CERIAS Tech Report 2004-42

ASSESSING STUDENT PERFORMANCE OUTCOMES IN AN INFORMATION SECURITY RISK ASSESSMENT, SERVICE LEARNING COURSE

by Melissa J. Dark

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Assessing Student Performance Outcomes in an Information Security Risk Assessment, Service Learning Course

Melissa J. Dark
Purdue University
401 N. Grant Street
West Lafayette, IN 47907
765-494-7661

mjdark@tech.purdue.edu

ABSTRACT

This focus of this paper is on the assessment of student performance in an information security risk assessment, service learning course. The paper provides a brief overview of the information security risk assessment course as background information and a review of relevant educational assessment theory with a focus on outcomes assessment. An example of how assessment theory was applied to this service learning course to assess student performance outcomes is described with the aim of sharing performance assessment methods with other educators. This material is based upon work supported by the National Science Foundation under Grant No. 0313871. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Categories and Subject Descriptors

K.6 **[Management of Computing and Information Systems]:** Security and Protection – a*uthentication, insurance, invasive software (e.g., viruses, worms, Trojan horses), physical security*, u*nauthorized access (e.g., hacking, phreaking).*

General Terms

Information Security Education, Information Security Management, Information Security Risk Assessment, Assessment of Student Performance, Outcomes Assessment.

SIGITE'04, October 28–30, 2004, Salt Lake City, Utah, USA.
Copyright 2004 ACM 1-58113-936-5/04/0010...$5.00.

INTRODUCTION

Service learning has been growing in popularity as colleges and universities seek ways to: 1) boost students' academic achievement, 2) foster students' sense of civic responsibility, 3) improve students' personal development skills, and 4) better prepare students to enter the workforce. Service learning is a teaching method that combines curriculum-based learning with meaningful service to the community. Service learning utilizes curriculum based learning to inform the practice of community based service and likewise uses community based services experiences as a means of enriching students curriculum based learning experience.

"In quality service-learning, the service project is designed to meet not only a real community need, but also *classroom goals*. By ensuring strong linkages between the service and the learning, students are able to improve their academic skills and apply what they learn in school to the broader community. Through service-learning, students demonstrate to teachers what they are learning and how they are meeting specific academic standards" [8]. By nature, service learning is focused on student performance.

At the same time that service learning is growing in popularity, outcomes-based assessment is becoming more prevalent among accrediting bodies, funding agencies, and therefore, colleges and universities. Outcomes are essentially what students should know and be able to do in order to demonstrate achievement of a stated learning goal. Outcomes refer to the both what students should know after instruction as well as what they should be able to do. Sometimes outcomes are called student outcomes, learning outcomes, and objectives. However, in practice outcomes often refer to something broader in focus than a learning objective. Outcomes may reflect tasks and skills found outside the class and outcomes are amenable to assessment [7].

Assessment is the systematic process used to obtain information about student achievement so that the information can be used to: 1) give feedback to students, 2) make educational decisions about students, and also 3) make decisions about program/instructional effectiveness. Many educators find it time consuming and/or difficult to conduct meaning outcomes-based assessment in traditional courses, and even more are daunted by the task of performing meaningful outcomes-based assessment when experimenting with a new teaching method, such as service learning. The purpose of this paper is to share with other faculty a model for how to conduct outcomes based performance assessment in a service learning course. By way of context, the class, entitled Information Security Risk Assessment, is described first. The paper then provides a review of relevant assessment theory with a focus on outcomes-based performance assessment. Finally, the paper provides a working example of how assessment theory was applied to this service learning course to assess student performance outcomes.

THE INFORMATION SECURITY RISK ASSESSMENT SERVICE LEARNING COURSE

The course came into existence for a couple of different reasons. First, the author was providing outreach/training workshops to K12 school corporations on how to better secure their information systems. The workshops had been held over a 1.5 year time span and attended by approximately 120 system administrators from over 30 school corporations in west central Indiana. Through the workshops, the need for more secure systems in K12 school corporations was apparent. This subsequently led to the idea that an intensive risk assessment experience could help these school corporations approach security in a more systematic and sustainable fashion. However, the workshops had been sponsored by a grant from the National Security Agency, hence there was also a need to continue to provide a service to these school corporations after the grant ended.

At the same time our faculty were analyzing weaknesses in our graduate curriculum. Many of our courses are mapped to the NSTISSI standards published by the National Security Telecommunications and Information Systems Security, a working group of the Committee on National Systems Security (CNSS) [1]. CNSS has been working on a new standard in the area of information security risk analysis; our institution did not have a course(s) that dealt specifically with information security risk analysis. Embedded within other classes, we discussed the role of risk assessment as it relates to software engineering, and systems analysis and design; however, the topic was covered briefly and only in theory. In these classes, our curriculum did not engage students in learning how to conduct an information security risk assessment in practice. Prior to adding this class, our students gained lower level recall or comprehension skills at best, but left our classes without being able to apply, analyze, or evaluate what they learned about information security risk assessment.

Given the need and our desire to help K12 school corporations improve their information security couple with the need to provide our students with higher level knowledge and skills in information security risk assessment, this class was developed. The course was first taught in Spring, 2004. Twenty-two graduate students and 2 upper-division undergraduate students enrolled in the course. In the fall of 2003, an invitation was sent out to 36 K12 school corporations to participate in the course. Six school corporations responded to the invitation and all six participated in the course.

A brief description of the course and the course objectives are paraphrased below. The course objectives are especially important as these are the outcome statements of what students should know and be able to do as a result of participating in the course. These outcome statements formed the foundation for the assessment system and instrument that was used in the class. More detailed information on the class is available in the following article [3].

Course Description

Students spend the first 7 weeks of the class learning through more traditional methods, i.e., lecture and reading. However, for the next 8 weeks of the class, students are assigned to a team tasked with performing an information security risk assessment for a client, which was a K12 school corporation in the west central area of Indiana.

A service learning course intends to provide an education experience:

- whereby students learn and develop through active participation in thoughtfully organized service experiences that meet actual community needs, that are integrated into the students' academic curriculum or provide structured time for reflection, and that enhance what is taught in school by extending student learning beyond the classroom and into the community.
- that increases the civic responsibility and citizenship of students in the course; this occurs by exposing students to societal inadequacies where they can use the community service experience as a foundation for learning 1) about oneself, 2) the academic discipline, 3) real world skills and techniques, and 4) how the discipline, skills and techniques intersect with the social world around us.
- that joins theory and practice, i.e., students experience the relevance of the subject to the real world. Students in service learning courses are empowered to make a difference with the skills they are learning in an environment where there is a need; furthermore, the learning experience and student learning outcomes are usually richer when there is a distinct and known need for the service.

Objectives

After completing the course, students should be able to:

- Conduct an information security risk assessment.
  - Perform asset identification and classification
  - Perform threat identification
  - Perform vulnerability identification
  - Perform control analysis
  - Perform likelihood determination
  - Conduct impact analysis
  - Conduct risk determination
  - Identify control recommendations
  - Document results
- Identify pertinent standards and regulations and their relevance to information security management.
- Describe legal and public relations implications of security and privacy issues.

EDUCATIONAL ASSESSMENT THEORY

Educational assessment is the process of gathering, describing, or quantifying information about learning or performance. The person or thing being assessed can range from the performance of students and instructors to that of instructional materials, courses, and entire degree programs. Educational assessment happens before, during, and after instruction and is done for a variety of purposes. Generally speaking the purposes are to inform, improve, and/or prove. Assessment that is conducted for the purpose of improvement is often called formative assessment (or formative evaluation) while assessment that is conducted for the purpose of determining the merit or worth of an object, thing, or performance is often called summative assessment (or summative evaluation).

Figure 1 is an assessment model depicting the what, when, and why dimensions of assessment. In the context of this paper and this course, the primary focus for the assessment was formative and summative assessment of student learning outcomes. The primary emphasis was on creating an assessment process that would provide students with feedback on their performance in the class that they could use to improve their achievement in the class. A secondary emphasis was to create an assessment process that at the end of the course could be used to make judgments about students' achievement at the end of the course. The assessment data that were collected can also be used to provide feedback about instructional materials; however that is not the focus of this paper.

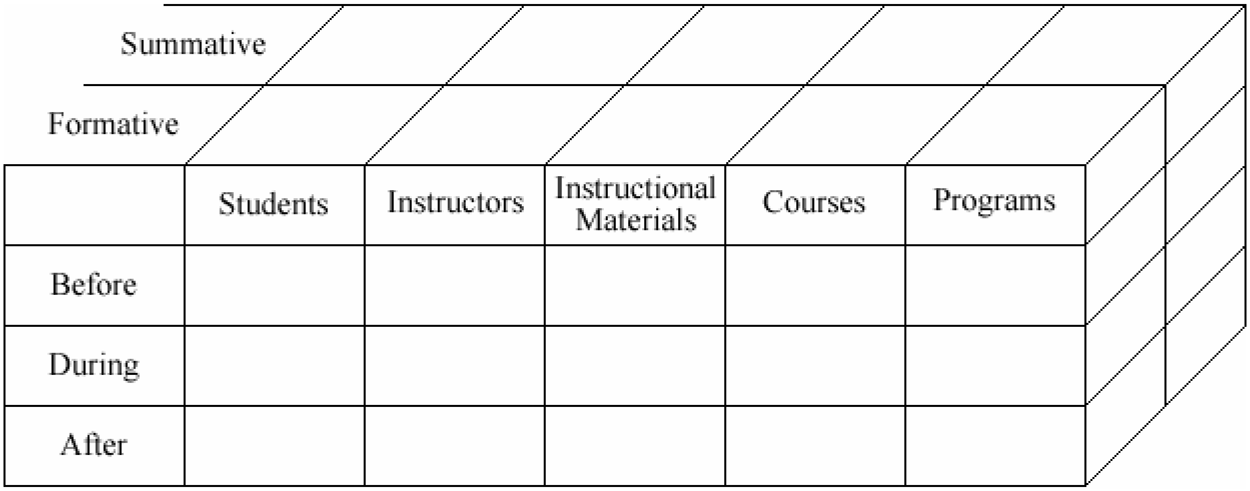

Figure 1: Assessment model.

In order to conduct performance assessment, there must be a methodology for gathering and quantifying information about performance. Regardless of the specific performance being assessed, all performance assessment includes measuring the degree or amount to which a characteristic, trait, or feature exists and using these data to make judgments about the desirability, value, or worth of the thing being evaluated. This usually involves three common steps: "1) identifying and defining the quality or attribute(s) that is to be measured; 2) determining a set of operations by which the attribute may be made manifest and perceivable, and 3) establishing a set of procedures or definitions for translating observations into quantitative or qualitative statements of degree or amount" [4]. The remainder of this paper describes how this process was followed to develop an assessment system that was used to both formatively and summatively assess student performance outcomes in this class.

ASSESSMENT OF STUDENT LEARNING OUTCOMES IN INFORMATION SECURITY RISK ASSESSMENT

Identifying the Attribute to be Measured and Determining a Set of Operations to Make the Attributes Manifest and Perceivable

Earlier in this paper, the course objectives (outcomes) were listed. The course objectives were the starting point for identifying the quality attributes to be measured. Each objective begins with an action verb that suggests what the student should be able to do at the end of the class. The focus of the course objectives is on the higher level learning outcomes, i.e., the application and synthesis of knowledge, as opposed to lower level cognitive skills such as verbal recall or comprehension. Traditional assessment methods, such as multiple choice, short answer, and essay tests, can be effective methods for assessing lower level cognitive skills, but they are not necessarily well-suited to assessment of higher level cognitive knowledge/skills. More appropriate in this case was the use of some type of performance assessment. Performance assessments are generally considered to be alternative assessments. While there are many different ways to assess performance, generally speaking, performance assessments 1) use a direct, real-world, overt and systematic approach to measure skills/abilities [6], 2) require students to "generate a response to a question rather than choose from a set of responses provided to them" [2], 3) "require reasoning about recurring issues, problems and concepts that apply in both academic and practical situations [7], and 4) require that students actively engage in generating complex responses entailing the integration of knowledge and strategies, not just use of isolated facts and skills [7].

The response that students generated was an information security risk assessment report for their client school corporation; the report was a direct, real-world product that was submitted for grading numerous times throughout the semester. In order to systematically grade the report, a performance checklist was developed that articulated the attributes or characteristics that well-developed information security risk assessment report should possess. A short excerpt from the checklist is presented in figure 2 (if you are interested in a full copy of the checklist, please contact the author at the email address provided in this paper). The checklist was used to understand the mental models that the student teams were creating. The report became a product of the students thinking that, when graded with the checklist, could provide information on where students' thinking was on track and where it was deficient. Deficiencies in thinking include both errant thinking as well as complete lack of understanding. When using the checklist to grade student reports, there were times when entire sections would be missing; this was usually indicative of students' lack of understanding the content. If there thinking was errant, then they usually had a draft section of the report and through grading it, their misunderstandings were observable and manifest.

The overall checklist consisted 5 sections and each section consisted of 3-4 subsections. Each subsection consisted of four items that are attributes of an effective information security risk assessment report. When designing a checklist, it can be useful to have an equal number of items in each subsection, so that the scale of what constitutes "excellent", "good", "fair", and "poor" are consistent. The sections and subsections were as follows:

1) system characterization
   a) meta-information
   b) operational environment of IT systems and data
   c) operational controls of IT systems and data
2) threat, vulnerability and control analysis
   a) meta-information
   b) threat identification
   c) vulnerability identification
   d) control analysis
3) risk determination
   a) meta-information
   b) likelihood determination
   c) impact analysis
   d) risk determination
4) control recommendations and results documentation
   a) meta-information
   b) control recommendations
   c) results documentation
5) format/style
   a) title page and report structure
   b) orderly presentation
   c) economy of expression
   d) grammar and punctuation

The first four sections of the checklist correspond directly to the information security risk assessment process as it is presented in the Risk Management Guide for Information Technology Systems [5]. The fifth section was developed to address the overall style, presentation, accuracy, etc., of the report, which is also a necessary component of being to conduct an information security risk assessment. Meta-information includes information about the purpose of each step, how the steps were performed, who performed the steps, and how the steps correspond to each other. The meta-information section is important because it requires students to explain, in their own words, the basic recall and comprehension knowledge that is normally assessed via tests.

Risk Determination
Metainformation
□ The report includes a detailed description of the purpose of these steps □ The report includes a detailed description of how these steps were performed □ The report includes information about who performed these steps □ It is apparent how output from step 4 corresponds to step 5, step 5 to step 6, step 6 to step 7, and step 7 to step 8
□ 4 Excellent □ 3 Good □ 2 Fair □ 1 Poor
Likelihood Determination
□ Likelihood determination considers threat source, motivation, and capability □ Likelihood determination considers the nature of the vulnerability □ Likelihood determination considers existence and effectiveness of existing controls □ Ratings (categories) for likelihood determination are fully described
□ 4 Excellent □ 3 Good □ 2 Fair □ 1 Poor
Impact Analysis
□ The adverse impact in terms of financial loss resulting from a successful threat exercise of a vulnerability is fully described □ The adverse impacts in terms of reputation resulting from a successful threat exercise of a vulnerability is fully described □ The adverse impact in terms of operations resulting from a successful threat exercise of a vulnerability is fully described □ Ratings (categories) for impact analysis are fully described
□ 4 Excellent □ 3 Good □ 2 Fair □ 1 Poor
Risk Determination
□ Risk determination is clearly tied to likelihood □ Risk determination is clearly tied to magnitude of impact □ Risk determination is clearly tied to adequacy of existing security controls □ Ratings for risk determination are fully described
□ 4 Excellent □ 3 Good □ 2 Fair □ 1 Poor

Scoring for Risk Determination
Add the following:
Number of Excellent ratings (0-4) _____x 4 = _____
Number of Very Good ratings (0- _____x 3 = _____
4) _____x 2 = _____
Number of Fair ratings (0-4) _____x 1 = _____
Number of Poor ratings (0-4) = _____ / by 16
Total Score: = ____ x 100 = _____
Score > 90 Excellent
Score 80-89 Very Good
Score 70-79 Fair
Score < 70 Poor

Figure 2: Risk determination section from the checklist.

Establishing a Set of Procedures for Translating Observations into Quantitative Statements about Degree/Amount

The next and last step in designing a valid and reliable performance assessment instrument is to establish a set of procedures for translating observations into quantitative statements about degree or amount. When doing this, it is important to think about 1) the importance of each subsection relative to the other subsections, and 2) the importance of each section relative to the other sections. In this particular checklist, each subsection was given equal weighting relative to the other subsections. However, the sections were weighted differently. The weighting used for the different sections was as follows: system characterization – 20%; threat, vulnerability, control analysis – 30%; risk determination 25%; control recommendations and results documentation – 20%; format and style – 5%.

For this performance assessment, an equal number of items was used for each subsection. Again, each item represented an attribute that was considered desirable in the students' work product. Students could earn a maximum of four points in any subsection and a minimum of zero. As shown in the last row in figure 2, the number of excellent scores received were then multiplied by four points, the number of good scores were multiplied by three points, the number of fair scores were multiplied by two points, and the number of poor scores were multiplied by one point. Then the points for that section were summed and divided by the total possible points to provide a percentage for that section. Scores for each section were then converted to points by multiplying the percentage by the weighting for the section. Finally, points for each section are summed for a total score out of 100 possible points. An example is provided in figure 3 below.

	Weighting	% on the Section	Section Points
System Characterization	20%	100	20
Threat, vulnerability, control analysis	30%	81.25	24.38
Risk determination	25%	100	25
Control recommendations/results documentation	20%	83.33	16.66
Format and style	5%	100	5
		Total Score	91.04

Figure 3: Algorithm for calculating scores.

BENEFITS AND DRAWBACKS

Similar to other methods for assessing student achievement, there are also benefits and drawbacks to using a performance checklist. This is true regardless of the performance task being assessed. A

One of the primary benefits is that an instrument like this is an effective communication tool. It can be used before the project starts to articulate expectations. A performance checklist can be used throughout the project to communicate strengths and weaknesses in performance to date and it can also be a useful mechanism to start a discussion about misunderstandings. A performance checklist is also an effective way to communicate final performance at the end. Generally, students appreciate knowing the criteria early and like revisiting expectations frequently through the use of the checklist. When used with teams, such as this course, the checklist can be an effective tool for facilitating discussion among team members. Using checklists iteratively can be both motivating and demotivating to students. Students have expressed that the like have a clear target to aim for in their performance. However, the first checklist that they get back is demotivating because their score is low. But as improvements are made with each draft that is submitted and as they see the improvements through increasing scores, they become motivated to do even better. When allowing for multiple drafts, it is actually possible to lose points as changes are made to the draft; this can be frustrating to students, especially those who are performance-oriented. It is important to communicate this possibility clearly and often to students. Peer grading was also used in this class in an attempt to determine the degree to which each team member contributed to the product; however, that is not the focus of this paper.

From an instructor's point of view, a checklist is helpful in providing a guide for grading papers in a consistent manner. Consistency is important when grading across teams and also across time, i.e., grading various iterations of a report from the same team. When grading across time, it is advisable to retain a copy of the previous version of the report and the completed checklist that accompanied that version. When students start losing, it is helpful to be able to return to previous versions. Sometimes the comparison is the comparing across versions that supplies the most meaningful formative feedback to students. When using a checklist, I do not require that students actually organize the report in the same order as the checklist is organized. Therefore, when grading student work, I often spend a lot of time flipping through the paper to find evidence of a particular subsection or item in a subsection. This can be time consuming; however, the checklist is meant to describe, not prescribe, how students write the report. Organizing the report in a coherent and logical fashion is part of the process of producing a real-world, direct, and overt performance. When designing a performance assessment, be careful not to create an instrument that is expeditious for you, the instructor, to use, but is overly formulaic and therefore, reduces student learning to lower level knowledge and skills.

When students are given detailed information about performance requirements, some students will try to play a numbers game by only making improvements to those sections that are weighted most heavily. By investing their time on those sections, they increase their chances of improving their grade, while still having a product that is lacking in certain areas. The best way to address this is to create interdependencies in the performance assessment. By creating interdependencies, students are forced to improve all sections or subsections because each relies on the other.

The process of designing, developing, using, and then revising a valid and reliable instrument for assessing student performance 1) forces articulation of my expectations, and 2) provides a vehicle for communication about the expectations and the degree to which students are meeting them before work begins, as it is being performed, and after its completion. While it is a laborious task, it can be worth the time investment

REFERENCES

[1] Committee on National Systems Security (2004). http://www.nstissc.gov/html/library.html

[2] CRESST Assessment Glossary (2004). http://www.cse.ucla.edu/CRESST/pages/glossary.htm

[3] Dark, M.J. (2004). Civic Responsibility and Information Security: An Information Security Management, Service Learning Course. *Proceedings of the Information Security Curriculum Development Conference, 2004.*

[4] Dark, M.J. (2004). Evaluation. In *Education and Technology: An Encyclopedia* (Kovalchik and Dawson, Eds). ABC CLIO: Santa Barbara, CA.

[5] NIST (2004). Risk Management Guide for Information Technology Systems. http://csrc.nist.gov/publications/nistpubs/index.html

[6] Northern Illinois University (2004). Assessment Terms. http://www.niu.edu/assessment/_resourc/asterms.shtml

[7] Sweeney, B. (1994). Glossary of Assessment Terms. http://www.teachermentors.com/RSOD%20Site/PerfAssmt/glossary.html#anchor96926

[8] W.K. Kellog Foundation (2004). *Learning in Deed.* http://learningindeed.org/index.html