The Assessment of Learning Outcomes in Information Assurance Curriculum

N. Paul Schembari  
East Stroudsburg University of Pennsylvania  
200 Prospect St.  
East Stroudsburg, PA 18301  
1-570-422-3661  
nschembari@esu.edu

Mike Jochen  
East Stroudsburg University of Pennsylvania  
200 Prospect St.  
East Stroudsburg, PA 18301  
1-570-422-3036  
mjochen@esu.edu

ABSTRACT
We present an overview of the design and conduct of learning outcomes assessment for an undergraduate information assurance curriculum. The described program of assessment provides for an evidence-based, decision-making process that can be used to inform faculty on changes needed to curriculum. While the conduct of the assessment cycle is not an insignificant one (developing outcomes and objectives, assessing student learning, collecting and analyzing assessment data, and using assessment data to guide conversation about curriculum), the benefits are great in terms of assisting faculty to make good choices when reviewing/revising curriculum (and at the course level: course content, teaching methodology, and assignments).

Categories and Subject Descriptors
K.3.2 [Computer and Information Science Education]: Computer Science Education.

General Terms
Security, Human Factors.

Keywords

1. INTRODUCTION
Most information assurance (IA) programs require some form of Learning Outcomes Assessment (LOA). This may be part of accreditation efforts through regional accreditation organizations such as Middle States [1], New England [2], or North Central [3]. Another reason that a program may be required to perform LOA is because of technical accreditation such as that earned from external accreditation bodies like ABET [4], or because of the possible future process for “Knowledge Unit Mapping” in the Center of Academic Excellence Program sponsored by the US National Security Agency and Department of Homeland Security [5]. Others decide to perform LOA because of the benefits gained - LOA allows programs to decide on their most important learning outcomes, measure student attainment of those outcomes, and use these metrics to help decide on needed improvements to their programs. For a good overview of the LOA process, we suggest the website of the National Institute for Learning Outcomes Assessment [6]. In this paper, we discuss our method for this assessment in an undergraduate IA program, pitfalls that we have experienced, and future plans for our assessment approach.

Of course, LOA is a very program specific process. For this reason, an overview of our IA program is needed. Our IA program is housed in a Computer Science Department at a regional comprehensive university which does not grant doctoral degrees. We offer both a Bachelor of Science (BS) in an IA discipline as well as a Master of Science in an IA discipline. Our LOA description will only cover the BS program since we have not yet implemented the LOA process for the MS program. Because the BS in Computer Science program in our department has received ABET accreditation, we decided that using our ABET LOA process would be a good starting point for our IA LOA effort. We built off this process and made adjustments that seemed appropriate for IA curriculum. For a description of ABET LOA, see the ABET website [4].

Our BS in an IA discipline (referenced as BSIA in all that follows) begins with a basis in core computer science. Students complete twelve credits in elementary programming and data structures (Java and C++), and courses in computer organization, assembler programming, operating systems, networking, and databases. Many of these courses are completed during the first two years of the program with the remainder in the third and fourth years. Also in these last two years, students complete the “core IA courses” - a set of six courses which cover purely IA topics. Table 1 presents the six core IA courses for the BSIA. In this table, course names have been altered for blinding purposes, and a sample textbook is given to indicate the material covered.

<table>
<thead>
<tr>
<th>Course</th>
<th>Textbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineering</td>
<td>Goodrich &amp; Tammasia [7]</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Landoll [8]</td>
</tr>
<tr>
<td>Network Security</td>
<td>Skoudis [9]</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Stallings [10]</td>
</tr>
<tr>
<td>IA Law and Ethics</td>
<td>No text used – students review case studies in IA ethics and law</td>
</tr>
<tr>
<td>IA Internship</td>
<td>No text used - students work for an employer performing IA functions</td>
</tr>
</tbody>
</table>

Table 1. Undergraduate IA courses

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Information Security Curriculum Development Conference 2013  
October 12, 2013, Kennesaw, GA, USA.

Copyright 2013 ACM 978-1-4503-2547-9/10/13...$10.00.
Students are also required to complete three elective courses, but these are not included in the LOA program since they vary by student. As described below, our LOA process has facets internal to the required classes as well as a more global approach. We have required in-class student assessment for the first five classes given in the Table 1, and not for the IA Internship course. The global assessment process is described in Section 2, the course-level assessments will be described in Sections 3 and 4.

Prior to creating in-class student assessment, we determined what we believed to be a good set of Program Level Objectives. These were defined as a basis to ensure our students achieve professional success after graduation. Then, we determined Student Learning Outcomes for our entire Program. The third step involved cross-referencing the Program Level Objectives and the SLOs, as described in Section 2.1. Finally, the course-level skills assessment questions were created based on these first three steps.

This process is illustrated as follows:

1. Create Program Level Objectives for Student Success
2. Determine Student Learning Outcomes for Program
3. Cross-Reference 1 & 2
4. Determine In-Course SLOs

2. PROGRAM-LEVEL ASSESSMENT
During the initial planning and design phases of our IA LOA effort, our faculty adopted program level objectives and student learning outcomes for all graduates of our IA undergraduate program. Program objectives are broad goals that we would expect our graduates to achieve. Student Learning Outcomes (SLO) are more specific goals that we expect our students to achieve by graduation. The SLOs support, and are mapped to, program level objectives.

Our faculty adopted the following program-level objectives for our BSIA LOA. Our students will achieve professional success due to:

1) a solid foundation in computer science and security theory, principles, and techniques;
2) a firm basis in science and mathematics, and the ability to apply their principles to computer security problems;
3) broad critical thinking skills;
4) teamwork and leadership skills to work and live in a global and diverse society;
5) strong oral and written communication skills;
6) a pursuit of life-long learning and mastery of emerging technologies;
7) an understanding of how to use their knowledge and skills for the benefit of society.

These objectives were settled upon as the set of long-term skills that we desire our graduates to have. Our faculty feels strongly that a good IA professional must understand the basics of the technology behind information, thus the strong link between our IA and computer science programs during the first two, foundational years of study. These program-level objectives reflect our philosophy that our graduates must be able to think critically, understand theory and practice of computer science and security, work well in a group/team environment, understand science and technology communicate well, and be good technological citizens of our global society. The program-level objectives were developed in parallel with the SLOs, given below. In this way, our faculty took a simultaneous top-down, bottom-up approach. Much thought and careful deliberation went into the process of identifying our objectives and SLOs.

Our faculty adopted the following more specific SLOs for our BSIA LOA. The program enables students to achieve, by the time of graduation:

a) An ability to apply knowledge of computing and mathematics appropriate to the discipline
b) An ability to analyze a problem, and identify and define the computing and security requirements appropriate to its solution
c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs
d) An ability to function effectively on teams to accomplish a common goal
e) An understanding of professional, ethical, legal, security and social issues and responsibilities
f) An ability to communicate effectively with a range of audiences
g) An ability to analyze the local and global impact of computing on individuals, organizations, and society
h) A recognition of the need for and an ability to engage in continuing professional development
i) An ability to use current techniques, skills, and tools necessary for computer security practice.
j) An ability to apply mathematical foundations, algorithmic principles, and computer security theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices especially security and availability.
k) An ability to apply security design and development principles in the construction of software systems of varying complexity.

These SLOs are closely aligned with the ABET outcomes, revised to focus particularly on security-related material and goals.

2.1 Mapping of SLOs to Program Objectives

The SLOs are mapped to specific Program Objectives. This mapping is as follows (listed by program-level objective):

1) a solid foundation in computer science and security theory, principles, and techniques
   Mapped to SLOs: A, B, C, I, J, and K

2) a firm basis in science and mathematics, and the ability to apply their principles to computer security problems;
   Mapped to SLOs: A, B, C, I, J, and K

3) broad critical thinking skills
   Mapped to SLOs: B, E, G, H, and J

4) teamwork and leadership skills to work and live in a global and diverse society
   Mapped to SLOs: D, E, F, G, and H

5) strong oral and written communication skills
   Mapped to SLOs: D, and F

6) a pursuit of life-long learning and mastery of emerging technologies
   Mapped to SLOs: A, B, H, and I

7) an understanding of how to use their knowledge and skills for the benefit of society
   Mapped to SLOs: E and G

2.2 The Feedback Loop

One of the important aspects of LOA is taking the information gained from the assessment and using it to make course improvements. As a department, we do this with an annual meeting at the end of each academic year. This typically falls one week after final grades are due on campus.

At this meeting the majority of the discussion concerns the Computer Science program, since most of our faculty teach in that program. However, we have also looked at the data gained from the BSIA and used this for suggested improvements. Of course, there is a fine line between LOA feedback and faculty rights to teach courses as they see fit. We have decided to use the feedback as suggestions and allow the instructors to determine the best method for using the feedback.

Some of the feedback from students (gathered in the form of surveys to current students, graduating students, and alumni) helped in our decision to rework the introductory programming sequence in the first two years of the program. We also will soon be teaching the IA core courses in a five-course sequence which spans from the second semester of the sophomore year so that students can complete one course per semester to complete these requirements.

In Section 4, below, we give the results of our course-level assessment. At the time of this writing, this feedback is being analyzed for course improvements.

3. COURSE-LEVEL ASSESSMENT

With regard to course-level assessment of students, we consider only the “pure” IA classes in our curriculum. Our department has also created methods for course assessment for the required courses in our ABET reviewed computer science program, and seven of these courses overlap with the BSIA program. These include our programming sequence, computer organization, assembler programming, and operating systems. For the junior- and senior-level BSIA courses, the subsections below illustrate the assessment activities by course name.

3.1 Assessment Skill Question Development

In order to assess student success in achieving course-level SLOs, the faculty decided to select a sample of questions or activities that would represent key skills for each class. Each question/activity selected would directly show undergraduate-level mastery of each SLO. The faculty on the departmental assessment committee met with the individual faculty that regularly teach each course under assessment. Each member of faculty that regularly teaches a given course developed a set of these skills questions/activities. The department assessment committee worked with the individual faculty to develop the assessment materials and to facilitate the whole department’s final approval of the chosen assessment materials for the entire curriculum. The questions/activities, when administered to the students, are assessed in a pass-fail manner.

One important aspect of LOA is manageability. For this reason, we decided to use approximately five questions in each of the required classes in the program. Since our students proceed through two years of ABET reviewed curriculum, following the same LOA, the total number of questions that a student will answer are approximately 75. We feel that breaking down these questions course by course provides for a more manageable process. (In the following sections, 25 questions will be illustrated, as taken from the courses which could be considered “pure” IA.)

3.2 Security Engineering Course

Our course in Security Engineering gives students an overview of the IA field, concentrating on the more technical aspects. We cover the core areas of confidentiality, integrity, and availability with synopses of access control, authentication, cryptography, malicious code, network security, and risk management.

To help assess our program and our students learning, we developed a set of skills questions, representing some of the basic knowledge students should obtain by the end of the course. This is considered the most basic knowledge that every graduate should have. In the last year, the following questions for skills assessment were given as part of the students’ final exam. Each question has a header for easy recognition, but this is not included when the question is given to the student.

1. [Goals] What are the three main security goals for the security engineer?
2. [KeyProperty] Which of the following is NOT an important principle of computer security?
a. The security of a cryptosystem is in the secrecy of its keys.
b. A cryptographic key must have a high degree of complexity.
c. Computer items must be protected only until they lose their value.
d. We should assume an attacker will use any method to circumvent our controls.

3. [Key#] Given a network of size n nodes and p links, using symmetric-key encryption, how many keys are required to support end-to-end encryption?

4. [AV] Which of the following is NOT a malware detection technology?
   a. Emulation
   b. Generic behavior
   c. Bootstrap channeling
   d. Signature recognition

5. [Firewall] Give two types of network firewalls.

The results of the student assessment are given in Section 4.1.

3.3 Risk Analysis Course

Our course in Risk Analysis gives students an overview of policy development and compliance. For the latter, we concentrate on the FISMA Certification and Accreditation process [11] since this can be considered a risk analysis approach to system security. Specifically, we concentrate on the NIST Special Publications 800-18, 800-37, 800-53, and 800-53A, all available from the NIST website [12], and have the students perform the FISMA risk analysis process on a live network. In recent years, we have performed this analysis on a high school computer network as well as the network of a local car dealership.

As in the Security Engineering class, to help assess our program and our students learning, we developed a set of skills questions, representing some of the basic knowledge students should obtain by the end of this course. Also, these questions were given as part of the students’ final exam:

1. [C&A] Define Certification and Accreditation for information systems
2. [Risk] What are the three most important characteristics of risk?
3. [Mitigation] What is Risk Mitigation?
4. [CommonCriteria] Why is the Common Criteria useful for Risk Analysis?
5. [Accreditation] What documentation is necessary for System Accreditation?

The results of the student assessment are given in Section 4.2.

3.4 Network Security Course

Our Network Security course provides students with the opportunity to complete in-depth laboratory exercises using commercial-off-the-shelf technology in order to examine the impact that network devices have on overall system security. Students complete approximately one laboratory exercise per week during a fourteen week semester. A key goal of these exercises is to help students gain insight into defensive computer network tactics, techniques, and procedures.

In order to measure student achievement on the SLOs in this course, the following questions were developed:

1. [Sniffing] What are the differences between active and passive sniffing?
2. [SourceRouting] List any potential issues with permitting source-routed traffic to traverse your network borders.
3. [CovertChannels] What can be done to prevent an attacker from implementing a covert channel via HTTP?
4. [Software] What is a stack-based buffer overflow and how can you defend against it?
5. [IDS/IPS] Define and give one example of Intrusion Detection System and one example of Intrusion Prevention System.

3.5 Cryptography Course

Our course in cryptography gives students an overview of cryptographic algorithms and how these can be programmed. We study the basics of substitution and transposition, consider both block and stream ciphers, and discuss encryption standards such as DES and AES. We also look at public key ciphers such as RSA and consider key exchange approaches such as Diffie-Hellman. Besides studying the algorithms and their programming, we also discuss some of the basics of cryptanalysis.

For our LOA in this course, we have created a set of skills questions for basic knowledge. These questions have not been used in class as of yet – we plan to do so during the Fall 2013 semester.

1. [BlockStream] What is the difference between a block cipher and a stream cipher?
2. [PublicPrivate] What are the roles of the public and private key?
3. [Key#MultipleTypes] How many keys are required for two people to communicate via a cipher?

3.6 IA Law and Ethics Course

Our IA Law and Ethics course requires students to analyze a set of case studies which force them to learn laws related to IA and consider the ethical aspects of each case. In fact, for each case study, the students are required to write a report which includes ethics, law, and already decided course cases which apply to the study. We have had students study cases which involve a variety of laws including Full Disclosure of Vulnerabilities, Freedom of Personal Speech vs. Business Speech, CALEA, Law Enforcement Password Disclosure, Workplace Privacy, Sniffing, Legality of Forensics Tools, MPAA, Sarbanes-Oxley, Liability in Online Banking, Virtual Property, etc.

For the LOA of this course, we decided to concentrate on three major aspects of the course: Privacy, Legality of Hacking, and Intellectual Property. The three questions given below comprised the final exam for this course in Spring 2013:

1. [Privacy] Should US Citizens have a constitutional right to privacy? That is, should the constitution be amended to include a “right to privacy”? How should this possible right be balanced with the needs of protection by law enforcement? How can law enforcement perform legal searches if encryption is used? Does encryption basically make privacy already possible?
2. [Hacking] If a person or corporate entity is under a cyberattack, should they be allowed to “hack-back”? [The students were provided with the following reference which debates this issue:
http://www.stepoecyberblog.com/2012/11/02/the-hackback-debate/

3. [IP] Does copyright law need to be updated, especially with regard to digital media? Recently, the Republican Study Committee released a policy document arguing in favor of reform, but this document was retracted after pressure from lobbying groups. The students were provided with the original document and an analysis taken from the following web page: [IP]

The results of this assessment are given in Section 4.3.

4. ASSESSMENT RESULTS

At the time of this writing, we have collected data from three of the courses under assessment – Security Engineering, Risk Analysis, and IA Law and Ethics. For these courses, the subsections below illustrate the assessment activities by course name. Due to the teaching cycle of when courses are offered in the curriculum, assessment data for two courses, Network Security and Cryptography, has yet to be collected. Data for these two courses will be collected during the 2013-2014 academic year.

In each subsection that follows, a table is given illustrating the student success or failure with each skill assessment. Success or failure is fully determined by the instructor of the course, but this usually means that a student was able to answer the question at a level equivalent to 70% correct. Also, the only students considered in this evaluation are those who received a “C” grade or higher in the class. Also note that our faculty make it a practice to avoid “teaching to the test”. Any review sessions, study periods, exercises, etc., which are held in or out-of-class are strictly done with regard to regular class practices and because of the assessment program.

At the end of each academic year, department faculty meet to discuss assessment data for the concluding year. At this time, faculty look for trends that may indicate that a change is needed to sustain practices and program objectives.

4.1 Security Engineering Course

In the Security Engineering course, the five questions listed in Section 3.1 were given to the students as part of the Fall 2012 Final Exam. For comparative purposes, the distribution of final grades in the class is given in the table below, including only those grades accepted in the BSIA program.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percent of Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>27%</td>
</tr>
<tr>
<td>B</td>
<td>27%</td>
</tr>
<tr>
<td>C</td>
<td>33%</td>
</tr>
</tbody>
</table>

The following table gives the results of the class on the LOA questions.

<table>
<thead>
<tr>
<th>Question Name</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals</td>
<td>100%</td>
</tr>
<tr>
<td>KeyProperty</td>
<td>23%</td>
</tr>
<tr>
<td>Key#</td>
<td>38%</td>
</tr>
</tbody>
</table>

To analyze these results, we see that 87% of the students were successful in the class (in terms of the Course Grade), but overall they had a poor understanding of cryptographic keys. Two results can be determined from this; that is, our LOA output: either the discussion of cryptographic keys needs to be improved, or less emphasis should be paid to this aspect of the course in this testing. To expand on the latter, should we have such a large emphasis in the LOA of the Security Engineering course on cryptographic keys when other aspects have not been evaluated for LOA?

4.2 Risk Analysis Course

In the Risk Analysis course, the five questions listed in Section 3.1 were given to the students as part of the Fall 2012 Final Exam. Here are the acceptable grades for the students in the course:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percent of Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>24%</td>
</tr>
<tr>
<td>B</td>
<td>47%</td>
</tr>
<tr>
<td>C</td>
<td>18%</td>
</tr>
</tbody>
</table>

Next, the results of the LOA:

<table>
<thead>
<tr>
<th>Question Name</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;A</td>
<td>100%</td>
</tr>
<tr>
<td>Risk</td>
<td>67%</td>
</tr>
<tr>
<td>Mitigation</td>
<td>87%</td>
</tr>
<tr>
<td>CommonCriteria</td>
<td>73%</td>
</tr>
<tr>
<td>Accreditation</td>
<td>100%</td>
</tr>
</tbody>
</table>

We see that the results in this class are much higher than in the Security Engineering class. In the academic year in question, these results were from the same set of students with the same instructor, so these variables are controlled to the degree they could be. A possible cause for the difference in results may be the difficulty level of the material. A second possible cause may be the fact that the questions for the Security Engineering course were not all written by the instructor, while for the risk analysis course, the questions were all written by the instructor.

4.3 IA Law and Ethics Course

In the IA Law and Ethics course, the three questions listed in Section 3.1 were given to the students as the Fall 2012 Final Exam (an essay based exam). Here are the acceptable grades for the students in the course:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percent of Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>56%</td>
</tr>
<tr>
<td>B</td>
<td>22%</td>
</tr>
<tr>
<td>C</td>
<td>11%</td>
</tr>
</tbody>
</table>

Next, the results of the LOA:

<table>
<thead>
<tr>
<th>Question Name</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>100%</td>
</tr>
<tr>
<td>Hacking</td>
<td>75%</td>
</tr>
<tr>
<td>IP</td>
<td>88%</td>
</tr>
</tbody>
</table>

Because of the type of class, we see that the students have a high level of success on the measured questions.
5. CONCLUSION
The process of implementing a program of assessment has enabled our faculty to understand that assessment is an ongoing process designed to promote thoughtful, introspection on the entire teaching-learning process. Assessment at the program level empowers faculty to examine every aspect of this teaching-learning process. Proper assessment and analysis will yield data that can be used to support, both quantitatively and qualitatively, future changes to curriculum, course assignments, course topics, teaching methodology, course delivery, and even the assessment process. Our initial round of assessment of our BSIA SLOs and program-level objectives demonstrate that we have many strengths in our program, but that we also have areas where we can make improvement, thus making the program even stronger. We plan to continue to refine our assessment of SLOs while we use data to refine our curriculum and teaching within the IA program. This process can serve to make any program stronger and more beneficial for future students.

REFERENCES