A Model Curriculum for Programs of Study in Information Security/Cybersecurity

March 2021

Michael E. Whitman, Ph.D., CISM, CISSP

Herbert J. Mattord, Ph.D., CISM, CISSP

KSU Institute for Cybersecurity Workforce Development

Kennesaw State University

3203 Campus Loop Road

Kennesaw, GA 30144

infosec@kennesaw.edu

Kennesaw State University was designated a National Center of Academic Excellence in Information Assurance Education by the National Security Agency and the Department of Homeland Security in 2004, 2007, 2012 and 2015.

Table of Contents

Introduction

Greetings! We would like to take this opportunity to thank you for allowing us to share our lessons learned in the development of Information Security & Cybersecurity Curriculum at KSU. As part of our ongoing commitment to Security education, we have decided to formally compile our information into a single packet and provide it to any who seek it, without any requirements, associated costs or restrictions. As a courtesy we would like to ask that if you like what you see and would like to adopt the contents in whole or in part, that you send us a letter indicating your intent. This is to allow us to maintain a contact within institutions that are adopting our curriculum and to gather feedback on its feasibility and use. This document begins with pieces of the overall curriculum model and continues through a discussion of the specific courses and programs implemented at Kennesaw State University. We then conclude with the intended next steps in the development of this curriculum. We invite you to participate in this process by forwarding suggestions, constructive criticisms, and ideas to us at the address above or by email to infosec@kenneaw.edu.

The following sections overview our experiences and findings in developing security curriculum. At the end of this discussion an abbreviated copy of our methodology is repeated with blank worksheet so that you may duplicate our process yourself.

For the purposes of this document, the terms information security and cybersecurity will be considered synonymous, regardless of the actual nuances that exist between the two terms. We will therefor describe the curriculum as security, except where it exists in our degree programs. We similarly refer to "IT programs" to describe all computing programs, like Management Information Systems (MIS), Information Systems (IS), Information Technology (IT), Computer Science (CS) and Software Engineering (SWE).

Statement of the Problem

One of the continuing challenges facing society is the security and protection of information assets. Advances in information security (InfoSec) and cybersecurity (CyberSec) have been unable to keep pace with advances in computing in general.[1] Daily, press accounts of dramatic computer theft, fraud and abuse are reported as leading to extensive economic loss. Continuous attacks on the American IT Infrastructure have highlighted the need for information security.[2]

According to the National Institute for Science and Technology (NIST), the demand for security professionals is dramatic and real, with an estimated shortfall of almost 3 million professionals in the next few years.[3]

Education in information security prepares students to recognize and combat information system threats and vulnerabilities[4]. The article "Integrating Security into the Curriculum" argues "an educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure".[5] The need is so great that the President of the US issued Presidential Decision Directive 63, the Policy on Critical Infrastructure Protection in May 1998, which prompted the National Security Agency to established outreach programs like the National Centers of Academic Excellence in Cybersecurity (CAE-C) programs. The mission of the NCAE-C is "to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that

- Establishes standards for cybersecurity curriculum and academic excellence,
- Includes competency development among students and faculty,
- Values community outreach and leadership in professional development,
- Integrates cybersecurity practice within the institution across academic disciplines,
- Actively engages in solutions to challenges facing cybersecurity education."[6]

According to the US Government document The National Strategy to Secure Cyberspace, "Education and outreach play an important role in making users and operators of cyberspace sensitive to security needs. These activities are an important part of the solution for almost all of the issues discussed in the National Strategy to Secure Cyberspace."[7] Even as part of the more recent National strategies: U.S. International Strategy for Cyberspace (May 2011) and the

Comprehensive National Cybersecurity Initiative (May 2009), there is a recognized national goal "To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace."[8]

There are two dominant technology curriculum guidelines currently in use. The first is the new ABET-CAC accreditation standards for programs in Cybersecurity, which – in addition to the general CAC computing requirements specify:

"These program criteria apply to computing programs using cybersecurity, cyber operations, computer security, information assurance, information security, computer forensics, or similar terms in their titles.

3. Student Outcomes

In addition to outcomes 1 through 5, graduates of the program will also have an ability to:

6. Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]

5. Curriculum

The curriculum requirements specify topics, but do not prescribe specific courses. These requirements are:

(a) At least 45 semester credit hours (or equivalent) of computing and cybersecurity course work. The course work must include:

1. Application of the crosscutting concepts of confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking.
2. Fundamental topics from each of the following:

   a) Data Security: protection of data at rest, during processing, and in transit.

   b) Software Security: development and use of software that reliably preserves the security properties of the protected information and systems.

   c) Component Security: the security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into larger systems.

   d) Connection Security: security of the connections between components, both physical and logical.

   e) System Security: security aspects of systems that use software and are composed of components and connections.

   f) Human Security: the study of human behavior in the context of data protection, privacy, and threat mitigation.

   g) Organizational Security: protecting organizations from cybersecurity threats and managing risk to support successful accomplishment of the organizations' missions.

   h) Societal Security: aspects of cybersecurity that broadly impact society as a whole.

3. Advanced cybersecurity topics that build on crosscutting concepts and fundamental topics to provide depth.

(b) At least 6 semester credit hours (or equivalent) of mathematics that must include discrete mathematics and statistics."[9]

The second dominant curriculum guideline is the ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline, by The Joint Task Force on Cybersecurity Education (JTF) which grew out of the Cyber Education Project (CEP).[10] This report specifies that cybersecurity programs include curriculum on:

- Data security
- Software security

- Component security
- System security
- Human security
- Organization security
- Societal security

but allows differences in technical and non-technical programs by providing "lenses" to influence the design of the programs.[11]

Earlier versions of these documents provided support for the development and evolution of the programs at KSU. In the early days, the IS 2002 (and IS 2010 http://www.acm.org/education/curricula-recommendations) guiding principles were adopted and revised for this curriculum model development:

1. "The model curriculum should represent a consensus from the InfoSec community.
2. The model curriculum should be designed to help InfoSec faculty produce competent and confident entry level graduates well suited to work-place responsibilities.
3. The model curriculum should guide but not prescribe. Using the model curriculum guidelines, faculty can design their own courses.
4. The model curriculum should be based on sound educational methodologies and make appropriate recommendations for consideration by InfoSec faculty.
5. The model curriculum should be flexible and adaptable to most IS/CS programs."[12]

The model discussed here is designed to allow security majors to move toward career fields that include and evolve through technical knowledge areas and into the management of security.

Goals and Objectives

This project is designed to increase the quality of security education by creating a curriculum model in security that provides students with technical and managerial skills needed for the modern workforce. The curriculum can be adopted by institutions with the desire to implement undergraduate or graduate security curriculum as individual courses, minors or concentrations, or majors. It is intended to provide adopters of the curriculum with the means to deliver a quality education with breadth and depth of the security common body of knowledge.

Approaches to Implementing Information Security Curricula

There are five approaches to implementing information security curricula:

1. Elements added to existing courses
2. Elements added to a capstone course or courses
3. Independent security courses
4. Security certificates / minors
5. Security degree programs

Elements added to existing courses

In this option, existing courses can have a security module added to reinforce the need to address information security at all junctures of organizational effort. This is a preferred technique and can be used in conjunction with other approaches. It is important to thread information security through a course, rather than adding it as a single module at the end. The following table provides examples of how information security could be integrated in existing courses.

Existing Course	Security Topics
Programming Principles	Software Assurance* Applied cryptography
Networking/Data Communications	Network security principles Network security tools (firewalls, IDPS, protocol sniffers)
Systems Analysis & Design	Security in the SDLC
Database Principles	Developing secure database structures Security tools for data management Privacy topics
Operating Systems	OS Hardening Configuration management

* see https://www.nist.gov/publications/software-assurance-common-body-knowledge-development-eventapril-4-6-2005national

Elements added to a capstone course or courses

In this second approach to adding security content, specific modules are added to specific capstone experiences or courses. In our program for example students have two classes that represent their capstone experience. In the first, they are exposed to strategic policy and planning in IT and presented with a number of guest speakers on various topics. In the second they are required to develop a system to solve a business problem, incorporating all aspects of learning to that point including database, data communications, programming, project management etc. By addressing strategic Information Security planning in the first course and having at least one speaker on an InfoSec topic, we integrate security into this course. By requiring the student teams to demonstrate how they used secure development techniques in the second we reinforce the concepts there.

Independent security courses

The third approach to implementing information security is to create single security courses. This is the approach most commonly used today. Many programs develop one or two classes in security. Unfortunately many of the classes labeled as security classes fail to address the overall comprehensive breadth and scope of what is information security. A class in theoretical cryptography, while interesting does not provide much value to an information security professional-to-be. This requires faculty to develop courses in the manner described in detail the subsequent sections, rather than implementing classes “that would be fun to teach.” Also indicated in subsequent sections are suggestions for topics and components of individual security classes.

Information security certificates / minors.

Continually increasing in frequency, the fourth option is to implement a cohesive set of classes, under the title of minor, concentration, specialization, or certificate. This requires detailed planning based on the desired focus and outcome of the program. In our case, we made a conscious decision to focus more on managerial information security, and less on technical information security. While we have courses in the technical arena, the bulk of the foundational courses are on the roles and responsibilities of an information security professional manager, rather than technical. This is purely a choice based on our strengths. There are many institutions out there that could, and should, consider implementing technical programs, if they have the resources and support to do so.

Security degree programs

In our mind, the ultimate goal for enhanced information security curriculum is the baccalaureate-level information security program. As indicated in the statement of the problem, there are several programs in the field that list bachelors or masters in security degrees (information security, information assurance, or cybersecurity). When you take a close look, many are mainstream computing programs with more of a security concentration or minor. Nothing wrong with that, but it tends to be misleading to the students. It takes a great deal of effort and support to create enough

courses to populate a program of this magnitude, and even more resources to offer it. It does represent the pinnacle of security education.

Which of these approaches should you consider? First one must examine the available resources, time, faculty, money, technology, and student demand. It may help to begin with the first two approaches and then slowly roll out additional approaches as demand presents itself, or just jump in.

Foundation Work

Education is recognized as a critical component to improve information security throughout the nation.[13] The development of a curriculum model would provide direct benefit to the various academic, business, and governmental agencies, to support formal education efforts. During the initial analysis phase, we, the authors, examined existing literature, reviewed other programs of interest and their implementations. We also examined current and emerging national and international standards and guidelines for the training of security professionals, instructional methods and materials from programs recognized as NSA centers of excellence across the country, and general recommendations and constraints from curriculum supporting organizations such as the AIS, ACM and ABET.

In developing the curriculum for our first security program, we used the "Backward Curriculum Design Process"[14] a well-known approach to curriculum design that begins with the desired outcomes and goals and works backward to learning objectives grouped into courses. The curriculum model seeks to answer the following question:

What should a security professional who graduates from a particular program be qualified to do, and what positions should they expect to be able to hold?

Information Security Position and Roles

As position descriptions are not sufficiently descriptive of the roles the individuals play in the information security function, the next step was to identify the roles information security professionals assume and then map them to the positions an individual should hold. The following sections are from the text Principles of Information Security, 7th ed © 2021 Cengage Learning.

"In an Information Security Roundtable interview with Andy Briney, Eddie Schwartz, then VP of Strategy at Guardent, described security positions as being classified into one of three areas: those that define information security programs, those that build the systems and create the programs to implement information security controls, and those that administer information security control systems and programs that have been created. The "definers" are managers who provide policy and planning and manage risk assessments. They are typically senior information security managers—they have extensive and broad knowledge but not a lot of technical depth. The builders are techies who create security technical solutions to protect software, systems, and networks. The administrators apply the techies' tools in accordance with the decisions and guidance of the definers; they provide day-to-day systems monitoring and use to support an organization's goals and objectives. By clearly identifying which type of role it is seeking and then classifying all applicants into these three types and matching them, the organization can recruit more effectively."[15]

A typical organization has several individuals with information security responsibilities. While the titles used within any specific organization may be different from one organization to the next, most of the job functions fit one of the following categories:

- Chief information security officer (CISO)
- Security managers
- Security technicians, administrators, and analysts
- Security staffer/watchstander

CISO

The CISO is primarily responsible for the assessment, management, and implementation of the program that secures the organization's information. The CISO may also be called the Manager for Security, the Security Administrator, or a

similar title. The CISO usually reports directly to the CIO, although in larger organizations one or more layers of management may exist between the two officers.

Security Managers

Security managers are accountable for the day-to-day operation of the information security program. They accomplish objectives identified by the CISO, to whom they report as shown in Figure 5-11, and resolve issues identified by technicians, administrators, analysts, or staffers whom they supervise. Managing technology requires an understanding of it, but not necessarily a technical mastery in its configuration, operation, and fault resolution. Within the information security community, there may be team leaders or project managers responsible for management-like functions, such as scheduling, setting priorities, or administering any number of procedural tasks, but who are not necessarily held accountable for making a particular technology function. The accountability for the actions of others is the hallmark of a true manager. The accountability found in true management roles can be used to differentiate between actual managers and other roles that may include the word manager in their job titles but in fact to not have such accountability.

Security Technicians, Administrators and Analysts

Security technicians are the technically qualified individuals who configure firewalls and IDSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technology is properly implemented. A security technician is usually an entry-level position; however, some technical skills are required, which can make it difficult for those new to the field. It is difficult to get a job without experience, and experience comes with a job. Just as in networking, security technicians tend to be specialized, focusing on one major security technology group (firewalls, IDS, servers, routers, or software), and further specializing in one particular software or hardware package within the group, like Checkpoint firewalls, Nokia firewalls, or Tripwire IDS. These technologies are sufficiently complex to warrant a high level of specialization. Security technicians who want to move up in the corporate hierarchy must expand their technical knowledge horizontally, gaining an understanding of the general, organizational issues of information security, as well as all technical areas.

The security administrator is a hybrid between a security technician and the security manager, described in the previous section. These individuals have both technical knowledge and managerial skill. They are frequently called upon to manage the day-to-day operations of security technology, as well as assist in the development and conduct of training programs, policy and the like. The security analyst is a specialized security administrator. In traditional IT, the security administrator corresponds to a systems administrator or database administrator, and the security analyst to a systems analyst. The systems analyst, in addition to security administration duties, also must analyze and design security solutions within a specific domain (firewall, IDS, antivirus). Systems analysts must be able to identify the users' needs, as well as understand the technological complexities and capabilities of the security systems they design.

Security Staffer or Watchstander

This is a catchall title that applies to the individuals who perform routine watch standing activities. It encompasses the people that watch intrusion consoles, monitor e-mail accounts, and perform other routine-yet-critical roles that support the mission of the information Security Department.

Why is it important to understand these roles?

In order to design curriculum, one must understand what it is you want the student to be able to accomplish upon graduation. As Stephen Covey advises "begin with the end in mind". In our curriculum development we use these roles were used as surrogates for positions and mapped to knowledge areas. The recent development of the NIST NICE Cybersecurity Workforce Model – published as NIST Special Publication 800-181, Revision 1, which provides additional knowledge into the knowledge, skills, abilities and tasks associated with cybersecurity roles.[16]

Knowledge areas represent the specific knowledge needed for each role, and when paired with a multi-level mastery model like Bloom's taxonomy[17], can be used to identify the level of depth of knowledge for each role. For example, a CISO may need great breadth of knowledge, but not as much depth of knowledge in an area as a technician would. The challenge is to completely map and verify the roles, knowledge areas, and levels of mastery needed.

Many programs take the short cut and jump straight to the certifications an information security professional could earn like: CISSP, SSCP, GIAC, Security+, CISA and CISM. However, programs are hesitant to implement coursework that is focused on a specific applied output. Universities in general prefer to focus more on the true knowledge areas that these certificates test, rather than the specifics of these exams. However, if we examine the content of some of the key certifications, we can begin to glimpse some of the knowledge areas we would need to integrate with our coursework.

The NICE Definitions of Security Roles and Responsibilities

In 2011, a new major initiative has been promoted by a joint group of Federal agencies: NIST, NSA & DHS to name a few. The National Initiative for Cybersecurity Education will have far-reaching implications for information security education in the very near future. What was once referred to as Information Assurance in the federal sector is now referred to as Cybersecurity. According the NIST NICE web site:

"The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Located in the Information Technology Laboratory at NIST, the NICE Program Office operates under the Applied Cybersecurity Division, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure."[18]

NIST NICE Cybersecurity Workforce Framework organizes security jobs (mainly in the public and military sectors) into seven categories:

- Securely Provision
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
- Analyze
- Collect & Operate
- Investigate

The following material is directly quoted from the Reference Spreasdhseet for the NICE Framework available from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material.

[Begin Block Quote]

SECURELY PROVISION (SP)

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

- Risk Management (RSK) - Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. Sample work roles: Authorizing Official/Designating Representative and Security Control Assessor.
- Software Development (DEV) - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. Sample work roles: Software Developer and Secure Software Assessor.

- Systems Architecture (ARC) - Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. Sample work roles: Enterprise Architect and Security Architect.
- Technology R&D (TRD) - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility. Sample work roles: Research & Development Specialist.
- Systems Requirements Planning (SRP) - Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs. Sample work roles: Systems Requirements Planner.
- Test and Evaluation (TST) - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT. Sample work roles: System Testing and Evaluation Specialist.
- Systems Development (SYS) - Works on the development phases of the systems development life cycle. Sample work roles: Information Systems Security Developer and Systems Developer.

OPERATE and MAINTAIN (OM)

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

- Data Administration (DTA) - Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data. Sample work roles: Database Administrator and Data Analyst.
- Knowledge Management (KMG) - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content. Sample work roles: Knowledge Manager.
- Customer Service and Technical Support (STS) - Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty. Sample work roles: Technical Support Specialist.
- Network Services (NET) - Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems. Sample work roles: Network Operations Specialist.
- Systems Administration (ADM) - Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration. Sample work roles: System Administrator.
- Systems Analysis (ANA) - Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both. Sample work roles: Systems Security Analyst.

OVERSEE and GOVERN (OV)

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

- Legal Advice and Advocacy (LGA) - Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and

makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings. Sample work roles: Cyber Legal Advisor and Privacy Officer/Privacy Compliance Manager.

- Training, Education, and Awareness (TEA) - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate. Sample work roles: Cyber Instructional Curriculum Developer and Cyber Instructor.
- Cybersecurity Management (MGT) - Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Sample work roles: Information Systems Security Manager and Communications Security (COMSEC) Manager.
- Strategic Planning and Policy (SPP) - Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements. Sample work roles: Cyber Workforce Developer and Manager and Cyber Policy and Strategy Planner.
- Executive Cyber Leadership (EXL) - Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work. Sample work roles: Executive Cyber Leadership.
- Program/Project Management (PMA) and Acquisition - Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle. Sample work roles: Program Manager, IT Project Manager, Product Support Manager, IT Investment/Portfolio Manager and IT Program Auditor.

PROTECT and DEFEND (PR)

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

- Cybersecurity Defense Analysis (CDA) - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats. Sample work roles: Cyber Defense Analyst.
- Cybersecurity Defense Infrastructure Support (INF) - Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities. Sample work roles: Cyber Defense Infrastructure Support Specialist.
- Incident Response (CIR) - Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities. Sample work roles: Cyber Defense Incident Responder.
- Vulnerability Assessment and Management (VAM) - Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. Sample work roles: Vulnerability Assessment Analyst.

ANALYZE (AN)

Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- Threat Analysis (TWA) - Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities. Sample work roles: Threat/Warning Analyst.

- Exploitation Analysis (EXP) - Analyzes collected information to identify vulnerabilities and potential for exploitation. Sample work roles: Exploitation Analyst.
- All-Source Analysis (ASA) - Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications. Sample work roles: All-Source Analyst and Mission Assessment Specialist.
- Targets (TGT) - Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies. Sample work roles: Target Developer and Target Network Analyst.
- Language Analysis (LNG) - Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities. Sample work roles: Multi-Disciplined Language Analyst.

COLLECT and OPERATE (CO)

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- Collection Operations (CLO) - Executes collection using appropriate strategies and within the priorities established through the collection management process. Sample work roles: All Source-Collection Manager and All Source-Collection Requirements Manager.
- Cyber Operational Planning (OPL) - Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations. Sample work roles: Cyber Intel Planner, Cyber Ops Planner and Partner Integration Planner.
- Cyber Operations (OPS) - Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities. Sample work roles: Cyber Operator.

INVESTIGATE (IN)

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence

- Cyber Investigation (INV) - Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering. Sample work roles: Cyber Crime Investigator.
- Digital Forensics (FOR) - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. Sample work roles: Law Enforcement /Counterintelligence Forensics Analyst and Cyber Defense Forensics Analyst.

[END BLOCK QUOTE]

The NCAE-C office at NSA regularly announces updates and improvements on the program to keep current with the latest developments by industry, government and NIST NICE standards.

Information Security Professional Certifications

The professional security certifications available are many, varied and change regularly. Rather than list the details of each certification, we will simply provide a ling to the host organization and encourage you to become familiar with the certifications most important to your curriculum efforts.

(ISC)2 Certifications - www.isc2.org

- Certified Information Systems Security Professional (CISSP) – a must have for security managers. Domains:
  1. Security and Risk Management

2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

The CISSP also offers advanced "concentrations" for those holding the CISSP in:

- Architecture
- Engineering
- Management

- Systems Security Certified Practitioner (SSCP) – appropriate for the security analyst or administration, similar to the CISSP, but over more "applied" material. Domains:
  1. Access Controls
  2. Security Operations and Administration
  3. Risk Identification, Monitoring and Analysis
  4. Incident Response and Recovery
  5. Cryptography
  6. Network and Communications Security
  7. Systems and Application Security
- Associate of $(ISC)^2$ – for those who wish to earn an $(ISC)^2$ certification but haven't earned met the experience requirement.

There are several other certifications available from $(ISC)^2$, visit the web site for more information.

ISACA – www.isaca.org

ISACA is the organization that offers the Certified Information Security Manager (CISM) the eminent certification for security managers. The CISM can provide executive management with an assurance that those earning the designation have the required background knowledge needed for effective security management and consulting. It is oriented toward information risk management and addresses management, design, and technical security issues at a conceptual level. Domains:

- Information Security Governance
- Information Risk Management
- Information Security Program Development and Management
- Information Security Incident Management

ISACA also offers several other specialized security certifications like the CRISC—Certified in Risk and Information Systems Control, visit the web site for more information.

Global Information Assurance Certification (GIAC) – www.giac.org

The certification side of SANS (http://www.sans.org) is known as the GIAC (http://www.giac.org). The GIAC family of certifications can be pursued independently or combined to earn the comprehensive certification, GIAC Security Engineer (GSE). Most GIAC certifications are offered in conjunction with SANS training. For more information on the GIAC security-related certification requirements, visit www.giac.org/certifications. GIAC certifications are offered in the following focus areas:

- Offensive Operations
- Cyber Defense
- Cloud Security

- Industrial Control Systems
- Digital Forensics & Incident Response
- Management, Legal & Audit

GIAC also offers several other specialized security certifications, visit the web site for more information.

CompTIA - www.comptia.org

The company that brought the first vendor-neutral professional IT certifications, the A+ series, comes the perfect first certifications for those entering the cybersecurity field.

- Security + Domains:
  - "Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
  - Monitor and secure hybrid environments, including cloud, mobile, and IoT
  - Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
  - Identify, analyze, and respond to security events and incidents"[19]
- Cybersecurity Analyst + Domains:
  - "Leverage intelligence and threat detection techniques
  - Analyze and interpret data
  - Identify and address vulnerabilities
  - Suggest preventative measures
  - Effectively respond to and recover from incidents"[20]

Established Standards, Models and Practices

Another major area of information that could be used to derive the skills needed to become a security professional lay in established standards, models and practices. There are three primary documents which guide the implementation and management of security programs. These are discussed in turn here, in an extract from Management of Information Security:

Among the most accessible places to find a quality security management model are U.S. federal agencies and international organizations. One of the most popular security management models has been ratified into an international standard. British Standard 7799 provides two components, each addressing a different area of security management practice. BS 7799:1, once known as ISO/IEC 17799 and now ISA 27002, is called "Information Technology – Code of Practice for Information Security Management." BS 7799:2 now known as ISO/IEC 27001 is called "Information security management: Specification with guidance for use." These documents are discussed in detail in the following sections. These are proprietary, and organizations wishing to adopt this model must purchase the rights to do so.

There are a number of alternatives. The first and foremost of these are free documents provided by the National Institute of Standards and Technology's Computer Security Resources Center (http://csrc.nist.gov). This site contains several publications, including ones containing models and practices.

ISO/IEC 27001/27002

One of the most widely referenced and often discussed security models is Information Technology – Code of Practice for Information Security Management, which was originally published as the British Standard BS 7799. This Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799 in 2000 and in 2005 as ISO/IEC 27002 as part of the new 27000 series of Information Security Management Systems (ISMS) standards. While the details of ISO/IEC 27002 are available only to buyers of the standard, the structure and general organization are well known:[21]

14.2 Security in development and support processes

14.3 Test data

15 Supplier relationships

15.1 Information security in supplier relationships

15.2 Supplier service delivery management

16 Information security incident management

16.1 Management of information security incidents and improvements

17 Information security aspects of business continuity management

17.1 Information security continuity

17.2 Redundancies

18 Compliance

18.1 Compliance with legal and contractual requirements

18.2 Information security reviews

Bibliography"[22]

NIST Special Publications (SP) - https://csrc.nist.gov/publications/sp800

The NIST documents use a common philosophy based on the implementation of the Risk Management Framework and their associated controls. The beauty of NIST SPs is that they have shifted their focus from exclusively federal government systems to recommendations for both public and private systems and they are completely free to download, making them great references for faculty and students alike. Key NIST SPs include:

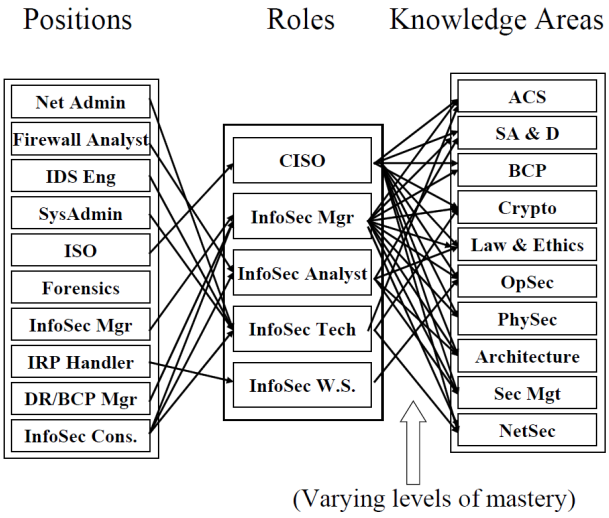
- SP 800-12 An Introduction to Information Security
- SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model
- SP 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems
- SP 800-30 Rev. 1 Guide for Conducting Risk Assessments
- SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
- SP 800-35 Guide to Information Technology Security Services
- SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
- SP 800-50 Building an Information Technology Security Awareness and Training Program
- SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations
- SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
- SP 800-55 Rev. 1 Performance Measurement Guide for Information Security
- SP 800-61 Rev. 2 Computer Security Incident Handling Guide
- SP 800-83 Rev. 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- SP 800-94 Rev. 1 Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-95 Guide to Secure Web Services
- SP 800-100 Information Security Handbook: A Guide for Managers
- SP 800-114 Rev. 1 User's Guide to Telework and Bring Your Own Device (BYOD) Security
- SP 800-115 Technical Guide to Information Security Testing and Assessment
- SP 800-123 Guide to General Server Security
- SP 800-124 Rev. 2 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

- SP 800-137A Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment
- SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-150 Guide to Cyber Threat Information Sharing
- SP 800-181 Rev. 1 Workforce Framework for Cybersecurity (NICE Framework)
- Many many more…

Mapping Positions and Roles to Knowledge Areas

With this information the curriculum designers can gain a better feel for what a graduate should know upon seeking a specific job category. The following figure illustrates this mapping.

In our case, we decided, based on conversations with our local curriculum advisory board, that KSU's information security coursework should be focused on preparing security administrators so that immediately upon graduation they would be prepared for career progression through security manager to CISO. As a result, selected learning objectives were tied to providing the appropriate level of mastery within each knowledge area felt to be critical to an individual's success in that program. We began with a two sets of information: the CISSP Common Body of Knowledge, and the CNSS (formerly NSTISSC) training standards (https://www.cnss.gov/CNSS/issuances/Instructions.cfm). From each of the following we examined introductory and advanced knowledge areas we felt were essential to this career progression.



Defining the Focus of the Program

At this point it is important to define the general thrust of the program and develop overall program objectives. Again, what is it we want our students to learn from the entire program? In order to do this we must define the focus of the program. In information security, there are three general types of programs:

Managerial InfoSec Program

The managerial program seeks to emphasize what we call the 5 "Ps" of Information Security: People, Planning, Policy, Programs and Projects. As is evident in the sample syllabus for the Management of Security later in this document, these areas focus more on the administration and management of information security, than the technological aspects. The managerial student should understand the types and purposes of various technical security controls, but may not necessarily be able to configure, implement or maintain them. Managerial security programs are frequently found in Colleges of Business, Information Systems Departments and other related areas.

Technical InfoSec Program

The other end of the security spectrum, the technical program focuses more on the technologies of information security. Students in these programs are expected to, in a very hands-on fashion, design, install, configure, test, and maintain various technical security controls and equipment. This could include firewalls, intrusion detection systems, operating systems hardening, etc. The technical student should understand the role and purpose of the managerial aspects, as the

technical implementations are guided by the managers in security, but may not be able to develop these areas. Technical security programs are frequently found in Colleges of Science, IT and Computer Science programs, technical colleges and schools, and other related areas.

Balanced InfoSec Program

The balanced InfoSec program is a combination of the managerial and technical programs seeking a balance between the two. Programs in this category generally will not have the level of depth in either management or technology aspect of security but will seek to provide an approach that well prepares the student for further education or experience in subsequent institutions or organizations. Balanced security programs will become the most prevalent programs, eventually replacing the technical programs in popularity.

Levels of Mastery

Using the detailed list of domains and knowledge areas from the CISSP and other sources we then began to identify what level of mastery was desired for each knowledge area. The taxonomy we used was derived in part from Bloom's taxonomy but simplified to a great extent. We chose four levels of desired mastery, defined as follows:

1. Understanding: At the understanding level, the student can identify key concepts when presented with a list of alternatives. The student has familiarized themselves with the selected knowledge area and can discuss key concepts.
2. Accomplishment: At the accomplishment level, the student can demonstrate the process necessary to use the knowledge area in a given scenario. The student has a deeper grasp on both theoretical and practical applications of the knowledge area.
3. Proficiency: At the proficiency level, the student can generate new examples of the application of the knowledge are. The student has demonstrated the ability to critically discuss knowledge area concepts and can easily relate their learning to others.
4. Mastery: At the mastery level, the student can not only freely create new knowledge of the area but can also evaluate and critique new knowledge created by others. This level is typically obtained through graduate level coursework, or extensive depth of curriculum.

An example in security policy could be:

Upon completion of identified material, the student should be able to:

- Understanding: Know and discuss importance of policy in the organization
- Accomplishment: Demonstrate procedures needed to design and implement policy
- Proficiency: Able to develop and implement a variety of security policies
- Mastery: Able to review and critique all types of security policy at all levels of the organization

Determining Numbers of Courses Needed

The next step was to determine how many courses would be needed, at a minimum to provide the student with the desired level of mastery in the target knowledge. This step was accomplished by organizing the similar content with corresponding learning objectives into class areas. This information then allowed us to identify minimal prerequisite areas for each class. We used the following template to facilitate this process:

Mapping Mastery Depth to Courses

We determined that three courses would provide this depth as indicated for a specialization. This table shows not only the total level of depth, but also the courses in which the depth would be obtained.

Knowledge and Skills Needed as Pre-requisites	Course Names	Knowledge and Skills Delivered

		Level of Mastery Desired U: Understanding A: Accomplishment P: Proficiency M: Mastery		
		Courses Implemented		
Domain	**Knowledge Area**	**Introduction**	**Technical**	**Management**
Access Controls				
	Access control fundamentals	U	A P	A
	Access control types	U	A P	A
	Access control attacks	U	A P	A
	Penetration testing methods	U	A	
Telecommunications* (Some knowledge areas are prerequisite)				
	Network types (LAN/WAN)			
	OSI reference model			
	TCP/IP protocol suite			
	Telecomm security management	U	A	
	Telecommunications threats and attacks	U	A	
	Remote access protocols	U	A	
Security Management				
	Security planning	U A		A P
	Security policies	U A		A P
	Personnel security	U A		A P
	Security personnel	U A		A P
	Data classification and storage	U A		A P
	Risk Management	U A		A P
	Security education, training and awareness program	U A		A P
	Change/configuration management	U A	A	A P
	Assessment strategies	U A	A P	A
Applications Security* (Some knowledge areas are prerequisite)				
	Systems development life cycles	A		
	Database development and management	A		
	Systems controls	U A	A	A
	Distributed applications	U		
	Object oriented concepts*			
	Knowledge based systems*			
	Application and systems attacks and	U	A P	A

		Level of Mastery Desired U: Understanding A: Accomplishment P: Proficiency M: Mastery		
		Courses Implemented		
Domain	Knowledge Area	Introduction	Technical	Management
	vulnerabilities			
	Malicious code	U A	A P	A
Cryptography				
	Cryptosystems	U	A	A
	Ciphers and encryption algorithms	U	A	A
	Asymmetric key systems	U	A	A
	Symmetric key systems	U	A	A
	Hybrid key systems	U	A	A
	Message authentication/message digests	U	A	A
	Public key infrastructure	U	A	A
	Key management	U	A	A P
	Digital signatures	U	A	A
	Alternative cryptosystems	U	A	A
	Security protocols	U	A	
Security Architecture				
	Security models	U	A	A
	Information systems evaluation criteria	U	A	A
	System certification and accreditation	U	A	A
	Security architectures	U	A	A
Operations Security				
	Operations concepts	U A	A	A P
	Threats and countermeasures	U A	A	A P
	Incident response	U A	A	A P
	Auditing	U A	A	A P
	Monitoring	U A	A	A P
Business Continuity Planning				
	Contingency planning	U A		A P
	Business continuity planning	U A		A P
	Disaster recovery planning	U A		A P
	Data backup and recovery methods	U A		A P
	Crisis management	U A		A P
Law and Ethics				

		Level of Mastery Desired U: Understanding A: Accomplishment P: Proficiency M: Mastery		
		Courses Implemented		
Domain	**Knowledge Area**	**Introduction**	**Technical**	**Management**
	Law categories and types	U A		A P
	Computer crimes	U A		A P
	Computer crime investigations	U A		A P
	Computer ethics	U A		A P
	Computer forensics procedures	U A	A	
Physical Security				
	Site selection and security	U A		A
	Guards	U		U
	Keys and locks	U		U
	Doors, walls and gates	U		U
	Intrusion detection systems	U		U
	Fire detection and suppression systems	U		U
	Biometrics	U	A	A
	CCTV	U		

As is obvious, there is substantial overlap both within and between courses with regard to the level of mastery. We found that in some cases, since our sequence of courses would permit a student to take the introduction course and then either the technical OR the managerial, that to obtain the desired level of mastery, duplication of certain levels would be necessary. Duplication between courses also serves to reinforce that desired level of depth. Also evident is the need to obtain both levels of understanding and accomplishment within the same course to reach the overall desired level of mastery.

It was then a simple matter to re-organize learning objectives in each of the target courses and begin searching for learning materials that would support each of these courses. Since the initial development, our learning objectives have evolved to represent in a more robust fashion what the students should be learning in each course. Learning objectives for each of the core courses implemented are presented with the course descriptions in the next section.

As a final note to this phase of the model curriculum, we would like to make the following recommendations: Courses and programs should be created in ways that:

- Involve all critical stakeholders. Just as in systems development, the use of representative groups from all interested parties (faculty, students, industry advisors) will serve to improve the final product.
- Create employable students or students who can advance academically. The bottom line is to create a resource that will be in demand. Unless students can expect employability upon completion, they may lose interest in the program, after an initial surge of interest due to the novelty of the program.
- Capitalize on available resources (faculty, classrooms, labs). We have found that existing labs can be easily modified to support the information security laboratory's unique requirements and exercises. We have also found a wealth of freeware and "hackerware" tools that provide realistic and valuable experiences to the students. Cultivating several key industry contacts has also resulted in several multi-thousand dollar donations in software and hardware.

- Support local / state / national program objectives like the National Strategy to Secure Cyberspace. Contributing to these types of programs not only provides visible and demonstrable credibility to the program, but serves as a basis for increasing the validity of your program should you decide to submit for national grants and industry support.

KSU's Security Program Development

Based on previous analysis of the literature and curriculum development and accreditation efforts as indicated in previous sections, the first foray into security at KSU was the implement of seven information security courses in 2000. These courses were designed to meet the national security standards of the time, as described previously, and to provide a foundation for the curriculum model. In the pilot project students could select individual courses of interest or a five-course sequence culminating in a Certificate, as major electives in a Bachelor of Science in Information Systems degree. They eventually evolved into the core of a Bachelor of Science in Information Security and Assurance Degree. Why ISA? Because BS-IS was already taken.

Undergraduate Certificate in ISA

The three core courses were shaped into a *Certificate in Information Security and Assurance (ISA)* to offer students both theoretical foundations and applied hands-on experiences with the tools and technologies used to protect information assets.

Upon examination of the textbooks, and other learning support materials available at the time of the design of our curriculum, we initially pilot tested the courses with trade press texts, modified to meet the needs of an academic environment, and supplemented with NIST SPs of the time. In almost every instance, the trade press texts proved severely lacked the depth and breadth needed for the classroom. As we developed our own lab exercises, we eventually approached a textbook publisher and collaborated to publish our first lab manual by agreeing to write a textbook to accompany it. We took the opportunity to use the mappings that we were using for our courses and design a text to provide a strong foundation for the first course in our sequence.

The curriculum is designed to encompass both technical details and managerial functions. The certificate begins with three core courses:

- Principles of Information Security & Assurance - An introduction to the various technical and administrative aspects of Information Security and Assurance, this course provides the foundation for understanding key issues associated with protecting information assets, developing protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. Learning objectives: After successful completion of the course students should be able to: identify and prioritize information assets; identify and prioritize threats to information assets; define an information security strategy and architecture; discuss the components of an incident response plan; describe legal and public relations implications of security and privacy issues; and outline a disaster recovery plan.
- Technical Applications in Information Security & Assurance - A detailed examination of the tools, techniques and technologies used in the securing of information assets, this course provides in-depth information on the software and hardware components of Information Security and Assurance. Topics covered include: firewall configurations, hardening Unix and NT servers and specific implementation of security models and architectures. Learning objectives: After successful completion of the course students should be able to: identify the components of Information Security Architectures; specify appropriate security models used in the architecture; identify specific weaknesses and strengths of the security of various networking operating systems; locate and recommend corrections to known vulnerabilities in network infrastructures; specify recommendations for the physical hardening of popular network components; and identify and specify the components of a technology-based security solution.
- Policy and Administration in Information Security & Assurance - A detailed examination of a systems-wide perspective of information security, beginning with a strategic planning process for security. Includes an examination of the policies, procedures and staffing functions necessary to organize and administrate ongoing security functions in the organization. Subjects include security practices, security programs, and continuity planning and disaster recovery planning. Learning objectives: After successful completion of the course students should be able to: write enterprise and issue-specific security policies; design a security

infrastructure; build a security team; select necessary security personnel; specify recommendations for the auditing of an information system for security; and design a disaster recovery/business continuity plan.

Students then selected two courses to complete the certificate. They may select these from

1. Computer Forensics and either Criminal Investigations or Criminal Law;
2. Unix Administration and Security and Data Communications Protocols;
3. Computer Law and Computer Ethics;
   And two courses from:

- Accounting Information Systems;
- EDP Auditing & Control;
- Accounting Auditing & Assurance;
- Internship or Cooperative Study.

BS-Information Security and Assurance

Development of the BS-ISA was an arduous, drawn-out project. It actually began in 2001, when we drafted the Certificate in ISA. In fact, when the faculty proposed the ISA Certificate, we intentionally used a separate prefix (ISA) instead of the department standard (CSIS) to prepare for the eventuality of a degree. Shortly after the certificate was implemented, we pulled up the overview of our BS in Information Systems and mused as to what a BS in ISA would look like. The program was then put back on the shelf to collect dust, as we really did not expect to be able to pursue it further. When Herb Mattord came on board as a full-time faculty member, he declared his mission to see the BS-ISA come to fruition. With the success of the Certificate – some 30+ certificates issued in just over 2 years, and with constantly full ISA classes, eventually the other faculty in the department began to agree with us that perhaps an additional major would be a good idea. At the time the department had close to 1400 majors in its four degree programs - BS in IS and CS, and MS in IS and CS.

We began the process much the same as the certificate was begun, by looking at the end product – the entry level InfoSec professional. We realized that industry would need instruction on the new academically prepared InfoSec professional, and would require a deviation from the traditional promote- from-within-IT, or hire someone else's InfoSec professional model. We began talking to a number of CISOs, CIOs and other regional IT professionals, including fellow CISSPs, to determine what they felt the fresh-college-InfoSec graduate should look like. We realized that what was missing in the discipline was the bridge between the technical half of infosec, and the managerial half. So our goal was to prepare an individual to work in either half, and eventually to reach the position of CISO.

We then went back to our 10 domains of knowledge and began expanding on the foundation provided by the certificate:

- ISA 3100 – Principles of ISA
- ISA 3200 – Applications in ISA
- ISA 3300 – Policy and Administration in ISA
- ISA 3350 – Computer Forensics

And began adding areas we found to be critical to the performance of both the InfoSec technical and managerial expert.

From the technical side we realized the heart of the technical professional was the protection of servers, and the use of information security technologies (firewalls, intrusion detection systems, antivirus etc.). So we create a split operating systems security class, focusing on the protection of client – and server- side security. This allows us to re-tool the 3200 class into a more traditional Network Security class, focusing on the Security Technologies necessary to protect organizations' perimeters. We also realized that one area that is lacking in many programs is a secure programming class. So we replaced the CS2 – type programming class with one designed to take what the students learn in their programming principles I class, and scrutinize it for security issues. We also added a scripting language (cgi etc) to this class for good measure.

From the managerial side, we added an incident response and disaster recovery class, to provide both the planning requirements and the actual hands-on incident response actions. This class is truly a hybrid between managerial planning and technical performance. We cap the program with a "how to be a CISO" capstone class, with a major soup-to-nuts security project, requiring the students to examine an organization (real or case) and design and partially implement a security solution.

The draft layout of this program was presented to numerous groups, including department advisory boards, and other experts in Information Security, both academic and practitioner. After final reviews, it was submitted through the university's curriculum approval process and eventually to the University System of Georgia's Board of Regents. It is customary for a new degree program to receive supplementary questions prior to the board review and vote. Our questions hit the heart of the issue – will the graduates find jobs, is there a demand both by students and by industry for the program?

Fortunately, the IT market had just begun recovery in earnest, and we were able to provide convincing arguments on both accounts. The board met and approved the degree within 5 minutes.

Now the work began. We had to fully flesh out the courses, including lab exercises, homework exercises, lecture notes and the like. To assist in this endeavor, we submitted a NSF proposal under the Federal Cyber Service: Scholarship for Service: Capacity Building Grant program and received a cooperative grant with Savannah State University. Currently the program has over 250 majors.

BS-Cybersecurity

In 2015, we received word that the University System of Georgia was interested in a cybersecurity degree as part of its eCampus program.

> "USG eCampus is a service unit of the University System of Georgia that assists SACSCOC-accredited USG institutions in administering quality, affordable, high-demand, post-secondary online degrees and credentials that address the workplace needs of Georgia and beyond. We leverage resources to imagine, design, and support affordable, quality higher education pathways to enhance the economic, cultural and social interests of the people of Georgia. Our vision is for Georgia to be the most highly-educated state in America, with graduates who utilize their knowledge and skills to make Georgia the most desirable place to live."[23]

The faculty, lead by Drs. Mattord and Whitman of the Department of Information Systems, Michael J. Coles College of Business, began to engage faculty from other colleges on campus, specifically the Departments of Information Technology and Computer Science from the College of Computing and Software Engineering, and the Department of Sociology and Criminal Justice of the College of Humanities and Social Science to develop a cutting-edge multidisciplinary degree program. Within two months, a team of faculty from the three colleges put together a proposal and received quick approval on campus and then from the Board of Regents. The resulting program included an IT foundation, with computer science programming classes, an ISA upper division, with some IT security courses integrated, and a number of optional concentrations, including a cyber crime track supported by SCJ.

To maintain some independence from any one college's influence, the BS-CYBR was housed in a newly created Institute for Cybersecurity Workforce Development. The ICWD was designed to be a multidisciplinary nexus for cybersecurity on campus. The ICWD Executive Director position was designed to report to a governance board consisting of the three Deans of the constituent colleges. The Director works with the Chairs of the departments staffing the courses within the BS-CYBR

While there was some migration of majors from existing degree programs, within four years, the BS-Cybersecurity swelled to over 600 majors, and continues to grow.

MS-Cybersecurity

In 2020, recognizing the increasing need for Cybersecurity professionals, a team of faculty from the development of the BS-Cybersecurity program began lobbying upper administration to allow the creation of a new Master of Science in

Cybersecurity. A team consisting of representatives of the IS Department, the IT Department, the Computer Science Department, the Software Engineering and Game Design Department, and the Sociology and Criminal Justice Department met and over a 2-week period hammered out the mission, purpose, learning outcomes, and curriculum model for the MS-Cybersecurity. Additional faculty contributed to the development of sample syllabi, adopting current graduate and undergraduate security courses to the new program, and expanding the proposal. The KSU graduate curriculum committee reviewed and quickly approved the program. The University System of Georgia Board of Regents approved the program on first reading, with minimal questions. The program went online in Fall 2020, and admitted over 100 students in its first semester.

One unique attribute of the MS-Cybersecurity is its 7-week session structure. Admitted students can take up to two classes per 7-week session, completing all 10 courses within one calendar year, if they so desire. While applicants must have foundations in computer infrastructure, programming, data communications/networking and cybersecurity, they were able to remediate those, initially with 5000-level classes. However, due to the massive initial demand for the program, and the impact of the COVID pandemic in 2020, which resulted in a hiring freeze in the USG, the 5000-level prerequisite foundation classes were replaced with self-paced, faculty-moderated, continuing education modules. This allows students to complete any missing foundations independently, between the time they are conditionally accepted and the first day of class. Students that fail to complete the foundation prerequisites are administratively dropped and must complete them before the next offering.

Also as a result of these factors, in an innovative move, KSU adopted a best practice used in the Georgia Institute of Technology, where graduate qualified faculty serve as the instructor of record for the course but are assisted by several other part-time or adjunct faculty members labeled as “Assistant Instructors”. This allows for larger-than-normal graduate class sizes, with an assistant instructor for each additional 35 students. With over 100 students enrolling in the first four courses, the initial classes quickly swelled to over 80 seats.

In Spring 2021, another group of over 120 students were admitted, swelling some class sizes to over 125 seats, requiring an instructor of record and three assistant instructors per class. Also in Spring 2021, the faculty decided to drop the Cybersecurity foundation prerequisite since one of the first courses undertaken is a Management of Cybersecurity course, using a text designed with the flexibility to be used as the first cybersecurity course in a business program.

The biggest challenge currently facing the program is the management of these large class sizes, given the limited number of qualified graduate faculty. The challenges are still being managed by KSU leadership. Once these challenges are more in-hand, future changes to the program could include the addition of elective courses.

The Draft Curriculum Model

Outcomes from the pilot program were incorporated into a proposed curriculum model. These outcomes included the adjustment of specific learning objectives across all core courses, adjusted use of laboratory exercises within each course, and the movement of some core material to more advanced classes (like forensics material from the technical course to the computer forensics course). Additional outcomes strengthened existing course relationships and validated instructional approaches. One specific outcome was the identification of a clear lack of academic texts to support the curriculum. As a result, we authored our own for several courses since then. These texts are now part of a suite of academic Information Security texts offered by Cengage/Course Technology, and listed later in this document.

Table 1 provides an overview of our first curriculum model.

Table 1: DRAFT CURRICULUM MODEL	
Subject	**Bloom's Levels of Knowledge (from [21])**
Prerequisite Knowledge	
General: Computing Foundations, Data Communications …	
Managerial: Also need Management, Accounting …	
Technical: Also need Operating Systems, Computer Org & Arch, Programming, Protocols …	
Foundation	
1.0 Introduction to Information Security	L1 – Knowledge Recognition & Differentiation in Context
1.1 Computer Law & Ethics	L2 – Comprehension Translation/Extrapolition Use of Knowledge
Technical Aspects of Information Security	
2.0 Technical Applications in InfoSec	L2 – Comprehension Translation/Extrapolition Use of Knowledge
2.1 Operating Systems Security	L3 – Application Knowledge
2.1.1 Windows NT/2000 Security	L4 – Analysis & L5 Synthesis
2.1.2 Linux/Unix Security	L4 – Analysis & L5 Synthesis
2.2 Network Security	L3 – Application Knowledge
2.3 Applied Cryptography	L3 – Application Knowledge
2.4 Computer Forensics	L3 – Application Knowledge
2.5 Firewalls & Intrusion Detection Sys	L3 – Application Knowledge
2.6 ?????	
Managerial Aspects of Information Security	
3.0 Management of Information Security (Policy & Administration)	L2 – Comprehension Translation/Extrapolation Use of Knowledge
3.1 Disaster Recovery/ Business Continuity Planning	L3 – Application Knowledge
3.2 Risk Management	L3 – Application Knowledge
3.3 Incident Response	L3 – Application Knowledge
3.4 Physical Security	L3 – Application Knowledge
3.5 Security Training & Awareness Pgms	L3 – Application Knowledge
3.6 ?????	
Outside Emphases	
O1 Criminal Justice	Varies
O2 Auditing	Varies

Implementation of the Draft Curriculum Model for New Programs

Our preliminary findings suggested that if an institution can only implement two courses, they will be best served implementing an introductory course, and then either a technical or managerial course depending on their preferences.

If the institution can implement more, an analysis of the intent of the program as described in previous sections will provide additional course recommendations, as illustrated in the table below.

Table 2: Implementation of the Proposed Curriculum Model

Based on the number of courses an Institution can implement, it is recommended that they should select the courses indicated. Question marks "?" are used to indicate alternatives.

	Number of Course the Institution can Implement in InfoSec						
↓ Courses:	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Introduction to InfoSec	*	*	*	*	*	*	*
Technical Applications in InfoSec		* or *	*	*	*	*	*
Management of InfoSec			*	*	*	*	*
Additional Courses Selected from: Network Security (Win2K/Unix), Adv. Network Security, Operating Systems Security, Auditing for Security, Computer Forensics, Criminal Justice, Criminal Law, Computer Ethics, Computer Law, Cryptography/ Cryptology, Secure Programming, Internship/Coops				?	? ?	? ? ?	? ? ? ?

Some suggestions based on institutional intent could be as follows:

Scenario 1: The institution can only implement one course:

For a general or technical program:

- Introduction to InfoSec

For a managerial or business program:

- Management of InfoSec (with heavy emphasis on foundation material).

Scenario 2: The institution can implement two courses:

For a general or technical program:

- Introduction to InfoSec
- Technical InfoSec (e.g. Network Security)

For a managerial or business program:

- Introduction to InfoSec
- Management of InfoSec

Scenario 3: The institution can implement three courses:

For all programs:

- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec (e.g. Network Security)

Scenario 4: The institution can implement four courses:

For a general or technical program:

- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec (e.g. Network Security)
- Advanced Technical topics such as:
    - Firewalls, IDS & VPNs
    - OS Security (Unix/Windows)
    - Computer Forensics

For a managerial or business program:

- Introduction to InfoSec
- Management of InfoSec
- Technical InfoSec
- Advanced Managerial topics such as:
    - Contingency Planning
    - Computer Law & Ethics
    - Security Policy
    - Security Governance/strategic planning

As additional courses are added additional technical or managerial topics can be added. Institutions can then begin drafting specific programs to include electives, existing courses etc. to support their desired outcomes.

KSU Security Degree Programs – catalog.kennesaw.edu

KSU offered its first security courses as special topics in 2000. In the 20+ years since then, the security offerings have expanded to multiple majors, minors, and certificate programs. To illustrate the breadth and depth of program possible in a single institution the current degree programs offered at KSU are listed here along with a link to the current catalog descriptions. Currently KSU has the following security programs:

- Bachelor of Business Administration in Information Security and Assurance
- Bachelor of Science in Cybersecurity
- Master of Science in Cybersecurity
- Bachelor of Science in Information Technology w/Cyber Operations Security Concentration
- Bachelor of Science in Computer Science w/Cyber and Network Security Concentration
- Undergraduate Certificate in Information Security and Assurance
- Undergraduate Certificate in Cybersecurity
- Graduate Certificate in Information Security
- Graduate Certificate in IT Security
- Undergraduate Minor in Information Security and Assurance
- Undergraduate Minor in Cybersecurity

BBA-Information Security and Assurance

The flagship degree in security at KSU, the BBA-ISA began as a BS degree in 2005, with a joint information systems/computer science foundation in a College of Science and Mathematics. In 2012, the Information Systems group split off from the Computer Science group and moved to the College of Business, requiring the degree to transition to a Bachelor of Business Administration degree, replacing the CSIS foundation with a traditional business core. The degree is now considered optimal for those seeking security management careers. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6221&returnto=3995 for the 2021 catalog.

Program Description

The purpose of the Bachelor of Business Administration with a major in Information Security and Assurance (BBA-ISA) program is to create technologically proficient, business-savvy information security professionals capable of applying policy, education & training, and technology solutions to protect information assets from all aspects of threats, and to manage the risks associated with modern information usage. Information security is the protection of the confidentiality, integrity, and availability of information while in transmission, storage, or processing, through the application of policy, technology, and education and awareness. Information assurance concerns information operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. This program spans both areas in its approach to the protection of information in the organization.

The Department of Homeland Security and the National Security Agency have jointly designated Kennesaw State University as a National Center of Academic Excellence in Cyber Defense Education with specialized focus areas in Security Policy Development & Compliance and Systems Security Administration.

General Education Core Curriculum (Areas A-E) (42 Credit Hours)

Lower Division Business Core (Area F) (18 Credit Hours)

- ACCT 2101: Principles of Accounting I
- ACCT 2102: Principles of Accounting II
- ECON 2105: Principles of Macroeconomics
- ECON 2106: Principles of Microeconomics
- ECON 2300: Business Statistics

- IS 2200: Information Systems and Communication

Leadership and Career Program (0 Credit Hours)

- BUSA 2150: Discovering My Major and Career
- BUSA 3150: Developing My Career Essentials
- BUSA 4150: Driving My Success

Major Requirements (54 Credit Hours)

Business Core (24 Credit Hours)

- BLAW 2200: Legal and Ethical Environment of Business
- MGT 3100: Management and Behavioral Sciences
- MKTG 3100: Principles of Marketing
- FIN 3100: Principles of Finance
- IS 3100: Information Systems Management
- MGT 3200: Operations Management
- ECON 3300: Applied Statistical and Optimization Models
- MGT 4199: Strategic Management

Major Field Requirements (24 Credit Hours)

- ISA 3010: Security Script Programming
- ISA 3100: Principles of Information Security
- ISA 3200: Network Security
- ISA 3210: Client Systems Security
- ISA 3300: Management of Information Security in a Global Environment
- ISA 4200: Perimeter Defense
- ISA 4220: Server Systems Security
- ISA 4820: Information Security and Assurance Programs and Strategies

Major Field Electives (6 Credit Hours) - Select 6 credit hours from the following:

- ISA 3710: International Issues in Information Security and Assurance
- ISA 4330: Incident Response and Contingency Planning
- ISA 4350: Management of Digital Forensics and eDiscovery
- ISA 4400: Directed Study in Information Security and Assurance
- ISA 4490: Special Topics in Information Security and Assurance
- ISA 4700: Emerging Issues in Information Security and Assurance
- ISA 4805: Penetration Testing
- IS 3040: IT Infrastructure
- IS 3220: Global IS Project Management
- IS 3920: Application Development II
- Any other courses from IS, ISA, and CRJU as approved by the Department.
- FTA 4100: Introduction to Information Security for FinTech

Business Electives (6 Credit Hours)

Six hours of credit from upper-division (3000-4000 level) course offerings outside the Major, but inside the Coles College of Business. ISA courses cannot be used here. (A maximum of six hours of credit in Information Security and Assurance Co-Ops and Internships may be used in this area. Co-Ops and Internships cannot be used in any other area.) ISA Students are encouraged to take IS courses in this area.

Program Total (120 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select ISA from the prefix menu.

Bachelor of Science in Cybersecurity

Developed in 2016 as an eMajor – which allows any student in any University System of Georgia institution to enroll in the program without special permission, the faculty developing the BS in Cybersecurity took the security coursework of the BBA-ISA and coupled it with an IT foundation. The resulting program is more suited for Security Operations Center employees and those desiring a more technical security degree. The BS-Cybersecurity is a multidisciplinary program, combining the efforts of the Information Security and Assurance faculty from the Department of Information Systems and Security, in the Michael J. Coles College of Business, with those of in the Departments of Information Technology, Computer Science and Software Engineering & Game Design departments in the College of Computing and Software Engineering (CCSE), and the Criminal Justice Faculty from the Department of Sociology and Criminal Justice from the Norman J. Radow College of Humanities and Social Sciences. As an interdisciplinary program, the BS-Cybersecurity is housed in the Institute for Cybersecurity Workforce Development, along with the MS-Cybersecurity. The program currently has over 650 majors. The BS-CYBR courses are staffed by the departments represented in the major. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6379&returnto=3995 for the 2021 course catalog.

Program Description

The purpose of the Bachelor of Science with a major in Cybersecurity (BS-CYBR) program is to create technologically capable, business-aware cybersecurity professionals capable of applying technical skills and the knowledge of security management to protect computerized information systems from a wide variety of of threats, and to manage the risks associated with modern information technology usage. Cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of information technology, law, policy, human factors, ethics, and risk management often in the context of adversaries.

The Department of Homeland Security and the National Security Agency have jointly designated Kennesaw State University as a National Center of Academic Excellence in Cyber Defense Education with specialized focus areas in Security Policy Development & Compliance and Systems Security Administration.

The Bachelor of Science with a major in Cybersecurity is a fully online degree that has the primary objective of meeting the high demand for professional degrees in cybersecurity. The degree has core requirements, major requirements, major specializations, and required electives. The major contains those courses considered fundamental to the cybersecurity field and the electives give the student some flexibility in choice.

General Education Core Curriculum (Areas A-E) (42 Credit Hours)

Lower Division Major Requirements (Area F) (18 Credit Hours)

- ACCT 2101: Principles of Accounting I
- ECON 2300: Business Statistics
  or
  STAT 2332: Probability and Data Analysis
- CSE 1321: Programming and Problem Solving I
- CSE 1321L: Programming and Problem Solving I Laboratory
- CSE 1322: Programming and Problem Solving II
- CSE 1322L: Programming and Problem Solving II Laboratory
- CSE 2300: Discrete Structures for Computing
  or
  MATH 2345: Discrete Mathematics

Major Requirements (37 Credit Hours)

Upper Division Technical Core (13 Credit Hours)

- CYBR 3123: Hardware and Software Concepts
- CYBR 3423: Operating Systems Concepts & Administration
- CYBR 4323: Data Communications & Networking
- CYBR 4423: Linux/Unix Administration

Upper Division Security Core (21 Credit Hours)

- CYBR 3100: Principles of Cybersecurity
- CYBR 3200: Network Security
- CYBR 3210: Client Systems Security
- CYBR 3300: Management of Cybersecurity in a Global Environment
- CYBR 4200: Perimeter Defense
- CYBR 4220: Server Systems Security
- CYBR 4330: Incident Response and Contingency Planning

Capstone (3 Credit Hours)

- CYBR 4810: Cyber Defense

Upper Division Major Specializations (9 Credit Hours)

All BS-CYBR students are required to take a minimum of 9 credit hours as an upper-level specialization. They must choose one of the following specializations and complete all the courses listed. The options are:

Systems Security Track

- CYBR 3153: Database Systems
- CYBR 4843: Ethical Hacking for Effective Defense
  or
  CYBR 4883: Infrastructure Defense
- CYBR 4350: Management of Digital Forensics and eDiscovery
  or
  CYBR 4853: Computer Forensics

Network Security Track

- CYBR 4333: Network Configuration & Administration
- CYBR 4833: Wireless Security
- CYBR 4893: Internet of Things: Applications and Security

Cyber Crime Track

- CRJU 1101: Foundations of Criminal Justice
- CYBR 3305: Technology and Criminal Justice
- CYBR 4305: Technology and Cyber Crime

Major Electives (9 Credit Hours)

- Students should choose 9 credit hours from the following:
- CYBR 3220: Global IS Project Management
- CYBR 3223: Software Acquisition and Project Management

- Any CYBR prefix course not included in your chosen concentration
- CYBR 3396: Cooperative Study
- CYBR 3398: Internship
- CYBR 4400: Directed Study
- CYBR 4490: Special Topics in Cybersecurity
- Any 3xxx or 4xxx IS/ISA/IT/CS/CSE/CRJU course for which the student can meet the prerequisites except certain specific restricted ISA or IT Security course (see an advisor for complete listing)

Free Electives (5 Credit Hours)

Program Total (120 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select CYBR from the prefix menu.

Master of Science in Cybersecurity

Another interdisciplinary program developed by a team including faculty from the Department of Information Systems and Security, Michael J. Coles College of Business, the Departments of Information Technology, Computer Science and Software Engineering & Game Design departments, College of Computing and Software Engineering (CCSE), and the Department of Sociology and Criminal Justice, Norman J. Radow College of Humanities and Social Sciences. The MS-Cybersecurity is also housed in the Institute for Cybersecurity Workforce Development. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=55&poid=6567 for the 2021 catalog.

Program Description

The Master of Science in Cybersecurity degree enhances career opportunities to supervise, design, develop, and operate a secure cyber environment. The program can be completed 100% online in 12 months by fully prepared applicants and employs a unique 7-week course structure allowing students to complete four courses per fall and spring semester while taking two subjects at a time.

Upon completion of the MS-Cybersecurity, students will be able to: strategize, design, develop, deploy, and lead cybersecurity efforts in the enterprise; prepare for, respond to, and recover from cybersecurity threats and incidents; manage cybersecurity risk to information assets; and select and apply appropriate tools and methodologies to solve real-world cyber problems.

Required Courses (30 Credit Hours)

- CYBR 7000: Cyber Law, Policy, and Enforcement
- CYBR 7050: Cybercrime Detection, Analysis, and Forensics
- CYBR 7100: Secure Application Development
- CYBR 7200: Securing Enterprise Infrastructure
- CYBR 7220: Mobile and Cloud Security
- CYBR 7240: Cyber Analytics and Intelligence
- CYBR 7300: Management of Cybersecurity
- CYBR 7350: Contingency Planning and Response
- CYBR 7400: Introduction to Cryptography and Its Application
- CYBR 7910: Capstone in Cybersecurity Practicum
  or
  CYBR 7930: Capstone in Cybersecurity Management

Program Total (30 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=55&navoid=4084 and select CYBR from the prefix menu.

Bachelor of Science in Information Technology with the Cyber Operations Security Concentration

The Bachelor of Science in Information Technology has a Cyber Operations Security concentration for students interested in serving as IT professionals with the ability to migrate to security positions later in their career. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6290 for the 2021 catalog.

Program Description

The Bachelor of Science in Information Technology degree has the primary objective of meeting the high demand for professional degrees in the strategy, development and administration of integrated computing, management, and information technology systems. The degree has core requirements, major requirements and required electives. The major contains those courses considered fundamental to the information technology field and the electives give the student some flexibility in choice.

General Education Core Curriculum (Areas A-E) (42 Credit Hours)

Lower Division Major Requirements (Area F) (18 Credit Hours)

- CSE 1321: Programming and Problem Solving I
- CSE 1322: Programming and Problem Solving II
- CSE 1321L: Programming and Problem Solving I Laboratory
- CSE 1322L: Programming and Problem Solving II Laboratory
- CSE 2300: Discrete Structures for Computing
  or
  MATH 2345: Discrete Mathematics
- TCOM 2010: Technical Writing
- STAT 2332: Probability and Data Analysis

Major Requirements (40 Credit Hours)

- CSE 3153: Database Systems
- CSE 3801: Professional Practices and Ethics
- IT 3003: Professional Development & Entrepreneurship
- IT 3123: Hardware and Software Concepts
- IT 3203: Introduction to Web Development
- IT 3223: Software Acquisition and Project Management
- IT 3423: Operating Systems Concepts & Administration
- IT 3883: Advanced Application Development
- IT 4323: Data Communications & Networking
- IT 4683: Management of Information Technology and Human Computer Interaction
- IT 4723: IT Policy and Laws
- IT 4823: Information Security Administration & Privacy
- IT 4983: IT Capstone

Upper Level Concentrations (15 Credit Hours)

All BSIT students are required to take a minimum of 15 credit hours in an upper-level concentration. They choose one of the four concentrations and complete any 4 of the courses listed for that concentration. The 5th course in the concentration can be a course from that same concentration or one of the other concentrations or IT Special Topics course or CSE Internship course.

Cyber Operations Security Concentration

Complete any four courses for a total of 12 credit hours from the following:

- IT 4833: Wireless Security
- IT 4843: Ethical Hacking for Effective Defense
- IT 4853: Computer Forensics
- IT 4863: Web and Mobile Application Security
- IT 4883: Infrastructure Defense
- IT 4893: Internet of Things: Applications and Security

5th Course Option - The 5th course can be any Cyber Operations Security concentration course not already elected or one of the following:

- CSE 4983: CSE Computing Internship
- IT 3503: Foundations of Health Information Technology
- IT 3703: Introduction to Data Analytics and Technology
- IT 4153: Advanced Database
- IT 4333: Network Configuration & Administration
- IT 4403: Advanced Web and Mobile Applications
- IT 4603: Introduction to Blockchain Technologies
- IT 4673: Virtual IT Systems
- IT 4713: Business Intelligence Systems
- IT 4490: Special Topics in Information Technology
- IT 4493: IT Undergraduate Research

Free Electives (5 Credit Hours)

Program Total (120 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select IT (or other prefix) from the prefix menu.

Bachelor of Science in Computer Science with the Cyber and Network Security Concentration

The computer science degree in the College of Computing and Software Engineering has added a security concentration to its offerings. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6193 for the 2021 catalog.

Program Description

The Bachelor of Science with a major in Computer Science program (BSCS) provides a blend of the foundations of computer science (CS) and applications in the information technology (IT) industry. The BSCS program emphasizes the study of computer systems architecture, software development, and data communications. Core technology areas include programming, computer architecture, operating systems, data communication, database systems, and software engineering. These areas are supported by a strong foundation in computing principles such as the design of programming languages, data structures, and operating system principles. The program includes a mathematics component and mathematics concepts are incorporated into many of the major courses.

General Education Core Curriculum (Areas A-E) (42 Credit Hours)

Lower Division Major Requirements (Area F) (18 Credit Hours)

- CSE 1321: Programming and Problem Solving I
- CSE 1321L: Programming and Problem Solving I Laboratory
- CSE 1322: Programming and Problem Solving II
- CSE 1322L: Programming and Problem Solving II Laboratory
- MATH 2202: Calculus II
- MATH 2345: Discrete Mathematics
- TCOM 2010: Technical Writing

Major Core Requirements (40 Credit Hours)

- CS 3305: Data Structures
- CS 3503: Computer Organization and Architecture
- CS 3502: Operating Systems
- SWE 3313: Introduction to Software Engineering
- CS 3410: Introduction to Database Systems
- CS 4306: Algorithm Analysis
- CS 3622: Fundamentals of Data Communications
- CS 4504: Parallel and Distributed Computing
- CS 4308: Concepts of Programming Languages
- CSE 3801: Professional Practices and Ethics
- CS 4850: Computer Science Senior Project
- STAT 2332: Probability and Data Analysis
- MATH 3260: Linear Algebra I

Major Electives (15 Credit Hours)

Cyber and Network Security Concentration (15 Credit Hours)

Required Courses (12 Credit Hours)

- CS 3626: Cryptography
- CS 4612: Software Security
- CS 4622: Computer Networks
- CS 4626: Computer and Network Security

Elective (3 Credit Hours) Choose One:

- CS 4491: Advanced Topics in Computer Science (in concentration)
- CS 4492: Undergraduate Research
- CSE 4983: CSE Computing Internship (in concentration)
- IT 4823: Information Security Administration & Privacy
- IT 4833: Wireless Security
- IT 4843: Ethical Hacking for Effective Defense
- IT 4853: Computer Forensics
- IT 4883: Infrastructure Defense

Free Electives (5 Credit Hours)

Program Total (120 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select CS (or other prefix) from the prefix menu.

Master of Science in Information Systems

The MSIS degree offered in the Michael J. Coles College of Business has an integral concentration of three security courses. The MSIS course were among the first security courses offered at KSU in 2000 as special topics. These courses are also part of the Graduate ISA Certificate. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=55&poid=6450 for the 2021 catalog.

Program Description

Coles MSIS teaches analysis, scoping and controlled use of business data and technology to refine processes, optimize decisions, and implement strategies to derive business value. Working professionals benefit from the hybrid nature of delivery and the flexible pace of study. Full time students benefit from professionally experienced professors and real-life opportunities for projects and industry engagements. Coles MSIS welcomes all majors and degrees from undergraduate education. The program also offers opportunity for an MBA-MSIS dual degree and an embedded graduate certificate in Information Security and Assurance for students.

The MSIS program teaches scoping, choice, assessment, deployment, management and secured use of information and computing technologies in the way they bring value to an organization with special emphasis on the following areas:

- Data Management and Business Intelligence Including Big Data
- Information Security Risk Management
- System Analysis and Design
- IT Project Management
- IT Strategy

Students take the same set of 10, 3-credit courses to complete the program within one calendar year.

Required Courses (30 Credit Hours)

- IS 7005: Informatics
- IS 7060: Information Systems Development Methods and Technologies
- IS 7080: Database Application Design and Implementation
- IS 7100: Advanced IT Project Management
- *IS 7200: Legal and Ethical Issues in Information Systems*
- *IS 7310: Governance, Risk Management, and Compliance*
- *IS 7320: Information Security Technologies*
- *IS 7330: Disaster Recovery/Business Continuity Planning*
- IS 7920: IT Customer Relationship Management
- IS 7935: Business Intelligence - Traditional and Big Data Analysis

Program Total (30 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=55&navoid=4084 and select IS from the prefix menu.

Information Security and Assurance Undergraduate Certificate - Stand-Alone

Offered by the Department of Information Systems and Security, the Undergraduate ISA certificate provides students with a stand-alone credential they can complete independent of any other degree program. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6222 for the 2021 catalog.

Program Description

The Certificate in Information Security and Assurance is designed for students with an interest in Information Security and its application in the expanding field of technology. The certificate program emphasizes the skills and knowledge necessary to protect and inspect systems, and to detect and react to threats to the security of information in those systems.

This certificate can not be awarded to students who earn the BBA with a major in Information Security and Assurance or the BS with a major in Cybersecurity.

Required Courses (15 Credit Hours)

- ISA 3100:Principles of Information Security
- ISA 3200:Network Security
- ISA 3210:Client Systems Security
- ISA 3300:Management of Information Security in a Global Environment
- ISA 4330:Incident Response and Contingency Planning

Program Total (15 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select ISA from the prefix menu.

Cybersecurity Undergraduate Certificate - Stand-Alone and Embedded

The Cybersecurity Certificate is offered through the Institute for Cybersecurity Workforce Development. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6374 for the 2021 catalog.

Program Description

The Certificate in Cybersecurity is designed for students with an interest in the security of computer networks and systems and its application in the expanding field of technology. The certificate program emphasizes the skills and knowledge necessary to protect and inspect systems, and to detect and react to threats to the security of information in those systems.

The certificate requires 15 semester hours (5 courses), and all coursework must be completed with a "C" or better.

Required Courses (15 Credit Hours)

- CSE 1321: Programming and Problem Solving I
- CSE 1321L: Programming and Problem Solving I Laboratory
- CYBR 3100: Principles of Cybersecurity
- CYBR 3200: Network Security
- CYBR 3210: Client Systems Security
- CYBR 3300: Management of Cybersecurity in a Global Environment

Program Total (15 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select CYBR from the prefix menu.

Information Security and Assurance Graduate Certificate

The graduate certificate program in information security and assurance is designed for both working professionals and graduate students. Students learn IT security technology through a hands-on virtual lab. Traditional classes teach how to secure and manage IT resources and how to plan, provide and manage system security incidents and disasters. Students also learn IT ethics and legalities including corporate and regulatory compliance in terms of methods, approaches, and governance.

Courses required for certificate: (12 Credit Hours)

Security Management

- IS 7310: Governance, Risk Management, and Compliance
  OR
  IT 6823: Information Security Concepts and Administration

Security Technology

- IS 7320: Information Security Technologies

Contingency Planning

- IS 7330: Disaster Recovery/Business Continuity Planning

Elective

- IS 7200: Legal and Ethical Issues in Information Systems
  OR
  IS 7305: Foundations of Information Security

Program Total (12 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=55&navoid=4084 and select IS from the prefix menu.

Information Technology Security Graduate Certificate

This certificate program is offered by the Department of IT, College of Computing and Software Engineering. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=55&poid=6522 for the 2021 catalog.

Program Description

The Graduate Certificate in Information Technology Security Program is designed for individuals to advance their knowledge and career options in the field of information security. The certificate program focuses on fundamental principles of securing networks and computer systems, hands-on experience with configuration, design, development and administration of security tools, and an awareness of industry best practices. Graduates from the program will build a strong foundation in pursuing a career in the information security field. The certificate can be taken as a stand-alone program or embedded as part of the Master of Science in Information Technology program.

Required Course (3 Credit Hours)

- IT 6823: Information Security Concepts and Administration

Elective Courses (9 Credit Hours)

Choose any three courses from the following:

- IT 7303: Data Privacy Technologies
- IT 7313: Physical IT Systems Security
- IT 7333: Enterprise Cloud and Wireless Security
- IT 7323: Computer Forensics
- IT 7343: Ethical Hacking: Network Security and Penetration Testing
- IS 7330: Disaster Recovery/Business Continuity Planning

Program Total (12 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=55&navoid=4084 and select IT (or IS) from the prefix menu.

Information Security and Assurance Minor

This program is offered by the Department of ISS, Michael J. College of Business. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6223 for the 2021 catalog.

Program Description

The Minor in Information Security and Assurance is designed for students with an interest in Information Security and its application in the expanding field of technology. The Minor emphasizes the skills and knowledge necessary to protect and inspect systems, and to detect and react to threats to the security of information in those systems. The Minor requires 18 semester hours (6 courses), and all coursework must be completed with a grade of "C" or higher.

Required Courses (15 Credit Hours)

- IS 2200: Information Systems and Communication
- ISA 3100: Principles of Information Security
- ISA 3200: Network Security
- ISA 3210: Client Systems Security
- ISA 3300: Management of Information Security in a Global Environment

Select one of the following (3 Credit Hours)

- ISA 4200: Perimeter Defense
- ISA 4220: Server Systems Security

Program Total (18 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select ISA from the prefix menu.

Cybersecurity Minor

The Cybersecurity minor is offered through the Institute for Cybersecurity Workforce Development. Visit http://catalog.kennesaw.edu/preview_program.php?catoid=54&poid=6375 for the 2021 catalog.

Program Description

The Minor in Cybersecurity addresses students with an interest in the application of information security controls on information systems. The Minor emphasizes the skills and knowledge necessary to defend networks and systems, and to detect and react to threats to those systems.

The Minor requires 18 semester hours (6 courses), and all coursework must be completed with a grade of "C" or higher.

Required Courses (18 Credit Hours)

- CSE 1321: Programming and Problem Solving I
- CSE 1321L: Programming and Problem Solving I Laboratory
- CYBR 3100: Principles of Cybersecurity
- CYBR 3200: Network Security
- CYBR 3210: Client Systems Security
- CYBR 3300: Management of Cybersecurity in a Global Environment
- CYBR 4330: Incident Response and Contingency Planning

Program Total (18 Credit Hours)

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3997 and select CYBR from the prefix menu.

Instructional Support Materials

In addition to the International Standards and Special Publications described earlier, there are an increasing number of materials which can support the design, development and instruction of various security topics.

Security Textbooks

There are a variety of academic textbooks currently available from various publishers. This was not always the case. As mentioned previously, back in 2000 when we began developing our first security courses, we were forced to use trade press books, and NIST Special Publications. Thus Drs. Whitman and Mattord began authoring texts just to have an academic suite of books to use in the various courses.

Over the years, the following texts have been written and used in course. Unfortunately, some were so niche, they have fallen behind in priority for the publisher. Some are part of a request by the authors to obtain the IP from the publisher to consider independent publication. The two flagship texts: Principles of Information Security and Management of Information Security are moving steadily forward and have been adopted by over 700 institutions globally.

Textbooks currently available from Cengage Learning:

- Principles of Information Security, 7th Edition (forthcoming late 2021), Whitman & Mattord https://www.cengage.com/c/principles-of-information-security-7e-whitman/9780357506431PF/
- Management of Information Security, 6th Edition (2020) Whitman & Mattord - https://www.cengage.com/c/management-of-information-security-6e-whitman/9781337405713PF
- Principles of Incident Response and Disaster Recovery, 3rd Edition (2020) Whitman & Mattord - https://www.cengage.com/c/principles-of-incident-response-and-disaster-recovery-3e-whitman/9780357508329PF

Older texts still available from Cengage Learning

- Hands-On Information Security Lab Manual, 4th Edition (2014) – Whitman, Mattord & Green - https://www.cengage.com/c/hands-on-information-security-lab-manual-4e-whitman/9781285167572PF/
- Guide to Network Security, 1st Edition (2013) – Whitman, Mattord, Mackey & Green - https://www.cengage.com/c/guide-to-network-security-1e-whitman/9780840024220PF/
- Guide to Firewalls and VPNs, 3rd Edition (2012) – Whitman, Mattord & Green - https://www.cengage.com/c/guide-to-firewalls-and-vpns-3e-whitman/9781111135393PF

Other texts formerly available from Cengage Learning (some are still available through third-party vendors)

- Readings and Cases in the Management of Information Security (2005) – Whitman & Mattord
- Readings and Cases in Information Security: Law and Ethics (2011) – Whitman & Mattord
- Roadmap to Information Security for IT and InfoSec Managers (2011) – Whitman & Mattord

If you would like additional information on these books (i.e. how well they worked in the class, or what support materials are included) please contact us. All Cengage Learning texts include instructor's ancillaries including PowerPoint slide shows, text banks, and instructor's guides. The MindTap editions also include supplemental learning materials, videos, vignettes and additional instructor support.

The Next Step: The Curriculum Development Project: Design Revision and External Evaluation

We are continually working to further design, revise, and seek external review of the curriculum model. It is our intent to obtain outside input on this model, and additional insight as to the quality of the learning objectives, course content and supporting materials needed to complete the curriculum model, as well as further explore knowledge areas.

Questions remaining include:

- What areas should be emphasized in a technical program vs. a managerial program vs. a balanced program?
- What other courses should be added to each area, and what should they entail?
- Are the proposed levels of knowledge appropriate or should additional depth be pursued?
- Are there sub-domains below the major and minor topics listed?

To answer these questions, we must consult with other experts in the field and obtain their insight. We plan to take the preliminary implementation and draft curriculum model to our peers for commentary. Your feedback will be used to further shape our annual security curriculum development workshop, held in conjunction with the ICWD Conference on Cybersecurity Education, Research, and Practice (https://cyberinstitute.kennesaw.edu/ccerp/index.php and https://digitalcommons.kennesaw.edu/ccerp/). This conference focuses on pedagogy and practice of security education, held annually in October at KSU. Look for the CFP in March/April, with the conference announcement going out in May. Contact us if you don't hear by then at infosec@kennesaw.edu.

We will continually synthesize all inputs and commentary from the workshop at CCERP and continue to refine the final model as a report sponsored by the KSU ICWD.

Broader Impacts of This Proposal

The ultimate purpose of the curriculum development project is to assist in the advancement of information security education in the country. We feel that many schools are struggling with the same problems that organizations are, in understanding what is needed to support the security of information, and what skills and qualifications are needed in a quality information security applicant. The core of this project is to improve education, by assisting instructors in understanding what must be taught. It seeks to enhance and support educational infrastructure, by providing a curriculum model that provides structure and guidance in the implementation of this critical coursework. Many instructors will be able to master the basics of organizational policy, planning, and staffing. The technical components of any curriculum are often the most difficult to master. A framework for the instruction of this technical content will provide strong guidance on the instruction of a wide variety of technical security components. Society will benefit as more qualified security personnel are created, improving the level of security of personal information in organizations around the country.

How you can help

This draft curriculum model is an ongoing effort to improve information security curriculum. Through our presentations and discussion across the US, we have spoken with a number of faculty members, all eager to learn about developing and implementing information security curriculum. You can help us in two ways:

1. Provide critical but constructive reviews of the curriculum model and materials presented here: Ask yourself the following questions:
   - Do the recommendations of this model seem comprehensive, robust and scalable? Why or why not?
   - Do the recommendations of this model follow established curriculum development guidelines?
   - Do the recommendations of this model work within established curriculum models for technology (or non-technology) programs?
   - What could be improved in this model?
2. Let us know you like or are using the curriculum model. Send us a letter on letterhead supporting the curriculum model developed. Your indication of support will be used in subsequent grant activities designed to improve the curriculum model.

Appendix: Security Curriculum Development Procedures for use at your institution:

I. Determine interest, scope and intent of the program.

Discuss within your department the desired scope and outcomes of a program in Information Security. At this point simply get buy-in that two or more courses in Information Security are desirable. If a concentration, specialization, certificate, or degree program is desired, additional information will be required.

Scope:

General Outcomes:

II. Determine stakeholder interest and guidance.

Organize a meeting with interested stakeholders, including industry representative of potential employers, alumni, students, and faculty. Obtain their general perception of the idea of courses/programs in Information Security. It may be useful to anonymously survey their opinions. Questions to ask could include:

1) Do you feel the department should consider another program? Why or why not?

2) Do you feel that graduates with coursework/certificate/degree in Information Security would be valuable to regional employers? Why or why not?

3) If the department should consider offering this program, what skills do you feel that the student should possess upon graduation?

Summarize the responses.

III. Form the curriculum development committee.

Form a working committee to begin determining the specific focus, objective, depth, etc of the program. Research the field of potential jobs in your area in Information Security. This information will assist in the selection of the focus of the program. Include the feedback from Step II. Identify available resources in terms of labs, faculty, and course offerings.

IV. Map desired positions to knowledge areas.

Using the methods outlined in the document, fill in the following table. Feel free to add/remove blanks as needed. If you feel the table in the document is satisfactory as completed go to the next step.

1) Only include the positions you want your students to be able to perform after they complete the program.

2) Include the Roles these positions map based on the definitions earlier.

3) Identify the knowledge areas that correspond to these roles. Use the materials provided earlier as a template. Do not try to map mastery levels yet.

V. Discuss the following constraints on the program.

The following questions should be discussed:

1) What should the focus of the courses/program be? Managerial, Technical, or Balanced?
2) How many courses in Information Security can we offer in this program?

3) What courses, that we currently offer, could be included or adapted to support this program?

If in answering question 1, the institution desires a security program but just hasn't made up its mind as to which emphasis it wishes to take, the following set of program objectives may assist. The following list of program objectives can be used to determine what focus you desire for your program. Check off the objectives you want graduates of your program to meet, or rather what qualities should your students possess upon graduation. Use caution, as it is our first tendency to check everything! Realize that this may not be feasible unless you are able to implement an entire degree program with 7 or more courses exclusively in Information Security related areas.

Once you have checked all desired qualities, the section immediately following the list will provide guidance on what type of program may be best suited for your desired outcomes.

Upon completion of the program the student will have the following qualities (Check all that apply):

[ ] 1. The graduate has a thorough understanding of the types and uses of Information Security policies, and can create examples bases on established frameworks.

[ ] 2. The graduate is able to recognize, define and implement firewall-related solutions to appropriate threats.

[ ] 3. The graduate possesses a detailed understanding of the process of organizational planning for information security at strategic, tactical and operational levels.

[ ] 4. The graduate possesses knowledge, skill and technical depth in implementing cryptographic solutions using appropriate methods, techniques and tools such as PKI and VPNs.

[ ] 5. The graduate has the ability to critically analyze and articulate positions on the legal and ethical implications and influences of Information Security, including relevant codes of ethics and federal and state laws.

[ ] 6. The graduate possesses the ability to evaluate a given computer operating system and implement "hardened" security measures to protect it.

[ ] 7. The graduate has detailed knowledge of the types, organization, responsibilities and qualifications of Information Security personnel in an organization..

[ ] 8. The graduate has the ability to conduct an effective vulnerability assessment of an organizations Information Security posture and report their findings in a meaningful format.

[ ] 9. The graduate can implement a risk management program including a detailed risk assessment, and recommend appropriate risk control strategies and measures.

[ ] 10. The graduate can articulate the composition of popular security models such as BIBA, Bell LaPadula, etc.

[ ] 11. The graduate can develop and manage plans for dealing with organizational contingencies such as incidents and disasters.

[ ] 12. The graduate can evaluate and recommend effective security architectures using security technologies, such as bastion hosts, screened subnets and demilitarized zones.

[ ] 13. The graduate can develop, implement and manage security programs designed to improve employee perception of information security, such as security education, training and awareness programs.

[ ] 14. The graduate is able to recognize, define and implement intrusion detection systems- based solutions to appropriate threats, including both host and network IDS.

[ ] 15. The graduate can evaluate and recommend improvements to the implementation of security procedures in handling personnel in the organization, including hiring, termination, and contract employee issues.

[ ] 16. The graduate is able to evaluate, define and implement defenses against malicious code attacks such as viruses, worms and denial of services.

[ ] 17. The graduate can critically discuss popular information security management practices, standards and models such as ISO 17799, NIST SPs 14 & 18, etc.

[ ] 18. The graduate is able to evaluate, define and implement defenses as part of counter intrusion measures against active and passive hacker attacks.

[ ] 19. The graduate has the ability to conduct Cost/Benefit Analyses on proposed security countermeasures and present to organizational stakeholders in a meaningful manner.

[ ] 20. The graduate is able to evaluate, define and implement effective access controls technologies and procedures in accordance with organizational policy.

Now that you have specified the desired learning outcomes for your program, add up the number of checks by ODD and EVEN answers. If you find substantially more checks by ODD numbers, say 3 or more, then your inclination is toward a managerial program. If you find substantially more checks by EVEN numbers, again 3 or more, then your inclination is toward a managerial program. If your two values are approximately equal (within 2 or fewer) your inclination is toward a balanced program. If you have a total of more than 16 checks in total, you are either very ambitious or desire a balanced program with an emphasis toward one or the other area.

Balance this information with the feedback obtained in step II.

VI. Define program objectives.

From the list above, and the information you have gathered and analyzed, identify the 6-10 program objectives that best map to what you want your students to have achieved upon completion of the material. You can use the list of 20 program objectives in Step V as a starting point.

VII. Determine the level of mastery desired in the program.

Based on desired level of mastery and focus of class determine the level of mastery desired. Perform this exercise within your program using the blank form. Using the following table as a starting point, you can add additional columns to represent additional courses to be added providing additional depth in managerial or technical areas. Also feel free to add or delete specific domain and knowledge area based on your findings in your curriculum efforts.

When finished, take a moment to verify that what you have just created matches the Management vs. Technical exercise created earlier. If you find you did not fill in many technical areas with desired depth beyond U (i.e. A or P) and yet you specified a technical program earlier, you may want to revisit one or both of these activities to determine your preferred path.

VIII. Determine the number of courses to offer.

Based on the constraints in Step V. List the number of courses you can offer in your program. Consider the following table in your decision, influence by the focus of your program (managerial vs technical).

IX. Determine the Prerequisite knowledge areas necessary to support the desired classes.

Using the following form as an example, list the classes desired in the middle, the knowledge to be taught in that class on the right, and then determine what a student should know coming into the class on the left. Then match that information to existing courses offered in the institution. If a prerequisite knowledge is needed but not currently taught, it may need to be added to the program.

X. Develop specific course learning objectives.

Now that the individual courses are becoming defined it is time to define the specific learning objectives that will go into each course. You can use the examples provides as a starting point.

1) Begin by using syllabi templates and adding other required components.

2) Add learning objectives

3) Select textbooks

4) Define evaluation methods

XI. Define laboratory components and required resources.

For each course identify any desired laboratory exercises. You can use the table of contents for the lab manual listed earlier for ideas.

For each exercise define what hardware and software components will be required.

Compare to an inventory of on-hand resources. If a desired resources is not available, determine if it can be acquired prior to the formal offering of the class, else look for alternatives. I find there is a substantial set of shareware/hackerware that is readily available and suitable for exercises. It's the name-brand hardware that tends to be difficult and expensive to acquire. Consider contacting industry advisors and "friends of the department" for contributions.

XII. Pilot test key courses.

Select a few key faculty members with experience in information security to pilot test individual courses.

Collect information on student satisfaction and performance in the various areas of each course.

XIII. Refine and revise as needed.

Self-explanatory.

About the Authors

Michael E. Whitman, Ph.D., CISM, CISSP is a Professor of Information Security and Assurance in the Information Systems Department, Michael J. Coles College of Business at Kennesaw State University, Kennesaw, Georgia, where he is also the Executive Director of the KSU Center for Information Security Education (infosec.kennesaw.edu). Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, Ethical Computing, and Curriculum Development Methodologies. He currently teaches graduate and undergraduate courses in Information Security Management. He has published articles in the top journals in his field, including Information Systems Research, Communications of the ACM, Information and Management, Journal of International Business Studies, and Journal of Computer Information Systems. Dr. Whitman is also the Co-Editor-in-Chief of the Journal of Cybersecurity Education, Research and Practice. He is a member of the Information Systems Security Association, the Association for Computing Machinery, and the Association for Information Systems. Dr. Whitman is also the co-author of Management of Information Security, Principles of Incident Response and Disaster Recovery, Readings and Cases in the Management of Information Security, The Guide to Firewalls and VPNs, The Guide to Network Security, and The Hands-On Information Security Lab Manual, among others, all published by Cengage. Prior to his career in academia, Dr. Whitman was an Armored Cavalry Officer in the United States Army, which included duties as Automated Data Processing Systems Security Officer (ADPSSO).

Herbert J. Mattord, Ph.D., CISM, CISSP completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner before joining the faculty of Kennesaw State University in 2002. Dr. Mattord is the Director of Education and Outreach for the KSU Institute for Cybersecurity Workforce Development (cyberinstitute.kennesaw.edu). Dr. Mattord is also the Co-Editor-in-Chief of the Journal of Cybersecurity Education, Research, and Practice. During his career as an IT practitioner, he has been an adjunct professor at Kennesaw State University, Southern Polytechnic State University in Marietta, Georgia, Austin Community College in Austin, Texas, and Texas State University: San Marcos. He currently teaches graduate and undergraduate courses in Information Security and Cybersecurity. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this textbook was acquired. Dr. Mattord is also the coauthor of Management of Information Security, Principles of Incident Response and Disaster Recovery, among others, all published by Cengage.

References:

---

[1] Pfleeger, C. and Cooper, D. “Security and Privacy: Promising Advances.” IEEE Software. 09/1997. 27-32.
[2] “Data Breaches” https://www.identityforce.com/blog
[3] NIST NICE “Cybersecurity Workforce Demand”
https://www.nist.gov/system/files/documents/2019/02/07/workforce_demand_111617_final.pdf
[4] Chin, S-K, Irvine, C.E., & Frinke, D. “An Information Security Education Initiative for Engineering and Computer Science.” Naval Postgraduate School Technical Report, NPSCS-97-003. Naval Postgraduate School, Monterey, CA. 12/1997.
[5] Irvine, C., Chin S-K., & Frincke, D. “Integrating Security into the Curriculum.” Computer. 31(12). 12/1998. 25-30.
[6] NSA/CSS. “National Centers of Academic Excellence in Cybersecurity (NCAE-C)” Viewed 03/15/2021 from
https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.
[7] “The National Strategy to Secure Cyberspace,” Viewed 03/15/2021 from https://georgewbush-whitehouse.archives.gov/pcipb/.
[8] The Comprehensive National Cybersecurity Initiative. Viewed 03/15/2021 from
https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
[9] ABET. “Criteria for Accrediting Computing Programs, 2021 – 2022” Viewed 03/15/2021 from
https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2021-2022/.
[10] JTF on Cybersecurity Education “Cybersecurity Curricula Guidelines” Viewed 03/15/2021 from
https://cybered.hosting.acm.org/wp/.
[11] JTF on Cybersecurity Education “Cybersecurity Curricula 2017” Viewed 03/15/2021 from https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.
[12] ACM, AIS & AITP. “IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems.” Viewed 03/15/2021 from https://aisel.aisnet.org/cais/vol11/iss1/1/.

[13] Chin, S-K, Irvine, C.E., & Frinke, D. “An Information Security Education Initiative for Engineering and Computer Science.” Naval Postgraduate School Technical Report, NPSCS-97-003. Naval Postgraduate School, Monterey, CA. 12/1997.
[14] Hutton, G. “Backward Curriculum Design Process” WWW Document. Viewed 5/1/2003. http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11_03.pdf.
[15] Whitman, M. and Mattord, H., Principles of Information Security, 7th Edition, 2021, Cengage Learning.
[16] Petersen, R., Santos, D., Smith, M., Wetzel, K., and Witte, G. NIST SP 800-181 Workforce Framework for Cybersecurity (NICE Framework) Viewed 03/15/2021 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.
[17] Bloom, B. S.; Engelhart, M. D.; Furst, E. J.; Hill, W. H.; Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain. New York: David McKay Company.
[18] NIST NICE “About” Viewed 03/15/2021 from https://www.nist.gov/itl/applied-cybersecurity/nice/about.
[19] CompTIA “Security +” Viewed 03/15/2021 from https://www.comptia.org/certifications/security#exampreparation.
[20] CompTIA “CompTIA CySA+” Viewed 03/15/2021 from https://www.comptia.org/certifications/cybersecurity-analyst.
[21] ISO ISO/IEC 27002 (2013) Information Technology – Security Techniques – Code of Practice for Information Security Controls.
[22] ISO ISO/IEC 27002 (2013) Information Technology – Security Techniques – Code of Practice for Information Security Controls.
[23] USG. “High-Demand, Online Degrees through University System of Georgia Institutions” viewed 03/14/2021 from https://ecampus.usg.edu/.