 2014.

CSC 562 Principles of Operating Systems (3:3) Techniques and strategies used in operating system design and implementation: managing processes, input/output, memory, scheduling, file systems, and protection. Prerequisites: Pr. grades of at least C (2.0) in CSC 261 and CSC 340 or permission of instructor. Notes: Successful completion of CSC 561 helpful.
CSC 580 Cryptography and Security in Computing (3:3) Modern development of cryptography and secure encryption protocols. Program security and viruses. Operating system protection. Network and distributed system security. Database security. Administering security. Prerequisites: Grades of at least C (2.0) in CSC 330 and one of CSC 471, CSC 561, CSC 562, or CSC 567, or permission of instructor.
CSC 583 Firewall Architecture and Computer Security (3:3) Firewall hardware and software technologies. Architectures, protocols and their applications. Prerequisites: Grades of at least C (2.0) in CSC 567 and CSC 580, or permission of instructor.
ISM 324 Secure Networked Systems (3:3) Networking and telecommunication concepts are described. Technical and organizational activities for securing distributed systems are presented. System security and information assurance methodologies, procedures and best practices are studied. Prerequisites: Restricted to IS majors and minors only.

Graduate:

Source: The University of North Carolina at Greensboro Graduate School Bulletin 2014-15, http://uncg.smartcatalogiq.com/en/2014-2015/Graduate-Bulletin, November, 24, 2014.

CSC 680 Advanced Topics in Computer Security (3:3) Topics in cryptography and computer security, including cryptographic protocols, Web server security, Java security, security in the healthcare domain, and experimental quantum cryptography. Prerequisites: CSC 339 and CSC 580
ISM 676 Information Security and Privacy (3:3) Study of the technical, managerial, and organization issues in systems security, including systems security models, analysis of business process and technology for systems security, and information assurance. Prerequisites: ISM 673 or permission of MSITM program director; admission to a UNCG graduate program

UNC Pembroke

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC Pembroke	
	BS in Computer Science
	http://www.uncp.edu/sites/default/files/Images_Docs/Academics/Colleges_Schools_and_Departments/Departments/Mathematics_and_Computer_Science/math_cs.pdf
CSC 1750	Introduction to Algorithms
CSC 1760	Introduction to Programming

UNC Pembroke

CSC 1850	Object-Oriented Programming
CSC 2150	Discrete Structures
CSC 2250	Fundamentals of Computer Systems
CSC 2260	Operating Systems and Networking
CSC 2650	Digital Logic
CSC 2850	Data Structures
CSC 2920	Software Development and Progessional Practices
CSC 3750	Programming Languages
CSC 4900	Advanced Software Project
	Electives with security:
CSC 3350	Network Management (includes security management)
CSC 3380	Programming for the World Wide Web (includes security)
CSC 4020	Introduction to Computer and Network Security
CSC 4350	Operating Systems (includes OS security)

BS in Information Technology

http://www.uncp.edu/sites/default/files/Images_Docs/Academics/Colleges_Schools_and_Departments/Departments/Mathematics_and_Computer_Science/math_cs.pdf

CSC 1300	WWW Information
CSC 1750	Introduction to Algorithms
CSC 1760	Introduction to Programming
CSC 1850	Object-Oriented Programming
CSC 1900	JAVA Programming
CSC 2050	Microcomputer Programming
CSC 2150	Discrete Structures
CSC 2250	Fundamentals of Computer Systems
CSC 2260	Operating Systems and Networking
CSC 2850	Data Structures
CSC 2920	Software Development and Progessional Practices
ITC 2060	Human-Computer Interaction
ITC 2080	Introduction to System Administration and Shell Scripting (includes security)
ITC 4940	Capstone Project in Information Technology
	Electives with security:
ITC 3250	System Administration (includes security)

Course Descriptions

Source: University of North Carolina at Pembroke 2013-14 Catalog, main: http://www2.uncp.edu/catalog/index.htm, computer science: http://www2.uncp.edu/catalog/html/math_cs.htm, November, 24, 2014.

CSC 3350. Network Management Presents the five conceptual areas of network management as defined by the International Organization for Standardization (ISO):

performance management, configuration management, accounting management, fault management, and security management. This course covers networking technologies such as Ethernet, bridges, and switches. It addresses network management architectures and protocols to lay the foundation for SNMP management, broadband management, and TNM. Some network management applications, tools to monitor network parameters, and network management systems to manage networks are included. Credit, 3 semester hours. PREREQ: CSC 1850, 2260.

CSC 3380. Programming for the World Wide Web In this course, students will gain experience with the programming techniques, technologies, and issues associated with the Internet. Topics include network programming with sockets, TCP/IP, the HTTP protocol, web-servers, browsers, security, authentication, distributed objects, and client-server computing. This is a project-oriented course in which students will be expected to develop software using a variety of programming languages. Credit, 3 semester hours. PREREQ: CSC 1850 or 1900 and CSC 2260.

CSC 4020. Introduction to Computer and Network Security This course provides an introduction to the theory and application of security in computer and network environments. Students will develop the skills necessary to address the security needs of enterprise and personal environments. The course covers cryptography, authentication, access control, security in operating systems, network security, and denial-of-service. Course projects will focus on the application of security tools to real world problems. Credit, 3 semester hours. PREREQ: CSC 2260.

CSC 4350. Operating Systems This course covers the basic functions of an operating system. Topics covered include process management and scheduling, memory management and paging algorithms, I/O management, file management, deadlock, and operating system security. Credit, 3 semester hours. PREREQ: MAT 2220.

ITC 2080. Introduction to System Administration and Shell Scripting
This course provides students with tools and techniques used in administration of computing systems. Unix/Linux and Windows will be among systems studied. Topics covered include file systems, files security, editors, file processing, shell scripting programming, and system utilities. Students will learn system installation, halting and booting the system, file and directory permission structures, print and disk quotas, device configuration and management, and user account administration. Students also explore tools and techniques used to script common tasks in operating system environments. Students will gain experience in writing scripts in Unix/Linux and Windows operating systems. Credit, 3 semester hours. PREREQ: CSC 1750 and 1760 or CSC 2050.

ITC 3250. System Administration This course introduces students to the essential knowledge and skills that system administrators possess. This course reviews the basic operating system concepts, including process and thread management, memory management, file systems, and input/output systems as well as various administration services. It covers system administration topics focuses on integrating systems and user support services. Topics explored include security, user and group administration, system update and maintenance, backup and restore technologies, as mass storage technologies. Credit, 3 semester hours. PREREQ: ITC 2080 and 2700.

UNC Wilmington

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

UNC Wilmington

BS in Computer Science

http://uncw.edu/csc/undergrad/checklists.html

CSC 131	Introduction to Computer Science
CSC 133	Discrete Mathematical Structures
CSC 231	Introduction to Data Structures
CSC 242	Computer Organization
CSC 331	Object-Oriented Programming and Design
CSC 340	Scientific Computing
CSC 342	Operating Systems
CSC 360	Formal Languages and Computability
CSC 380	Design and Analysis of Algorithms
CSC 385	Professional and Ethical Issues in Computer Science (privacy & security)
CSC 434	Programming Languages
CSC 450	Software Engineering
CSC 455	Database Design and Implementation
	Electives with security:
CSC 105	Introduction to Computing and Computer Applications (sec considerations)
CSC 446	Grid Computing (security mechanisms)

BS in Information Technology

http://uncw.edu/bsit/current.html

CIT 110	Introduction to Information Technology
CIT 204	Digital Media (security & encryption)
CIT 225	Platform Technologies
CIT 310	Web Page Development
CIT 324	Network Security Management (sec technologies, methodologies & practice)
CIT 352	Systems Administration
CIT 410	Web Application Development (web site security)
CIT 411	Information Systems Analysis
CIT 425	Human Computer Interfaces
CIT 480	IT Resource Planning and Management
CIT 213	Introduction to Databases: Techniques and Technologies (DB security)
CIT 320	Network Fundamentals
CSC 131	Introduction to Computer Science
CSC 385	Professional and Ethical Issues in Computer Science
MIS 315	Management of Database Systems
MIS 316	Business Application Development

Course Descriptions
Undergraduate:

Source: University of North Carolina Wilmington 2014-15 Undergraduate Catalogue, http://catalogue.uncw.edu/content.php?catoid=17&navoid=1080, November, 24, 2014.

CSC 105 - Introduction to Computing and Computer Applications Credits: 3
Basic computer concepts for non-CSC majors. Elements of computing systems and organization; computer communications including the Internet; applications such as word processing; spreadsheets; data base management; and the rudiments of programming in a current programming language. Social and technical issues including legal, ethical, and security considerations. Students who have passed MIS 105 may not enroll in CSC 105. Partially satisfies University Studies IV: Building Competencies/Information Literacy.
CSC 385 - Professional and Ethical Issues in Computer Science Credits: 3
Prerequisite: ENG 101 or equivalent and junior or senior standing in computer science or information technology. Ethical and professional issues arising from the impact of computer science and related technologies on society. Topics include ethical issues, obligations of professional practice, privacy and security, intellectual property, work and health issues, and the impact of emerging technologies. Students will give both oral and written presentations and participate in the discussion of case studies. Partially satisfies University Studies IV: Building Competencies/Writing Intensive. Partially satisfies University Studies IV: Building Competencies/Information Literacy.
CSC 446 - Grid Computing Credits: 3 (CSC 546) Prerequisites: CSC 344 or CSC 231. Grid computing software components, standards, web services, security mechanisms, schedulers, resource brokers, workflow editors, grid portals, and grid computing applications.
CIT 204 - Digital Media Credits: 3 Prerequisite: CIT 110 or equivalent. Introduction to technologies of the Internet. Web-page design; graphics and animation; client/server concepts; collaborative computing and group work; network publishing; security and encryption; audio, video, and image compression; ethical issues and privacy; e-commerce; client-side Web programming; and dynamic Web-page generation.
CIT 213 - Introduction to Databases: Techniques and Technologies Credits: 3
Prerequisite: CIT 110. Fundamental concepts of database management systems, including advantages of using database management systems, data modeling, relational database design, query-building, security, privacy and ethical issues, and introductions to Web-based processing, Big Data concepts, and non-relational models.
CIT 324 - Information Security Management Credits: 3 (MIS 324) Prerequisite: CIT 110 or MIS 213. Current standards of due care and best business practices in Information Security. Includes examination of security technologies, methodologies, and practices. Focus is on evaluation and selection of optimal security posture. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning, and security policy formulation and implementation.
CIT 410 - Web Application Development Credits: 3 Prerequisite: CIT 310. A structured approach to building and maintaining dynamic and interactive Web sites. With an emphasis on application, design and development, students will gain a thorough

understanding of server-side scripting, form validation, and Web-site security while advancing their understanding of database design principles and SQL. Students will create a database-driven Website.

MIS 317 - Technology of E-Business Credits: 3 Prerequisite: MKT 441 and admission to Cameron School of Business. A study of current technologies impacting a firm's ability to create and maintain an e-business presence. The course has two major topic thrusts. The first focus is the hardware necessary to support e-business, including telecommunication concepts, networks, wireless Web, firewalls, secure servers, and Internet protocols and standards. The second focus is the current advances in Web languages to enable transactions to be more transparent between companies. (This course does not satisfy any requirements or electives for students pursuing an IS option.)

MIS 324 - Information Security and Assurance Credits: 3 (CIT 324) Prerequisite: Junior Standing and (MIS 213 or CSC 121). Examination of current standards of due care and best business practices in Information Security. Focus is on evaluation and selection of optimal security posture. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning and security policy formulation and implementation.

Western Carolina University

Programs

DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

Western Carolina University

BS in Computer Science

http://catalog.wcu.edu/preview_program.php?catoid=33&poid=4185&hl=computer+Science

CS 220	Social and Ethical Issues of Computing Credits: 1
CS 263	Software Engineering Credits: 3
CS 350	Computer Organization Credits: 3
CS 351	Data Structures and Algorithms Credits: 3
CS 352	Organization of Programming Languages Credits: 3
CS 363	Software Development Credits: 3
CS 370	Operating Systems Credits: 3
CS 453	Database Systems Credits: 3
CS 465	Computer Networking Credits: 3
CS 495	Capstone I Credits: 2
CS 496	Capstone II Credits: 2
	Electives with security:
CS 210	Internet Security and Ethics
CS 430	Information Security I
CS 431	Information Security II

Course Descriptions

Source: Western Carolina University Undergraduate Catalog 2014-2015, http://catalog.wcu.edu/content.php?catoid=33&navoid=902, November, 24, 2014.

CS 210 - Internet Security and Ethics Credits: 3 Types of Internet-based attacks, counter-measures, and the ethical issues that arise. Hacking, viruses, worms, spam, identity theft, cryptography, intellectual property, software piracy. (P4)
CS 430 - Information Security I Credits: 3 Cryptography, authentication, integrity, and non-repudiation; trusted intermediaries, key distribution, and certification; access control and firewalls; attacks and counter-measures. Prerequisites & Notes PREQ: 151. COREQ: 465.
CS 431 - Information Security II Credits: 3 Software reverse engineering, program security, operating systems and database systems security, security administration and audits (prevention, detection, and response), standards for information assurance. Prerequisites & Notes PREQ: 430. COREQ: 370.

Winston-Salem State University

Programs
DISLOSURE: Only core/required classes offered for each program are listed. Refer to each respective institution for program details. Data current as of November, 2014.

Winston-Salem State University

BS in Computer Science
http://catalog.wssu.edu/preview_program.php?catoid=13&poid=779&returnto=603

CSC 1105	Compter Science Colloquium
CSC 2131	Professional Development Seminar (Enroll at least once per year)
CSC 2310	Introduction to Computer Software Systems
CSC 2320	Introduction to Computer Hardware Organization
CSC 2331	Data Structures
	Information Security Option:
CSC 3325	Introduction to Information Security
CSC 4330	Introduction to Cryptography
CSC 4360	Hardware and Media Security
CSC 4370	Web-based Database Management Systems
CSC 4001	Special Topics In Computer Science
CSC 3130	Computer Science Internship
CSC 3691	Computer Science Co-Op

CSC 33xx, CSC 43xx (Approved by Department Chairperson)

BS in Information Technology
http://catalog.wssu.edu/preview_program.php?catoid=13&poid=802&returnto=603

CSC 1105	Computer Science Colloquium
CSC 1307	Introduction to Computer Technology

Winston-Salem State University

CSC 1308	Introduction to Programming
CSC 2131	Professional Development Seminar (Enroll at least once per year)
CSC 2310	Introduction to Computer Software Systems
CSC 2320	Introduction to Computer Hardware Systems
	Advanced Courses (42 semester hours)
CSC 3321	Operating Systems
CSC 3322	Computer Architecture
CSC 3323	System Administration I
CSC 3325	Introduction to Information Security
CSC 3332	Fundamentals of Information Systems
CSC 3351	Data Communications
CSC 3355	Principles of Database Management
CSC 4323	System Administration II
CSC 4350	Software Engineering
CSC 4355	Database Management Design
CSC 4356	Web Programming
CSC 4388	Systems Design and Development
CSC 4389	Computer Communications Networks
CSC 4391	Computer Science Co-op OR CSC 4392 Computer Technology Seminar

Course Descriptions

Source: Winston-Salem State Univeristy Undergraduate Catalog 2013-2015, http://catalog.wssu.edu/content.php?catoid=13&navoid=607, November, 24, 2014.

CSC 1307 - Introduction To Computer Technology Credits: 3 hrs Topics include the history and overview of computer hardware and software. It provides more advanced exposure to commonly used software, including database programming, spreadsheet functions, computer graphics applications design, desk-top publishing, ethics, security, and other applications. Laboratory work required. Prerequisite(s): Enrollment in the Information Technology Major.

CSC 3323 - System Administration I Credits: 3 hrs This course prepares students to administer a computer system. Intensive laboratory experiences develop skills in operating system administration, software configuration, fundamentals of security, and procedures in a networked environment. Prerequisite(s): CSC 3321.

CSC 3325 - Fundamentals of Information Security Credits: 3 hrs. This course provides an essential introduction to the basics of information and computer security. Topics include information security goals and principles, access control, malicious software, basic applied cryptography, basic network security, and privacy issues in computing systems. Prerequisite(s): CSC 2310.

CSC 3332 - Fundamentals of Internet Systems Credits: 3 hrs This course addresses the structure and functionality of the Internet and software that exploits it. Topics include mark up languages, Web tools, static dynamic and active Web pages, multimedia in Web applications, communication protocols, client-server computing, scripting, group

communication support, e-commerce, and security. Topics also include systems for organizing and coordinating work at different sites that exploit the Internet, and architectures to exploit the distributed computational power offered by the Internet. Prerequisite(s): CSC 2184.
CSC 3355 - Principles of Database Management Credits: 3 hrs This course covers concepts of logical and physical data structures, data security, and accuracy. It includes an overview of basic approaches to database organization and implementation and hands-on interaction with at least one hierarchical, network, or relational model database. Prerequisite(s): CSC 2320.
CSC 4323 - System Administration II Credits: 3 hrs A continuation of CSC 3323 – System Administration I, this course provides more comprehensive exposure to PC operating system administration, client-server administration, network administration, UNIX/Linux administration, and system security. Prerequisite(s): CSC 3323.
CSC 4330 - Introduction to Cryptography Credits: 3 hrs. This course provides a thorough background in cryptography. It will cover the history of cryptography, the mathematics which underlies major cryptographic schemes, basic cryptographic primitives, advanced cryptographic primitives and applied cryptography. Prerequisite(s): MAT 2337 or Permission of the Department Chairperson.
CSC 4360 - Hardware and Media Security Credits: 3 hrs. This course provides a survey of security topics related to hardware security and digital media security. It covers aspects of how computer hardware is designed or modified to prevent hacking, both for desktop computers and also for digital video and video gaming systems. It also covers security and privacy issues in low-power computer settings such as smart cards and RFID. Prerequisite(s): CSC 3322, CSC 3325 and MAT 2337.
CSC 4370 - Web-based Database Credits: 3 hrs. This course focuses on the fundamental concepts and technologies involved in the development of database driven web applications. Topics include integrating databases into the Web environment, internet applications with database interactions, transaction management, web database security, semi structured data management and XML. Prerequisite(s): 3355.

Appendix E

University of North Carolina System to ACM Guideline Knowledge Area Maps

Table 28- Computer Science classes to ACM CS IAS Guideline Map

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
Appalachian State University	BS				1	1	3	45%
		CS 3430	R	IAS/Defensive Programming				
		CS 3760	E	IAS/Platform Security				
		CS 3770	E	IAS/Cryptography				
		CS 4435	E	IAS/Web Security				
		CS 4520	E	IAS/Platform Security				
Appalachian State University	MS				0	0	1	9%
		CS 5520	R	IAS/Platform Security				
East Carolina University	BA				2	1	1	36%
		CSCI 4000	R	IAS/Foundational Concepts in Security				
		CSCI 4300	R	IAS/Defensive Programming & IAS Secure Software Engineering				
		CSCI 4540	E	IAS/Network Security				
East Carolina University	MS				0	0	1	9%
		SENG 6247	E	IAS/Secure Software Engineering				
East Carolina University	BS				2	1	1	36%
		CSCI 4000	R	IAS/Foundational Concepts in Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		CSCI 4300	E	IAS/Defensive Programming & IAS Secure Software Engineering				
		CSCI 4540	E	IAS/Network Security				
Elizabeth City State University	BS				1	1	1	27%
		CSC 260	R	IAS/Foundational Concepts in Security				
		CSC 410	R	IAS/Network Security				
		BMIS 410	R	IAS/Network Security				
		CSC 420	E	IAS/Platform Security				
Fayetteville State University	BS				1	1	1	27%
		CSC 403	R	IAS/Foundational Concepts in Security				
		CSC 490	R	IAS/Foundational Concepts in Security				
		CSC 323	E	IAS/Defensive Programming				
		CSC 380	E	IAS/Network Security				
NC A&T State University	BS				2	1	3	55%
		COMP 450	R	IAS/Platform Security				
		COMP 476	R	IAS/Network Security				
		COMP 120	E	IAS/Foundational Concepts in Security				
		COMP 170	E	IAS/Web Security				
		COMP 320	E	IAS/Foundational Concepts in Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		COMP 321	E	IAS/Principles of Secure Design				
		COMP 420	E	IAS/Network Security				
		COMP 421	E	IAS/Security Policy and Governance				
NC A&T State University	PhD				3	2	4	82%
		COMP 821	R	IAS/Platform Security				
		COMP 823	R	IAS/Threats and Attacks				
		COMP 620	E	IAS/Foundational Concepts in Security, IAS/Principles of Secure Design, IAS/Security Policy and Governance				
		COMP 621	E	IAS/Web Security				
		COMP 627	E	IAS/Network Security				
		COMP 722	E	IAS/Web Security				
		COMP 723	E	IAS/Threats and Attacks				
		COMP 724	E	IAS/Platform Security				
		COMP 725	E	IAS/Principles of Secure Design & IAS/Defensive Programming				
		COMP 726	E	IAS/Network Security				
		COMP 727	E	IAS/Secure Software Engineering				
		COMP 750	E	IAS/Network Security				
		COMP 755	E	IAS/Platform Security				
		COMP 829	E	IAS/Secure Software Engineering				
		COMP 875	E	IAS/Platform Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		COMP 876	E	IAS/Platform Security				
NC A&T State University	MS				3	2	4	82%
		COMP 620	R	IAS/Foundational Concepts in Security, IAS/Principles of Secure Design, IAS/Security Policy and Governance				
		COMP 621	R	IAS/Web Security				
		COMP 726	R	IAS/Network Security				
		COMP 627	E	IAS/Network Security				
		COMP 722	E	IAS/Web Security				
		COMP 723	E	IAS/Threats and Attacks				
		COMP 724	E	IAS/Platform Security				
		COMP 725	E	IAS/Principles of Secure Design & IAS/Defensive Programming				
		COMP 727	E	IAS/Secure Software Engineering				
		COMP 750	E	IAS/Network Security				
		COMP 755	E	IAS/Platform Security				
NC State University	M				1	1	3	45%
		CSC 540	R	IAS/Defensive Programming				
		CSC 570	R	IAS/Network Security				
		CSC 513	E	IAS/Web Security				
		CSC 515	E	IAS/Defensive Programming & IAS/Secure Software Engineering				
		CSC 522	E	IAS/Defensive Programming				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		CSC 547	E	IAS/Platform Security				
		CSC 574	E	IAS/Network Security				
		CSC 575	E	IAS/Network Security				
NC State University	BS				3	1	2	55%
		CSC 246	R	IAS/Platform Security				
		CSC 200	E	IAS/Foundational Concepts in Security				
		CSC 340	E	IAS/Defensive Programming				
		CSC 405	E	IAS/Foundational Concepts in Security & IAS/Principles of Secure Design				
		CSC 413	E	IAS/Web Security				
		CSC 422	E	IAS/Defensive Programming				
		CSC 440	E	IAS/Defensive Programming				
		CSC 453	E	IAS/Network Security				
		CSC 474	E	IAS/Network Security				
NC State University	PhD				1	2	4	64%
		CSC 540	R	IAS/Defensive Programming				
		CSC 570	R	IAS/Network Security				
		CSC 513	E	IAS/Web Security				
		CSC 515	E	IAS/Defensive Programming & IAS/Secure Software Engineering				
		CSC 522	E	IAS/Defensive Programming				
		CSC 547	E	IAS/Platform Security				
		CSC 574	E	IAS/Network Security				
		CSC 575	E	IAS/Network Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		CSC 705	E	IAS/Platform Security				
		CSC 712	E	IAS/Secure Software Engineering				
		CSC 743	E	IAS/Secure Policy and Governance				
		CSC 774	E	IAS/Network Security & IAS/Threats and Attacks				
NC State University	MS				1	2	3	55%
		CSC 540	R	IAS/Defensive Programming				
		CSC 570	R	IAS/Network Security				
		CSC 513	E	IAS/Web Security				
		CSC 515	E	IAS/Defensive Programming & IAS/Secure Software Engineering				
		CSC 522	E	IAS/Defensive Programming				
		CSC 547	E	IAS/Platform Security				
		CSC 574	E	IAS/Network Security				
		CSC 575	E	IAS/Network Security				
UNC Asheville	BS				0	0	2	18%
		CSCI 331	R	IAS/Platform Security				
		CSCI 444	E	IAS/Web Security				
UNC-Chapel Hill	PhD				0	0	0	0%
UNC-Chapel Hill	BA				1	2	0	27%
		COMP 380	E	IAS/Foundational Concepts in Security				
		COMP 382	E	IAS/Foundational Concepts in Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		COMP 535	E	IAS/Foundational Concepts in Security, IAS/Cryptography, IAS/Network Security				
UNC-Chapel Hill	BS				1	2	0	27%
		COMP 380	E	IAS/Foundational Concepts in Security				
		COMP 382	E	IAS/Foundational Concepts in Security				
		COMP 535	E	IAS/Foundational Concepts in Security, IAS/Cryptography, IAS/Network Security				
UNC-Chapel Hill	MS				1	1	1	27%
		COMP 721	E	IAS/Defensive Programming				
		COMP 722	E	IAS/Secure Software Engineering				
		COMP 734	E	IAS/Network Security				
UNC Charlotte	MS				3	3	4	91%
		ITIS 6200	R	IAS/Foundational Concepts in Security, IAS/Principles of Secure Design, IAS/Security Policy and Governance				
		ITCS 5146	E	IAS/Network Security				
		ITCS 6144	E	IAS/Platform Security				
		ITCS 6164	E	IAS/Web Security				
		ITIS 5220	E	IAS/Threats and Attacks				
		ITIS 5221	E	IAS/Threats and Attacks, IAS/Principles of Secure Design				
		ITIS 6120	E	IAS/Defensive Programming				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
		ITIS 6130	E	IAS/Secure Software Engineering				
		ITIS 6150	E	IAS/Defensive Programming				
		ITIS 6164	E	IAS/Web Security				
		ITIS 6167	E	IAS/Network Security				
		ITIS 6177	E	IAS/Platform Security				
		ITIS 6201	E	IAS/Foundational Concepts in Security				
		ITIS 6210	E	IAS/Web Security				
		ITIS 6230	E	IAS/Security Policy and Governance				
		ITIS 6240	E	IAS/Cryptography				
		ITIS 6320	E	IAS/Platform Security				
		ITIS 6362	E	IAS/Foundational Concepts in Security, IAS/Security Policy and Governance				
		ITIS 6420	E	IAS/Security Policy and Governance				
UNC Charlotte	BA				1	1	0	18%
		ITCS 1203	E	IAS/Foundational Concepts in Security				
		ITCS 4131	E	IAS/Network Security				
		ITCS 4146	E	IAS/Network Security				
UNC Charlotte	BS				2	1	1	36%
		ITCS 4146	R	IAS/Network Security				
		ITIS 3200	R	IAS/Foundational Concepts in Security, IAS/Principles of				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
				Secure Design, IAS/Security Policy and Governance				
		ITCS 1203	E	IAS/Foundational Concepts in Security				
		ITCS 4131	E	IAS/Network Security				
UNC Greensboro	BS				0	2	1	27%
		CSC 562	R	IAS/Platform Security				
		CSC 580	E	IAS/Cryptography				
		CSC 583	E	IAS/Network Security				
UNC Greensboro	MS				0	1	2	27%
		CSC 680	E	IAS/Cryptography, IAS/Web Security				
		CSC 676	E	IAS/Security Policy and Governance				
UNC Pembroke	BS				1	2	2	45%
		CSC 3350	E	IAS/Network Security				
		CSC 3380	E	IAS/Web Security				
		CSC 4020	E	IAS/Foundational Concepts in Security, IAS/Cryptography, IAS/Network Security				
		CSC 4350	E	IAS/Platform Security				
UNC Wilmington	BS				2	1	0	27%
		CSC 385	R	IAS/Foundational Concepts in Security				
		CSC 105	E	IAS/Principles of Secure Design				
		CSC 446	E	IAS/Network Security				

UNC School (CIP 11.0701)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Core 1 Fulfilled (#/3)	Core 2 Fulfilled (#/3)	Electives Fulfilled (#/5)	% ACM IAS Guideline being delivered. (# KA's offered / 11 KA's)
Western Carolina University	BS				3	2	1	55%
		CS 210	E	IAS/Foundational Concepts in Security				
		CS 430	E	IAS/Cryptography, IAS/Web Security				
		CS 431	E	IAS/Principles of Secure Design, IAS/Threats and Attacks, IAS/Defensive Programming				
Winston-Salem State University (Security Option)	BS				3	1	3	64%
		CSC 3325	R	IAS/Foundational Concepts in Security, IAS/Principles of Secure Design, IAS/Security Policy and Governance				
		CSC 4330	R	IAS/Cryptography				
		CSC 4360	R	IAS/Platform Security				
		CSC 4370	R	IAS/Web Security				
		CSC 1307	E	IAS/Foundational Concepts in Security				
		CSC 3323	E	IAS/Platform Security				
		CSC 3332	E	IAS/Web Security				
		CSC 3355	E	IAS/Defensive Programming				
		CSC 4323	E	IAS/Platform Security				

Table 29- Information Technology classes to ACM IT IAS Guideline Map

UNC School (CIP 11.0103)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Fulfilled (max 11)	% ACM IT IAS Guideline being delivered. (KA's offered / 11 KA's)
East Carolina University	BS				6	55%
		ICTN 4200	R	IAS/Attacks, IAS/Vulnerabilities		
		ICTN 4201	R	Lab for ICTN 4200		
		ICTN 4800	R	IAS/Fundamental Aspects, IAS/Security Domains, IAS/Information States, IAS/Security Services		
		ICTN 4801	R	Lab for ICTN 4800		
UNC Charlotte	MS				11	100%
		ITIS 6200	R	IAS/Fundamental Aspects, IAS/Security Mechanisms, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities		
		ITIS 5220	E	IAS/Security Services, IAS/Vulnerabilities		
		ITIS 5221	E	IAS/Security Domains		
		ITIS 5250	E	IAS/Fundamental Aspects, IAS/Forensics		
		ITIS 6150	E	IAS/Security Domains		
		ITIS 6167	E	IAS/Security Domains, IAS/Vulnerabilities, IAS/Information States		
		ITIS 6210	E	IAS/Security Mechanisms		
		ITIS 6220	E	IAS/Policy, IAS/Attacks		
		ITIS 6230	E	IAS/Operational Issues		
		ITIS 6240	E	IAS/Security Mechanisms		

UNC School (CIP 11.0103)	Degree	Classes with a Security Element	Required or Elective	Most closely maps to ACM IAS Guideline	Fulfilled (max 11)	% ACM IT IAS Guideline being delivered. (KA's offered / 11 KA's)
		ITIS 6362	E	IAS/Operational Issues, IAS/Policy, IAS/Threat Analysis Model		
		ITIS 6420	E	IAS/Policy, IAS/Attacks		
UNC Pembroke	BS				5	45%
		ITC 2080	R	IAS/Information States		
		ITC 3250	E	IAS/Security Mechanisms, IAS/Security Domains, IAS/Security Services, IAS/Vulnerabilities		
UNC Wilmington	BS				11	100%
		CIT 204	R	IAS/Security Mechanisms, IAS/Forensics, IAS/Information States		
		CIT 324	R	IAS/Fundamental Aspects, IAS/Operational Issues, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities		
		CIT 410	R	IAS/Attacks, IAS/Vulnerabilities		
		CIT 213	R	IAS/Security Domains		
Winston-Salem State University	BS				7	64%
		CSC 3325	R	IAS/Fundamental Aspects, IAS/Security Mechanisms, IAS/Policy, IAS/Security Domains, IAS/Security Services, IAS/Threat Analysis Model, IAS/Vulnerabilities		

Table of Figures

Table of Tables