MAPPING TO THE NSA KU'S – CAE APPLICATION

CAE APPLICATION PROCESS AND GENERAL CYBERSECURITY CURRICULUM DISCUSSION

Anne Kohnke, PhD
University of Detroit Mercy

AGENDA

- **Tamara Shoemaker, *Director Center for Cyber Security & Intel Studies***
  - **My Role with University of Detroit Mercy - Recertification Coordinator**
- **The New Academic Requirements**
- **The NIETP Online Application**
- **Information to Gather Beforehand**
- **Sample Syllabi**
- **The Application Components**
- **Discussion / Q & A**

NEW ACADEMIC REQUIREMENTS FOR CAE CD

- **11 Mandatory Knowledge Units (2YR)**
- **5 Additional Mandatory Knowledge Units (4YR)**
- **5 Optional (Actually, 4YR must have these)**
- **1 or more Focus Areas (truly optional)**
- **Letter of Designation**
- **8 Measurement Criteria**
- **NIETP online application submission**

NEW ACADEMIC REQUIREMENTS: CORE KNOWLEDGE UNITS (KU'S)

CORE Knowledge Units
(2 year programs)

- Basic Data Analysis
- Basic Scripting or Introductory Programming (4 yr core)
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

CORE Knowledge Units
(4 + year programs + 2 year core)

- Databases
- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

11 CORE KU's + **6 CORE KU's** for 4 year programs for a total of **17 KU's**

CAE_IA-CD_KU.pdf

Also, you must choose 5 Optional Ku's

17+5 = 22 KU's for 4 Yr

Plus, optional focus areas

Optional Knowledge Units

- Advanced Cryptography
- Advanced Network Technology and Protocols
- Algorithms
- Analog Telecommunications
- Cloud Computing
- Cybersecurity Planning and Management
- Data Administration
- Data Structures
- Database Management Systems
- Digital Communications
- Digital Forensics
  - Device Forensics
  - Host Forensics
  - Media Forensics
  - Network Forensics
- Embedded Systems
- Forensic Accounting
- Formal Methods
- Fraud Prevention and Management
- Hardware Reverse Engineering
- Hardware/Firmware Security
- IA Architectures
- IA Compliance
- IA Standards
- Independent/Directed Study/Research
- Industrial Control Systems
- Intro to Theory of Computation
- Intrusion Detection
- Life-Cycle Security
- Low Level Programming
- Mobile Technologies
- Network Security Administration
- Operating Systems Hardening
- Operating Systems Theory
- Overview of Cyber Operations
- Penetration Testing
- QA / Functional Testing
- RF Principles
- Secure Programming Practices
- Security Program Management
- Security Risk Analysis
- Software Assurance
- Software Reverse Engineering
- Software Security Analysis
- Supply Chain Security
- Systems Programming
- Systems Certification and Accreditation
- Systems Security Engineering
- Virtualization Technologies
- Vulnerability Analysis
- Wireless Sensor Networks

17 FOCUS AREAS (FA'S)

- **These are truly optional and an institution may differentiate itself by offering one or more Focus Areas (FA's)**

MEASUREMENT CRITERIA (0 – 8)

	0. Letter of Intent that Shows Eight Measurement Criteria				
	1. Outreach/Collaboration				
		a. Shared curriculum			
		Add links			
		Add pdf's			
		Justification for Selectd Criteria			
	2. Center for IA/CD Education				
		Add links/pdf's/justification for selected criteria			
	3. A Robust and Active IA/CD Academic Program				
		Add links/pdf's/justification for selected criteria			
	4. IA/CD is Multidisciplinary Within the Institution				
		Add links/pdf's/justification for selected criteria			
	5. Practice of IA Encouraged Throughout the Institution				
		Add links/pdf's/justification for selected criteria			
	6. Student-based IA/CD/Cybersecurity Research				
		Add links/pdf's/justification for selected criteria			
	7. Number of IA/CD/Cybersecurity faculty and course load				
		Add links/pdf's/justification for selected criteria			
	8. Faculty active in current IA/CD/Cybersecurity practice and research				
		Add links/pdf's/justification for selected criteria			

DATA GATHERING PROCESS

- **Start with the CAE Requirements and Resources link on the NIETP site**
- **A Guide for Mapping Courses to Knowledge Units (Ku's)**
- **New User Registration**
- **Identify and Update All Syllabi**

DATA GATHERING PROCESS

- **Obtain spreadsheet = *CAE_KU_Mapping_Matrix***
- **Obtain Mapping Guide (screen shots of online application)**
- **Determine what fields are necessary for online application**
- **Determine 5 Optional KU's**
- **Determine what courses to map the KU's**
- **Obtain Measurement Criteria = *CAE CD 4Yr Criteria – 2016***
- **Course Syllabi**

DATA GATHERING

	A	B	C	D	E
1	All links below take you to the datasheet for that KU.				
2	**Core 2Y Knowledge Units**		**Optional Knowledge Units**		
3		Basic Data Analysis	Advanced Cryptography	Hardware Reverse Engineering	Secure Programming Practices
4		Basic Scripting	Advanced Network Technology and Protocols	Hardware/Firmware Security	Security Program Management
5		Cyber Defense	Algorithms	IA Architectures	Security Risk Analysis
6		Cyber Threats	Analog Telecommunications	IA Compliance	Software Assurance
7		Fundamental Security Design Principles	Cloud Computing	IA Standards	Software Reverse Engineering
8		Information Assurance Fundamentals	Cybersecurity Planning and Management	Independent/Directed Study/Research	Software Security Analysis
9		Introduction to Cryptography	Data Administration	Industrial Control Systems	Supply Chain Security
10		Information Technology System Components	Data Structures	Intro to Theory of Computation	Systems Programming
11		Networking Concepts	Database Management Systems	Intrusion Detection	Systems Certification and Accreditation
12		Policy, Legal, Ethics and Compliance	Digital Communications	Life-Cycle Security	Systems Security Engineering
13		Systems Administration	Digital Forensics	Low Level Programming	Virtualization Technologies
14			Device Forensics	Mobile Technologies	Vulnerability Analysis
15	**Core 4Y Knowledge Units**		Host Forensics	Network Security Administration	Wireless Sensor Networks
16		Databases	Media Forensics	Operating Systems Hardening	
17		Network Defense	Network Forensics	Operating Systems Theory	
18		Network Technology and Protocols	Embedded Systems	Overview of Cyber Operations	
19		Operating Systems Concepts	Forensic Accounting	Penetration Testing	
20		Probability and Statistics	Formal Methods	QA / Functional Testing	
21		Programming	Fraud Prevention and Management	RF Principles	

Fig. 1 Main Sheet - 2014 CAE KU Mapping Matrix

BASIC DATA ANALYSIS

		Courses	ABC-123	DEF-456			
Click here to return to KU Listing			(Click Here) READ THIS FIRST: This matrix is for the purpose of mapping				
Basic Data Analysis							
Provide students with basic abilities to manipulate data into meaningful information.							
	Topics						
		Summary statistics					
		Graphing/Charts					
		Spreadsheet Functions					
		Problem Solving					
	Outcomes						
	Students will be able to:						
		Apply standard statistical inference procedures to draw conclusions from data					

SOFTWARE ASSURANCE

Courses	ABC-123	DEF-456				
Click here to return to KU Listing		(Click Here) READ THIS FIRST:				
Software Assurance						
The intent of this KU is to provide students with the ability to describe why software assurance is important to the development of secure systems and describe the methods and techniques that lead to secure software.						
Topics						
Robust programming						
Secure Software Concepts, Requirements, Design, Implementation and Testing						
Secure Development Life-Cycle Phases: requirements, design, development, testing, deployment, operations, maintenance and disposal.						
Software testing and acceptance						
Threat modeling						
Fuzz testing						
BUG BAR						
Characteristics of secure software						
Secure Software is not software that implements security functions (e.g., crypto, access control)						
Outcome:						
Students will be able to describe the importance of secure software, and the programming practices and development processes and methodologies that lead to secure software.						

All links below take you to the datasheet for that KU.

Core 2Y Knowledge Units (KU)

KU1	Basic Data Analysis **(INFO COMPLETE)
KU2	Basic Scripting
KU3	Cyber Defense **(INFO COMPLETE)
KU4	Cyber Threats **(INFO COMPLETE)
KU5	Fundamental Security Design Principles **(INFO COMPLETE)
KU6	Information Assurance Fundamentals **(INFO COMPLETE)
KU7	Introduction to Cryptography **(INFO COMPLETE)
KU8	Information Technology System Components **(INFO COMPLETE)
KU9	Policy, Legal, Ethics and Compliance **(INFO COMPLETE)
KU10	Networking Concepts **(INFO COMPLETE)
KU11	Systems Administration **(INFO COMPLETE)

Core 4Y Knowledge Units

KU12	Databases **(INFO COMPLETE)
KU13	Network Defense **(INFO COMPLETE)
KU14	Network Technology and Protocols **(INFO COMPLETE)
KU15	Operating Systems Concepts **(INFO COMPLETE)
KU16	Probability and Statistics **(INFO COMPLETE)
KU17	Programming

Letter of Intent, 8 Measurement Criteria (MC)

LETTER	Letter of Intent
MC1	Center for CD Education
MC2	Cyber Defense Academic Program
MC3	Student-based Cyber Defense Research
MC4	Cyber Defense Faculty and Course load
MC5	Cyber Defense Faculty Expertise and Research
MC6	Cyber Defense is a Multidisciplinary practice at the Institution
MC7	Institution Information Systems (IS) Security Plan
MC8	Cyber Defense Outreach Beyond the Institution

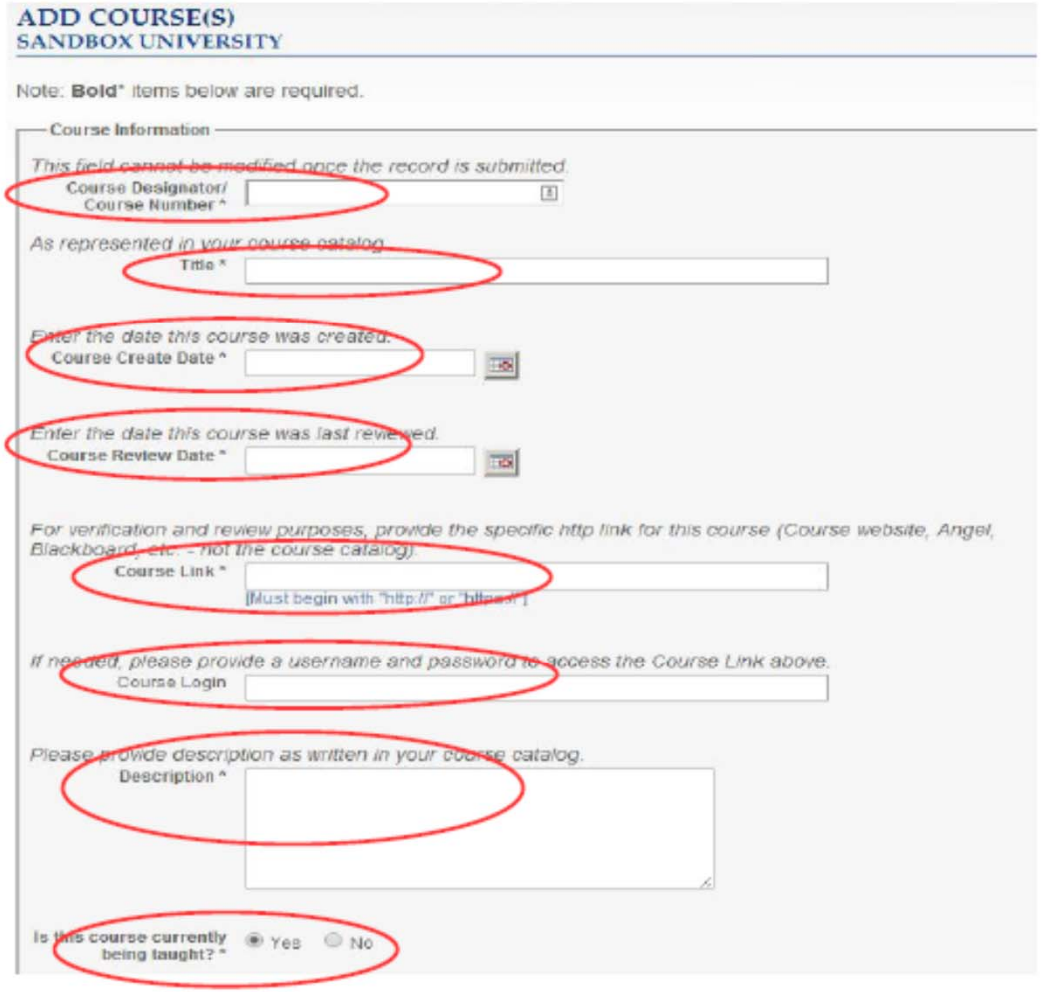
Optional Knowledge Units (OKU)

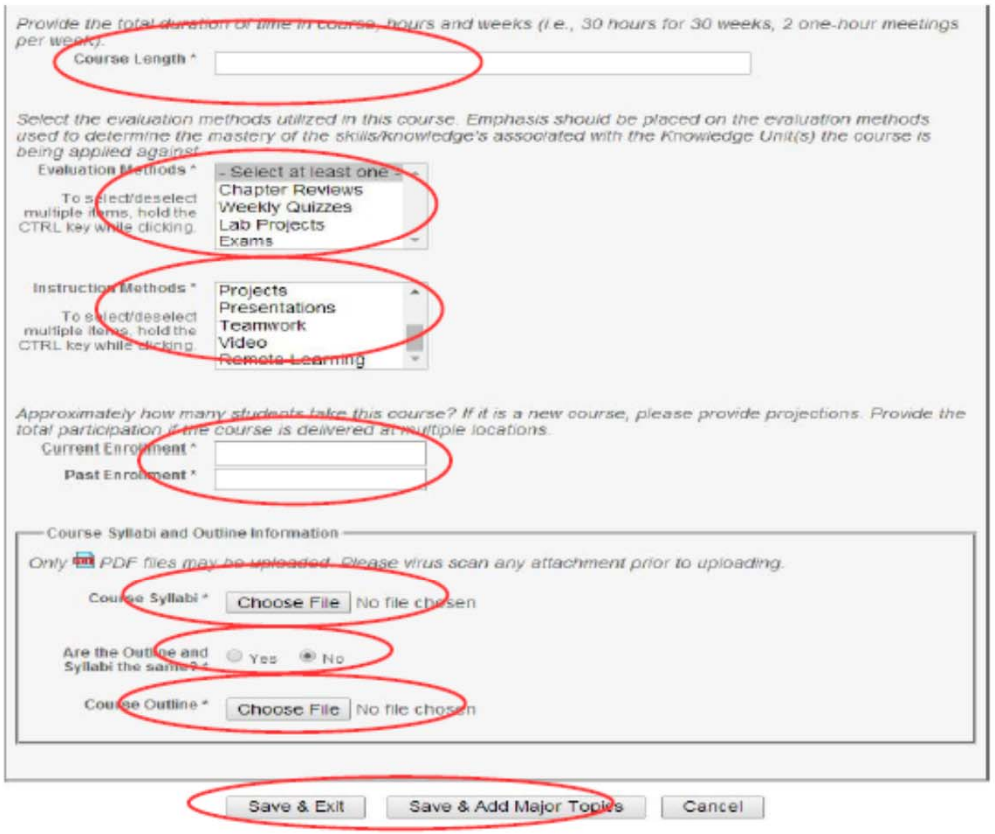
OKU1	Software Assurance **(INFO COMPLETE)
OKU2	IA Compliance **(INFO COMPLETE)
OKU3	IA Standards **(INFO COMPLETE)
OKU4	Supply Chain Security **(INFO COMPLETE)
OKU5	Life Cycle Security **(INFO COMPLETE)

UDM Courses (CIS)

1	CIS 5100	Object Oriented Development
2	CIS 5300	Software Assurance **(COURSE INFO COMPLETE)
3	CIS 5400	Software Management **(COURSE INFO COMPLETE)
4	CIS 5700	(Information Assurance) Cybersecurity Principles **(COURSE INFO COMPLETE)
5	CIS 5730	Cyberlaw **(COURSE INFO COMPLETE)
6	CIS 5740	Advanced Topics in Information Systems **(COURSE INFO COMPLETE)
7	CIS 5750	Information Assurance Technologies **(COURSE INFO COMPLETE)
8	CIS 5770	Cyber Defense Operations **(COURSE INFO COMPLETE)
9	CIS 5910	Information Audit **(COURSE INFO COMPLETE)

Add Courses


ADD COURSE(S)
SANDBOX UNIVERSITY
Note: Bold* items below are required.
Course Information
This field cannot be modified once the record is submitted.
Course Designator/ Course Number *
As represented in your course catalog.
Title *
Enter the date this course was created.
Course Create Date *
Enter the date this course was last reviewed.
Course Review Date *
For verification and review purposes, provide the specific http link for this course (Course website, Angel, Blackboard, etc. - not the course catalog).
Course Link *
[Must begin with "http://" or "https://"]
If needed, please provide a username and password to access the Course Link above.
Course Login
Please provide description as written in your course catalog.
Description *
Is this course currently being taught? * Yes No


Provide the total duration of time in course, hours and weeks (i.e., 30 hours for 30 weeks, 2 one-hour meetings per week).
Course Length *
Select the evaluation methods utilized in this course. Emphasis should be placed on the evaluation methods used to determine the mastery of the skills/knowledge's associated with the Knowledge Unit(s) the course is being applied against.
Evaluation Methods *
- Select at least one -
Chapter Reviews
Weekly Quizzes
Lab Projects
Exams
To select/deselect multiple items, hold the CTRL key while clicking.
Instruction Methods *
Projects
Presentations
Teamwork
Video
Remote Learning
To select/deselect multiple items, hold the CTRL key while clicking.
Approximately how many students take this course? If it is a new course, please provide projections. Provide the total participation if the course is delivered at multiple locations.
Current Enrollment *
Past Enrollment *
Course Syllabi and Outline Information
Only PDF files may be uploaded. Please virus scan any attachment prior to uploading.
Course Syllabi * Choose File No file chosen
Are the Outline and Syllabi the same? * Yes No
Course Outline * Choose File No file chosen
Save & Exit
Save & Add Major Topics
Cancel

Add Course Topics

Add Objectives

Courses	ABC	DEF						
Click here to return to KU Listing	(Click Here) READ THIS FIRST: This matrix is for the purpose of mapping your curriculum to the NSA/DHS CAE in IA/CD Knowledge Units (KUS). Recommend that you start by filling in individu							

KU1 Basic Data Analysis

Provide students with basic abilities to manipulate data into meaningful information.

KU Topics	Course Topic Numbers & Major Topics	Course Topic Description	Book/Supplemental Material Title	Course Objective Number	Course Objective	Is Topic Covered In Textbook?	Chapter/ Title	Supplemental Material Author
Summary statistics	CIS 5700 - Unit 2: Risks and Responses (sessions 3, 4 and 5), Case Exercise Two	Students will be able to compile security event data into summary statistics;	Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper	2/ 3, 4	Students will be able to compile summary statistics for the purpose of analysis	In asigned reasings	n/a	Anderson, K. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper", 2005.
Graphing/Charts	CIS 5700 - Unit 2: Risks and Responses (sessions 3, 4 and 5), Case Exercise Two	Students will utilize a tool to draw data driven graphic representations of data	Statistical Analysis for Dummies; MS Risk Analyzer An add-in product for Microsoft Excel	2/1 and case exercise two	Students will be able to prepare decision support graphics from a data source using an embedded grahic tool	In asigned reasings	n/a	Schmuller, Joseph, "Statistical Analysis with Excel – for Dummies 3rd Ed.", Wiley
Spreadsheet Functions	CIS 5700 - Unit 2: Risks and Responses (sessions 3, 4 and 5), Case Exercise Two	Students will utilize a tool to perform basic descriptive and inferential analyses	Statistical Analysis for Dummies	2/1 and case exercise two	Students will be able to present clear graphic evidence to support risk analysis	In asigned reasings	n/a	Schmuller, Joseph, "Statistical Analysis with Excel – for Dummies 3rd Ed.", Wiley
Problem Solving	CIS 5700 - Unit 2: Risks and Responses (sessions 3, 4 and 5), Case Exercise Two	Students will be able to perfrom basic security analytics functions for the purpose of solving applied security porobmes and concerns	Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis — Problemsolvingtechniqes.com	2/8 Lab 2	Students will be able to describe how statistics are used to assign probabilities, perform a risk estimation using statistical inference, solve a security problem, or concern using quantitative methods, provide practical policy recommendations based on probability, create risk strategies based on probability and impact	In asigned reasings	n/a	A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, CIA 2009; Freedman, D. A. Statistical Models and Causal Inferences: A Dialogue with the Social Sciences
Outcomes								
Students will be able to:								
Apply standard statistical inference procedures to draw conclusions from data	CIS 5700 - Unit 2: Risks and Responses (sessions 3, 4 and 5), Case Exercise Two, slide deck 4a		Schou, Information Assurance for the Enterprise, Chapters Four and Fourteen					
			Shoemaker, Cybersecurity: The Essential Body of Knowledge, Chapters Seven and Eighteen					
			Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It.					
			ISO/DIS 31000 (2009). Risk management — Principles and guidelines on implementation					
			Anderson, K. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper", 2005.					
			Schmuller, Joseph, "Statistical Analysis with Excel – for Dummies 3rd Ed.", Wiley					
			A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, CIA 2009					
			Freedman, D. A. Statistical Models and Causal Inferences: A Dialogue with the Social Sciences					

CIS 5300 Software Assurance

Click here to return to KU Listing

ADD NEW COURSE

Add Course Information

Course Number	**CIS 5300**
Title	Secure Software Assurance
Course Created Date	1991-1992 AY AY
Course Review Date	fall 2015 - by McNichols Faculty Assembly (MFA)
** **Course Link**	https://knowledge.udmercy.edu
Course Login	
Description	This course is rooted in the monitoring and control principles that are itemized in the Software Support Process of the ISO/IEEE 12207 -2008 Standard and detailed by various national standards cited above. Essentially, rather than assurance what we are studying is the mechanism that is used to make the software process visible and reliable. This is normally established at three levels in the software organization, strategic processes, project infrastructure and individual testing. We are going to examine all three of these from a top down perspective. We will move from the model that defines and relates all of these processes, through the specific itemization of the activities and tasks embodied within this framework, down to specific practices used to verify, validate, audit and resolve software assurance issues. In addition we are going to examine the software sustainment process as an adjunct to monitoring. Upon completion of this course, students will be able to: Create a software architecture that embodies the principles of software security, minimizes attack surfaces, and presents an adequate defense in depth against common attacks; Analyze and prepare a comprehensive response to risk across the development lifecycle that incorporates conventional best practices for software security; Differentiate weaknesses in code and the associated practices that create those weaknesses and execute a set of tool-based unit testing methodologies to ensure that exploitable code is caught and fixed; Perform end-to-end security verification and validation activities that incorporate various standard certification and accreditation solutions; Design a measurement program that produces a reliable set of quantitative data for use in business decision making
Is this course currently being taught?	Yes - Taught Winter 2015 - next taught Spring 2016
Course Length	35 contact hours per semester - one 2.5 hour meeting/week
Evaluation Methods	Five section quizzes - four projects - final team project - final examination
Instruction Methods	Asynchronous lectures - synchronous recitations - team project work
Current Enrollment	17 Winter 2015
Past Enrollment	12 Winter 2014
Course syllabi	upload file
Are the online and syllabi the same?	yes
Course Outline	upload file

Add Major Topics (Multiple topics are entered separately)

Topic Number	**Unit 1**	**Unit 2**	**Unit 3**	**Unit 4**	**Unit 5**	**Unit 6**
Major Topic	Basic Concepts and Principles (sessions 1 and 2)	Building Rugged Software (sessions 3 and 4)	Adopting Secure Coding Practices (session 5 through 7)	Secure Software Verification & Validation (session 9 and 10)	Measurement and Metrics for Software Assurance (session 11 and 12)	Secure Sustainment (session 13 and 14)
Topic Description	The student will know Fundamental Software Security Concepts. The student will enumerate functional and Operational Dangers to Software. The student will utilize the Common Weakness Enumeration (CWE)/Common Vulnerability Enumeration (CVE) to understand: Attacks, o Attackers: Types and Motivations, Attack Methods, Probable Points of Attack, Attack Surfaces	The student will know how to do Threat and Risk Understanding. The student will know how to build an Assurance Case. The student will know how to development of defense-in-depth mitigation strategies based on assurance objectives. The student will know how to develop evidence based confidence estimates. The student will know how to do security Requirements Development and Analysis. The student will understand the principles of Secure Design	The student will understand common vulnerabilities in code. The student will know common weaknesses in code. The student will know common coding errors. The student will understand how to execute patch Management. The student will know how to do vulnerability Prioritization. The student will understand application Configuration issues. The student will know how to execute unit testing. The student will be able to use common coding Tools and Technologies	Student will be able to Document the Assurance Case. Student will be able to design the Verification and Validation Plan. Student will be able to plan and develop Test Cases. Student will be able to design test and Review Follow-up Procedures. Student will be able to integrate system and Acceptance Testing including; Dynamic Analysis Methods; Static Analysis Methods; Tools and Technologies for Verification & Validation; and Other Testing Processes. Student will understand the use of penetration Testing and Ethical Hacking. Student will be able to execute reviews and Audits for the purpose of certification and accreditation (C&A)	Student will be able to define the Metrics and Measurement Process for software assurance. The student will understand the relationship between Metrics and Software Security including; Metrics and Management Control, Benchmarks for Process Improvement, Formal Certification of Secure Systems, Formal Measurement Data-Gathering Processes. The student will know criteria for Selection of Measures including; Lifecycle Classifications, FIPS 199 Classifications, Common Criteria classifications. The student will understand software Reliability Management. The student will know qualitative Security Characteristics	The student will understand Baselining and Baseline Management. The student will know how to do Operational Assurance (sensing). The student will know how to do operational Testing. The student will know how to do vulnerability identification and monitoring of Latent Vulnerabilities. The student will know how to do change Analysis and Authorization (SOW). The student will know how to do change Evaluation and Re-integration
Is this Topic covered in a textbook?	Yes	Yes	Yes	Yes	Yes	Yes
Is this Topic covered in Supplemental Material?	Yes	Yes	Yes	Yes	Yes	Yes
Book/Supplemental Material Title	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide
Chapter/Title	Chapter 1, "Defining a Discipline" Chapter 4, "A Risk Management Framework," pp. 42-73	Chapter 5, "Knowledge for Secure Software," ;Chapter 3, "Introduction to Software Security Touchpoints	Chapter 4, "Code Review with a Tool"; dynamic testing of an application	Chapter 7, "Risk Based Security Testing" pp. 187-204; Chapter 9, "Software Security Meets Security of Operations" pp. 223-235	Part III: Chapter 10 "An Enterprise Software Security Program" pp. 239-256	Chapter Nine "Software Security Meets Security Operations"
Supplemental Material Author	Saltzer & Schroeder," The Protection of Information in Computer Systems", "Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software"; Chapter 1, "Introduction"; Chapter 2, "Dangers and Damage", Common Attack Pattern Enumeration and Classification: CAPEC List Release 1.6	The Open Web Application Security Project: Threat Risk Modeling, http://www.owasp.org/index.php/Threat_Risk_Modeling; Arguing Security – Creating Security Assurance Cases https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html SQUARE Lite: Case Study on VADSoft Project http://www.sei.cmu.edu/reports/08sr017.pdf; Improving Web Application Security: Threat Modeling http://msdn.microsoft.com/en-us/library/ff648644.aspx	Creating a Patch and Vulnerability Management Program http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf; CVSS: A Complete Guide to the Common Vulnerability Scoring System, pp. 6-9 http://www.first.org/cvss/cvss-guide.pdf; WE-352: Cross-Site Request Forgery (CSRF) http://cwe.mitre.org/data/definitions/352.html	Technical Guide to Information Security Testing and Assessment; http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. The OWASP Top 10: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project	FIPS 199: Standards for Security Categorization of Federal Information and Information Systems http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf; NIST 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories, pp 9-33 http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf; NIST 800-55: Performance Measurement Guide for Information Security, pp. 9-19, 31-33, A2-A24 http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf; NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations, pp, 6-25, E1-E4, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf	NIST SP 800-128: Guide for Security Configuration Management of Information Systems http://csrc.nist.gov/publications/drafts/800-128/draft_sp800-128-ipd.pdf; "Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software"- Chapter 12, "Secure Software Sustainment" https://buildsecurityin.us-cert.gov/bsi/940 SI/version/default/part/AttachmentData/data/CurriculumGuideToTheCBK.pdf

Add Objectives (each entered separately)

Objective Number	1. Evaluate the applicability of Saltzer and Schroeder to software development life cycle elements	1. Prepare a threat model to evaluate and prioritize security threats	1. Evaluate vulnerabilities and weaknesses for future remediation	1. Prepare a specific assurance case for a given software security application	1. Prioritize security risk and impact based on a sensitivity level [D]	1. Create a practical and valid change request process
Objective Number	2. Evaluate the effect of software exploitation in real-world terms [A]	2. Develop an assurance case and mitigations for security threats	2. Evaluate proper patch management practices	2. Interpret static test cases to prove the validity of an assurance case	2. Select an appropriate set of measures for an application [A]	2. Create a practical change authorization process
Objective Number	3. Apply the CWE/CVE to appropriate places in life cycle elements [A]	3. Synthesize and justify a design traceable to security mitigations	3. Develop an assurance case and an appropriate set of tests for unit testing	3. Prepare an appropriate set of static tests	3. Develop a persistent set of measurement benchmarks [A]	3. Create a coherent and correctly labeled baseline and Baseline Management Ledger
		4. Justify a design based on risk prioritization	4. Perform unit testing on code	4. Interpret the results of static tests and suggest mitigations	4. Develop a comprehensive set of measures of qualitative correctness	4. Create a focused analysis process that generates meaningful decision data about status
			5. Evaluate common coding tools and technologies			

VERIFY DATA – LOOK AT IT THROUGH THE EYES OF AN AUDITOR

- **Course syllabi**
- **Created 9 DEV courses in Blackboard and populated each course**
  1. **CIS 5100 Object Oriented Development**
  2. **CIS 5300 Software Assurance**
  3. **CIS 5400 Software Management**
  4. **CIS 5700 (Information Assurance) Cybersecurity Principles**
  5. **CIS 5730 Cyberlaw**
  6. **CIS 5740 Advanced Topics in Information Systems**
  7. **CIS 5750 Information Assurance Technologies**
  8. **CIS 5770 Cyber Defense Operations**
  9. **CIS 5910 Information Audit**

VERIFY DATA – LOOK AT IT THROUGH THE EYES OF AN AUDITOR

- **Is the Bb course complete? Is anything missing? (syllabus/module/PPT's/lectures/assignments/quizzes/etc.)**
- **Does the course description match what is in the syllabus?**
- **Where is the KU taught? What course? What module/week/chapter/session?**
- **What are the assignments? Does the assignment teach/reinforce/apply the KU?**

MEASUREMENT CRITERIA 0

Letter of Intent		
Click here to return to KU Listing		
	Letter of Intent as CAE-CDE and statement of CAE-CDE mission and purpose.	
	Provide official notice regarding the institutional intent to participate in the CAE-CDE program. Provide formal documentation showing the establishment of an official “Cyber Center” within the institution. Letter should be on institution letterhead, signed by the Dean or higher, contain information about the Cyber Defense program and name the POC from the institution. Letter should also state accreditation information and any pertinent accomplishments in the cyber defense field. The letter should be addressed to:	
	National Security Agency Attn: CAE Program Office 9800 Savage Road	
	Ft. Meade, MD 20755-6804	
	Mandatory requirement	

MEASUREMENT CRITERIA 1

	Center for IA/CD Education	
	Click here to return to KU Listing	
	"Center" for CD Education.	
	The institution must have an officially established organization serving as the focal point for its CD educational program (physical or virtual). The center should provide the following services: program guidance and oversight, general cyber defense information, and collaboration and outreach opportunities among students, faculty, and other institutions. Additionally, the center must be supported by a website that is dynamic, current and visible within the institution and the community at large.	
	Overall Point value: 10 points mandatory	
a.	**Cyber Center**	
	Show formal documentation of the designation of Cyber "Center." This can be included in the letter of intent. (For the purpose of this document, the word "Center" is used in a general sense). The "Center" must have the endorsement from a Dean or higher. **Point Value: 5 points mandatory**	
b.	**"Cyber Center" Website**	
	Provide an operational hyperlink to the "Cyber Center" website. This "Cyber Center" should provide program guidance, general CD information and promote collaboration and interaction with other students, faculty, and programs. The "Cyber Center" and its website must be operational, dynamic, current and visible within the institution and to the community at large. Evidence provided should include, but is not limited to:	
	information about the CD program of study and faculty, "Cyber Center" points of contact, links to student CD activities, institutional security resources and awareness, as well as up-to-date links to key CD resources such as other academic institutions, government sites, conferences, workshops, and CD news.	
	Point Value: 5 points mandatory	

MEASUREMENT CRITERIA 2

Cyber Defense Academic Program

Click here to return to KU Listing

	Cyber Defense Academic Program	
	The CD program of study is central to a vibrant and mature CAE for Cyber Defense Education program. The institutional must show its CD academic requirements and explain how students participate and successfully complete the CD curriculum.	
	Overall Point value: 17 mandatory/20 maximum	
	a. Cyber Defense Program of Study	
	Describe the CD program of study offered by the institution. What department(s) oversee the program? What types of CD curriculum paths are offered, i.e., CD major, minor, certificate program? What courses are required for those paths that satisfy the CAE requirements for all the mandatory KU requirements and at least five operational KU requirements? Provide the course path that map to the KUs. Provide a sample of a student transcript, completion letter or certificate. (Please note – Only the CD curriculum program(s)/path(s) identified in this criterion, are allowed to be marketed as CAE-CDE Curriculum Path(s)/Program(s) at an institution, if application is approved. If additional curriculum path(s)/program(s) are identified after this application is submitted, the onus is on the institution POC to confirm all core KUs are covered and the POC must identify the additional path(s)/program(s) in the re-designation application).	
	Point Value: 10 points mandatory	
	b. Availability of Subscription-based, on-line CD publications	
	Provide evidence that students and faculty have access to subscription-based, on-line CD journals, books and other publications. How are these resources integrated into the curriculum and provided to students? Provide sample course materials showing references to these resources or hyperlinks to instructor webpages offered to students. ***Point Value: Up to 5 points/2 mandatory***	
	c. Overview of Student Participation in program	
	Provide information on the student enrollment over the last 3 years to include current participants and graduates. Provide numbers of students that have participated/graduated in the last 3 years.	
	Point Value: 5 points mandatory	

MEASUREMENT CRITERIA 3

Student-based Cyber Defense Research

Click here to return to KU Listing

Student-based Cyber Defense Research

The institution must show how it fosters student research in CD. This item focuses on **STUDENT**- based research as it contributes to evolution of theory and practice in the field of cyber defense. Research should related back to one or more of the KUs.

Overall Point value: 12 mandatory/25 maximum

a. Research requirements for CD program participants

Although the depth of the research may vary, both undergraduate and graduate students should be encouraged to analyze Cyber Defense issues and offer solutions or recommendations. What are the research requirements for students participating in the CD program of study? Provide links to 5 to 10 of the best CD theses, dissertations, papers or projects produced by these students within the last 3 years. **Link to actual papers required – not a subscription service.**

Point Value: Up to 10 points/1 point per paper or project/5 points mandatory

b. Cyber Defense Physical/Virtual Labs

Show that physical and/or virtual labs and equipment are available and demonstrate how these resources are used by students and faculty to support the Cyber Defense program of study. Evidence provided should include either a description or links to information about the lab resources available as well as samples of lab projects or exercises.

Point Value: Up to 5 points/2 points mandatory

c. List of courses requiring research and/or labs

Provide a list of CD courses that require research papers or labs and links to the course syllabi. Courses need to be either current or taught within the last 3 years.

Point Value: Up to 10 Points/1 point per course/5 courses mandatory

MEASUREMENT CRITERIA 4

Cyber Defense Faculty and Course load

Click here to return to KU Listing

	Cyber Defense Faculty and Course load	
	The institution must demonstrate that it has someone responsible for the overall CD program of study and sufficient faculty members, either full- or part-time, teaching at least one CD course. The criterion requires a link to the biography or curriculum vitae for each faculty member. It must be possible to locate all faculty members from the University website.	
	Overall Point Value: 9 points mandatory/20 points maximum	
	a. Head of the Cyber Defense Program of Study	
	Identify by name the full-time employee or employees with overall responsibility for the CD program of study at the institution. Evidence must include a job description and biography or CV.	
	Point Value: 5 points mandatory	
	b. Additional full-time Cyber Defense faculty members	
	Identify by name full-time faculty members teaching the courses in the CD program of study. Evidence must include a job description and biography or CV. Also required is the department where they teach and course load.	
	Point Value: 2 point each/4 points mandatory/10 points maximum	
	c. Part-time or Adjunct Cyber Defense Faculty members	
	Identify by name part-time or adjunct faculty members teaching the courses in the CD program of study. Evidence must include a job description and biography or CV. Also required is the department where they teach and course load.	
	Point Value: 1 point each/5 points maximum	

MEASUREMENT CRITERIA 5

Cyber Defense Faculty Expertise and Research

Click here to return to KU Listing

Cyber Defense Faculty Expertise and Research

The institution must show that the faculty members are CD experts and are active in current CD practice and research. Cyber Defense faculty members should be contributing their CD knowledge to publications, presentations, and professional societies as well as seeking grants for CD resources and mentoring CD students.

Overall Point Value: 9 points mandatory/41 points maximum

a. Faculty authored Cyber Defense publications

Provide evidence of faculty contributions to peer reviewed publications on CD topics to include refereed journals and conference proceedings within the last 3 years**. Provide links to actual papers not a subscription service.**

Point Value: 2 points per paper/2 papers mandatory/10 points maximum

b. Published books or chapters of books on Cyber Defense/Cybersecurity

Books/chapters must focus on Cyber Defense/Cybersecurity and have been published within the last 5 years. Provide title, authors and date published. Identify specific chapters if authoring a chapter of a book. Papers published in a conference proceedings will be accepted in 5A, not 5B.

Point Value: 5 points per book/1 point per chapter/10 points maximum

c. Cyber Defense Presentations

Provide evidence that faculty members present CD content at major Regional/National/International conferences and events within the last 3 years. Provide a synopsis of the involvement. This can include guest lecturer at other institutions or government organizations.

Point Value: 1 point per conference/2 presentations mandatory/6 points maximum

d. Professional societies

Provide evidence that faculty members are CD subject matter experts for accrediting bodies and professional societies. (e.g., ACM, IEEE, regional accreditation, professional accreditation, etc.). Faculty members are active members in CD/Cybersecurity organizations (e.g., ISSA, Cyberwatch, Infraguard, etc.). List involvement for the last 3 years.

Point Value: 2 points per review or membership/2 points mandatory/6 points maximum

e. Writing Cyber Defense Grants and external funding

Provide evidence that CD faculty members write grants and obtain funding for CD education and/or research or lab equipment. Provide a synopsis of the grant to include date and approximate monetary value. Provide links to organization providing the grant or links to a news article. Provide an explanation if funding or grants are not obtained.

Point Value: 2 points per award or funding/6 points maximum

f. Support to Cyber Defense Student activities

Provide evidence that CD faculty members support their student by serving as mentors or advisors to student led activities. Evidence can include links to student clubs, Cyber Defense Exercises, etc.

Point Value: 1 points per program/1 mandatory/3 points maximum

MEASUREMENT CRITERIA 6

Cyber Defense is a Multidisciplinary practice at the Institution

Click here to return to KU Listing

	Cyber Defense is a Multidisciplinary practice at the Institution	
	The institution must demonstrate that CD is not treated as a separate discipline, but integrated into related fields.	
	Overall Point Value: 7 points mandatory/15 points maximum	
	a. Cyber Defense Concepts taught in other fields of study	
	Provide evidence that CD topics are taught in courses outside the CD program of study department and its courses. Courses taught outside the CD program of study could be technical or non-technical. For example: health practitioners learning about privacy and patient data protection; accountants learning about data backup and protection; or non-credit continuing education courses on IT security basics. Provide course name and syllabus with cyber modules highlighted.	
	Points: 2 point per course/2 courses mandatory/up to 10 points.	
	b. Non-Cyber Defense courses encourage papers or projects in CD topics.	
	Courses taught outside the CD program require papers/projects/posters/etc. For example: health care practitioners write a paper on the importance of safeguarding patient health care records. Provide links to 5 to 10 best papers or projects on CD within 3 years of application. **Link to actual papers required – not a subscription service. Paper/projects should correspond to courses provided in 6a.**	
	Points: 1 point per item (3 mandatory)/only 2 items per course/up to 5 points.	

MEASUREMENT CRITERIA 7

Institution Information System (IS) Security Plan

Click here to return to KU Listing

Institution Information System (IS) Security Plan

Overall Point Value: 16 points minimum/20 points maximum

a. Security plans or polices

Provide links to the CD/IS Security Plan(s) or policies for the institution to show how it practices institutional security.

Points: 5 points mandatory

b. Institutional Cyber Security/Information Security Officer

Provide the name, title and job description for the individual responsible for the information IS program at the institution.

Points: 5 points mandatory

c. Implementation of Cyber Security Practices

Provide evidence of how the institutional implements its CD Security plan through awareness, training and tutorials, log in security banners, user acknowledgements, on- line help and good security practice guides. (e.g., Students, faculty and staff are required to take computer based training or on-line tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc.)

Points: 6 points mandatory/10 points maximum

MEASUREMENT CRITERIA 8

MC8 Outreach/Collaboration

Click here to return to KU Listing

Cyber Defense Outreach Beyond the Institution

The institution must demonstrate how CD is extended beyond the normal boundaries of the institution.

Overall Point Value: 15 mandatory/30 maximum

a. Shared Curriculum and advancing Cyber Defense Educational practice.

Show how the institution shares it CD curriculum or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities within the last 3 years. Provide information about sponsorship or participation in CD curriculum development workshops or colloquia or faculty sharing events for any of the types listed above within the last 3 years.

Point Value: Up to 5 points/3 points mandatory

b. Reciprocity of Credit

Provide evidence of written agreements showing that the institution accepts credit in CD courses and/or prerequisite courses from other academic institutions. (e.g., Accepting academic credit in CD courses from minority institutions, two-year community colleges, or technical schools). Must show the course designator and how it translates to the accepting school.

Point Value: Up to 5 points/3 points mandatory

c. Sponsorship or participation in Cyber Defense Exercises and Competitions

Provide evidence of participation in or sponsorship of CD exercises and competitions within the last 3 years.

Point Value: Up to 5 points

d. CAE Collaboration

Show how the institutions partners in CD research or shared classes/events with other CAE institutions.

Point Value: Up to 5 points

e. Cyber Defense Business/Industry Collaboration

Show how the institution partners with companies and other employers to identify CD needs of potential employers and encourage student internships. Show how the institution works with employers and students to support job placement.

Point Value: Up to 5 points

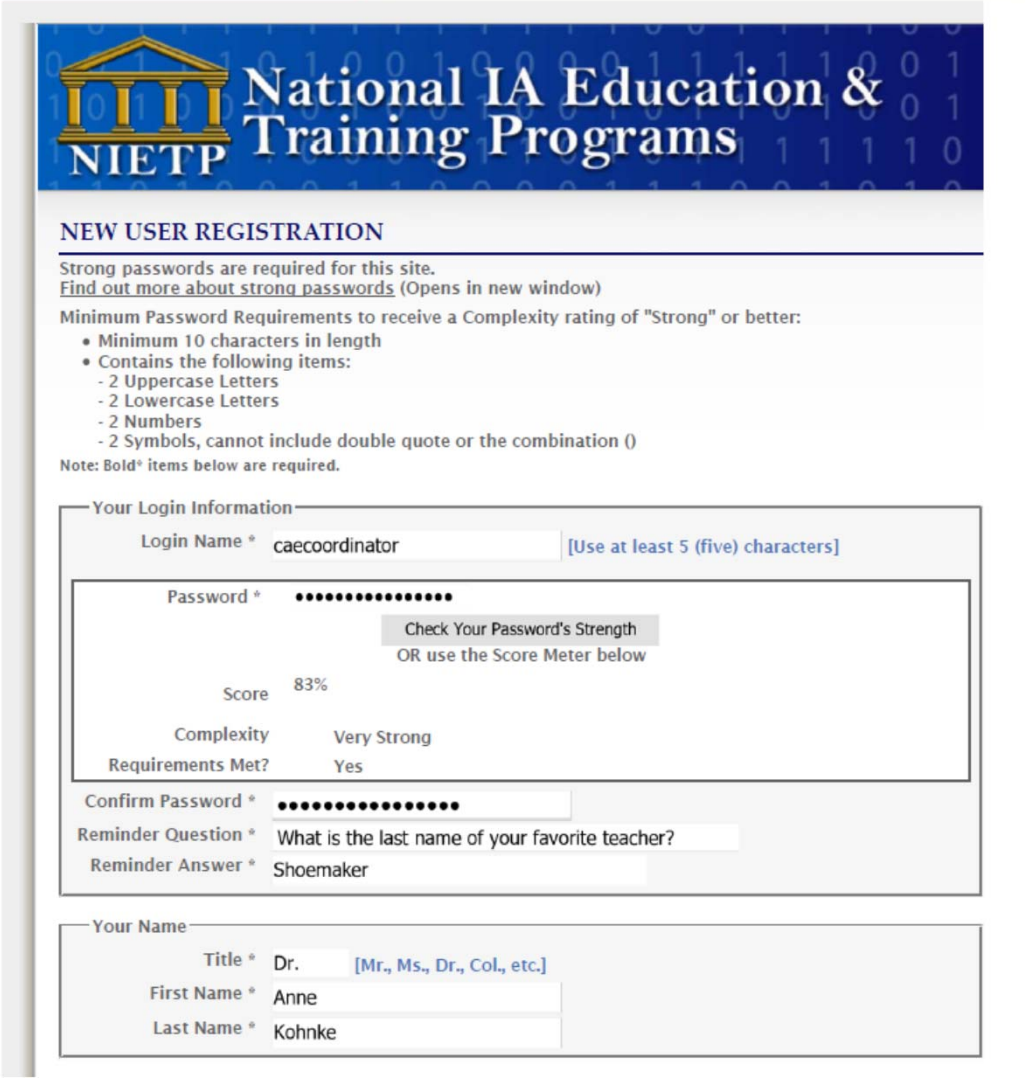
f. Community Outreach

Show how the institution sponsors CD events for the community at large. Events could include CD awareness and education for local schools, adult education centers, and senior centers. Examples of events could be computer “check-up” days, protecting personal information in cyber space, or preventing and recovering from a “virus”.

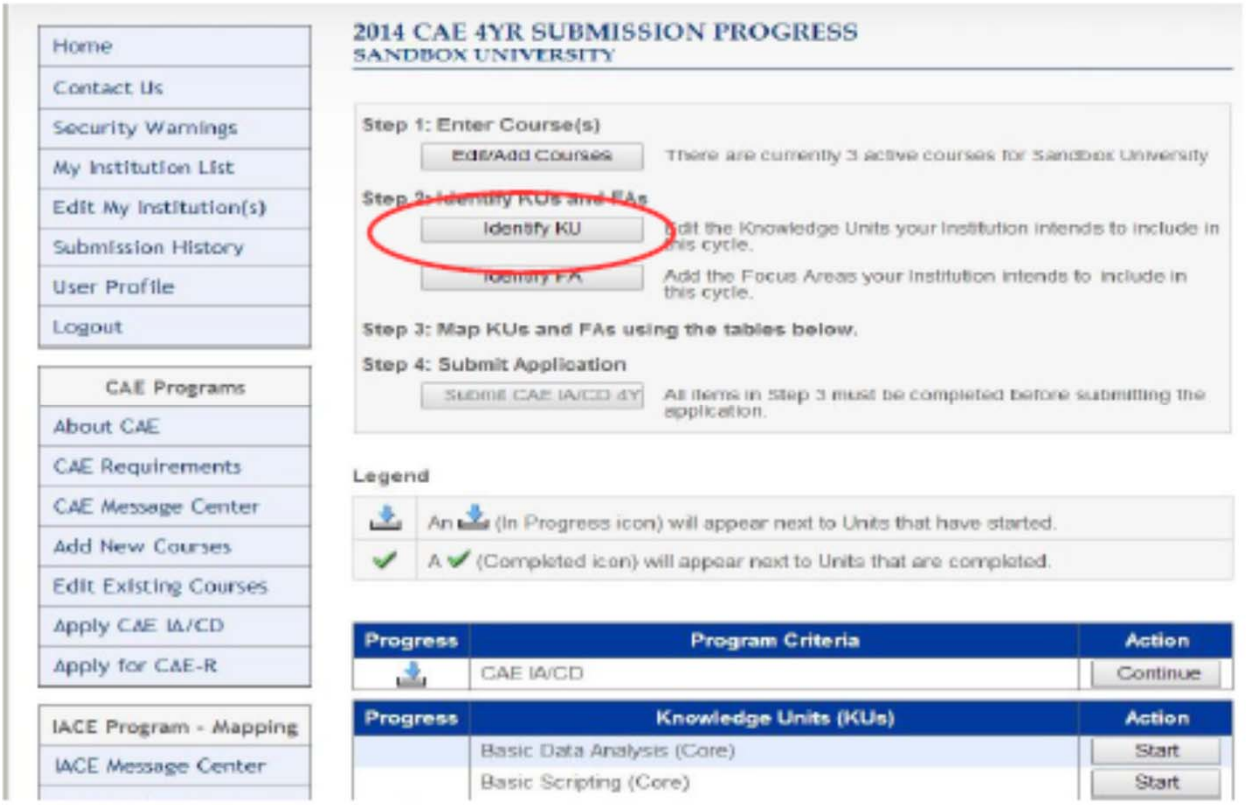
Point Value: Up to 5 points/2 mandatory

NEW USER REGISTRATION

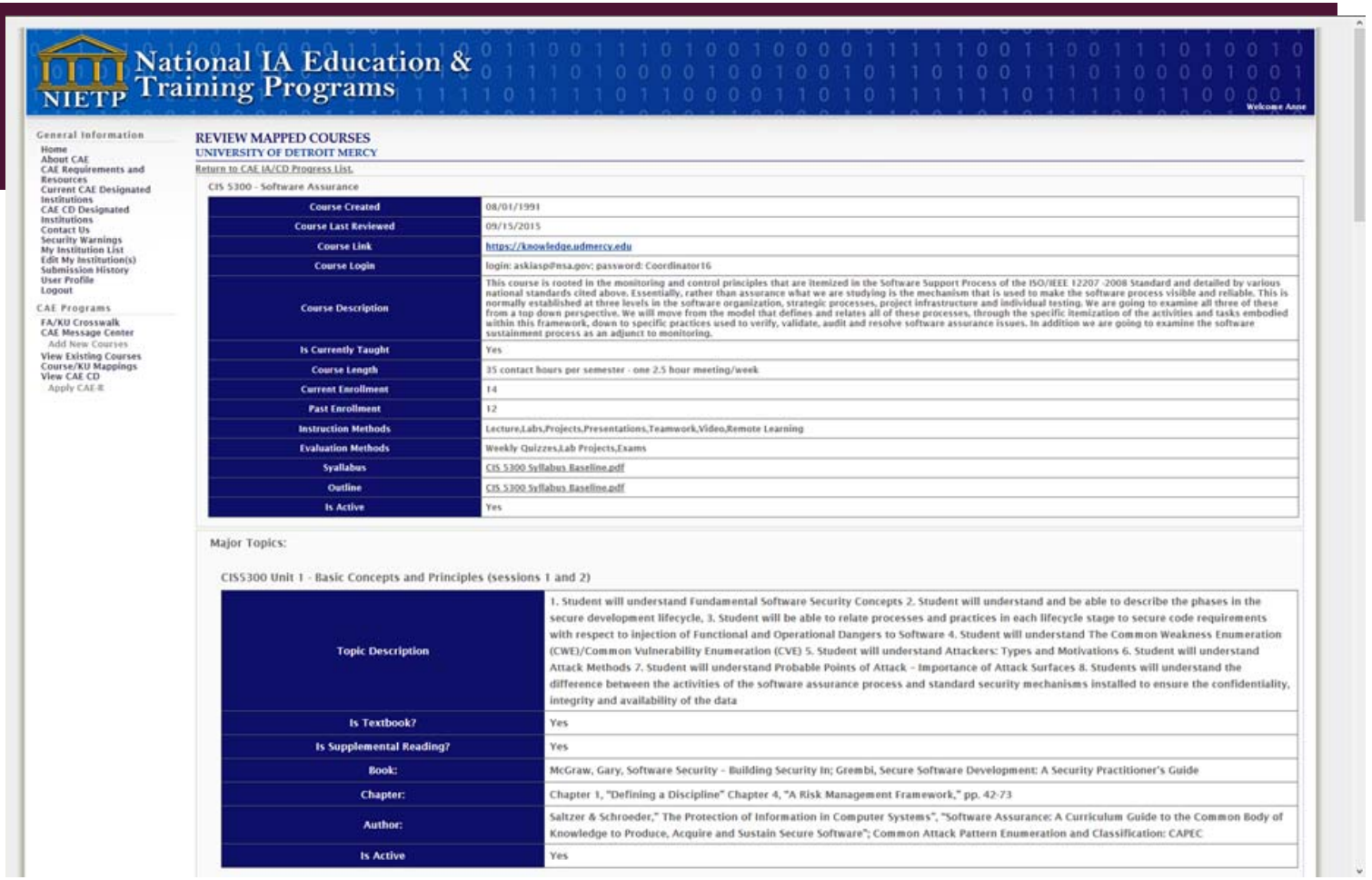
- Establish the point of contact (POC) on the National IA Education & Training Programs (NIETP) website
- **New User Registration**
- **Create a login with POC permissions** – only one individual can be the POC
- AskCAEIAE@nsa.gov = **Karen Leuschner,** National CAE Program Manager = **extremely helpful!!**



IDENTIFY THE KNOWLEDGE UNITS FOR YOUR INSTITUTION



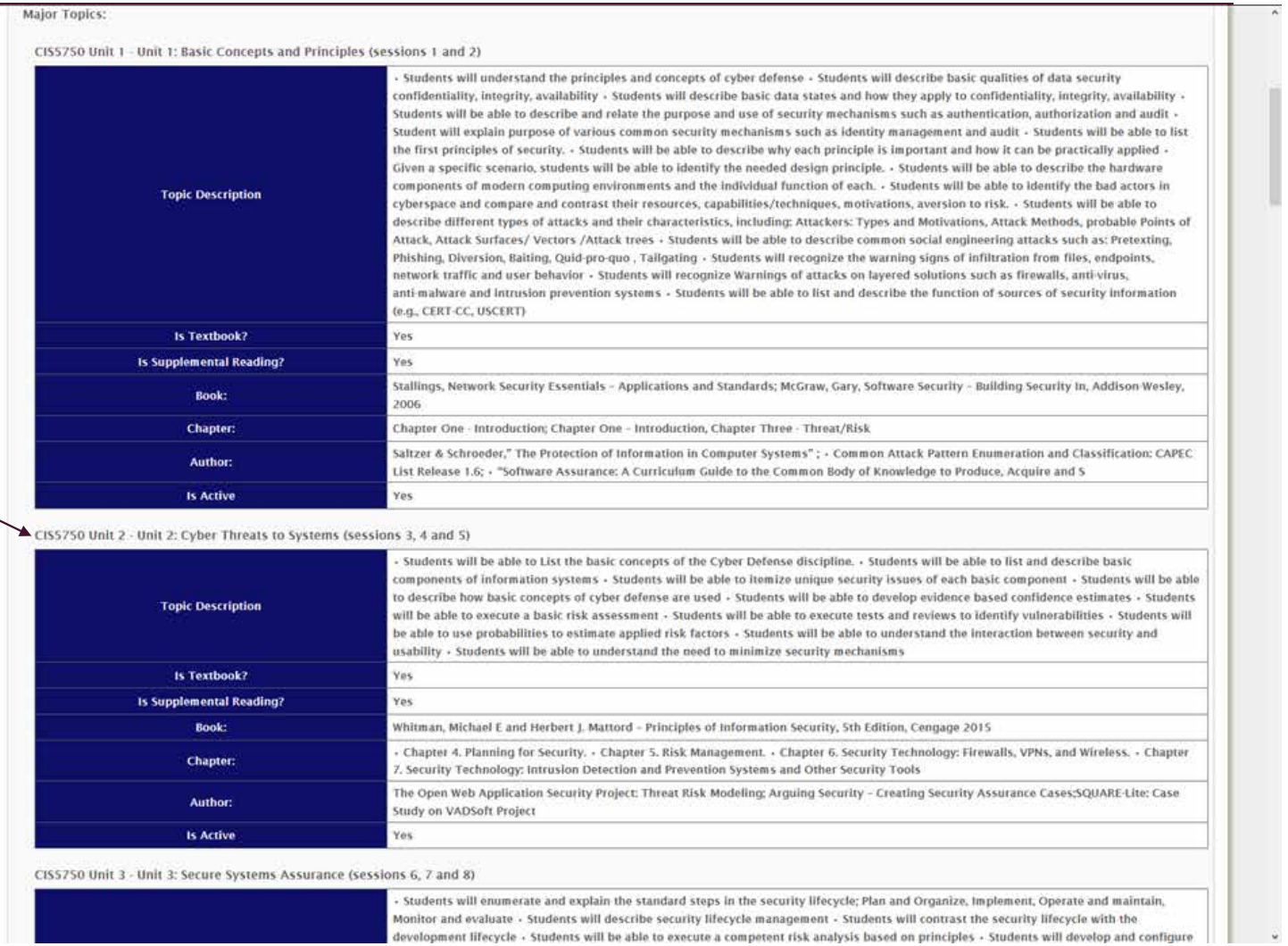
ADD COURSES


National IA Education & Training Programs
NIETP
Welcome Anne
General Information
Home
About CAE
CAE Requirements and Resources
Current CAE Designated Institutions
CAE CD Designated Institutions
Contact Us
Security Warnings
My Institution List
Edit My Institution(s)
Submission History
User Profile
Logout
CAE Programs
FA/KU Crosswalk
CAE Message Center
Add New Courses
View Existing Courses
Course/KU Mappings
View CAE CD
Apply CAE R
REVIEW MAPPED COURSES
UNIVERSITY OF DETROIT MERCY
Return to CAE IA/CD Progress List.
CIS 5300 - Software Assurance
Course Created 08/01/1991
Course Last Reviewed 09/15/2015
Course Link https://knowledge.udmercy.edu
Course Login login: asklasp@nsa.gov; password: Coordinator16
Course Description This course is rooted in the monitoring and control principles that are itemized in the Software Support Process of the ISO/IEEE 12207 -2008 Standard and detailed by various national standards cited above. Essentially, rather than assurance what we are studying is the mechanism that is used to make the software process visible and reliable. This is normally established at three levels in the software organization, strategic processes, project infrastructure and individual testing. We are going to examine all three of these from a top down perspective. We will move from the model that defines and relates all of these processes, through the specific itemization of the activities and tasks embodied within this framework, down to specific practices used to verify, validate, audit and resolve software assurance issues. In addition we are going to examine the software sustainment process as an adjunct to monitoring.
Is Currently Taught Yes
Course Length 35 contact hours per semester - one 2.5 hour meeting/week
Current Enrollment 14
Past Enrollment 12
Instruction Methods Lecture,Labs,Projects,Presentations,Teamwork,Video,Remote Learning
Evaluation Methods Weekly Quizzes,Lab Projects,Exams
Syallabus CIS 5300 Syllabus Baseline.pdf
Outline CIS 5300 Syllabus Baseline.pdf
Is Active Yes
Major Topics:
CIS5300 Unit 1 - Basic Concepts and Principles (sessions 1 and 2)
Topic Description 1. Student will understand Fundamental Software Security Concepts 2. Student will understand and be able to describe the phases in the secure development lifecycle, 3. Student will be able to relate processes and practices in each lifecycle stage to secure code requirements with respect to injection of Functional and Operational Dangers to Software 4. Student will understand The Common Weakness Enumeration (CWE)/Common Vulnerability Enumeration (CVE) 5. Student will understand Attackers: Types and Motivations 6. Student will understand Attack Methods 7. Student will understand Probable Points of Attack - Importance of Attack Surfaces 8. Students will understand the difference between the activities of the software assurance process and standard security mechanisms installed to ensure the confidentiality, integrity and availability of the data
Is Textbook? Yes
Is Supplemental Reading? Yes
Book: McGraw, Gary, Software Security - Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide
Chapter: Chapter 1, "Defining a Discipline" Chapter 4, "A Risk Management Framework," pp. 42-73
Author: Saltzer & Schroeder," The Protection of Information in Computer Systems", "Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software"; Common Attack Pattern Enumeration and Classification: CAPEC
Is Active Yes

ADD TOPICS

Labeled each Topic with:

- **Course name**
- **Unit**



Major Topics:

CIS5750 Unit 1 - Unit 1: Basic Concepts and Principles (sessions 1 and 2)

Topic Description	• Students will understand the principles and concepts of cyber defense • Students will describe basic qualities of data security confidentiality, integrity, availability • Students will describe basic data states and how they apply to confidentiality, integrity, availability • Students will be able to describe and relate the purpose and use of security mechanisms such as authentication, authorization and audit • Student will explain purpose of various common security mechanisms such as identity management and audit • Students will be able to list the first principles of security. • Students will be able to describe why each principle is important and how it can be practically applied • Given a specific scenario, students will be able to identify the needed design principle. • Students will be able to describe the hardware components of modern computing environments and the individual function of each. • Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk. • Students will be able to describe different types of attacks and their characteristics, including: Attackers: Types and Motivations, Attack Methods, probable Points of Attack, Attack Surfaces/ Vectors /Attack trees • Students will be able to describe common social engineering attacks such as: Pretexting, Phishing, Diversion, Baiting, Quid-pro-quo , Tailgating • Students will recognize the warning signs of infiltration from files, endpoints, network traffic and user behavior • Students will recognize Warnings of attacks on layered solutions such as firewalls, anti-virus, anti-malware and intrusion prevention systems • Students will be able to list and describe the function of sources of security information (e.g., CERT-CC, USCERT)
Is Textbook?	Yes
Is Supplemental Reading?	Yes
Book:	Stallings, Network Security Essentials - Applications and Standards; McGraw, Gary, Software Security - Building Security In, Addison Wesley, 2006
Chapter:	Chapter One - Introduction; Chapter One - Introduction, Chapter Three - Threat/Risk
Author:	Saltzer & Schroeder," The Protection of Information in Computer Systems" ; • Common Attack Pattern Enumeration and Classification: CAPEC List Release 1.6; • "Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and S
Is Active	Yes

CIS5750 Unit 2 - Unit 2: Cyber Threats to Systems (sessions 3, 4 and 5)

Topic Description	• Students will be able to List the basic concepts of the Cyber Defense discipline. • Students will be able to list and describe basic components of information systems • Students will be able to itemize unique security issues of each basic component • Students will be able to describe how basic concepts of cyber defense are used • Students will be able to develop evidence based confidence estimates • Students will be able to execute a basic risk assessment • Students will be able to execute tests and reviews to identify vulnerabilities • Students will be able to use probabilities to estimate applied risk factors • Students will be able to understand the interaction between security and usability • Students will be able to understand the need to minimize security mechanisms
Is Textbook?	Yes
Is Supplemental Reading?	Yes
Book:	Whitman, Michael E and Herbert J. Mattord - Principles of Information Security, 5th Edition, Cengage 2015
Chapter:	• Chapter 4. Planning for Security. • Chapter 5. Risk Management. • Chapter 6. Security Technology: Firewalls, VPNs, and Wireless. • Chapter 7. Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools
Author:	The Open Web Application Security Project: Threat Risk Modeling; Arguing Security - Creating Security Assurance Cases;SQUARE-Lite: Case Study on VADSoft Project
Is Active	Yes

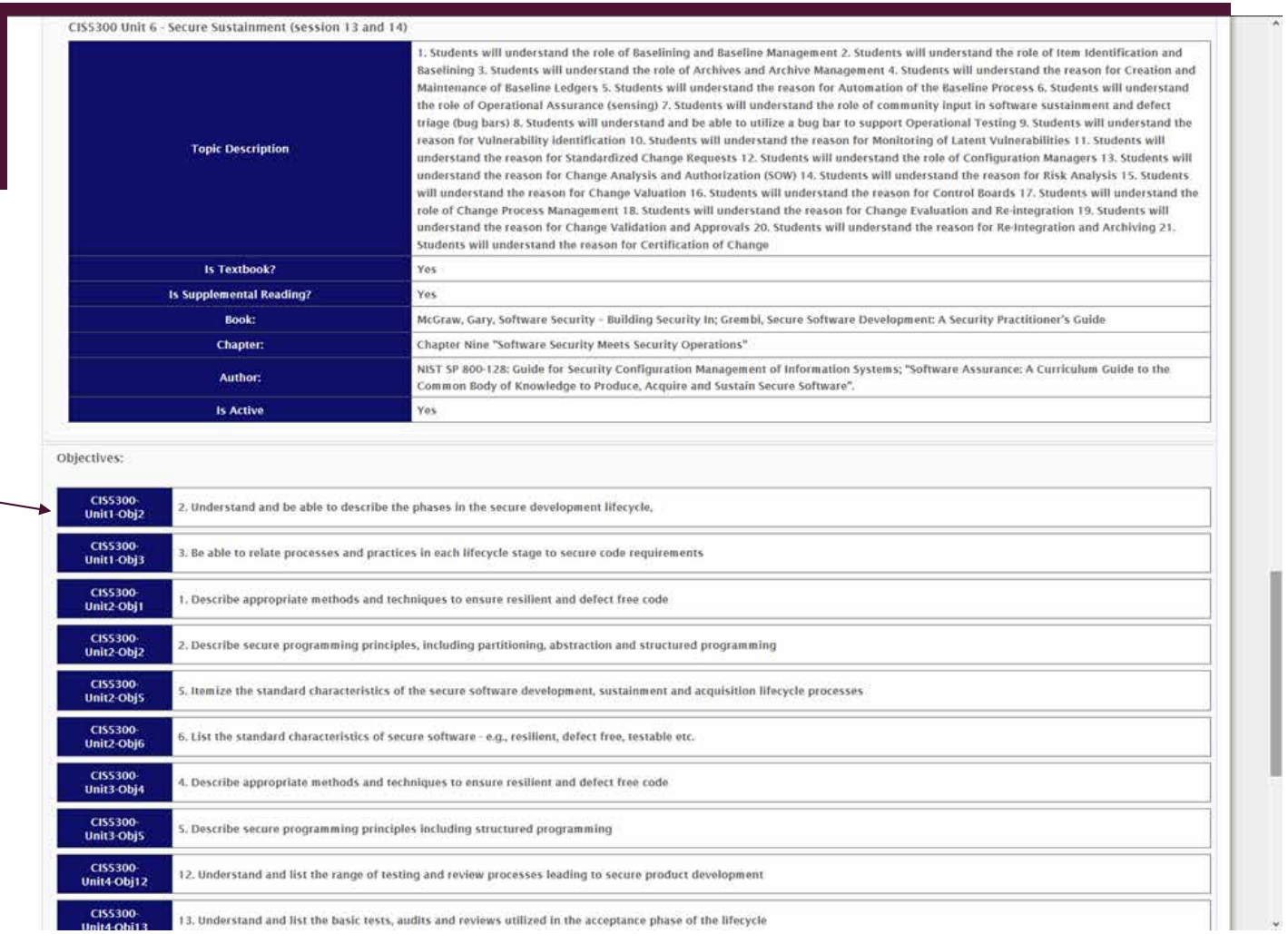
CIS5750 Unit 3 - Unit 3: Secure Systems Assurance (sessions 6, 7 and 8)

	• Students will enumerate and explain the standard steps in the security lifecycle; Plan and Organize, Implement, Operate and maintain, Monitor and evaluate • Students will describe security lifecycle management • Students will contrast the security lifecycle with the development lifecycle • Students will be able to execute a competent risk analysis based on principles • Students will develop and configure

ADD OBJECTIVES

Labeled each Objective with:

- **Course name**
- **Unit**
- **Objective #**



CIS5300 Unit 6 - Secure Sustainment (session 13 and 14)

Topic Description	1. Students will understand the role of Baselining and Baseline Management 2. Students will understand the role of Item Identification and Baselining 3. Students will understand the role of Archives and Archive Management 4. Students will understand the reason for Creation and Maintenance of Baseline Ledgers 5. Students will understand the reason for Automation of the Baseline Process 6. Students will understand the role of Operational Assurance (sensing) 7. Students will understand the role of community input in software sustainment and defect triage (bug bars) 8. Students will understand and be able to utilize a bug bar to support Operational Testing 9. Students will understand the reason for Vulnerability identification 10. Students will understand the reason for Monitoring of Latent Vulnerabilities 11. Students will understand the reason for Standardized Change Requests 12. Students will understand the role of Configuration Managers 13. Students will understand the reason for Change Analysis and Authorization (SOW) 14. Students will understand the reason for Risk Analysis 15. Students will understand the reason for Change Valuation 16. Students will understand the reason for Control Boards 17. Students will understand the role of Change Process Management 18. Students will understand the reason for Change Evaluation and Re-integration 19. Students will understand the reason for Change Validation and Approvals 20. Students will understand the reason for Re-integration and Archiving 21. Students will understand the reason for Certification of Change
Is Textbook?	Yes
Is Supplemental Reading?	Yes
Book:	McGraw, Gary, Software Security – Building Security In; Grembi, Secure Software Development: A Security Practitioner's Guide
Chapter:	Chapter Nine "Software Security Meets Security Operations"
Author:	NIST SP 800-128; Guide for Security Configuration Management of Information Systems; "Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software".
Is Active	Yes

Objectives:

CIS5300-Unit1-Obj2	2. Understand and be able to describe the phases in the secure development lifecycle,
CIS5300-Unit1-Obj3	3. Be able to relate processes and practices in each lifecycle stage to secure code requirements
CIS5300-Unit2-Obj1	1. Describe appropriate methods and techniques to ensure resilient and defect free code
CIS5300-Unit2-Obj2	2. Describe secure programming principles, including partitioning, abstraction and structured programming
CIS5300-Unit2-Obj5	5. Itemize the standard characteristics of the secure software development, sustainment and acquisition lifecycle processes
CIS5300-Unit2-Obj6	6. List the standard characteristics of secure software - e.g., resilient, defect free, testable etc.
CIS5300-Unit3-Obj4	4. Describe appropriate methods and techniques to ensure resilient and defect free code
CIS5300-Unit3-Obj5	5. Describe secure programming principles including structured programming
CIS5300-Unit4-Obj12	12. Understand and list the range of testing and review processes leading to secure product development
CIS5300-Unit4-Obj13	13. Understand and list the basic tests, audits and reviews utilized in the acceptance phase of the lifecycle

SYLLABUS

Highlighted each Unit and only those objectives that were mapped to the KU's

Unit 4: Criminal Law (session 10 and 11)

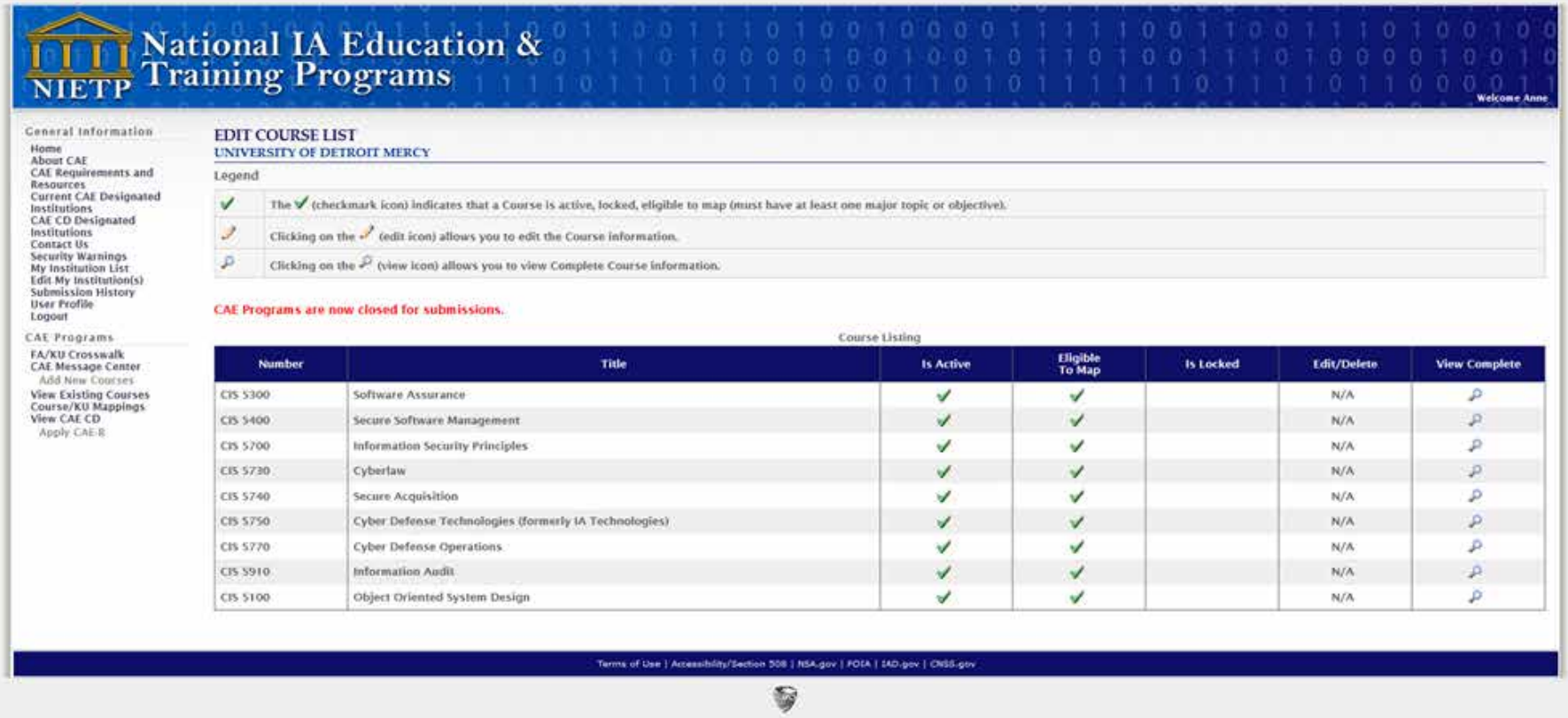
Key Content Topics:

- Students will describe the problems related to criminal investigation in cyberspace
- Students will be able to prepare logical profiles of internet unsubs
- Students will create an effective forensic investigation process
- Students will create a set of standard responses to cybercrime incidents
- Students will create an effective chain of custody
- Students will be able to identify specific areas of criminal exploitation
- Students will be able to perform end-to-end investigations leading to trial
- Students will implement oversight and control of evidence collection and preservation

Unit Learning Objectives:

1. Apply forensic techniques to cyber-criminal investigation
2. Apply the rules of evidence to cyber-criminal investigation
3. Perform effective evidence gathering
4. Execute systematic chain of custody and evidence assurance
5. Generate appropriate and useful cyber-criminal profiles
6. Ensure a stable state of evidence preservation
7. Perform standard testimony in a cyber-criminal case
8. Execute systematic evolution of cyber-criminal investigation
9. Ensure compliance with the rules of court in all cyber-criminal cases

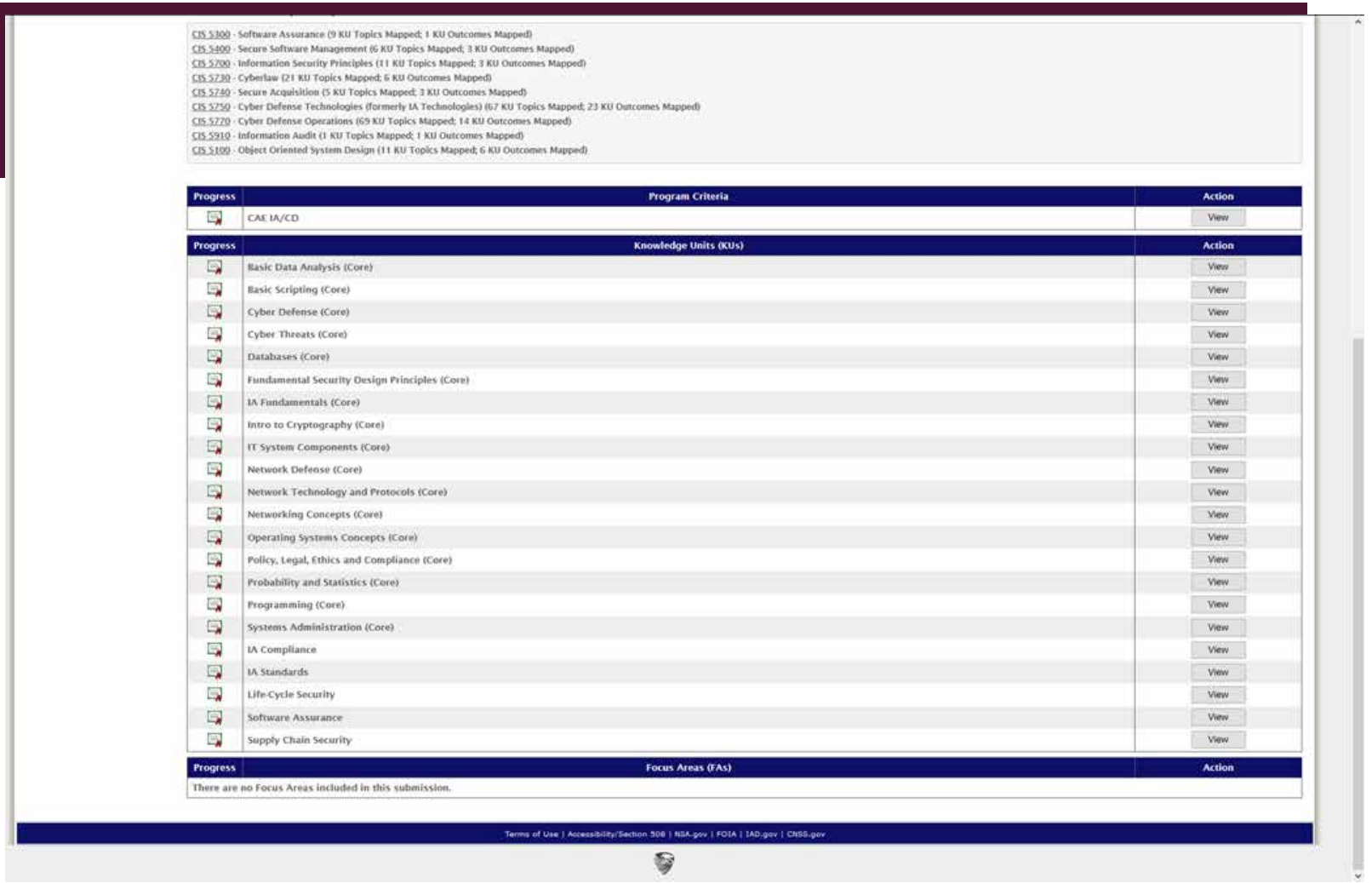
READY TO MAP TO THE KU'S



KU MAPPING

- **KU's were selected**
- **Courses entered**
- **Topics entered**
- **Objectives entered**

- **Now you can map.**



CIS 5300 - Software Assurance (9 KU Topics Mapped; 1 KU Outcomes Mapped)
CIS 5400 - Secure Software Management (6 KU Topics Mapped; 3 KU Outcomes Mapped)
CIS 5700 - Information Security Principles (11 KU Topics Mapped; 3 KU Outcomes Mapped)
CIS 5730 - Cyberlaw (21 KU Topics Mapped; 6 KU Outcomes Mapped)
CIS 5740 - Secure Acquisition (5 KU Topics Mapped; 3 KU Outcomes Mapped)
CIS 5750 - Cyber Defense Technologies (formerly IA Technologies) (67 KU Topics Mapped; 23 KU Outcomes Mapped)
CIS 5770 - Cyber Defense Operations (69 KU Topics Mapped; 14 KU Outcomes Mapped)
CIS 5910 - Information Audit (1 KU Topics Mapped; 1 KU Outcomes Mapped)
CIS 5100 - Object Oriented System Design (11 KU Topics Mapped; 6 KU Outcomes Mapped)

Progress	Program Criteria	Action
	CAE IA/CD	View

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis (Core)	View
	Basic Scripting (Core)	View
	Cyber Defense (Core)	View
	Cyber Threats (Core)	View
	Databases (Core)	View
	Fundamental Security Design Principles (Core)	View
	IA Fundamentals (Core)	View
	Intro to Cryptography (Core)	View
	IT System Components (Core)	View
	Network Defense (Core)	View
	Network Technology and Protocols (Core)	View
	Networking Concepts (Core)	View
	Operating Systems Concepts (Core)	View
	Policy, Legal, Ethics and Compliance (Core)	View
	Probability and Statistics (Core)	View
	Programming (Core)	View
	Systems Administration (Core)	View
	IA Compliance	View
	IA Standards	View
	Life-Cycle Security	View
	Software Assurance	View
	Supply Chain Security	View

Progress	Focus Areas (FAs)	Action
There are no Focus Areas included in this submission.		

KU MAPPING TOPICS

- **Selected *KU-Basic Data Analysis***
- **Select each Topic**

MAP KNOWLEDGE UNIT: BASIC DATA ANALYSIS
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the ✓ completed icon (checkmark) next to Items that have been mapped.

Knowledge Unit Topics & Outcomes

Mapped	Topic
	Graphing/Charts
	Problem Solving
	Spreadsheet Functions
	Summary Statistics

Mapped	Outcome
	Students will be able to apply standard statistical inference procedures to draw conclusions from data.

Return to CAE IA/CD Progress List

KU MAPPING TOPICS

- **Selected *KU-Basic Data Analysis***
- **Map the Course – *CIS 5100 Object Oriented System Design***

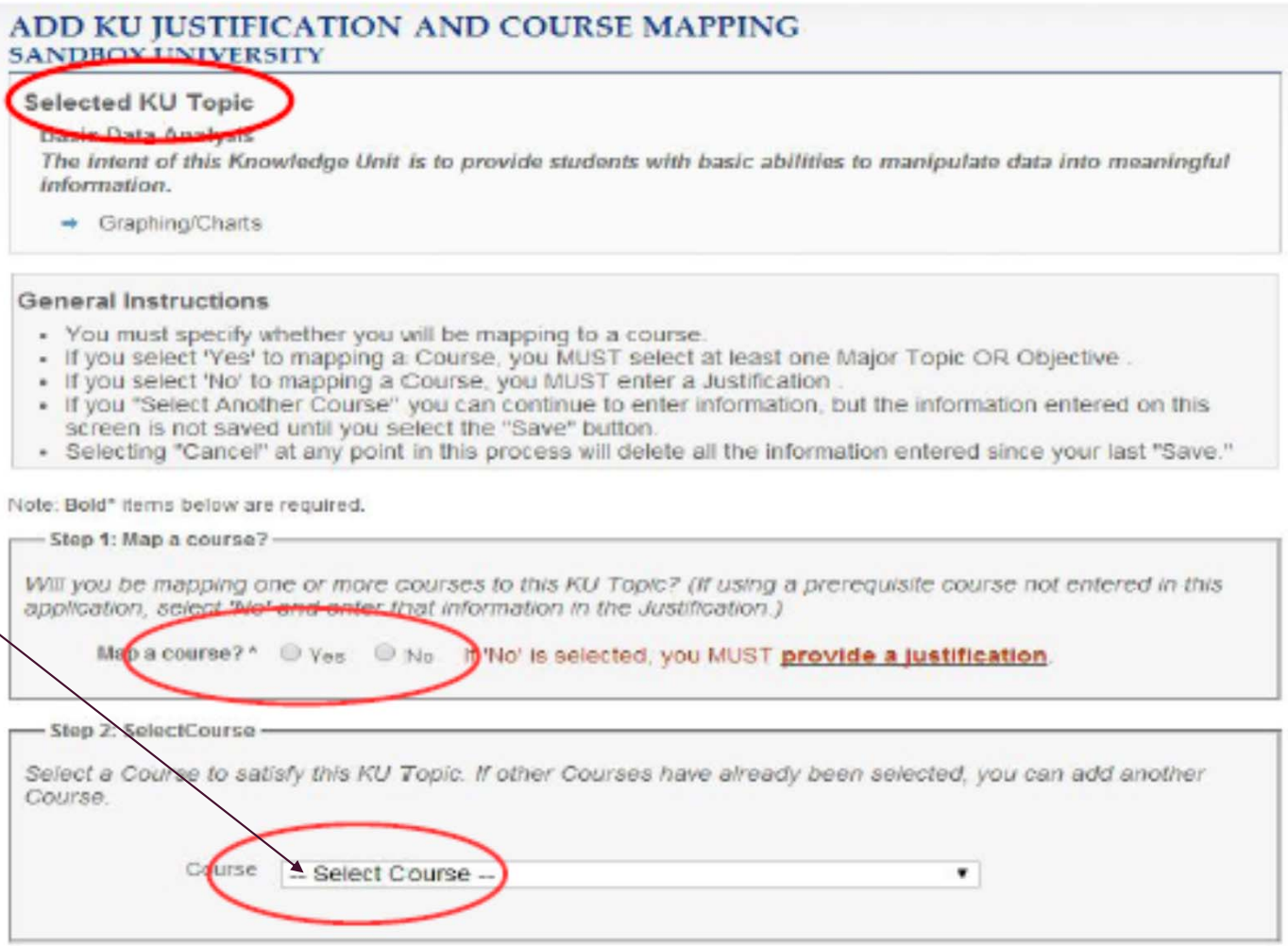


Fig. 29 Add Justification and Course Mapping – Topics (top third)

KU MAPPING TOPICS

- **Select Topics**
- **Select Objectives**

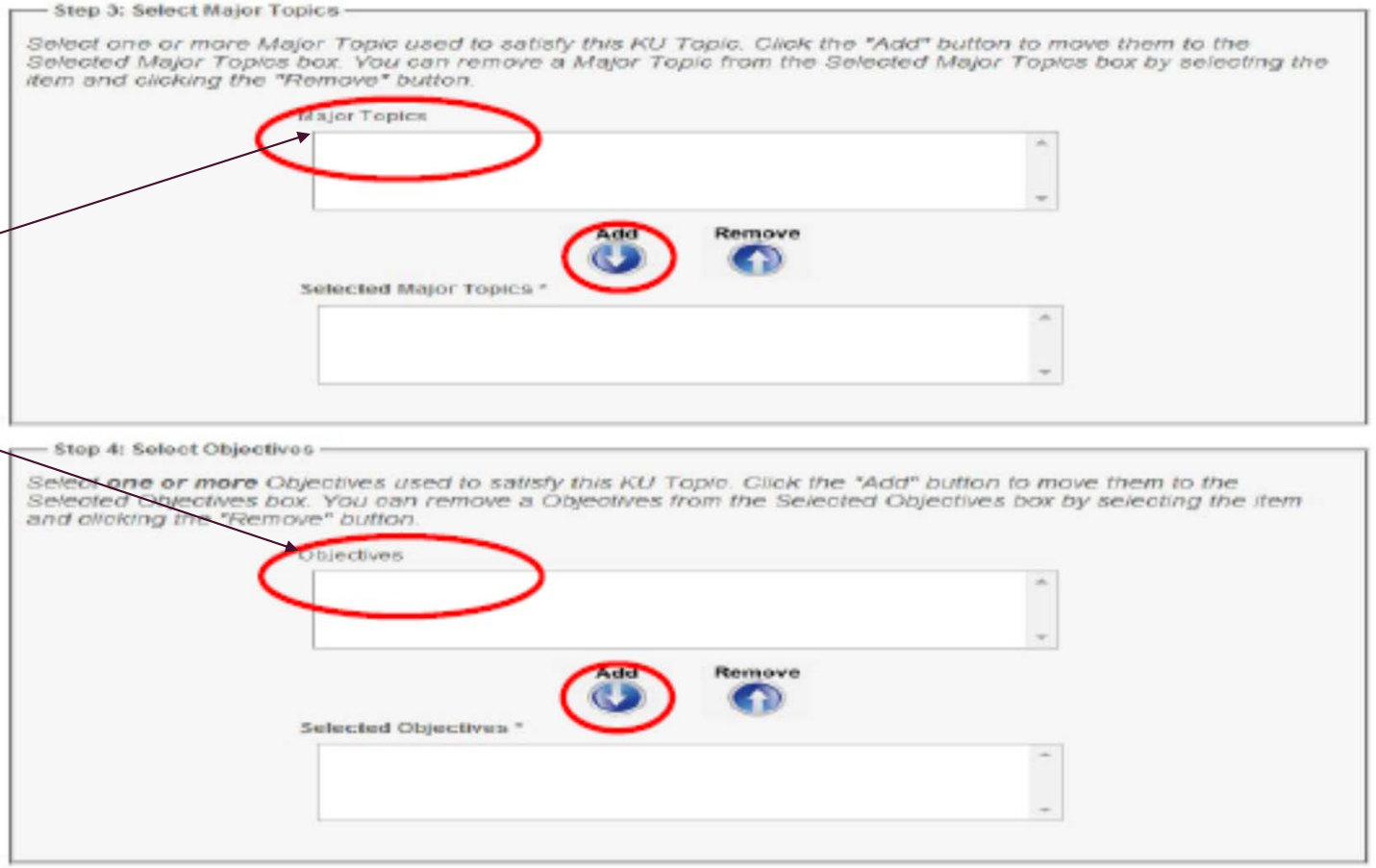
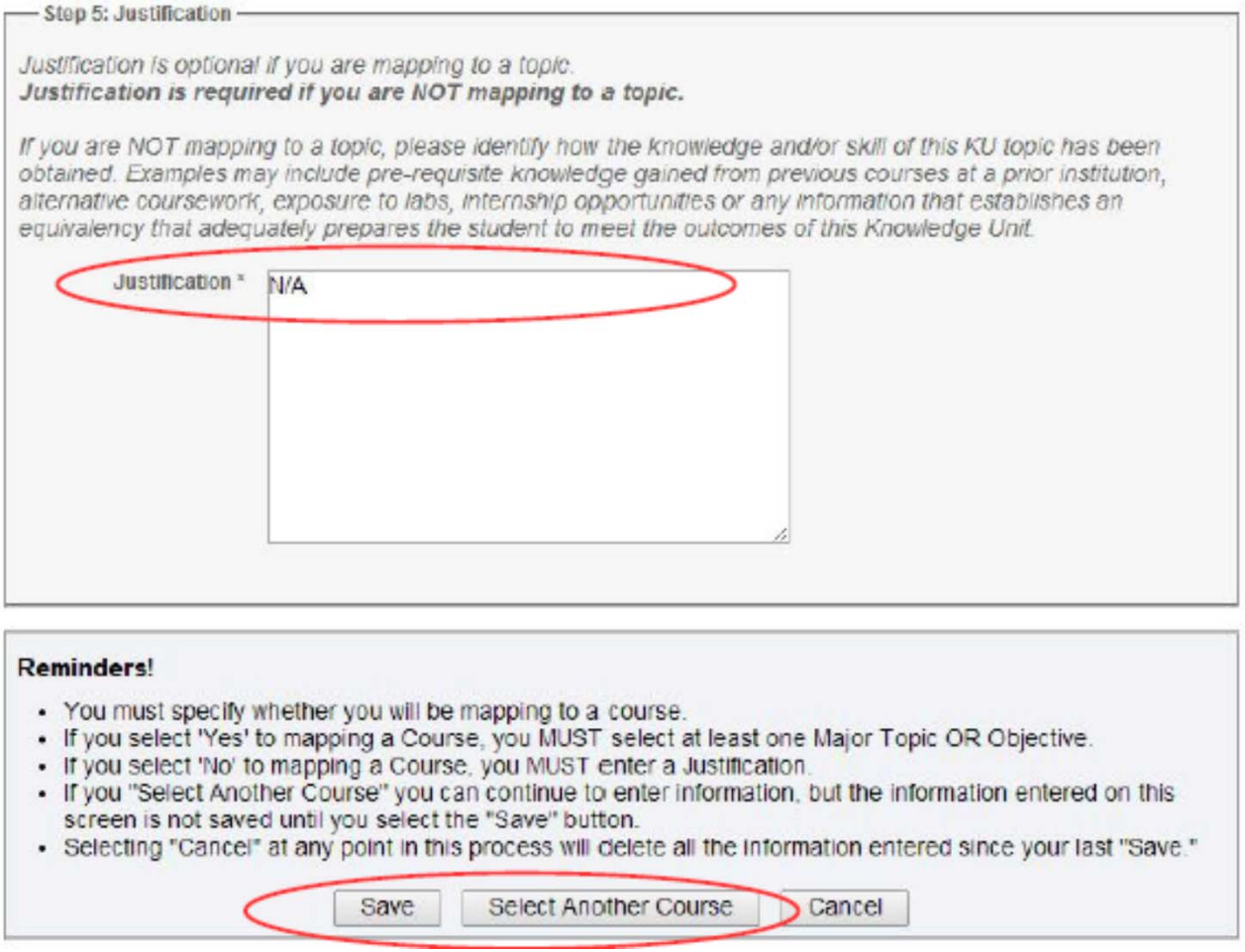


Fig. 30 Add Justification and Course Mapping – Topics (middle third)

KU MAPPING TOPICS

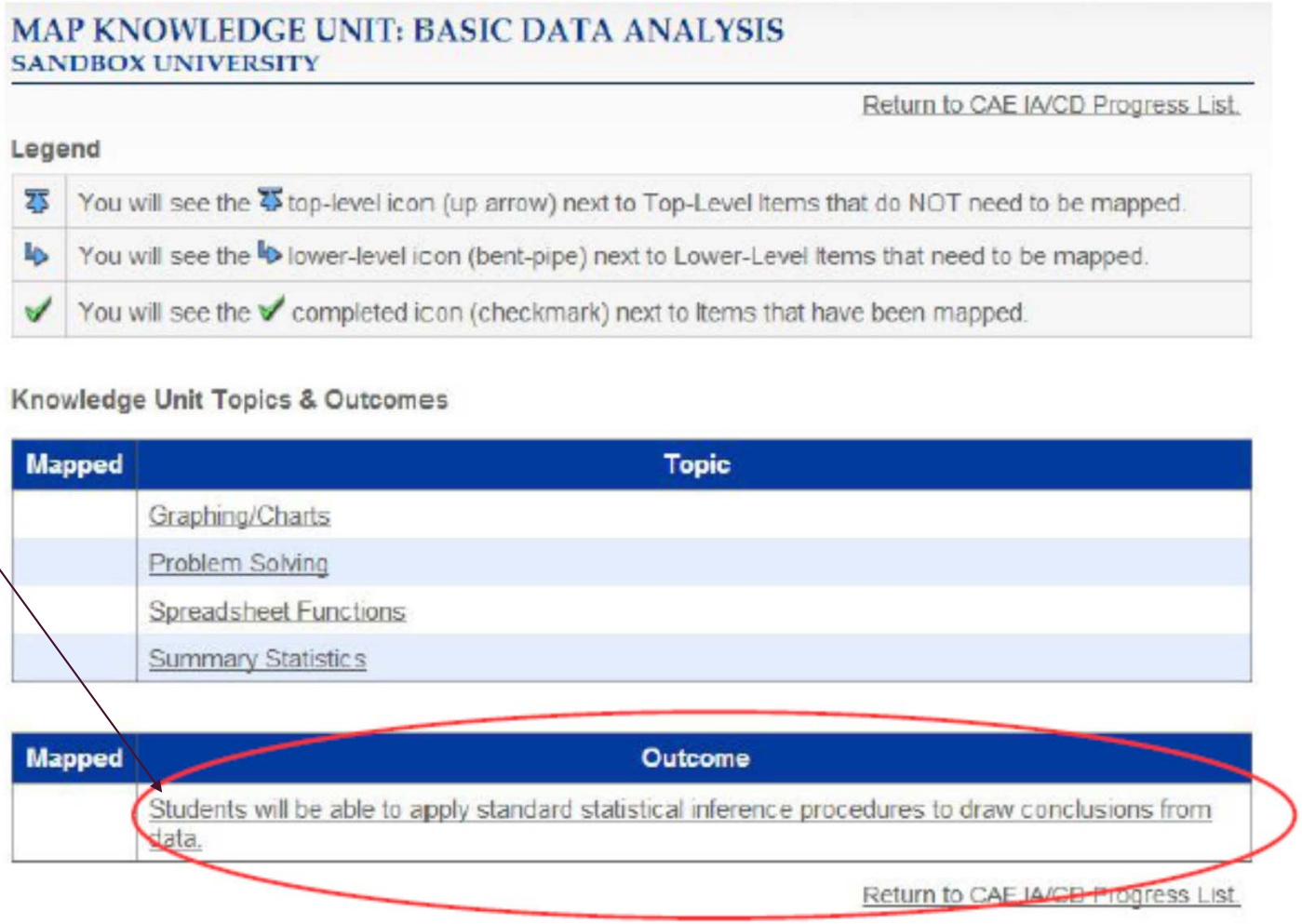
- **Justification Box—only required when a course topic is not explicitly covered in the course material**

The "Justification" box (Fig. 30) is only required when a course topic matching the KU topic is not explicitly covered in the course material but is either required prerequisite knowledge for the course. (e.g., CCNA, CISSP, Network+, etc.) or will be achieved through an activity in the course.



KU MAPPING OUTCOMES

- **Selected *KU-Basic Data Analysis***
- **Select each Outcome**



MAP KNOWLEDGE UNIT: BASIC DATA ANALYSIS
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the completed icon (checkmark) next to Items that have been mapped.

Knowledge Unit Topics & Outcomes

Mapped	Topic
	Graphing/Charts
	Problem Solving
	Spreadsheet Functions
	Summary Statistics

Mapped	Outcome
	Students will be able to apply standard statistical inference procedures to draw conclusions from data.

Return to CAE IA/CD Progress List

KU MAPPING OUTCOMES

- **Selected *KU-Basic Data Analysis***
- **Map the Course – CIS 5100 Object Oriented System Design**

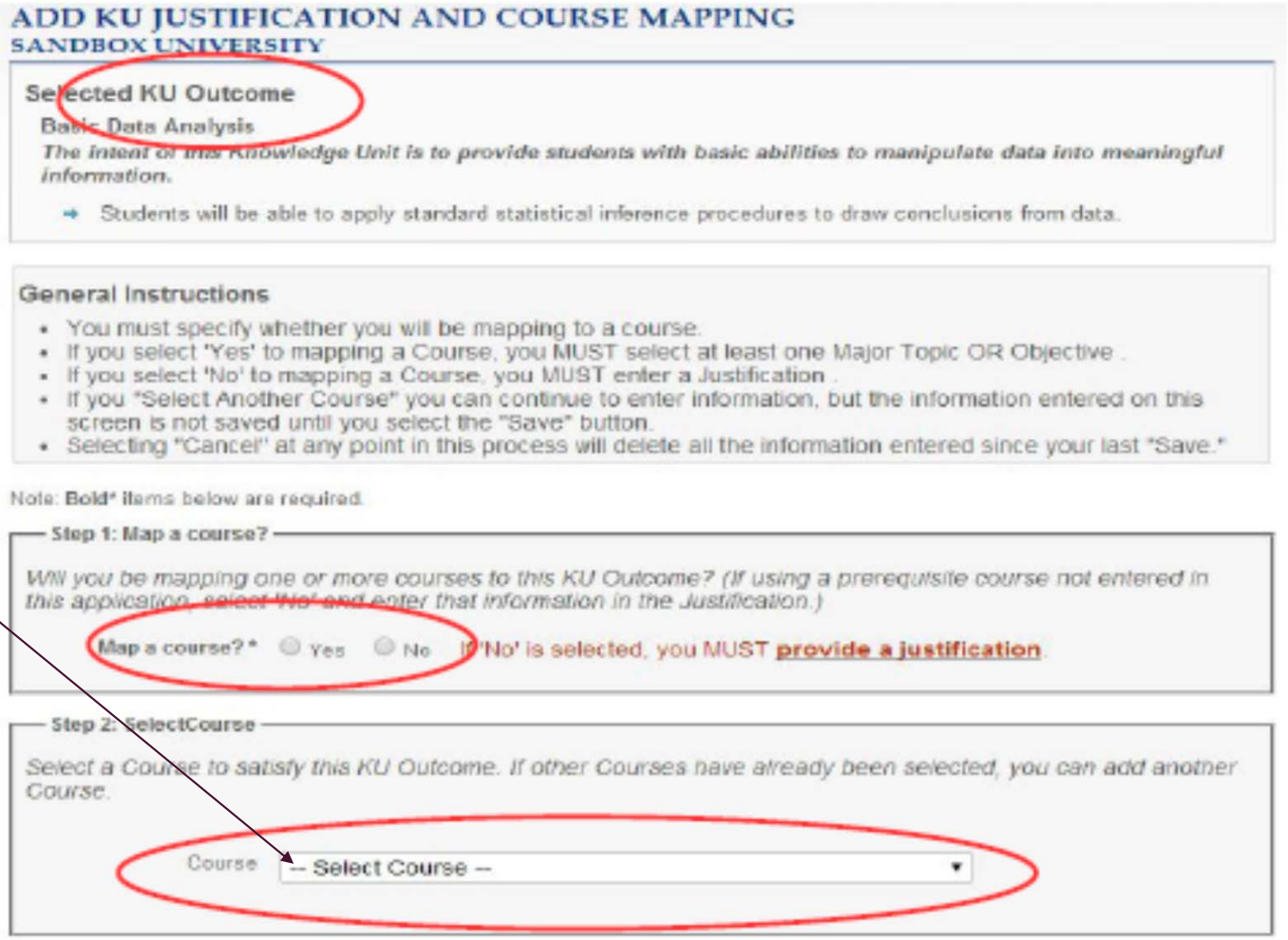


Fig. 33 Add Justification and Course Mapping – Outcomes

KU MAPPING OUTCOMES

- **Selected *KU-Basic Data Analysis***
- **Map the Course Topics**
- **Map the Course Objectives**

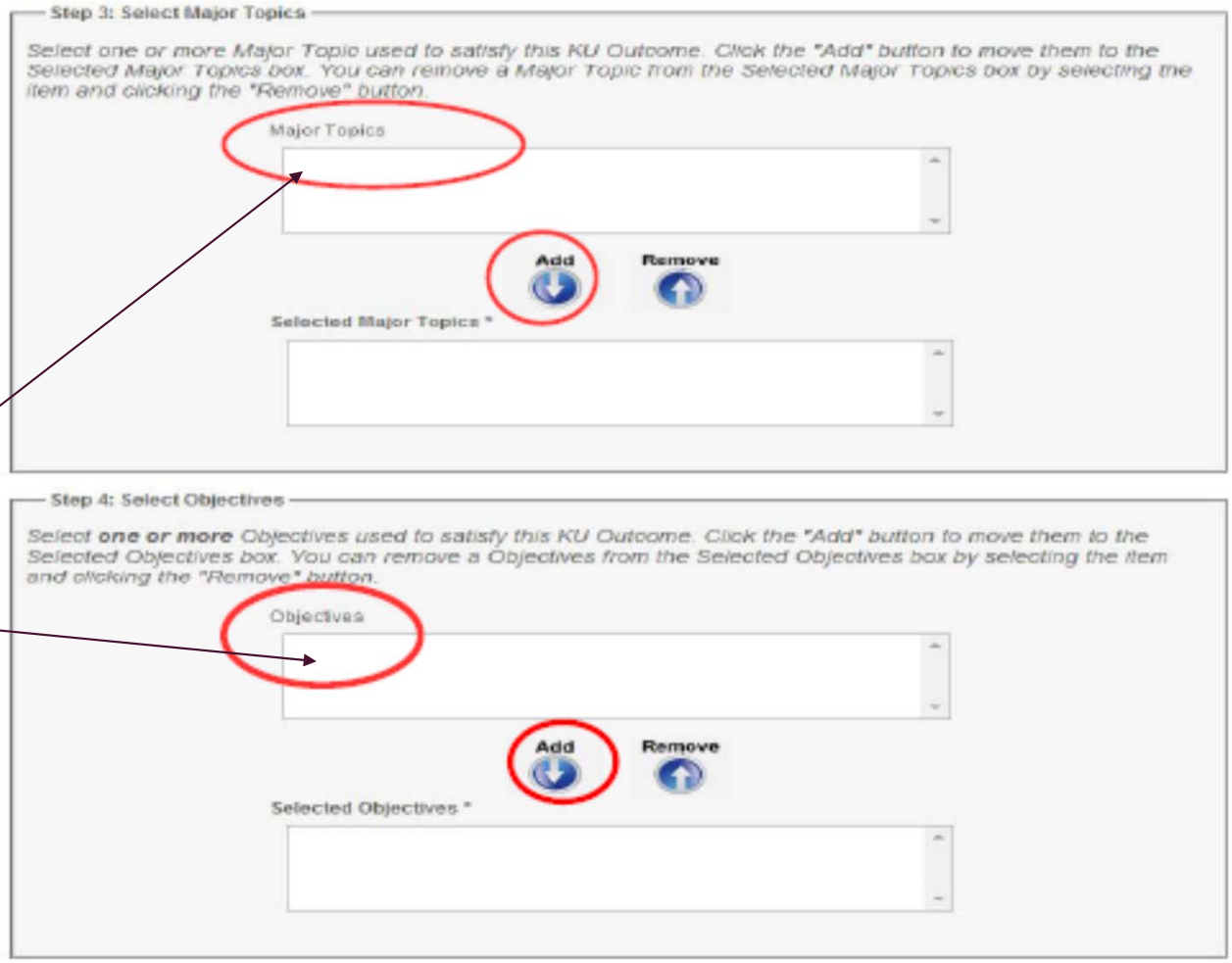
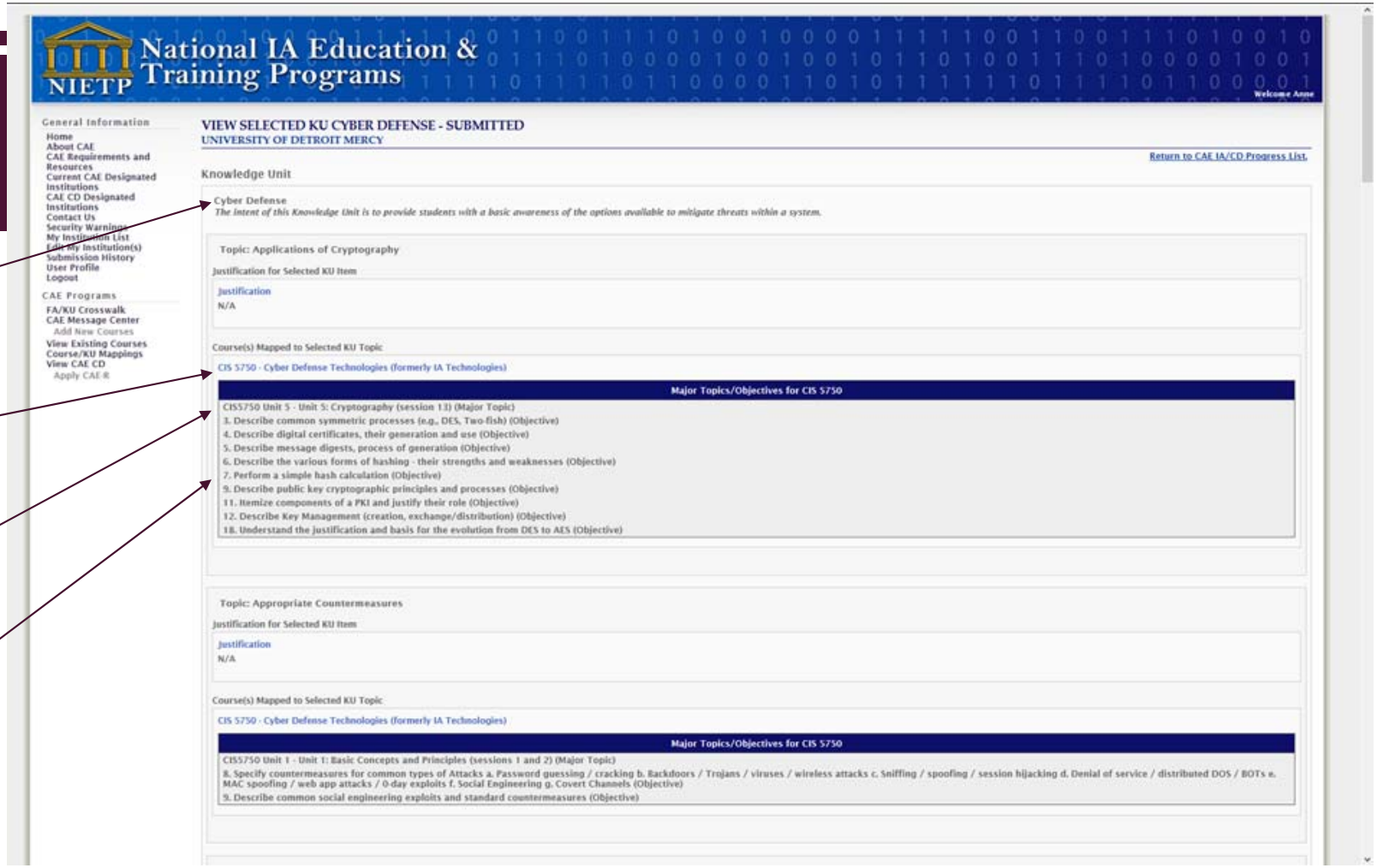


Fig. 34 Add Justification and Course Mapping – Outcomes

KU MAPPING

- **KU – Cyber Defense**
- **Course – CIS 5750 Cyber Defense Technologies**
- **Major Topic – Cryptography**
- **Objectives (9)**

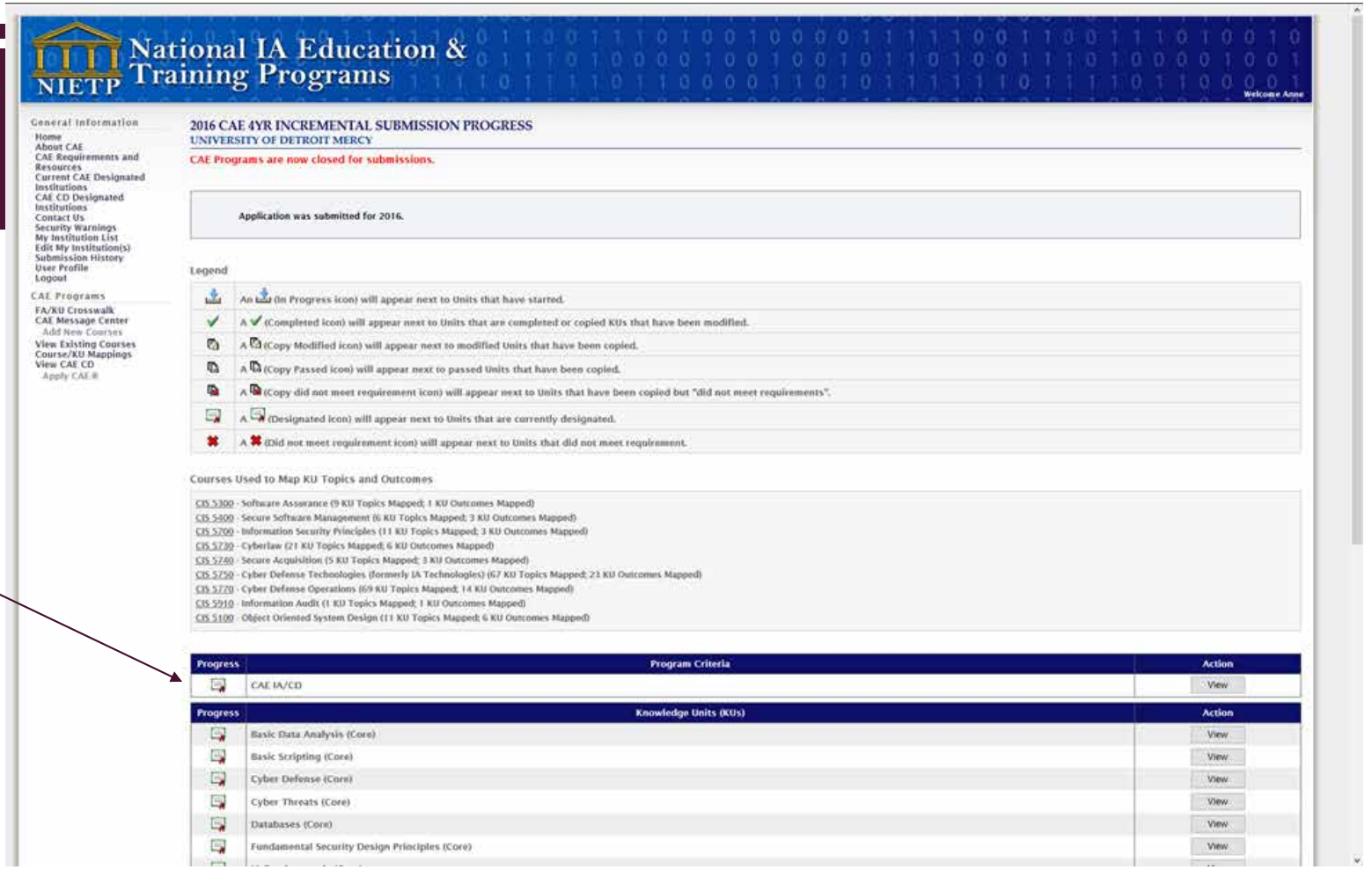


CHECKLIST

STEP 1 - Add New Courses	Step 2 - Map KU's to Courses			
Add (9) New Courses	**(22) KU/OKU Topic and Outcomes Mapping**	**Entered in NIETP**	**Reviewed**	**Completed**
CIS 5100, Object Oriented Development	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	KU2, Basic Scripting	X	X	X
	KU17, Programming	X	X	X
CIS 5300, Software Assurance	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	OKU1, Software Assurance	X	X	X
CIS 5400, Secure Software Management	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	OKU5, Life-Cycle Security	X	X	X
CIS 5700, Information Security Principles	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	KU1, Basic Data Analysis	X	X	X
	KU16, Probability and Statistics	X	X	X
CIS 5730, Cyberlaw	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	OKU2, IA Compliance	X	X	X
	OKU3, IA Standards	X	X	X
	KU9, Policy, Legal, Ethics, and Compliance	X	X	X
CIS 5740, Secure Acquisition	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	OKU3, IA Standards	X	X	X
	OKU4, Supply Chain Security	X	X	X
CIS 5750, Cyber Defense Technologies	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	KU3, Cyber Defense	X	X	X
	KU4, Cyber Threats	X	X	X
	KU5, Fundamental Security Design Principles	X	X	X
	KU6, Information Assurance Fundamentals	X	X	X
	KU7, Introduction to Cryptography	X	X	X
	KU8, Information Technology System Components	X	X	X
	KU10, Networking Concepts	X	X	X
	KU12, Databases	X	X	X
CIS 5770, Cyber Defense Operations	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	KU3, Cyber Defense	X	X	X
	KU4, Cyber Threats	X	X	X
	KU11, Systems Administration	X	X	X
	KU13, Network Defense	X	X	X
	KU14, Network Technology and Protocols	X	X	X
	KU15, Operating Systems Concepts	X	X	X
CIS 5910, Information Audit	Add New Course	X	X	X
Edit Syllabus, save as .PDF	Upload syllabus	X	X	X
	OKU2, IA Compliance	X	X	X
	OKU3, IA Standards	X	X	X

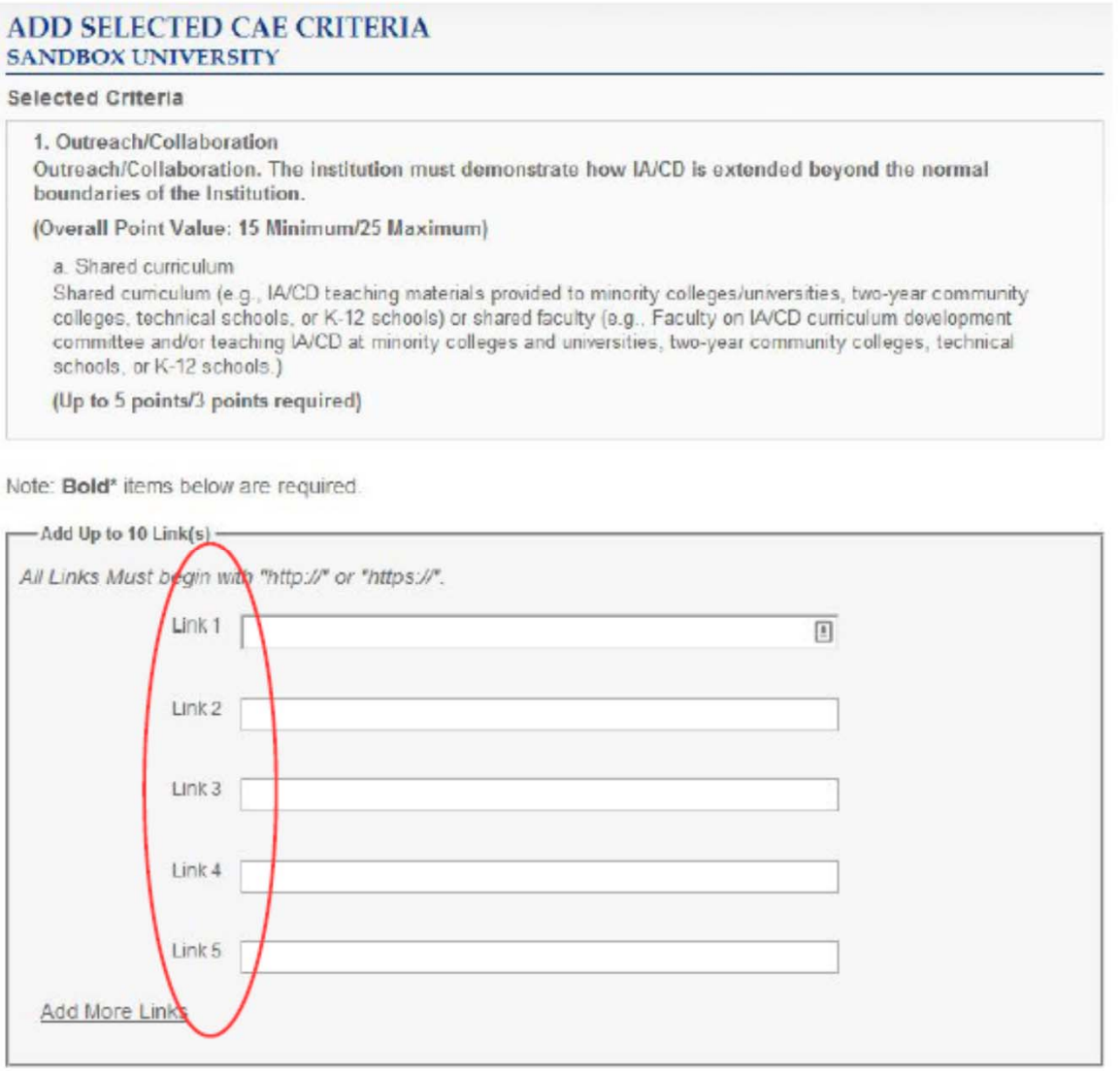
MEASUREMENT CRITERIA

Access the 8 Measurement Criteria (Called Program Criteria in App)

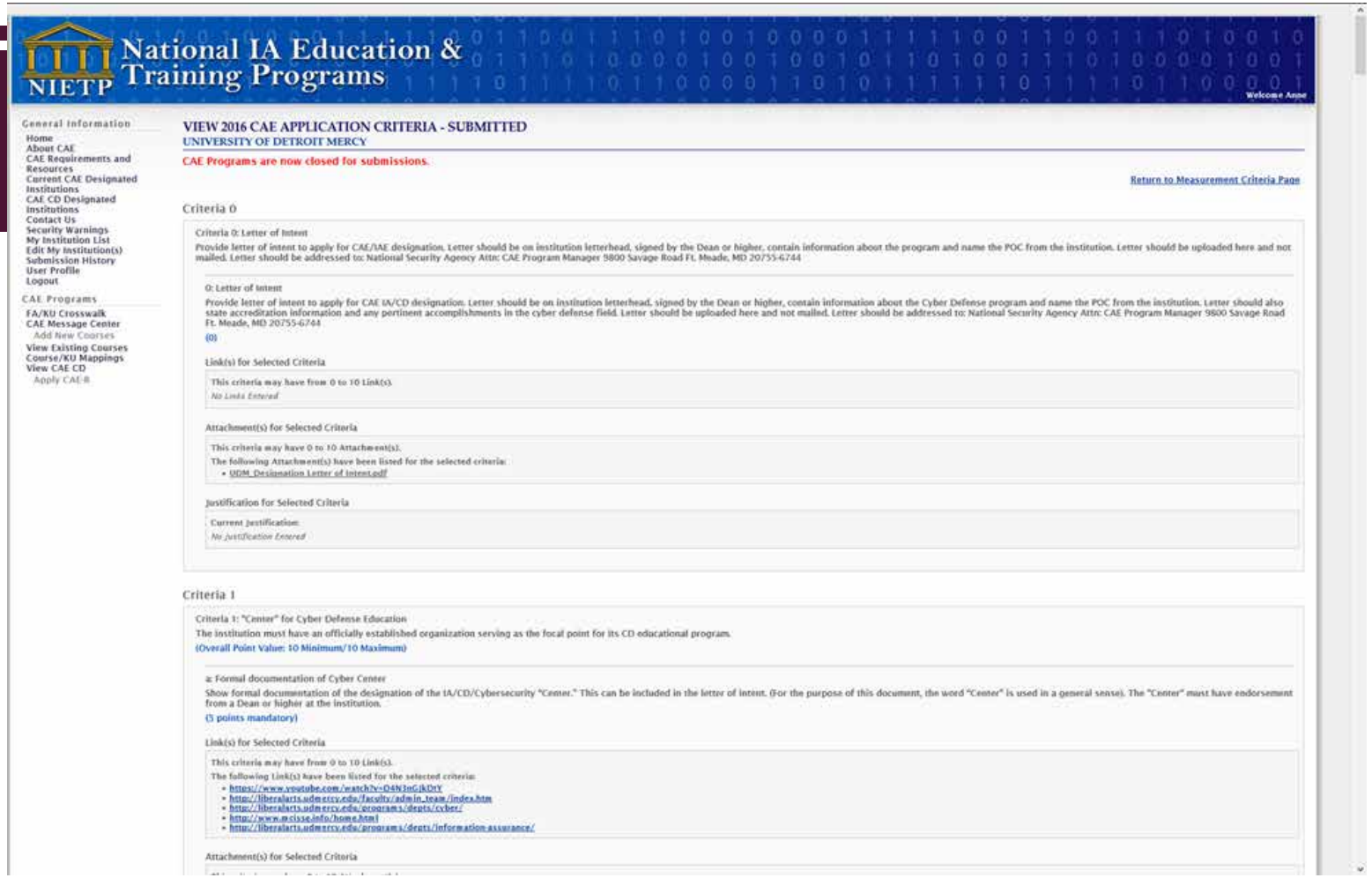


MEASUREMENT CRITERIA

For each Criteria, you enter links, .pdf docs, and text in a text box

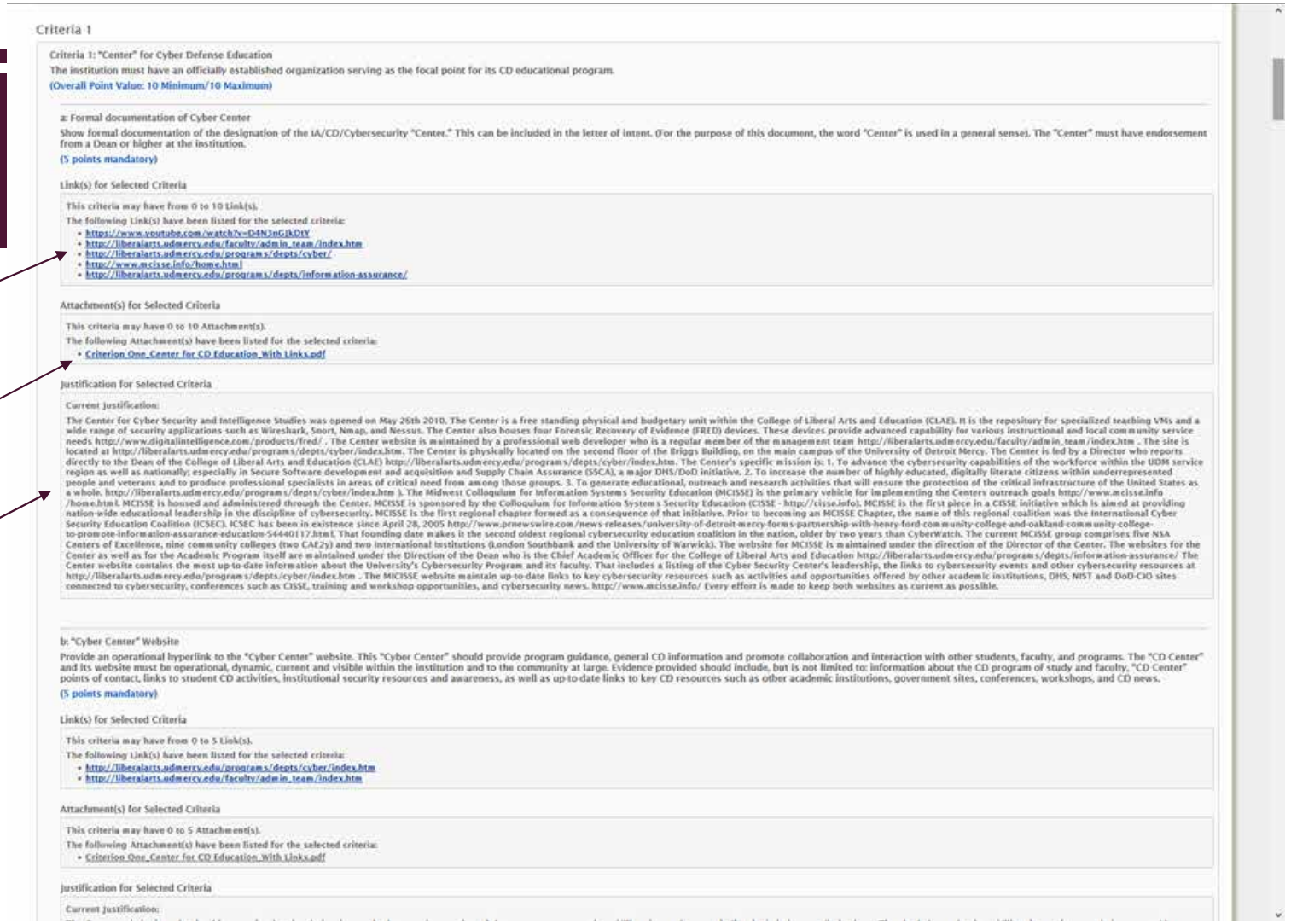


MEASUREMENT CRITERIA 0



MEASUREMENT CRITERIA

- **Links**
- **.pdf docs**
- **Text**



Criteria 1

Criteria 1: "Center" for Cyber Defense Education

The institution must have an officially established organization serving as the focal point for its CD educational program.

(Overall Point Value: 10 Minimum/10 Maximum)

a: Formal documentation of Cyber Center

Show formal documentation of the designation of the IA/CD/Cybersecurity "Center." This can be included in the letter of intent. (For the purpose of this document, the word "Center" is used in a general sense). The "Center" must have endorsement from a Dean or higher at the institution.

(5 points mandatory)

Link(s) for Selected Criteria

This criteria may have from 0 to 10 Link(s).

The following Link(s) have been listed for the selected criteria:

- https://www.youtube.com/watch?v=D4NJnGjkDtY
- http://liberalarts.udmercy.edu/faculty/admin_team/index.htm
- http://liberalarts.udmercy.edu/programs/depts/cyber/
- http://www.mcisse.info/home.html
- http://liberalarts.udmercy.edu/programs/depts/information-assurance/

Attachment(s) for Selected Criteria

This criteria may have 0 to 10 Attachment(s).

The following Attachment(s) have been listed for the selected criteria:

- Criterion One_Center for CD Education_With Links.pdf

Justification for Selected Criteria

Current Justification:

The Center for Cyber Security and Intelligence Studies was opened on May 26th 2010. The Center is a free standing physical and budgetary unit within the College of Liberal Arts and Education (CLAE). It is the repository for specialized teaching VMs and a wide range of security applications such as Wireshark, Snort, Nmap, and Nessus. The Center also houses four Forensic Recovery of Evidence (FRED) devices. These devices provide advanced capability for various instructional and local community service needs http://www.digitalintelligence.com/products/fred/ . The Center website is maintained by a professional web developer who is a regular member of the management team http://liberalarts.udmercy.edu/faculty/admin_team/index.htm . The site is located at http://liberalarts.udmercy.edu/programs/depts/cyber/index.htm. The Center is physically located on the second floor of the Briggs Building, on the main campus of the University of Detroit Mercy. The Center is led by a Director who reports directly to the Dean of the College of Liberal Arts and Education (CLAE) http://liberalarts.udmercy.edu/programs/depts/cyber/index.htm. The Center's specific mission is: 1. To advance the cybersecurity capabilities of the workforce within the UDM service region as well as nationally; especially in Secure Software development and acquisition and Supply Chain Assurance (SSCA), a major DHS/DoD initiative. 2. To increase the number of highly educated, digitally literate citizens within underrepresented people and veterans and to produce professional specialists in areas of critical need from among those groups. 3. To generate educational, outreach and research activities that will ensure the protection of the critical infrastructure of the United States as a whole. http://liberalarts.udmercy.edu/programs/depts/cyber/index.htm). The Midwest Colloquium for Information Systems Security Education (MCISSE) is the primary vehicle for implementing the Centers outreach goals http://www.mcisse.info /home.html. MCISSE is housed and administered through the Center. MCISSE is sponsored by the Colloquium for Information Systems Security Education (CISSE - http://cisse.info). MCISSE is the first piece in a CISSE initiative which is aimed at providing nation-wide educational leadership in the discipline of cybersecurity. MCISSE is the first regional chapter formed as a consequence of that initiative. Prior to becoming an MCISSE Chapter, the name of this regional coalition was the International Cyber Security Education Coalition (ICSEC). ICSEC has been in existence since April 28, 2005 http://www.prnewswire.com/news-releases/university-of-detroit-mercy-forms-partnership-with-henry-ford-community-college-and-oakland-community-college-to-promote-information-assurance-education-54440117.html, That founding date makes it the second oldest regional cybersecurity education coalition in the nation, older by two years than CyberWatch. The current MCISSE group comprises five NSA Centers of Excellence, nine community colleges (two CAE2y) and two international institutions (London Southbank and the University of Warwick). The website for MCISSE is maintained under the direction of the Director of the Center. The websites for the Center as well as for the Academic Program itself are maintained under the Direction of the Dean who is the Chief Academic Officer for the College of Liberal Arts and Education http://liberalarts.udmercy.edu/programs/depts/information-assurance/ The Center website contains the most up-to-date information about the University's Cybersecurity Program and its faculty. That includes a listing of the Cyber Security Center's leadership, the links to cybersecurity events and other cybersecurity resources at http://liberalarts.udmercy.edu/programs/depts/cyber/index.htm . The MICISSE website maintain up-to-date links to key cybersecurity resources such as activities and opportunities offered by other academic institutions, DHS, NIST and DoD-CIO sites connected to cybersecurity, conferences such as CISSE, training and workshop opportunities, and cybersecurity news. http://www.mcisse.info/ Every effort is made to keep both websites as current as possible.

b: "Cyber Center" Website

Provide an operational hyperlink to the "Cyber Center" website. This "Cyber Center" should provide program guidance, general CD information and promote collaboration and interaction with other students, faculty, and programs. The "CD Center" and its website must be operational, dynamic, current and visible within the institution and to the community at large. Evidence provided should include, but is not limited to: information about the CD program of study and faculty, "CD Center" points of contact, links to student CD activities, institutional security resources and awareness, as well as up-to-date links to key CD resources such as other academic institutions, government sites, conferences, workshops, and CD news.

(5 points mandatory)

Link(s) for Selected Criteria

This criteria may have from 0 to 5 Link(s).

The following Link(s) have been listed for the selected criteria:

- http://liberalarts.udmercy.edu/programs/depts/cyber/index.htm
- http://liberalarts.udmercy.edu/faculty/admin_team/index.htm

Attachment(s) for Selected Criteria

This criteria may have 0 to 5 Attachment(s).

The following Attachment(s) have been listed for the selected criteria:

- Criterion One_Center for CD Education_With Links.pdf

Justification for Selected Criteria

Current Justification:

CAE SUBMITTED SUCCESSFULLY!