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

Table of Contents

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 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. The 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 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 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 (JTFCE), 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
- Organizational 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

sim

Many programs take the short cut and jump straight to the certifications an information security professional could earn like: CISSP, SSCP, GIAC, Security+, 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 Cyber.9 (e)7.8 (nv)14 (,)2 (j60.003 Tw210.-1.5 ( )E-9 (D)1 (h)2.2 (e)-4 Tcnv)14 (,)2 (j60..444

- 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 (c)1.1 (es)12.6 (s)1.6 (es)1.-1.3 ( )10

- Exploitation Analysis (EXP-A): Analyzes collected information to identify vulnerabilities and potential for exploitation. Sample work roles: Exploitation Analyst
- All-Source Analysis (AS-A): 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

- 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 frCID 57 >>BDC /pan <</MCID 71 >>BDC006 Tw 1.03 (s)-1.4 (v)-5.

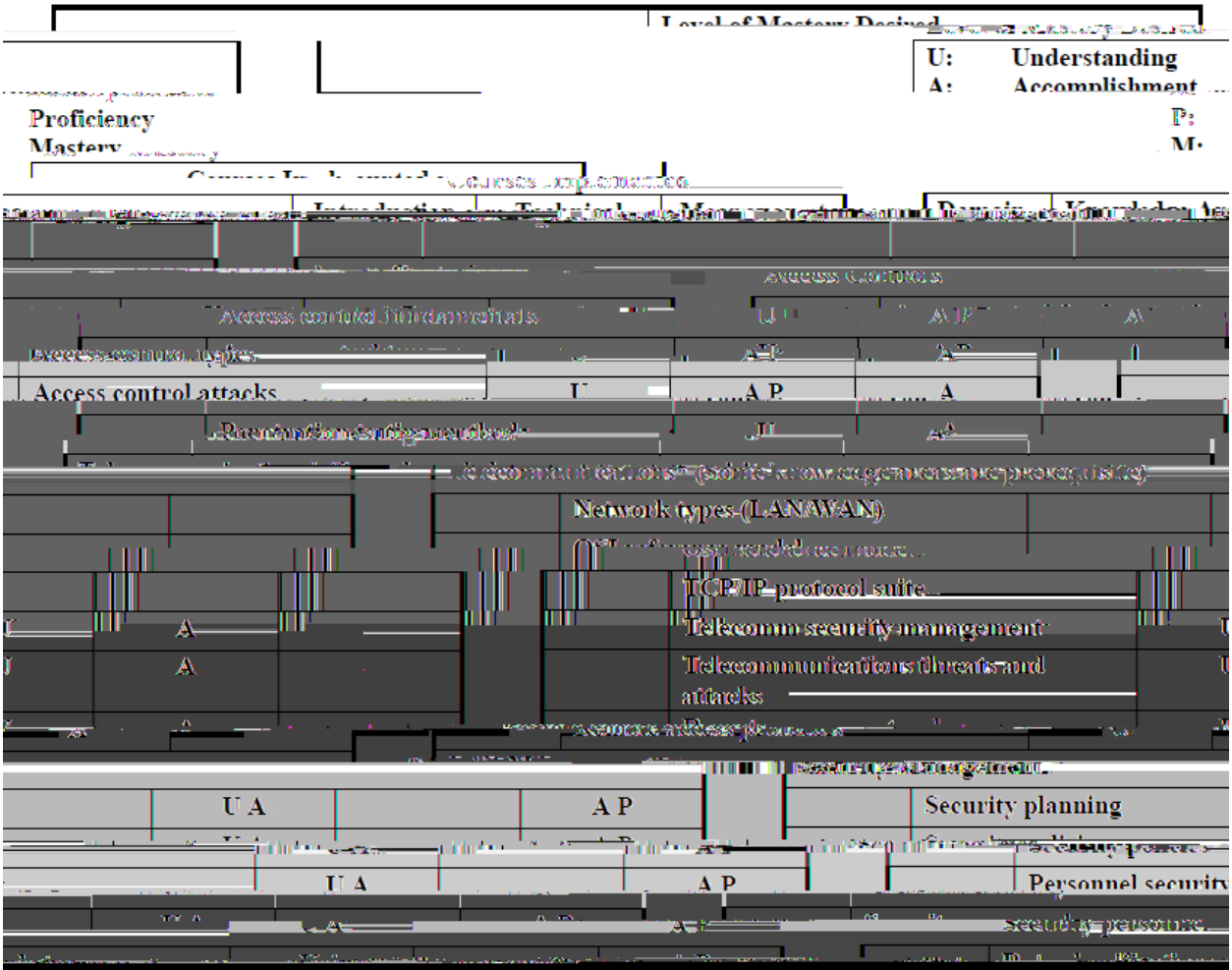
- SP 800-137A Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment
- SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-150 Guide to Cyber Threat Information Sharing
- SP 800-181 Rev. 1 Workforce Framework for Cybersecurity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

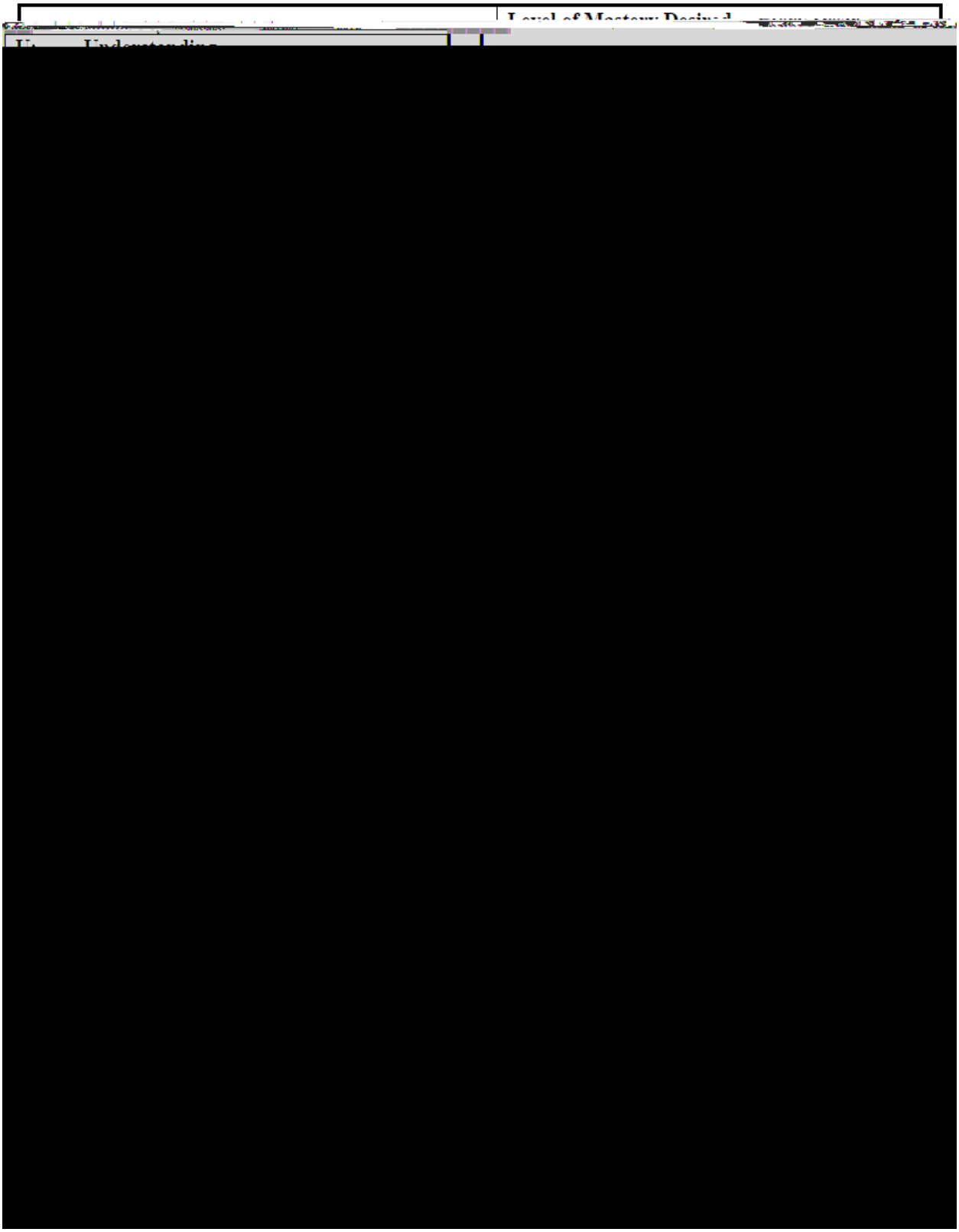
Mapping Positions and Roles to Knowledge Areas

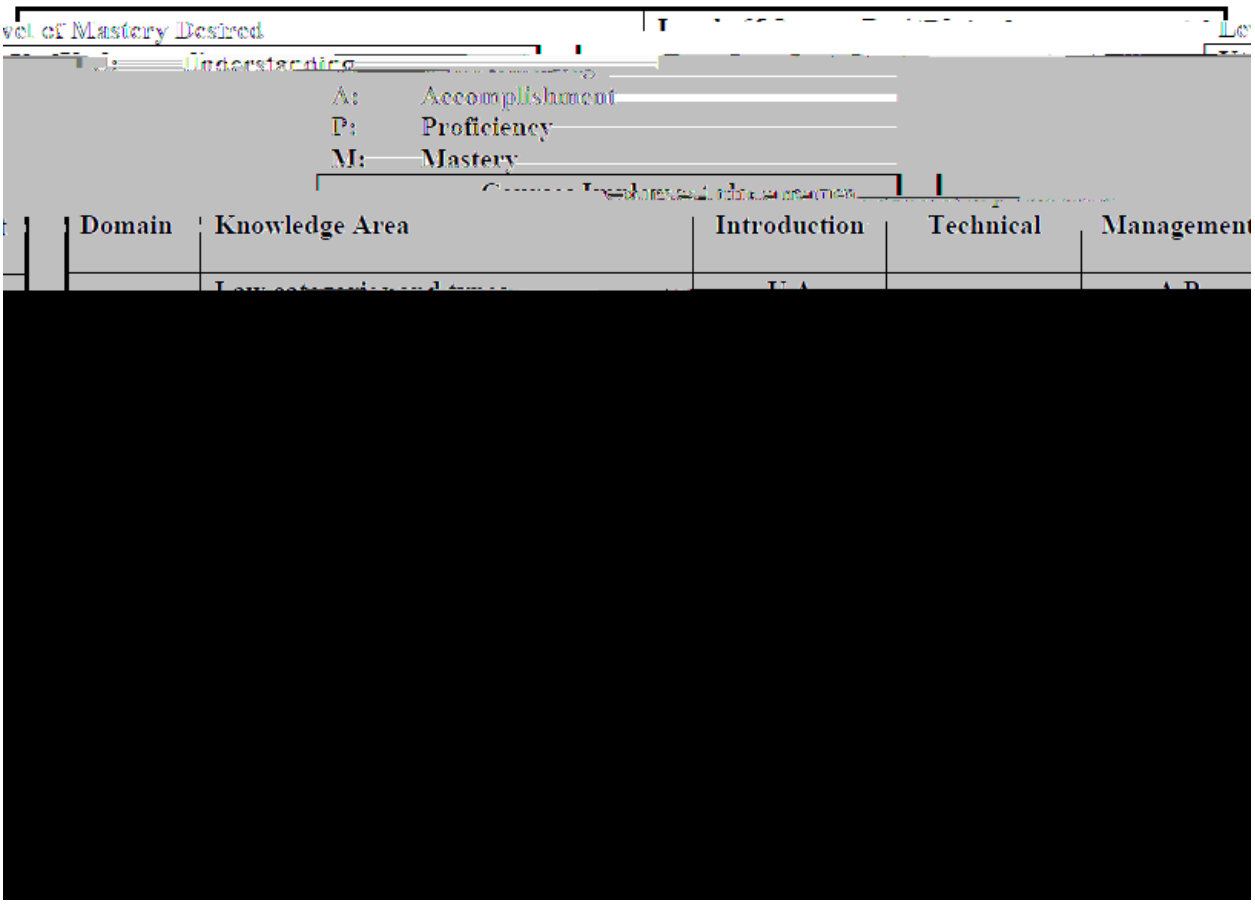
With this information the curriculum designers can gain a better feel for what a graduate should know upon graduating for a specific job category. The following figure illustrates this mapping.

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, our 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-

technical implementations are guided by the managers in security, but may not be able to develop these areas. Technical security


U: Understanding
Proficiency
Access control fundamentals
Access control types
Access control attacks
Network types (LAN/WAN)
TCP/IP protocol suite
Telecommunications threats and attacks
Security planning
Personnel security





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 in 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 student should be learning in each course. The 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 easily be 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 several 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 BSIS 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. At 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 hands-on and managerial functions. The certificate begins with three core courses:

- Principles of Information Security & Assurance: An introduction to the various technical and administrative aspects

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 other 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

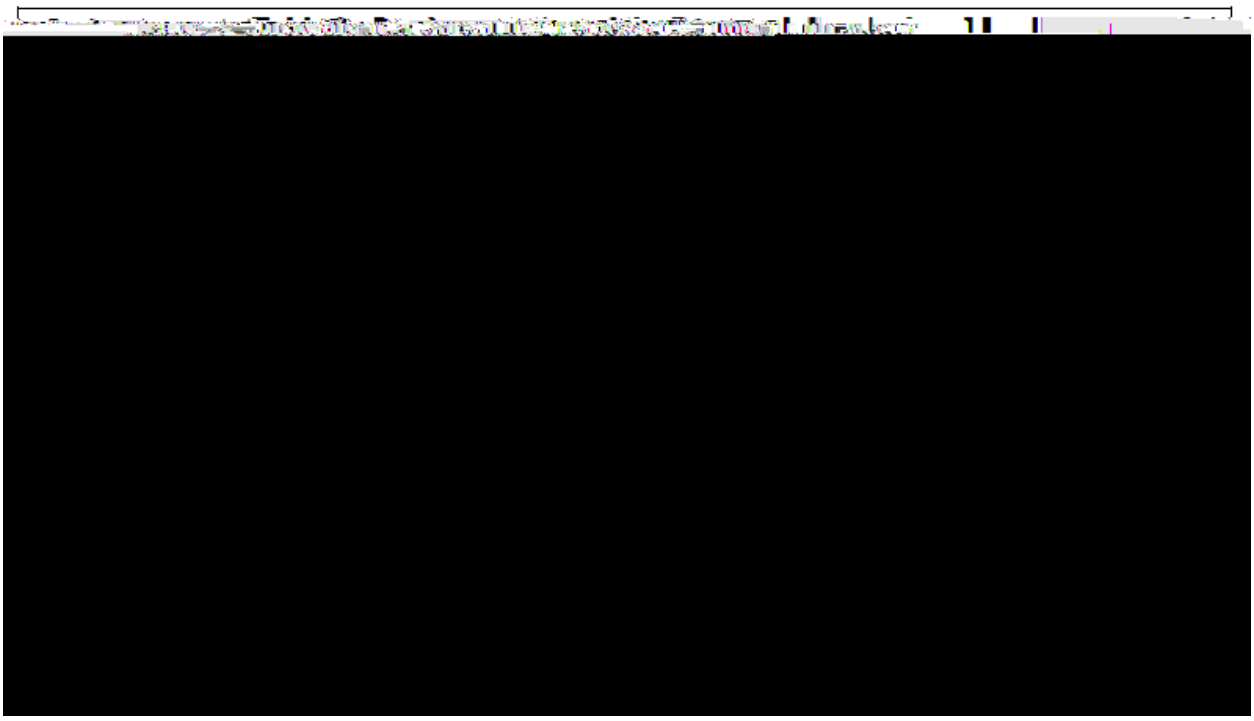
Development of the BS ISA was an arduous, drawn-out project. It actually began in 2001, when we drafted the Certificate in ISA. In fact, when the faculty proposed the ISA Certificate, we intentionally used a separate prefix (ISA) instead of the department standard (CIS) to prepare for the eventuality of a degree. Shortly after the certificate was implemented, we pulled up the oven and a separate prefix (ISA)

From the managerial side, we

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 near lack of academic texts to support the curriculum. As a result, we authored our own for

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.



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
-

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

- IS 2200 Information Systems and Communication

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

- 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 Operation Tw 0.489 27.4.9 (m)-9.4(a)-6 (n)-0.7 (t)]TJ 0 Tc 0 Tw 14.043 0 Td 0adissf Marketing

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 a Major – 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

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

- 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

- CYBR 4810 Cyber Defense

All BSCYBR 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

- 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

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

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

- 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 meet the prerequisites except certain specific restricted ISA or IT Security course (see an4T.2 (I.)-3 (e1)5-3.1 (v10.9 (it)-3 (rir)10.7 (4f)1.55rir)10.7 (46.6

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 al

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.

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 engagement. 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 fol (p)2.2 (e)-3 (c)5

Information Security and Assurance Undergraduate Certificate – Stand-Alone

Offered by the Department of Information Systems and Cybersecurity, 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=6232 for the 2021 catalog.

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 empha ( )-11.3 (p)2.3i2&(ts)1.7 (wi)13.6 2

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=6774 for the 2021 catalog.

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.

- CSE 1321: Programming and Problem Solving
- CSE 1321L:

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)

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

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

Information Security and Assurance Minor

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

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.

- 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

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

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.

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 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.

- 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

For course descriptions visit: http://catalog.kennesaw.edu/content.php?catoid=54&navoid=3927 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, D. 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 courses. 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

The Next Step: The Curriculum Development Project: Design Revision and Extern 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 subdomains 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.

How you can help

This draft curriculum model is an ongoing effort to improve information security curricu Through our presentations and discussion across th

Appendix: Security Curriculum Development Procedures fo

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 of 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 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 grae .[0.1 6oes 51.7 (es)12.6 ueo eP <<22.6 (r)3.e, 51.kogaeee endld detrheni8-6 i27m re(e)-6m6 (r4-6

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

[ ] 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 control logics 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. From your results, (

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)

About the Authors

Michael E. Whitman, Ph.D., CISM, CISSP is a Professor of Information Security and Assurance in the Information Syst Department, Michael J. Coles College of Business at Kennesaw State University, Kennesaw, Georgia, where he is also th 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 Computin 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 ... h)2.3 (is)9.5 (c)-17(L)-7)-3 (ri.3 ( )]Ti3 (lt)7.-6.7 (re)7(an)2.2 (ag)2.