Communications of the IIMA

Volume 9 | Issue 1 Article 6

2009

A Framework for Improving Information Assurance Education

Daniel P. Manson
California State Polytechnic University Pomona

Steven S. Curl
California State Polytechnic University Pomona

Javier Torner
California State Polytechnic University Pomona

A Framework for Improving Information Assurance Education

Daniel P. Manson
California State Polytechnic University Pomona
USA
dmanson@csupomona.edu

Steven S. Curl
California State Polytechnic University Pomona
USA
scurl@csupomona.edu

Javier Torner
California State University San Bernardino
USA
jtorner@csusb.edu

ABSTRACT

As a field of growing importance, information assurance is dedicated to protecting our information systems and related assets. In order for this field to deliver on its promise, effective information assurance education, both in the classroom and beyond, is essential. However, relatively little empirical research has been done on the effectiveness of information assurance education in the classroom. Faculty developing and teaching information assurance curricula can choose from differing industry and government standards as well as a range of methods for delivering this education. As a first step toward building a research framework for better assessing the effectiveness of information assurance education, this paper describes an initial research study of information assurance curricula and related teaching methods. Surveys and interviews of faculty teaching information assurance were conducted to determine their assessment of existing standards and the best means for improving the educational experience for students. The results obtained provide the beginning of a framework for further research in this area.

INTRODUCTION

The National Security Agency defines information assurance (IA) as "The protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats" (National Security Agency, 2009a). Recent congressional hearings have emphasized the importance of cyber security, going so far as to propose the creation of an Office of the National Cybersecurity Advisor (Condon, 2009). Obviously, the need for graduates with extensive knowledge in IA has never been greater. In response to this need, a growing number of academic programs have emerged with specializations in information assurance. These programs now include 94 schools designated as Centers of Academic Excellence in Information Assurance Education (CAE) by the National Security Agency and Department of Homeland Security.

Government Standards

While the need to teach information assurance as a separate body of knowledge is clearly important, the task of deciding what to include in the curriculum remains. Curricula have been found to vary greatly from one academic program to another. To qualify as a Center of Academic Excellence, CAE schools must map their curricula to government standards developed by the Committee on National Security Systems (CNSS) for Information Security personnel (INFOSEC). Regulations are issued in the form of numbered directives or instructions such as CNSS Instruction 4012 (standard for senior systems managers) or a National Security Telecommunications and Information Systems Security Instruction (NSTISSI). These standards include the following:

- Information Systems Security (INFOSEC) Professionals, NSTISSI 4011,
- Senior Systems Managers, CNSSI 4012,
- System Administrators (SA), CNSSI 4013,
- Information Systems Security Officers, CNSSI 4014,
- System Certifiers, NSTISSI 4015, and
- Risk Analyst, CNSSI 4016.

The source for these standards were from NSA Information Assurance Courseware Evaluation Program (NSA, 2009b).

As a prerequisite for applying to CAE status, schools must map to NSTISSI 4011 and at least one other IA courseware evaluation standard in the CNSS for the NSTISSI 4011 through 4016 series. The NSTISSI 4011 standard includes seven topic areas, which are listed below:

- Automated Information Systems (AIS) Basics,
- Security Basics,
- Communications Basics,
- NSTISSI Basics,
- NSTISSI Planning and Management,
- NSTISSI Policies and Procedures, and
- System Operating Environment.

The source for this information is from National Training Standard for Information Security (Infosec) Professionals (NSTISSI, 1994).

Industry Standards

For industry professionals, the information assurance certification of choice is the Certified Information Systems Security Professional (CISSP) designation. To become a CISSP, a candidate must have five years of experience in the information security field or four years plus a college degree, pass an examination covering the 10 domains of the CISSP Common Body of Knowledge (CBK), and be endorsed by a current CISSP holder. The ten CBK domains are as follows:

- Access Control,
- Application Security,
- Business Continuity and Disaster Recovery Planning ,
- Cryptography,
- Information Security and Risk Management,
- Legal, Regulations, Compliance and Investigations,
- Operations Security,
- Physical (Environmental) Security,
- Security Architecture and Design, and
- Telecommunications and Network Security.

The information is from ISC(2) Education and Certification (ISC(2), 2009).

In October 2007, the Department of Homeland Security (DHS) released its own IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. One of the main goals of this publication is to provide "a content guideline that can be leveraged to facilitate cost-effective professional development of the IT workforce, including future skills training and certifications, academic curricula, or other affiliated human resource activities" (Department of Homeland Security, 2007a).

The DHS IT Security EBK includes the following competency areas:

- Data Security,
- Digital Forensics,
- Enterprise Continuity,
- Incident Management,
- IT Security Training and Awareness,
- IT Systems Operations and Maintenance,
- Network Security and Telecommunications,
- Personnel Security,
- Physical and Environmental Security,
- Procurement,
- Regulatory and Standards Compliance, and
- Risk Management.

The information is from Department of Homeland Security (DHS, 2007a, page 43).

The EBK was developed with input from many existing standards, programs and policies. Some of these contributing resources are listed below:

- DoD 8570.1 IA Training and Certification Framework,
- Committee on National Security Systems (CNSS) Training Standards,

- National Institute of Standards and Technology SP-800 Series, and
- Models (COBIT, SSE-CMM, CMMi).

The information is Department of Homeland Security publication (DHS, 2007b).

Prior researchers have looked at several different approaches to developing information assurance curriculum. Researchers have encouraged curriculum developers to utilize government resources, such as the National Security Agency (NSA), the National Institute for Standards and Technology (NIST), and the Committee on National Security Systems (CNSS) as sound resources toward making security education and training a goal (Bogolea and Wijekumar, 2004). Whitman and Mattord (2005) used the CISSP and NSA (NSTISSI) training standards to develop introductory and advanced knowledge areas they felt were essential to information assurance career progression. Manson and Curl (2003) compared the ISECON model curriculum approach and topic areas to the NSTISSI 4011. While prior research has looked at these existing standards, IA curriculum research has not looked at delivery modes and methods and has not yet included the DHS IT Security EBK.

By examining the certification requirements set by two common standards and one emerging standard, this research hopes to identify common themes and provides useful insights into the design and delivery of information assurance curriculum. These standards include NSA NSTISSI 4011 standard, the CISSP domains, and the DHS IT Security competency areas. As delivery modes and methods of information assurance education vary greatly, this research hopes to identify the most desirable current delivery modes and methods for different areas.

METHODOLOGY

The study was implemented in two phases: (1) a web-based survey was developed and given to assess the design and delivery of instruction for the three competing information assurance standards under investigation (NSA, CISSP, and DHS), and (2) a series of interviews were conducted using faculty experts in the information assurance field.

For the first phase, e-mail invitations were sent to the entire roster of 94 Centers of Academic Excellence as well as faculty from schools involved with a National Science Foundation grant for information assurance curriculum of which one of the authors was a co-principal investigator. The survey instrument included a section for identification and demographic information followed by questions asking participants to evaluate the seven sections of the NSA standard, the ten CISSP domains, and the fourteen DHS IT Security competency areas. Participants were informed that all names, e-mail addresses, and phone numbers would be kept confidential. In sum, participants were asked to evaluate a total of 31 topics. Eleven responses were received.

Survey Questions

The survey asked seven broad questions of participants, as described in the following sections.

1. *Please provide the following demographic information. All names, e-mail, and phone numbers will be kept confidential. You will be provided with a summary copy of the completed survey.* The purpose of the first question was to gather information about the responding individual and institution. Information requested included the contact name,

university name, approximate number of information assurance students enrolled, e-mail address, and phone number.

2. *Please rank the teaching methods used to teach the following topics in information assurance courses.* The second question sought to determine the most and least used instructional methods, by topic, and to distinguish between the method used and the method preferred. The ability to discern actual from preferred is important since, in many instances dealing with new technology, the preferred method may involve facilities not yet available to the instructor. Shortfalls in this area could indicate need for future funding initiatives.

3. *Please rate the importance of teaching the following topics in information assurance courses.* This question was asked to determine which among the 31 competing topics should be given priority. It is always important to know how to best allocate limited resources and the opinion of faculty experts should go a long way toward guiding the structure of future IA curricula.

4. *How many information assurance courses are used to teach the following topics?* Question four was asked to determine the relative emphasis placed on specific topic areas by schools participating in the survey. Answers to this question can serve as a benchmark for schools wishing to develop information assurance curricula.

5. *Please list information assurance topics that are not listed above that you believe are important to teach.* The purpose of question five was to assess perceived deficiencies among the three competing standards under investigation. Participants could provide up to five additional topics beyond the 31 provided in the survey.

6. *Please list the names of what you believe are your top five information assurance courses.* This question was asked to determine which courses were perceived as most important to teaching IA and to distinguish courses from the topics. The ability to identify important courses is important for schools wishing to determine best practice when creating and updating their own information assurance curricula. Participants could provide the names of up to five top courses.

7. *Please list any comments on the above survey. Thank you for your time and participation.* Question 7 was asked to help determine if any flaws existed in the survey and to help improve future surveys of this nature.

SURVEY RESULTS

The survey was completed by eleven respondents out of the group of 94 Centers of Academic Excellence. In most cases, the respondents completed all questions.

Please rate the importance of teaching the following topics in information assurance courses. Participants were asked to rank the importance of topics for each of the three standards under investigation. Scores were averaged. The results are shown in Table 1. For NSTISSI, the most important topic was Security Basics with a rating of 2.73 and least important was Policies and Procedures with 1.36. For CISSP, the most important was Telecommunications at 2.82 with Cryptography coming in last at 2.00. For DHS, Data Security was rated most important at 2.64 with Strategic Security Management rated least important at 1.90.

Table 1. Importance of IA Topics.

NSTISSI:	Avg
AIS Basics	1.64
Basics	1.73
Com	2.45
Planning	1.55
Policies	1.36
Security	2.73
System Ops	2.36

CISSP:	Avg
Access	2.55
Apps Sec	2.55
Crypto	2.00
Disaster	2.45
Env Sec	2.09
Legal	2.18
Ops Sec	2.27
Risk Mgmt	2.36
Sec Arch	2.18
Telecom	2.82

DHS:	Avg
Apps Security	2.40
Continuity	2.00
Data Security	2.64
Env Secure	2.09
Forensics	1.91
Incident	2.27
Net Secure	2.55
Personnel	1.91
Procurement	1.27
Regulatory	2.00
Risk	2.20
Strategic	1.90
Sys Ops	2.09
Training	1.91

How many information assurance courses are used to teach the following topics? Participants were asked to report the number of courses offered for each of 31 topics covered by the three standards under study. The results are shown in Table 2. For NSTISSI, System Operations received the greatest emphasis with 19 courses while Automated Information Systems received only 8 courses of time. For CISSP, Applications Security received the most attention at 23 courses while Disaster and Legal tied for last place at 15 courses each. For DHS, Incident Response was given the most attention at 29 courses with Procurement coming in last at only 10 courses.

Table 2. IA Courses Taught by Standard.

NSTISSI:	Total Courses
AIS	8
Basics	12
Com	18
Planning	11
Policies	11
Security	17
System Op	19

CISSP:	Total Courses
Access Control	16
Apps Sec	23
Cryptography	18
Disaster Recov.	15
Physical Sec	17
Legal	15
Ops. Sec	16
Risk Mgmt	20
Sec. Arch.	20
Telecom	20

DHS:	Total Courses
Apps Secure	24
Continuity	15
Data Secure	12
Physical Sec.	14
Forensics	17
Incident	29
Net Security	21
Personnel	16
Procurement	10
Regulatory	15
Risk	17
Strategic	13
Sys Ops	18
Training	21

Please list information assurance topics that are not listed above that you believe are important to teach. Topics believed to be important but not covered by any of the existing standards under investigation were biometrics, cyber attacks, data mining, malware engines and payloads, and project management and security. No priority was given to these topics as each was listed once. The topics are shown in Table 3.

Table 3. Important Topics not Listed.

Topics not Listed	Frequency
Biometrics	1
Cyber attacks	1
Data mining	1
Malware engines & payloads	1
Project management and security	1

Please list the names of what you believe are your top five information assurance courses. Grouping the courses by subject area generated the results shown in Table 4. Computer/Information security received the highest number of citations, followed by network security, computer forensics, cryptography, and applications/database security. The remaining seven courses were grouped into "other" and included cyber warfare, disaster planning & recovery, legal issues, and risk management.

Table 4. Top Rated IA Courses.

Course Name	Frequency
Computer/Information Security	14
Network Security	12
Computer Forensics	5
Cryptography	5
Applications/Database	4
Other	7

Please rank the teaching methods used to teach the following topics in information assurance courses. Grouping the responses for this question revealed a clear preference for the lecture method of teaching information assurance courses. Lecture was the most used and preferred teaching method for all three IA standards. Video was the least used method for all three IA standards. The methods are shown in Table 5.

Table 5. Teaching Methods.

IA Standard	Most Used	Least Used	Preferred Method
NSTISSI 4011	Lecture	Video	Lecture
CISSP ISC(2)	Lecture	Video	Lecture
DHS	Lecture	Video	Lecture

INTERVIEWS

As a follow-up to the survey we conducted interviews with a second group of information assurance faculty. The goal of these interviews was to gain a second set of qualitative data on

use of information assurance standards and related teaching methods. Six faculty who did not participate in the survey were interviewed. Interviewees had been teaching information assurance courses from 3 to 10 years.

Information assurance courses taught included IS Audit, Security, Computer Forensics, Network security, Ethical hacking, Information, OS Hardening, IT Security Governance, Disaster Recovery and Continuity, Networking Fundamentals and Vulnerabilities, and Countermeasures.

Information assurance standards used in developing courses included COBIT, ITIL, CNSS 4011, 4012, and 4013, CISSP ISC(2), Security +, and CISCO. Interviewees indicated that skill level courses were more likely to use vendor and the Security+ entry level certification standards.

Most faculty interviewed were familiar with the CISSP ISC(2) industry standard and believed it to be relevant in teaching. Only one faculty was familiar with the DHS standard. Appendix B provides a summary of the interview questions and answers.

CONCLUSIONS

The most obvious result from the interviews is that the DHS standard is largely unknown among faculty teaching information assurance and has not yet received a formal place in the classroom. Other standards are better known, which like the CISSP have relevance in practice or like the NSA have established federal programs to support them. Brenda Oldfield, Director, Cyber Education & Workforce Development. National Cyber Security Division was a primary author of the DHS EBK. Ms. Oldfield was interviewed for this paper and said the DHS EBK was originally intended "to present a framework outlining the competency and skills required for a basic IT security workforce" (Oldfield, 2009). When Ms. Oldfield was asked how the DHS EBK can be used by educators developing IA curriculum and teaching IA courses, she responded that "two professors are currently writing a book how to do this. That might be an unintended outcome. It might be used as a compliment to existing CNSS standards. The CNSS originated with national security systems, and was pushed out as a result of the CAE program" (Oldfield, 2009).

It should be noted that while interview respondents did not have familiarity with the DHS Essential Body of Knowledge, survey respondents were, in fact, teaching DHS topics. The top two courses taught based on the limited survey results were the DHS EBK topics for incident response and application security. It is also true that there is significant overlap at the topic level for all three IA standards.

LIMITATIONS

The limited response to the survey was a disappointment. One reason could be that each information assurance standard was broken into many components, perhaps making the survey much more difficult to answer. The large number of teaching methods in the survey may have caused confusion and made the survey more difficult. Future researchers may consider asking for responses at the standard level, with an option for respondents to provide additional input within the each standard. Also, teaching methods could be limited to three or four, such as lecture, on-line, lab, and other.

DIRECTIONS FOR FUTURE RESEARCH

It is clear that the importance and number of information assurance standards is increasing. Researchers may wish to study which information assurance standards are being used in academia and whether teaching parts of one standard are more important than the overall standard. It may be useful to determine if curricula are being tailored toward certification to favor one or more information standards. Also, it may be worth looking at how United States curriculum standards compare with European and other international standards.

Additional research is needed to study the effectiveness of teaching methods used in information assurance courses. Future questionnaires could be augmented with a question on "how do instructors assess the effectiveness of their method of instruction". It would be interesting to find out how different instructors "measure" effectiveness.

The interviews provided some contradiction and insight when combined with the limited survey results. Although survey respondents appeared to prefer lecture as the primary teaching method for information assurance courses, interview respondents seemed to downplay the value of lecturing and instead emphasized the importance of lab and hands-on information assurance learning activities. Future researchers should look into the relationship between lecture and hands-on teaching in information courses and perhaps identify some best practices in this area.

The interviews also highlighted the lack of knowledge regarding the DHS Standard. One goal of the DHS was to establish a national skill baseline in information assurance for both the public and private sectors. It is also clear that whether they know it or not, faculty are teaching DHS EBK topic areas. Future research should look closely at whether this standard is having the desired impact.

Finally, discipline accreditation requirements are increasingly emphasizing information assurance topics. The ABET 2008 curriculum includes security in many core and elective topic areas and could be included in future research on information assurance standards (ACM, 2008).

REFERENCES

ACM (2008). Computer Science Curriculum 2008: An Interim Revision of CS 2001Report from the Interim Review Task Force. http://www.acm.org//education/curricula/ComputerScience2008.pdf.

Bogolea, B. and Wijekumar, K. (2004). Information security curriculum creation: a case study. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM, New York, NY, 59-65. DOI= http://doi.acm.org/10.1145/1059524.1059537

Condon, S. (2009). A bill to shift cybersecurity to White House. In cnet news, March 20, 2009. http://news.cnet.com/8301-13578_3-10200710-38.html.

Department of Homeland Security (2007a). *Information Technology Security Essential Body of Knowledge* at http://www.us-cert.gov/ITSecurityEBK/EBK2007.pdf

Department of Homeland Security (2007b) IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. *EDUCAUSE Live!* (Slide 11). November 14, 2007.

ISC(2). CISSP Certification and Education. Retrieved on May 4, 2009 from http://www.isc2.org/cissp/default.aspx.

Manson, D. & Curl, S. (2003). A Comparison of Academic and Government Information Security Curriculum Standards. Information Systems Education Journal. Volume 1, Number 39 http://isedj.org/1/39/ December 27, 2003

National Security Agency (2009a). *Frequently Asked Questions: Terms and Acronyms.* Retrieved April 19, 2009 from http://www.nsa.gov/about/faqs/terms_acronyms.shtml.

National Security Agency (2009b). *Information Assurance Courseware Evaluation Program.* Retrieved April 19, 2009 from http://www.nsa.gov/ia/academic_outreach/iace_program/index.shtml

NSTISSI (1994). National Security Telecommunications and Information Systems Security Instruction No. 4011. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

Whitman, M. & Mattord, H. (2005). Designing and Teaching Information Security Curriculum. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSec CD Conference'04. http://portal.acm.org/citation.cfm?id=1059524.1059526.

Appendix A
Names of Top Five Information Assurance Courses.

#	Course One	Course Two	Course Three	Course Four	Course Five
1	Microsoft Windows Server OS	Unix/Linux Fundamentals	Microsoft Windows Networking	Introduction to Information Security	Network Security Fundamentals
2	Communication Basics	Security Basics	Telecommunication and Network Security	Systems and Application Security	Security Risk Management
3	Information System Security	Computer and Network Forensics	Managing Information Security	Legal and Ethical Issues in Information Assurance	Cryptography
4	Computer Security-- core course that includes OS, network, and software	Database Security	Network Security	Cryptography	Digital Forensics
5	Comp Security & Malware				
6	Network Security	Information Security	Disaster Planning and Recovery for IT	Computer Security	Computer Forensics
7	Fundamentals of Security	Risk Analysis / C&A	Applied Network Security	Applied Computer Cryptography	Legal Impacts of Computer Security

	Engineering				Solutions
8	Introduction to Information Security	Advanced Networking and Security	Cryptography	Information Warfare	Digital Forensics
9	Information Management	Principles of Information Security	Digital Forensics	Senior Systems Management	
10	Computer & Network Security	Software & Web Site Security	Securing the Enterprise Network	The Business of Information Security	Introduction to Networking and Security

Appendix B
Summary of Interview Questions and Responses

Question	Response One	Response Two	Response Three	Response Four	Response Five	Response Six	Response Seven
How long have you been teaching information assurance courses?	8 years	10 years	4 years	4 years	3 years	7 years	6 years
What information assurance courses have you taught/do you teach?	Network Security, Ethical Hacking, Information Assurance (OS Hardening), IT Security and Governance, Disaster Recovery, Network Fundamentals.	IS Audit (undergraduate and graduate), Internet Security, Quality Assurance, Computer Forensics.	Linux Administration and Security.	Vulnerabilities and Counter-measures, Practical Computer Security.	Teach introduction to infrastructure, web application.	Co-taught security architecture and analysis. Also teach Special Topics: Information Assurance and Security.	Information Risk Management, Network Security Architecture, Digital Investigations, Governance and Policy in Information Technology
What information assurance courses have you developed?	IT Security Governance, Disaster Recovery and Continuity.	None.	Security + class.	Vulnerabilities and Counter-measures.	None. Working on hacking techniques and security techniques.	Special Topics: Information Assurance and Security.	Computer Forensics
What information assurance standards have you used in developing courses?	CISSP, CISCO, COMPTIA, NSTISSI 4011, 4013.	N/A	Security +.	CISSP. Also COMPTIA Security +.	Do work with ISSA (CISSP) a little bit.	I have not used information assurance standards in developing courses.	NIST, ISO-27000 series
What information assurance standards do you believe are the most relevant in teaching IA courses? Why?	CISSP and Security+. Because Security+ are basic skills. CISSP is good because it has a broad coverage of topics but does not tell us how to teach.	COBIT for its adaptability 4011 and 4012 have a government feel to them.	Will use Certified Ethical Hacker. It gives students a lot of practical experience. Security + is a good introduction.	None.	Hands-on… trying to figure out how it works. You can teach theory but until it actually comes to doing it, I don't think it sink in.	I try to give my students an idea of the different types of standards that exist. Depending on what they go into different standards may apply.	I like to use standards such as the ISO and ANSI since they are fundamentally applicable to all environments and are considered "international" standards.

Question	Response One	Response Two	Response Three	Response Four	Response Five	Response Six	Response Seven
What information assurance standards are the least relevant to teach? Why?	Non-mainstream. Specific vendor tasks. We don't teach to certify Checkpoint firewall.	4011 and 4012 have a government feel to them.	None.	Have always held that certificates are nice but not really relevant. They teach you a technique but not overall theory.	None.	CISSP. It is a great breadth of knowledge but not a lot of depth. Students should look for and apply the standards that are most applicable to their specific area.	Any standards that are hardware, software or technology specific since they change too rapidly.
What teaching methods are the most relevant in IA courses?	Two areas. Integrated lecture/lab built upon case studies and case objectives.	Lecture for theory. Introduce by lecture, then do hands-on. For example, password cracking is hands-on.	I usually go over material in class. The one thing I don't like is the cookbook type of textbooks. I like students to have to figure out things for themselves.	Hands-on methods rather than lecture. In lecture they do not get to try and see how they work.	Have always held that certificates are nice but not really relevant. They teach you a technique but not overall theory.	For the types of courses I teach it is discussion and projects. For the graduate course the project applies the underlying methodology that we teach.	My preferred teaching methods are to encourage active participation and discussions in class, supported by outside classroom activities (hands-on technology).
What teaching methods are the least relevant in IA courses?	Cookie cutter lab or no labs. Pure lecture.	Too much lecture. If you only lecture, students are not going to apply it.	I am not a big fan of lecturing. You don't keep the students with you.	Don't know.	Just talking about things in theory without real hands-on	I think lectures are probably the least effective.	No answer.
How familiar are you with the ISC(2) CBK?	Familiar.	Know six of the ten very well. For the remaining ones I have an average understanding.	Not familiar.	Pretty familiar.	Not familiar.	Very high level, summary level for all of these.	I am very familiar with the Common Body of Knowledge an all its areas.
How familiar are you with the NSTISSO 4011 standard?	Familiar.	The NSTISSI 4011 standards are the basis for my Internet Security course.	Not familiar.	Have started looking at it. Not familiar with it yet.	Not familiar.	Very high level, summary level for all of these.	Yes, I am familiar with the National Training Standard for Information Systems Security.
How familiar are you with the DHS EBK?	Not familiar.	Not familiar.	Not familiar.	Not familiar.	Not familiar.	Very high level, summary level for all of these.	I am familiar with it.
Would you like to add any additional comments on teaching IA courses?	Students need a solid base in networking and programming courses. Also soft skills, writing, and communication skills.	Be careful with any kind of practical hands-on experience. You have to secure the learning environment and cover ethical and legal issues.	Nothing.	Nothing.	Get the students hands-on experience.	Bringing in what is happening today and relating it to the material is necessary.	My strategy when teaching IA related courses is to ensure that students learn to differentiate standards and frameworks from process and procedures.