9-1-2010

Development of Information Technology Auditing Teaching Modules: An Interdisciplinary Endeavor between Seidenberg and Lubin Faculty

Chienting Lin
Seidenberg School of CSIS

Li-Chiou Chen
Seidenberg School of CSIS

Kaustav Sen
Lubin School of Business

May 11, 2010

Thinkfinity Cornerstone 3: Interdisciplinary Informatics - Grant Application (2nd Round)

Final Project Report

Development of Information Technology Auditing Teaching Modules: An Interdisciplinary Endeavor between Seidenberg and Lubin Faculty

PI: Chienting Lin, Assistant Professor of Information Technology, Seidenberg School of CSIS
Co-PI: Li-Chiou Chen, Assistant Professor of Information Technology, Seidenberg School of CSIS
Co-PI: Kaustav Sen, Associate P rofessor of Accounting, Lubin School of Business

Email: { clin, lchen, ksen } @ pace.edu

Project Goals

A) Please outline your original goals.

The original goals of the project were to develop interdisciplinary Information Technology (IT) Auditing teaching modules, to be integrated into courses offered by both Business and Information Technology disciplines during Fall 2009 and Spring 2010. IT Auditing is an interdisciplinary field which requires understanding audit, control, technology and security concepts in accordance with audit standards, guidelines, and best practices. Thus, IT Auditing requires interdisciplinary knowledge across IT and Accounting/Auditing domains. With increasing use of IT in business processes, the demand for IT Auditors is increasing rapidly, offering a lucrative career path. Acquiring IT Audit related knowledge and skills will help our students improve their career opportunities by exploring this growing field.

Based upon the curriculum content areas of the CISA Exam as well as the ISACA Model Curriculum, we proposed the following three interdisciplinary teaching modules for IT Auditing: 1) IT Auditing Frameworks & Business Continuity; 2) IT Lifecycle Management & Service Delivery; and 3) Protection of Information Assets.

We had developed the three teaching modules. Each individual module can be covered in one to two weeks. The entire set of three IT Auditing modules can then be covered in 3-4 weeks of class time. For each of the individual modules, we had developed presentation slides, reading lists and online quizzes based on the CISA Exam. We had also identified an overarching case study to be used throughout the three individual modules for continuity reasons.

B) What progress have you made towards your original goals on your project to date?

May 11, 2010

We have achieved our original goals of the project. The progress of the project is listed as below.

1. **Instructional materials for the three course modules**: We have created three IT auditing teaching modules. Each module includes a set of slides, student online quizzes similar to the official CISA exam questions, and a case study.
2. **Student learning outcomes**: We have incorporated the teaching modules in three courses, including ACC 375 Accounting Information Systems, CIT251 (originally IT300) Overview of Computer Security, and CIT352 (originally IT304) Internet and Network Security. We had covered the intended topics and subsequently assessed students' learning of these materials.
3. **Student evaluation of teaching modules:** We collected feedback from students regarding their learning experience using an anonymous web-based survey. The results from the survey will help us to improve the teaching modules in the future.
4. **Publications**: We have published a paper regarding the development of IT auditing curriculum design in the 2009 Colloquium for Information Systems Security Education.

Activities

C) What activities have been completed to contribute to meeting/progressing toward these goals?

Our project activities are described as below in details.

1. Develop teaching modules
   We had developed comprehensive teaching materials for each of the three modules. The teaching modules integrate and summarize concepts and topics from sources including CISA review manual, computer security and accounting information systems textbooks, and professional IT auditing publications [1, 2, 3]. Using any one of these three sources is inadequate for preparing our students to take the CISA exam. The standard textbooks in computer security and accounting information systems touch upon the fundamental principles and concepts needed for understanding the subjects in depth. On the other hand, the CISA review manual provides specific description of the subjects but do not elaborate on the foundation needed for proper learning. Hence, we integrated the materials from both standard textbooks, CISA review manual and professional publications to tailor the teaching modules in meeting the need of our students.

2. Incorporate teaching modules into classes
   Unlike experienced professionals who want to get CISA certified, our student body consists of a group with very little real world experience. In order to focus their learning effort to match the topics relevant for the CISA exam, we developed three sets of new lecture materials. We give two specific examples below.

Example 1: IT Audit concepts are covered in one chapter of a standard textbook in Accounting Information Systems. However, for accomplishing the goals of this project, we decided to highlight specific features ofCOBIT (Control Objectives for Information and related Technology) and its importance to IT Auditing. COBIT is the control framework developed by ISACA, the organization that offers the CISA certification (e.g. see www.isaca.org/**cobit**/). The typical AIS textbook bases its discussions on the COSO framework of internal control, which while widely accepted, does not focus on the technology aspects of systems auditing.

Example 2: Various network security control methods, such as firewalls, virtual private networks and intrusion detection systems, are typically taught in Internet and Network Security classes. These topics are usually presented in a way to teach security professionals in designing and implementing these controls methods but not to teach IT auditors in examining the vulnerabilities of the implementation. We had designed our lecture to specifically highlight the security issues IT auditors should examine in order to improve the internal controls of network security.

3. Conduct a web based survey
   We have conducted a web survey to collect student opinions on our teaching modules. The survey collected data on demographics, student rating (in 5 point Likert scale) on lectures, online tests, and impact on their career choices. The survey questions are listed in Table 1 below.

4. Publish a paper regarding IT auditing curriculum design
   We have published a paper in the 2009 Colloquium for Information Systems Security Education [4]. This paper provided an example of developing an interdisciplinary IT Auditing curriculum by mapping the CNSSI /NSTISSI standards with the prevailing ISACA IT Auditing Model Curriculum. IT Auditing involves assisting public or private organizations in ensuring that their information technologies and business systems are adequately protected and controlled. Consequently, IT Auditing professionals need to have a solid grounding in information technology, information assurance, auditing process, as well as regulatory and compliance frameworks. Through our standard mapping processes, we were able to discover the discrepancies between IA and Auditing and proceeded to redesign our current IA curriculum. Specifically, we have proposed a new IT Auditing course that addresses IT Auditing-specific topics, as part of an IT Auditing concentration in both undergraduate and graduate levels. Since CNSSI/NSTISSI standards have been mapped extensively to IA curriculum offered by the universities designated as NSA's Centers of Academic Excellence in Information Assurance Education (CAEIAE), our mapping can provide CAEIAE universities with suggestions on how to enhance their current IA curriculum in order to train IT Auditing professionals.

5. Establish a project web site to demonstrate project outcomes

We established a project web site (http://csis.pace.edu/~lchen/ita/) to further disseminate our results and publications. This effort will help other Pace faculty who teach in the IT auditing area accessing our teaching modules and other relevant resources.

D) What activities have not been completed? Please indicate why they have not been completed.

We have accomplished all the tasks proposed in this project. However, we will reserve the traveling budget to participate a conference in 2011 and the computer budget for software purchase in Fall 2010 in enhance our courses.

Project Outcomes & Impacts

E) Please outline the outcomes you have received as a result.

We have summarized our outcomes in the three tables below. Table 1 summarizes the topics covered in each teaching module. Table 2 lists the courses that had incorporated the teaching modules in Fall 2009 and Spring 2010 and the student learning outcomes in these courses. From the student learning outcomes, we confirmed that students have learned the topics well in order to complete the online tests and case study reports. Table 3 summarizes our student evaluation survey and the results from the survey. The survey results again confirm that our teaching modules have drawn students' interests in learning topics in IT auditing.

Course Modules	Subtopics	Content Provider
Module 1: IT Auditing Frameworks & Business Continuity (1 Week)	• Standards and Guidelines for IT Auditing • Internal Controls & Audit Planning Process • Audit Evidence Process & Audit Reporting • Control Framework: COBIT, COSO, ISO 27001-2 • Risk Management Methodologies • Business Impact Analysis (BIA) • Development of Continuity & Recovery Plans	Dr. Sen / Lubin
Module 2: IT Lifecycle Management& Service Delivery (1 Week)	• Infrastructure Planning & Implementation • Service Center Management Standards • Security Management Concepts • Service Level management practices • Functionality of Hardware and Network • Database Administration Practices • System Resiliency Tools and Techniques	Dr. Lin / Seidenberg

Module 3: Protection of Information Assets (1-2 Weeks)	• Information Assets Security Management • Attack Methods & Techniques • Logical IT Security & Access Control • Networking Protocols & Network Security • Encryption Algorithm Techniques • Physical and Environmental Security • Security Testing & Assessment Techniques • Security Incident Management	Dr. Chen / Seidenberg

Table 1: Contents of each teaching modules

Semester	Course number (CRN)	Course Modules Incorporated	Number of students in the class	Student learning outcomes
Spring 2010	ACC 375 (20056 and 20057)	Module 1	20056: 39 20057: 39	25 questions @ 10 points = 250 max 20056: 236.2 (mean), 37.7 (sd) 20057: 230.6 (mean), 50.3 (sd)
Spring 2010	IT304 (21241)	Module 3	11	25 questions @ 1 points = 25 max 20057: 15.8 (mean), 5.6 (sd)
Fall 2009	IT300 (71078 and 71791)	Module 1 & 2	71078: 11 71791 : 7	Group case study reports and presentation slides

Table 2: Summary of Results from Courses Incorporating the Teaching Modules

Number of Participants	78 in total 8 from IT304 (10%) 70 from ACC375 (90%)
Average age	22
Gender	47% : Male 53% : Female

Working full time	Yes 10% No 90%
Have heard about Certified Information Systems Auditor exam before this class	Yes: 19% No 81%
Average hours of studying the ITA materials	5.6 hours

Table 1: Summary of demographics

Survey Item / Average / (Standard Deviation)	**Category average /Standard deviation**
Q1. The contents of the lectures improve my knowledge in information technology auditing. 4.2 (0.7)	Lecture: 4.2 (0.7)
Q2. The lecture has a well-designed theme in information technology auditing. 4.2 (0.7)	
Q3. The lecture has sufficient supporting course materials, such as handouts, slides, textbook materials, for me to understand and review the topics discussed.	
Q4. The contents of the lectures covers topics that I would like to learn in information technology auditing. 4.2 (0.8)	
Q5. The questions asked in the Blackboard test are covered in the class. 4.1 (0.8)	Online tests: 4.2 (0.8)
Q6. The test stimulates my further interests in learning other topics in information technology auditing. 4.3 (0.7)	
Q7. The questions asked in the Blackboard test are covered in the materials (handouts, slides, etc) handed out in the class. 4.0 (0.8))	
Q8. The test questions are clear and helpful for reviewing the class materials. 4.2 (0.7)	
Q9. This class improves my knowledge and skills in the area of information technology auditing. 4.3 (0.7)	Overall Assessment: 3.9 (0.8)
Q10. After taking this class, I am even more interested in the information technology auditing area than I did. 4.2 (0.6)	
Q11. I will be interested in taking other information technology auditing related classes. 4.0 (0.7)	
Q12. I will be interested in taking the CISA exam in the future. 3.8 (0.9)	

Table 3: Summary of Survey Results

F) Has your project impacted students? If so, how many?
Our project has made significant impacts by providing students with abundant learning materials in IT auditing. The impacts can be illustrated by student comments from the course survey. Below are examples of student comments on our teaching utilizing the IT auditing materials designed in this project.

"Preparing for the test helped me in many different way(s). It helped me prepare for the final exams as well as learn about a lot of things that I feel are useful in the real business world. I see a lot of these things done at my internship and it actually interesting learning about it through this program."

"The course material is very helpful, especially for those in the work force, because it provides an understanding of security in technology and why it is so important to be able to access only those controls related to your tasks."

"This helped me learn about what the CISA exam is about and I am looking forward taking that."

G) Has your project impacted other faculty members? If so, how many?

The teaching modules we have developed can be easily incorporated in other courses in the Accounting and the IT departments. For example, ACC 366 Forensics Accounting, ACC 461 Auditing I ACC 362 Auditing II, CIT 354 Computer Forensics, and IT 666 Information Security Management. Our project web site will also provide various instructional resources in IT auditing to other faculty.

H) Were there any unintended outcomes achieved?

We were planning to purchase a laptop in order to host the project web site and conduct evaluation survey. While conducting this project, we discovered that we need more support in acquiring instructional resources instead of a laptop. Our project web site and evaluation can be hosted on Seidenberg School web server and Qualtrics for free. We therefore request to reallocate our hardware budget to instructional software budget. The instructional software will assist in developing hands-on IT auditing learning exercises for future works.

I) Do your outcomes reflect the change or benefit you were hoping to receive?

Our outcomes reflect the benefits that we are hoping to achieve for the project. These benefits can be explained in the following aspects:

Broaden the depth in IT auditing knowledge: Through our teaching modules, the instructor can provide student more in-depth knowledge in IT auditing. Lubin students were able to be benefited from these materials that incorporate topics in Information Security and Seidenberg students are benefited from materials in auditing and controls.

Highlight career opportunity for students: There was little awareness of the CISA exam before students were exposed to the teaching modules we designed. After taking our classes, 81% of students became aware of it. Our teaching modules have made a significant difference in their awareness of the exam and therefore allow them to pursue another career opportunity.

J) How has your project furthered the Thinkfinity Cornerstone you selected?

We have achieved the following goals of Thinkfinity Cornerstone 3 (Interdisciplinary Informatics):

1. Create web-based resources for instructional delivery and assessment: We have created the slides and online tests for the teaching materials we proposed. All of our project outcomes will be accessible through our project web site.

2. The design and development of course modules for interdisciplinary programs: We have developed course modules in IT auditing that combines knowledge domains in both Computer Security and Accounting. The course modules have also been incorporated in both IT programs and Accounting program.

Future Plans

K) Describe your future plans for sustaining the program or project.

We plan to further expand our effort in developing IT auditing teaching materials by the following activities:

1. Prepare publications in this area to further disseminate our results.
2. Expand our evaluation and apply for an IRB exempt review based on our evaluation in order to publish our results from the evaluation.
3. Incorporate the course modules in other courses in Fall 2010.
4. Seek for future funding opportunity, such DoD IASP grant, to establish an interdisciplinary IT auditing curriculum implemented in both Lubin and Seidenberg schools.

References

1. ”IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting ” April 2004 IT Governance Institute.

2. Tools, Techniques and Tips for IT Auditors: Strategies for Complying With Section 404 by J. Grenough (ISACA Journal2006)

3. SAS 70 for Sarbanes-Oxley Compliance by M. Coe (ISACA Journal 2006)

4. Chienting Lin and Li-Chiou Chen. (2009). “Development of an Interdisciplinary Information Technology Auditing Program,” Proceedings of the 13th Colloquium for Information Systems Security Education, Seattle, WA, June 1-3, 2009.

Appendix

A. Course Syllabi for IT300, IT304, and ACC375 (also accessible through project web site http://csis.pace.edu/~lchen/ita/)

B. Case Study

C. Selected student reports/presentation slides on the case study

D. Slides for the teaching modules (also accessible through project web site http://csis.pace.edu/~lchen/ita/)

Computer Security Overview (IT300 CRN: 71078)

Fall 2009

Instructor: Li-Chiou Chen
Office : Goldstein Academic Center 320 (PLV)
Office hours: 1-6 PM Wednesday (PLV) or by appointments
Phone (PLV office): 914-7733907
Email: lchen@pace.edu (Use this subject format to send me emails: "IT300-Your last name-topic".)

Class Meetings

Wednesday 6:00-8:45PM, Goldstein Academic Center 300

Course Goal

This course is to introduce the basic concepts in computer security for undergraduate students with introductory background in computing. Computer security is important in an era when computer systems are handling most of personal information, organizational transactions, and critical infrastructures. Information technology professionals should be able to recognize the vulnerabilities of their computer systems, possible threats from inside and outside of an organization and security technologies to mitigate the threats. After taking this class, students will be able to

- recognize software vulnerability, threats against information systems, and network attacks,
- understand basic concepts in cryptography, such as private encryption and public key encryption,
- understand security technology in communication and ecommerce, such as Secure Socket Layer,
- understand technology to mitigate security threats and operate commonly used security tools, such as firewalls and intrusion detection systems,
- be aware of legal and policy issues related to corporate information security, and
- understand basic concepts on risk management for information assets.

In addition, students will gain hand-on experience by investigating security problems through lab exercises. Using a group project, the class will encourage students to develop further interests in a specific topic in computer security.

Textbooks

Panko: Raymond R. Panko, Corporate Computer and Network Security, 2nd Edition, 2009, Pearson/Prentice Hall, ISBN: 0-13-185475-5.

Secure Web Development Teaching (SWEET) Modules – Will be distributed by the Instructor.

Grading

Lab assignments	35%
Term project	20%
Midterm exam	20%
Final exam	20%
Participation	5%

Assignment Guidelines

- All assignments should be typed and hard copies should be handed in during class meeting.
- All assignments should be returned in class on the due date. No late homework is accepted unless approved in advance.

Term Project

- TBA

Academic Honesty and Integrity

- You are encouraged to discuss readings, class contents and questions with other students. However, all homework assignments, quizzes and the exam should be done on an individual basis. Pace students are expected to maintain academic honesty and integrity defined by the CSIS and the Pace University policy.
- Read the White Hat Oath and White Hat Agreement. Sign the White Hat Agreement and hand it in during the first meeting.

Resources

- The Pace University Writing Center offers tutorial services in writing as well as handouts and reference materials on writing for student use in person or via the web at www.pace.edu/dyson/writingcenter. The staff of instructor and student tutors can assist students in understanding writing assignments and criteria and can help students with any stage of the writing process, from brainstorming topics to revision of rough drafts. The writing center is located at NY-Birnbaum Library, 2nd Floor, 346-1085; PLV-Mortola Library, 3rd Floor, 773-3942.
- The Pace University Library offers digital libraries through its web site (http://appserv.pace.edu /library/). Digital libraries, such as ACM Digital Library and IEEE Society Digital Library, are good sources to search for security related reports, articles and papers.

Course Calendar

Week	Date	Topics	Readings	Assignment due
1	09/09	Introduction	Panko Ch1	Lab 1 Student Information Sheet Singed White Hat Agreement
2	09/16	Basics on computer networks, TCP/IP, Linux Basics)	Panko Module A Lecture Notes	Lab 2: Ubuntu Linux basics Lab instructions Lab VM
3	09/23	Attack Methods	Panko Ch1	Lab 3: Port scanning
4	09/30	Cryptography	Panko Ch3 SWEET Modules: Cryptography	Lab 4: Public key encryption

5	10/07	Cryptography	Panko Ch4	Lab 5: Hashing and Stegnography
6	10/14	Access Control	Panko Ch5	Lab 6: Password Security
7	10/21	**Midterm Exam**		**Midterm Exam Review**
8	10/28	Firewalls	Panko Ch6	Lab 7: Firewalls
9	11/04	Host and Data Security	Panko Ch7	Lab 8: Host Hardening
10	11/11	Application Security	SWEET Modules: Secure Web Transactions	Lab 9: Browser Security and SSL (OpenSSL)
11	11/18	Security Regulation & Compliance	Panko Ch2 Lecture Notes	Lab 10: IT auditing
12	11/25	No class (Thanksgiving)		
13	12/02	Incident Handling	Panko Ch9	
14	12/09	Project presentation		Project report
15	12/16	**Final Exam**		**Final Exam Review**

Last modified: September 1st, 2009 by Li-Chiou Chen.

IT304 Internet and Network Security (CRN: 21214)

Spring 2010

Instructor: Dr. Li-Chiou Chen
Office : Goldstein Academic Center 320 (Pleasantville)
Office hours: Wednesday 1-6PM
Phone: 914-7733907
Email: lchen@pace.edu (Use this subject format to send me emails: "IT304-Your last name-topic".)

Class Meetings

Wednesday 6:00-8:45PM, Goldstein Academic Center 315

Course Goal

This course gives an in-depth and **hands-on** look at network defense concepts and techniques. Along with examining different network defense strategies, this course will explore the advancement of network security implementations. Students will be introduced to the following topics:

- Network Defense Fundamentals
- Security Policy Designs & Implementation
- Network Traffic Signatures
- Virtual Private Network (VPN) Concepts and Implementation
- Intrusion Detection System Concepts
- Intrusion Detection: Incident Response
- Firewall Configuration and Management
- Strengthening Defense through Ongoing Management
- Web Application Security
- Wireless Security and DNS Security

Textbooks

Required

Weaver: Randy Weaver (2006). "Guide to Network Defense and Countermeasures," Second Edition, Thomson Course Technology. ISBN: 1418836796.

Secure Web Development Teaching Modules – Will be distributed by the Instructor.

Supplemental

Stallings: William Stallings and Lawrie Brown (2008). "Computer Security: Principles and Practice," Prentice Hall. ISBN: 0106004245.

Grading

Lab assignments	35%
Midterm exam	20%
Term project	20%

Final exam	20%
Participation	5%

Lab report Guidelines

- All lab instructions can be downloaded from the class web site and the lab reports should be typed.
- Both the electronic copies and the hard copies should be handed in after the class or before the due dates.

Term Project

- TBA

Academic Honesty and Integrity

- You are encouraged to discuss readings, class contents and labs with other students. However, all quizzes and the exam should be done on an individual basis. Pace students are expected to maintain academic honesty and integrity defined by the CSIS and the Pace University policy.
- Read the White Hat Oath and White Hat Agreement. Sign the White Hat Agreement and hand it in during the first meeting.

Resources

- The Pace University Writing Center offers tutorial services in writing as well as handouts and reference materials on writing for student use in person or via the web at www.pace.edu/dyson/writingcenter. The staff of instructor and student tutors can assist students in understanding writing assignments and criteria and can help students with any stage of the writing process, from brainstorming topics to revision of rough drafts. The writing center is located at NY-Birnbaum Library, 2nd Floor, 346-1085; PLV-Mortola Library, 3rd Floor, 773-3942.
- The Pace University Library offers digital libraries through its web site (http://appserv.pace.edu/library/). Digital libraries, such as ACM Digital Library and IEEE Society Digital Library, are good sources to search for security related reports, articles and papers.

Course Calendar

Week	Date	Topics	Readings	Assignment due
1	01/20	Overview of Computer Security and Computer Networks	Ch.1	Lab 1: Simple Network Tools
2	01/27	Overview of Network Attacks	Lecture Notes	Lab 2: Stress Testing
3	02/03	Risk Analysis & Security Policy	Ch.2 & 3	Lab 3: Risk Analysis
4	02/10	Snow – class cancelled		
5	02/17	Signature Analysis	Ch.4	Lab 4: Signature Analysis in Wireshark
6	02/24	Intrusion Detection Systems	Ch.7-8	Lab 5: Intrusion Detection with Snort and BASE
7	03/03	Virtual Private Networks	Ch.5-6	Lab 6: VPN testing
8	03/10	Midterm Exam		

9	03/17	Firewalls	Ch.9-11	Lab 7: Linux Firewall
10	03/24	Web Security (HTTP & HTML)	SWEET Module: Web Introduction	Lab 8: HTTP & Web Proxy (Ubuntu VM)
11	03/31	Web Security (Web Vulnerability)	SWEET Module: Web Server Vulnerability	Lab 9: Web vulnerability testing on Web Goat (Ubuntu VM)
12	04/07	No Class: Spring Break		
13	04/14	Web Security (Penetration Test)	SWEET Module: Penetration testing	Lab 10: Web site penetration test on BasStore (Ubuntu VM)
14	04/21	IT Auditing	Lecture Notes	Lab 11 IT Auditing Online Test
15	04/28	Project Presentation		**Final Project Report**
16	05/05	Final Exam		

Last modified: Jan. 11th, 2010 by Li-Chiou Chen.

Lubin School of Business
Pace University
Spring 2010
New York City Campus

Course Information
Accounting Information Systems (AIS)

Instructor Information
Dr. Kaustav Sen
Office: Room W484, One Pace Plaza
Phone: (212) 618 – 6413
Email: ksen@pace.edu

Office Hours:
Tue 2.30-6 pm
Thu 1.00-2.30 pm

Textbooks
Accounting Information Systems by M. Romney & P. Steinbart, Prentice Hall (Customized Edition, available at Pace University bookstore).

Course Description

The purpose of this course is to provide students with the conceptual and technical foundations of contemporary accounting and information systems. The course covers design, management and control of information systems for accountants and auditors. Topics in design and control include database concepts, flowcharting, and computer security. Business processes, such as revenue and expenditure cycles in a computerized environment are explained. Additionally, students are required to complete projects using software such as Peachtree and Microsoft Access. This course prepares students for possessing the required skills for working in a computerized accounting environment.

Course Overview

In *Statement of Financial Accounting Concepts No. 2*, the Financial Accounting Standards Board defined accounting as being an information system. It also stated that the primary objective of accounting is to provide information useful to decision makers. Accounting information systems (AIS) course focuses on understanding how the accounting system works: how to collect data about an organization's activities and transactions; how to transform that data into information that management can use to run the organization; and how to ensure the availability, reliability, and accuracy of that information. The AIS course not only helps students develop specialized computer skills on a basis of accountability and control, but also complements the other accounting courses students take.

Learning Objectives
By the end of ACC 375, students will:
1. Explain the role an AIS plays in a company's value chain and learn how the AIS can add value to a business.
2. Identify the major internal and external parties that an AIS interacts with and the

type of information it provides each user.
3. Learn the major transaction cycles present in most companies and the ways information is stored in computer-based information systems.
4. Prepare and use data flow diagrams and various flowcharts to understand, evaluate, and design information systems.
5. Use a general ledger software and database to collect accounting data to provide decision makers with information.
6. Explain basic control concepts and why computer control and security are important.
7. Compare and contrast the approaches and techniques that are used to commit computer fraud.
8. Identify the objectives of an information system audit, and describe the four-step approach necessary for meeting these objectives.

Teaching Methodology

A combination of lecture, discussion, case-study and problem-solving is used.

Course Requirements and Grading

- Students' grade determination factors are stated below:

Midterm exam	30
Final exam	40
Assignments (3 at 10 points each)	30
Total	100

- Letter grade in response to the above cumulative percentage point is provided below:

A- and A	> 90%
B- to B+	80-89%
C- to C+	70-79%
D to D+	60-69%
F	< 60%

Normally, the median grade in a course such as ACC 375 at Pace has been C+ or B-.

Both the mid-term and final will be closed-book in-class exams. The final will be non-cumulative and will cover all material discussed after the midterm. The exams are based on the textbook, additional handouts and class discussion.

Effective Learning Tips:

You can get the maximum benefit from the course only when you have read the assigned chapter before you come to the class; be attentive and participate in the class discussion; and practice the homework in a timely fashion. **Please read the following learning tips carefully:**

1. All lecture notes, assignment solutions, and course materials for using Peachtree software will be posted in the course website at http://blackboard.pace.edu/.

2. This course requires approximately 5-7 hours, on average, of preparation for each class period. This includes review of the previous class, completing the assignments and preparing for the next class. Please make sure that you can commit to the time requirements before you register for this course.
3. No make-up exams allowed without a doctor's note presented in the very next class. Zero grades for missed exams.
4. In the current accounting curriculum, this is the only accounting information system course. However, a large part of the material in this course is new. The accounting information systems play a very important part of the accounting function. You have to focus on the issues and be enthusiastic about the materials in order to get the most out of this course.

Specific Issues

In the current accounting curriculum, this is the only AIS course. However, it is a very important part of the accounting function and is growing. While you have other accounting courses that you are probably taking now which are building on earlier courses, a large part of the material in this course is new. You have to focus on the issues and be enthusiastic about the materials in order to get the most out of this course.

The course covers topics that are relevant for any accounting function where knowledge of information systems is useful. The emphasis in this course is not to prepare you for any professional exam; rather give you concepts that will help you better prepare for a professional exam or be able to find a challenging career.

Assignments (10 points each)

1. Computer based assignment using Microsoft Access.

2. Control and Audit of AIS (CPA practice questions): You can access these questions using Blackboard and complete it before the day of the final exam.

3. Case presentation in class (2 member group). The schedule of the group discussions are listed in the weekly schedule.

Web/Internet Support

Please visit http://blackboard.pace.edu and select ACCT-375 Accounting Information Systems. As a major portion of this class will require on-line access and communication, it is recommended that you have access to the Internet on a regular basis. The course materials will be available on the Blackboard website for this course. All announcements will be posted there as well. All assignments should be turned in electronically using the digital drop-box feature in Blackboard. All communication will done using email. ***Blackboard uses your Pace email to communicate. Please make sure you either check your Pace email account regularly or have set it up to forward messages to another email that you access on a regular basis. You will not be able to operate in this class without email and Internet access.***

Rules of Professional Conduct

The Lubin School of Business prepares students for careers as business professionals. As part of that preparation we expect all students to behave as a professional throughout studies at the school. Following is a list of the specific rules of conduct that we expect students to observe in this course.

- Please do not talk to others, eat, put feet up on seats or table, comb hair, put on make up, loudly chew gum, or engage in any other non-professional conduct during the class periods. Students who persist in disrupting the learning environment will be asked to leave the class.
- Students are expected to come to every class, to arrive on time, and to stay through the entire class. If you miss a class, it is your responsibility to find out what you may have missed from a fellow-student. ***We will not respond to e-mails requesting such information because of unauthorized absence, late arrival or early departure.***
- Students should turn off cell phones during class time.

E-Mail Etiquette:

- Students must include *full name and section number* on any e-mails *and* attachments send to instructors. We will *not* reply to e-mails that lack this basic information.
- Students must also write in the *subject area* a short description of e-mail (e.g., ACC204 question). Otherwise, it is likely that the e-mail will be deleted by system's spam scanner or deleted by instructor without being opened.
- Do not use the e-mail list on *Blackboard* for any purpose unrelated to this course.
- E-mails in the course are a form of business communication. We expect students to compose e-mails with the same attention to correct grammar and syntax, politeness and professional tone that apply to all forms of business correspondence.

Class Decorum

Students' private talks disturbing class learning environment is **extremely** prohibited. ***A student will be asked to leave the classroom for the remainder of that class if his/her talking or whispering voice is so loud to disturb the class learning environment.*** **No cell phones or pagers** should be in an activation mode in the classroom. If a phone or pager goes off, you will be asked to leave the classroom for the remainder of the class.

Policy of reviewing students' examination books

- Students will **NOT** be allowed to keep their midterm or final exams. However, full-period exams will be reviewed afterwards and critiqued during class. Note-taking is highly recommended at this time.
- Scantron cards will **NOT** be returned to students. Students must mark their answers in the examination books so that they can verify it after instructor's answers are announced during the critique exam section. Final exams can be reviewed in the instructor's presence or by appointment with the Department secretary.

Tutorial Help

Accounting tutorial is provided on the second floor of the downtown building (41 Park Row) with no charge to students. Students are advised to engage in adequate self-study before using this service in order to derive fuller value from contact with the tutors.

Academic Integrity

All members of the Pace community are expected to behave with honesty and integrity. ***Do not plagiarize and cheat in either computer projects or exam. Cheating penalties are severe.*** You are expected to conduct yourself with integrity. If you cheat, plagiarize, or aid someone else in cheating, you violate a trust. Cheating includes, but not limited to, copying answers on tests or assignments, glancing at nearby test papers, stealing, plagiarizing and illicitly giving or receiving help on computer projects, exams or assignments. The Undergraduate Catalog includes the following advisory for students on Academic Integrity:

> Students must accept the responsibility to be honest and to respect ethical standards in meeting their academic assignments and requirements. Integrity in the academic life requires that students demonstrate intellectual and academic achievement independent of all assistance except that authorized by the instructor. The use of an outside source, including electronics sources, in any paper, report or submission for academic credit without the appropriate acknowledgement is plagiarism. It is unethical to present as one's own work the ideas, words or representations of another without the proper indication of the source. Therefore, it is the student's responsibility to give credit for any quotation, idea or data borrowed from an outside source.
>
> Students who fail to meet the responsibility for academic integrity subject themselves to sanctions ranging from a reduction in grade or failure in the assignment or course in which the offense occurred to suspension or dismissal from the University.

To encourage academic integrity in students' written submissions, the Lubin School of Business subscribes to "Turnitin.com," which describes itself as follows:

> We [Turnitin.com] prevent and detect plagiarism by comparing submitted papers to billions of pages of content located on the Internet and our proprietary databases. The results of our comparisons are compiled, one for each paper submitted, in custom "Originality Reports." These reports are sent to participating educators, who access the results by logging into their Turnitin account(s). (www.turnitin.com)

As a condition of participating in the program, all required papers may be subject to submission for textual similarity review to Turnitin.com for the detection of plagiarism. All submitted papers will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism of such papers. No student papers will be submitted to Turnitin.com without a student's

written consent and permission. If a student does not provide such written consent and permission, the instructor may:

1. Require a short reflection paper on research methodology;
2. Require a draft bibliography prior to submission of the final paper;
3. Require the cover page and first cited page of each reference source to be photocopied and submitted with the final paper.
4. Require other steps as deemed appropriate by the instructor.

Students can get help on how to use resources properly in their research and writing from many sources. This site (http://www.pace.edu/library/pages/instruct/plaig.html) provides links to useful information. The Library also offers an online tutorial on doing research for papers called "APOLLO." The tutorial is the first item under Student Resources at the link just presented.

Reasonable Accommodations For Students With Disabilities

The University's commitment to equal educational opportunities for students with disabilities includes providing reasonable accommodations for the needs of students with disabilities. To request an accommodation for a qualifying disability, a student must self-identify and register with the Coordinator of Disability Services for his or her campus. No one, including faculty, is authorized to evaluate the need and arrange for an accommodation except the Coordinator of Disability Services. Moreover, no one, including faculty, is authorized to contact the Coordinator of Disability Services on behalf of a student. For further information, please see Information for Students with Disabilities on the University's web site.

Class schedule

Week	Topics	Chapter	Case
1	Business Processing: Overview	2	
	Systems Development and Documentation Techniques	3	
2	Relational Databases	4	3-1
	Database Design Using the REA Data Model	15	
3	Design of the Revenue Cycle	10	10-1,2
4.	Design of the Expenditure Cycle	11	11-1,2
5.	Computer Lab		
6.	**Midterm**		
7.	Computer Lab		
9.	Computer Fraud and Abuse	5	5-1,2
8.	Control and Accounting Information Systems	6	5-3, 6-1
10.	IS Controls for System Reliability-Part 1	7	7-1&2
11.	IS Controls for System Reliability-Part 2	8	8-1
12.	Auditing Computer-Based IS	9	9-1
13.	General Ledger and Reporting System / SOX	14	
	Review for Final		
14.	**Final**		

IT300 – Lab10: IT Auditing Case Study: Real-Wire

Your Names: _____

Real-Wire is a public electronic funds transfer network with its head office and major computer switch based in Chicago. It is currently under contract to the Department of Treasury to assist in E-Commerce and Electronic Funds Transfer (EFT) initiatives when federal systems are overloaded. They have handled overload processing, which has increased their workload by 15-20 percent on occasions. The company has computer switches in each capital city throughout the United States, including Alaska and Hawaii, that are linked into a national communications network. Approximately 200 financial institutions (banks, building societies, credit unions) use the network to provide Automatic Teller Machine and Point-Of-Sale services to their customers.

Real-Wire has only been in operation for 20+ years, but during that time it has been very successful. When the United States began to deregulate its financial markets in 1985 and foreign banks began to enter the marketplace, Real-Wire obtained substantial new business because it could offer these financial institutions immediate EFT services.

As a consultant specializing in information systems control and audit, you have been hired by the managing director of Real-Wire to examine the state of controls within the EFT system. She explains to you that an increasing number of potential customers are requesting some type of independent assurance that controls within the system are reliable. Accordingly, she has decided to initiate a controls review of the entire system so that a third-party "letter of comfort" can be provided to potential customers.

The initial part of your controls review focuses on the main switch in Chicago. As part of your review, you examine the status of disaster recovery planning for the switch. In terms of short-term recovery, controls appear to be in place and working. Backup tapes for all data and programs are stored both on-site and off-site to enable recovery if programs or data are lost for some reason. In addition, protocols for short-term recovery are well-documented, and operators seem familiar with and well-trained in these protocols. From time to time they have to exercise these protocols because some temporary system failure occurs. Real-Wire claims to offer its customers 24-hour service. The director states its personnel recognize the criticality of being able to perform efficient, effective system recovery in a timely manner.

When you examine controls over long-term disaster recovery, however, the situation is different. There is no long-term disaster recovery plan, nor are operators and other personnel trained in recovery protocols for a major disaster. For example, it is uncertain how Real-Wire

would recover from a fire that destroyed the switch or an event that caused major structural damage to the switch.

As a result of your findings, you meet with the managing director to find out why controls in this area are so weak when controls in other areas seem strong. She is surprised by your concern for long-term disaster recovery. She argues that for three reasons it is not cost-effective to prepare a long-term disaster recovery plan and to practice recovery protocols on a regular basis:

First, she believes a plan is useless because, in the event of a major disaster, timely recovery is impossible anyway. She points out that it would take several days for the telephone company to reconfigure all the data communication lines to another site. Even if Real-Wire had another switch available immediately, it would not operate during this period.

Second, she argues that Real-Wire's customers would not tolerate a decrease in their service levels when disaster recovery exercises were carried out. Unless disaster recovery protocols are practiced regularly, she argues, they are useless.

Third, she contends that eventual recovery will not be a problem anyway. Operations can simply be transferred to one of the switch in one of the capital cities. While the telephone company reconfigures data communication lines to the other switch, backup files can be flown to the site with plenty of time to spare. She argues that the customers of Real-Wire recognize that they will not be able to use their EFT facilities during the recovery period, but they accept this situation as a risk of doing business. The only other alternative, she argues, is to replicate all switching facilities in each capital city, and this clearly is not cost-effective.

Please prepare a short report as a team to address the following question from this case:

References: ISO 27002-17799 (section 14) and NIST SP800 (both are included in Lab10 folder)

1. Outline how you intend to respond to the managing director's comments in your report to the board of directors on the state of controls in Real-Wire computer operations.

2. What federal laws apply to Real-Wire? List and explain each applicable law and describe how it could be used to support your audit.

3. Do they have an intranet that uses TCP/IP heavily? Do they have any security software installed? What would be your major security concerns?

4. The Office of the Controller of the Currency plans to review them next year. What would you recommend?

IT300 – Lab10: IT Auditing Case Study: Real-Wire

Your Names: Daniel Molda and Jasdomin Tolentino

Real-Wire is a public electronic funds transfer network with its head office and major computer switch based in Chicago. It is currently under contract to the Department of Treasury to assist in E-Commerce and Electronic Funds Transfer (EFT) initiatives when federal systems are overloaded. They have handled overload processing, which has increased their workload by 15-20 percent on occasions. The company has computer switches in each capital city throughout the United States, including Alaska and Hawaii, that are linked into a national communications network. Approximately 200 financial institutions (banks, building societies, credit unions) use the network to provide Automatic Teller Machine and Point-Of-Sale services to their customers.

Real-Wire has only been in operation for 20+ years, but during that time it has been very successful. When the United States began to deregulate its financial markets in 1985 and foreign banks began to enter the marketplace, Real-Wire obtained substantial new business because it could offer these financial institutions immediate EFT services.

As a consultant specializing in information systems control and audit, you have been hired by the managing director of Real-Wire to examine the state of controls within the EFT system. She explains to you that an increasing number of potential customers are requesting some type of independent assurance that controls within the system are reliable. Accordingly, she has decided to initiate a controls review of the entire system so that a third-party "letter of comfort" can be provided to potential customers.

The initial part of your controls review focuses on the main switch in Chicago. As part of your review, you examine the status of disaster recovery planning for the switch. In terms of short-term recovery, controls appear to be in place and working. Backup tapes for all data and programs are stored both on-site and off-site to enable recovery if programs or data are lost for some reason. In addition, protocols for short-term recovery are well-documented, and operators seem familiar with and well-trained in these protocols. From time to time they have to exercise these protocols because some temporary system failure occurs. Real-Wire claims to offer its customers 24-hour service. The director states its personnel recognize the criticality of being able to perform efficient, effective system recovery in a timely manner.

When you examine controls over long-term disaster recovery, however, the situation is different. There is no long-term disaster recovery plan, nor are operators and other personnel trained in recovery protocols for a major disaster. For example, it is uncertain how Real-Wire would recover from a fire that destroyed the switch or an event that caused major structural damage to the switch.

As a result of your findings, you meet with the managing director to find out why controls in this area are so weak when controls in other areas seem strong. She is surprised by your concern for long-term disaster recovery. She argues that for three reasons it is not cost-effective to prepare a long-term disaster recovery plan and to practice recovery protocols on a regular basis:

First, she believes a plan is useless because, in the event of a major disaster, timely recovery is impossible anyway. She points out that it would take several days for the telephone company to reconfigure all the data communication lines to another site. Even if Real-Wire had another switch available immediately, it would not operate during this period.

Second, she argues that Real-Wire's customers would not tolerate a decrease in their service levels when disaster recovery exercises were carried out. Unless disaster recovery protocols are practiced regularly, she argues, they are useless.

Third, she contends that eventual recovery will not be a problem anyway. Operations can simply be transferred to one of the switch in one of the capital cities. While the telephone company reconfigures data communication lines to the other switch, backup files can be flown to the site with plenty of time to spare. She argues that the customers of Real-Wire recognize that they will not be able to use their EFT facilities during the recovery period, but they accept this situation as a risk of doing business. The only other alternative, she argues, is to replicate all switching facilities in each capital city, and this clearly is not cost-effective.

Please prepare a short report as a team to address the following question from this case:

References: ISO 27002-17799 (section 14) and NIST SP800 (both are included in Lab10 folder)

1. Outline how you intend to respond to the managing director's comments in your report to the board of directors on the state of controls in Real-Wire computer operations.

We intend to respond to the managing director's comments with an IT focused plan designed to restore operability in a timely manner at an alternate site. This will include obtaining and installing necessary hardware components, obtaining and loading any backup media, restoring critical operating systems and application software, restoring system data, testing system functionality including security controls, connecting systems to a network or other external system, and operating alternate equipment successfully.

2. What federal laws apply to Real-Wire? List and explain each applicable law and describe how it could be used to support your audit.

The Federal Information Security Management Act of 2002 (FISMA), the Gramm-Leach-Bliley Act of 1999 (GLBA), and the Sarbanes-Oxley Act of 2002 all apply to Real Wire. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided by another contractor. Real-Wire is currently under contract to the Department of Treasury to assist in E-Commerce and Electronic Funds Transfer (EFT) initiatives when federal systems are overloaded. GLBA provides for periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization. At Real-Wire, there is no long-term disaster recovery plan, nor are operators and other personnel trained in recovery protocols for a major disaster, such as a fire.

3. Do they have an intranet that uses TCP/IP heavily? Do they have any security software installed? What would be your major security concerns?

In our assessment, we determined that Real Wire is using TCP/IP heavily due to the type of business they are in. Unfortunately Real-Wire does not have strong software security installed on there intranet. Due to the fact that they are a financial company it is very likely that they will need a strong security force to deter attackers. There is a high chance that hackers and intruders could attack this company because of the government aspect of the business they are involved in.

4. The Office of the Controller of the Currency plans to review them next year. What would you recommend?

We recommend the use of the Federal Information Security Management Act of 2002 (FISMA) in order to protect their data. Real Wire should focus on long-term solutions and general policies to ensure the timely back-up of their information. For example, they should back up data once a day or on a monthly/weekly basis and transfer it to a safe location away from headquarters and natural disasters. Second server redundancy would also help in this case.

Real-Wire State of Controls

Short Term Recovery:
- •Appears to Be In Order
- •People and Processes are in Place

Long Term Recovery:
- •No Disaster Recovery Plan In Place
- •Operators and Other Personel Not Trained in Recovery

Issue:
- •Managing Director MisInformed About what can be accomplished with DR

Key Items to Be Addressed In A Disaster Recovery Plan

- An I/T focused plan designed to restore operability in a timely basis at an alternate site
- Causes of Disruptions
- Potential for Additional Disruptions
- Status of Physical Infrastructure
- Type of Damage
- Items to Be Replaced
- Estimated time to restore normal process

Recovery Procedures

- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Operating alternate equipment successfully.

Module 1: IT Auditing, Governance and Business Continuity

ACC 375: 4/27&29/2010

Module 1.1: IT Auditing

- Questions to be addressed in module 1.1 include:
  - What are the scope and objectives of audit work, and what major steps take place in the audit process?
  - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
  - How can a plan be designed to study and evaluate internal controls in an AIS?
  - How can computer audit software be useful in the audit of an AIS?

THE NATURE OF AUDITING

- Auditors used to audit around the computer and ignore the computer and programs.
  - Assumption: If output was correctly obtained from system input, then processing must be reliable.
- Current approach: Audit through the computer.
  - Uses the computer to check adequacy of system controls, data, and output.
  - SAS-94 requires that external auditors evaluate how audit strategy is affected by an organization's use of IT.
  - Also states that auditors may need specialized skills to:
    - Determine how the audit will be affected by IT.
    - Assess and evaluate IT controls.
    - Design and perform both tests of IT controls and substantive tests.

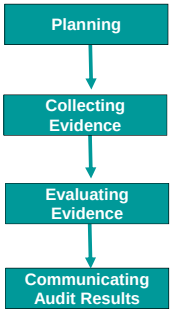
THE NATURE OF AUDITING

- The internal auditor's responsibilities include:
  - Review the reliability and integrity of operating and financial information and how it is identified, measured, classified, and reported.
  - Determine if the systems designed to comply with these policies, plans, procedures, laws, and regulations are being followed.
  - Review how assets are safeguarded, and verify their existence.
  - Examine company resources to determine how effectively and efficiently they are used.
  - Review company operations and programs to determine if they are being carried out as planned and if they are meeting their objectives.

THE NATURE OF AUDITING

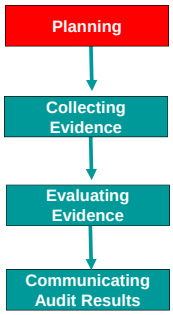
- **Types of Internal Auditing Work**
  - Three different types of audits are commonly performed.
    - Financial audit
    - Information systems audit
    - **Operational or management audit**

THE NATURE OF AUDITING



- **An Overview of the Auditing Process**
  - All audits follow a similar sequence of activities and may be divided into four stages:
    - Planning
    - Collecting evidence
    - Evaluating evidence
    - **Communicating audit results**

THE NATURE OF AUDITING



- **Audit Planning**
  - Purpose: Determine why, how, when, and by whom the audit will be performed.
  - The first step in audit planning is to establish the scope and objectives of the audit.
  - An audit team with the necessary experience and expertise is formed.
  - Team members become familiar with the auditee by:
    - Conferring with supervisory and operating personnel;
    - Reviewing system documentation; and
    - Reviewing findings of prior audits.

THE NATURE OF AUDITING

- The audit should be planned so that the greatest amount of audit work focuses on areas with the highest risk factors.
- There are three types of risk when conducting an audit:
  - Inherent risk
  - Control risk
  - **Detection risk**

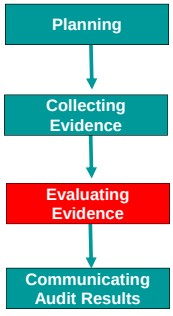
THE NATURE OF AUDITING

- **Collection of Audit Evidence**
  - Much audit effort is spent collecting evidence.

THE NATURE OF AUDITING

- **Collection of Audit Evidence**
  - The following are among the most commonly used evidence collection methods:
    - Observation
    - Review of documentation
    - Discussions
    - Physical examination
    - Confirmation
    - Re-performance
    - Vouching
    - **Analytical review**

THE NATURE OF AUDITING



- **Evaluation of Audit Evidence**
  - The auditor evaluates the evidence gathered in light of the specific audit objective and decides if it supports a favorable or unfavorable conclusion.
  - If inconclusive, the auditor plans and executes additional procedures until sufficient evidence is obtained.
  - Two important factors when deciding how much audit work is necessary and in evaluating audit evidence are:
    - Materiality
    - **Reasonable assurance**

THE NATURE OF AUDITING

- **Communication of audit results**
  - The auditor prepares a written (and sometimes oral) report summarizing audit findings and recommendations, with references to supporting evidence in the working papers.
  - Report is presented to:
    - Management
    - The audit committee
    - The board of directors
    - Other appropriate parties
  - After results are communicated, auditors often perform a follow-up study to see if recommendations have been implemented.

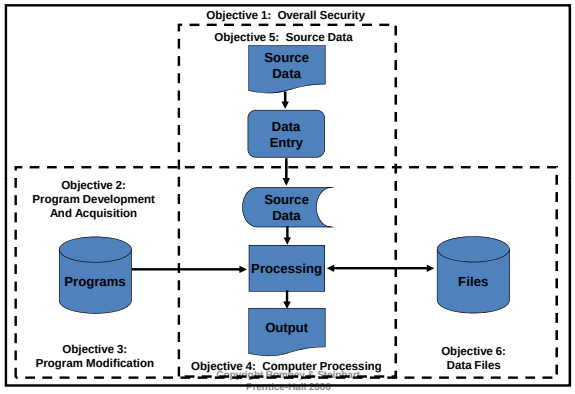
THE NATURE OF AUDITING

- ***The Risk-Based Audit Approach***
  - A risk-based audit approach is a four-step approach to internal control evaluation that provides a logical framework for carrying out an audit. Steps are:
    - Determine the threats (errors and irregularities) facing the AIS.
    - Identify control procedures implemented to minimize each threat by preventing or detecting such errors and irregularities.
    - Evaluate the control procedures.
    - **Evaluate weaknesses (errors and irregularities not covered by control procedures) to determine their effect on the nature, timing, or extent of auditing procedures and client suggestions.**

INFORMATION SYSTEMS AUDITS

- The purpose of an information systems audit is to review and evaluate the internal controls that protect the system.
- When performing an information system audit, auditors should ascertain that the following objectives are met:
  - Security provisions protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.
  - Program development and acquisition are performed in accordance with management's general and specific authorization.
  - Program modifications have management's authorization and approval.

IS COMPONENTS AND AUDIT OBJECTIVES



OBJECTIVE 1: OVERALL SECURITY

- **Types of security errors and fraud faced by companies:**
  - Accidental or intentional damage to system assets.
  - Unauthorized access, disclosure, or modification of data and programs.
  - Theft.
  - Interruption of crucial business activities.

OBJECTIVE 1: OVERALL SECURITY

- **Control procedures to minimize security errors and fraud:**
  - Developing an information security/protection plan.
  - Restricting physical and logical access.
  - Encrypting data.
  - Protecting against viruses.
  - Implementing firewalls.
  - Instituting data transmission controls.
  - Preventing and recovering from system failures or disasters, including:
    - Designing fault-tolerant systems.
    - Preventive maintenance.
    - Backup and recovery procedures.
    - Disaster recovery plans.
    - Adequate insurance.

OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

- **Types of errors and fraud:**
  - Two things can go wrong in program development:
    - Inadvertent errors due to careless programming or misunderstanding specifications; or
    - Deliberate insertion of unauthorized instructions into the programs.

OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

- **Control procedures:**
  - The preceding problems can be controlled by requiring:
    - Management and user authorization and approval
    - Thorough testing
    - Proper documentation

OBJECTIVE 3: PROGRAM MODIFICATION

- **Control Procedures**
  - When a program change is submitted for approval, a list of all required updates should be compiled by management and program users.
  - Changes should be thoroughly tested and documented.
  - During the change process, the developmental version of the program must be kept separate from the production version.
  - When the amended program has received final approval, it should replace the production version.
  - Changes should be implemented by personnel independent of users or programmers.
  - Logical access controls should be employed at all times.

OBJECTIVE 3: PROGRAM MODIFICATION

- To test for unauthorized program changes, auditors can use a source code comparison program to compare the current version of the program with the original source code.
  - Any unauthorized differences should result in an investigation.
  - If the difference represents an authorized change, the auditor can refer to the program change specifications to ensure that the changes were authorized and correctly incorporated.

OBJECTIVE 3: PROGRAM MODIFICATION

- Two additional techniques detect unauthorized program changes:
  - Reprocessing
    - On a surprise basis, the auditor uses a verified copy of the source code to reprocess data and compare that output with the company's data.
    - Discrepancies are investigated.
  - Parallel simulation
    - Similar to reprocessing except that the auditor writes his own program instead of using verified source code.
    - Can be used to test a program during the implementation process.

OBJECTIVE 4: COMPUTER PROCESSING

- **Processing Test Data**
  - Involves testing a program by processing a hypothetical series of valid and invalid transactions.
  - The program should:
    - Process all the valid transactions correctly.
    - Identify and reject the invalid ones.
  - All logic paths should be checked for proper functioning by one or more test transactions, including:
    - Records with missing data
    - Fields containing unreasonably large amounts
    - Invalid account numbers or processing codes
    - Non-numeric data in numeric fields
    - Records out of sequence

OBJECTIVE 4: COMPUTER PROCESSING

- The following resources are helpful when preparing test data:
  - A listing of actual transactions
  - The transactions that the programmer used to test the program
  - A ***test data generator program***, which automatically prepares test data based on program specifications

OBJECTIVE 4: COMPUTER PROCESSING

- **Concurrent audit techniques**
  - Millions of dollars of transactions can be processed in an online system without leaving a satisfactory audit trail.
  - In such cases, evidence gathered after data processing is insufficient for audit purposes.
  - Also, because many online systems process transactions continuously, it is difficult or impossible to stop the system to perform audit tests.
  - Consequently, auditors use ***concurrent audit techniques*** to continually monitor the system and collect audit evidence while live data are processed during regular operating hours.

OBJECTIVE 4: COMPUTER PROCESSING

- **Concurrent audit techniques use *embedded audit modules*.**
  - These are segments of program code that:
    - Perform audit functions;
    - Report test results to the auditor; and
    - Store collected evidence for auditor review.
  - Are time-consuming and difficult to use, but less so if incorporated when programs are developed.

OBJECTIVE 4: COMPUTER PROCESSING

- **An *ITF technique* places a small set of fictitious records in the master files:**
  - May represent a fictitious division, department, office, customer, or supplier.
  - Processing test transactions to update these dummy records will not affect actual records.
  - Because real and fictitious transactions are processed together, company employees don't know the testing is taking place.

OBJECTIVE 4: COMPUTER PROCESSING

- **The *snapshot technique* examines the way transactions are processed.**
  - Selected transactions are marked with a special code that triggers the snapshot process.
  - Audit modules in the program record these transactions and their master file records before and after processing.
  - The selected data are recorded in a special file and reviewed by the auditor to verify that all processing steps were properly executed.

OBJECTIVE 4: COMPUTER PROCESSING

- **The *system control audit review file (SCARF)* uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance.**
- Data recorded in a SCARF file or *audit log* include transactions that:
  - Exceed a specified dollar limit;
  - Involve inactive accounts;
  - Deviate from company policy; or
  - Contain write-downs of asset values.
- Periodically the auditor:
  - Receives a printout of SCARF transactions;
  - Looks for questionable transactions among them; and
  - Investigates.

OBJECTIVE 4: COMPUTER PROCESSING

- ***Audit hooks* are audit routines that flag suspicious transactions.**
- Example: State Farm Life Insurance looking for policyholders who change their name or address and then subsequently withdraw funds.
- When audit hooks are used, auditors can be informed of questionable transactions as they occur via ***real-time notification***, which displays a message on the auditor's terminal.

OBJECTIVE 4: COMPUTER PROCESSING

- ***Continuous and intermittent simulation (CIS)*** **embeds an audit module in a database management system.**
- The module examines all transactions that update the DBMS using criteria similar to those of SCARF.
- When a transaction has audit significance, the module:
  - Processes the data independently (similar to parallel simulation);
  - Records the results;
  - Compares results with those obtained by the DBMS.
- If there are discrepancies, details are written to an audit log for subsequent investigation.
- Serious discrepancies may prevent the DBMS from executing the update.

OBJECTIVE 4: COMPUTER PROCESSING

- **Analysis of Program Logic**
  - If an auditor suspects that a particular program contains unauthorized code or serious errors, a detailed analysis of the program logic may be necessary.
  - Done only as a last resort because:
    - It's time-consuming
    - Requires programming language proficiency
  - To perform the analysis, auditors reference:
    - Program flowcharts
    - Program documentation
    - Program source code.

OBJECTIVE 4: COMPUTER PROCESSING

- **The following software packages can help:**
  - Automated flowcharting programs
  - Automated decision table programs
  - Scanning routines
  - Mapping programs
  - **Program tracing**

OBJECTIVE 5: SOURCE DATA

- **Audit Procedures: Tests of Controls**
  - Observe and evaluate data control department operations and specific data control procedures
  - Verify proper maintenance and use of data control log
  - Evaluate how items recorded in the error log are handled
  - Examine samples of accounting source data for proper authorization
  - Reconcile a sample of batch totals and follow up on discrepancies
  - Trace disposition of a sample of errors flagged by data edit routines

Record Name: Employee Weekly Time Report	Field Names: Employee Number	Last Name	Department Number	Transaction Code	Week Ending (Date)	Regular Hours	Overtime Hours	Comments
Input Controls								
Financial totals						✓	✓	
Hash totals	✓							
Record counts								Yes
Cross-footing balance								No
Key verification	✓					✓	✓	
Visual inspection								All fields
Check digit verification	✓							
Pre-numbered forms								No
Turnaround document								No
Edit program								Yes
Sequence check	✓							
Field check	✓		✓			✓	✓	
Sign check								
Validity check	✓		✓	✓	✓			
Limit check						✓	✓	
Reasonableness test						✓	✓	
Redundant data check	✓	✓	✓					
Completeness test				✓	✓	✓	✓	
Overflow procedure								
Other								

OBJECTIVE 5: SOURCE DATA

- **Auditors should ensure the data control function:**
  - Is independent of other functions
  - Maintains a data control log
  - Handles errors
  - Ensures overall efficiency of operations
- Usually not feasible for small businesses and PC installations to have an independent data control function.

OBJECTIVE 5: SOURCE DATA

- **To compensate, user department controls must be stronger over:**
  - Data preparation
  - Batch control totals
  - Edit programs
  - Physical and logical access restrictions
  - Error handling procedures
- These procedures should be the focus of the auditor's systems review and tests of controls when there is no independent data control function.

OBJECTIVE 6: DATA FILES

- The sixth objective concerns the accuracy, integrity, and security of data stored in machine-readable files.
- Data storage risks include:
  - Unauthorized modification of data
  - Destruction of data
  - Disclosure of data
- Many of the controls discussed in Chapter 8 protect against the preceding risks.
- If file controls are seriously deficient, especially with respect to access or backup and recovery, the auditor should strongly recommend they be rectified.

OBJECTIVE 6: DATA FILES

- ***Auditing-by-objectives*** is a comprehensive, systematic, and effective means of evaluating internal controls in an AIS.
  - Can be implemented using an audit procedures checklist for each objective.
  - Should help the auditor reach a separate conclusion for each objective and suggest compensating controls.
- A separate version of the checklist should be completed for each significant application.

OBJECTIVE 6: DATA FILES

- **Compensating Controls**
  - Strong user controls
  - Effective computer security controls
  - Strong processing controls

COMPUTER SOFTWARE

- ***Computer audit software (CAS)*** or ***generalized audit software (GAS)*** are computer programs that have been written especially for auditors.
- Two of the most popular:
  - Audit Control Language (ACL)
  - IDEA
- Based on auditor's specifications, CAS generates programs that perform the audit function.
- CAS is ideally suited for examination of large data files to identify records needing further audit scrutiny.

COMPUTER SOFTWARE

- CAS functions include:
  - Reformatting
  - File manipulation
  - Calculation
  - Data selection
  - Data analysis
  - File processing
  - Statistics
  - **Report generation**

OPERATIONAL AUDITS OF AN AIS

- Techniques and procedures in operational audits are similar to audits of information systems and financial statement audits.
- The scope is different.
  - IS audit scope is confined to internal controls
  - Financial audit scope is limited to system output.
  - Operational audit scope is much broader and encompasses all aspects of information systems management.
- Objectives are also different in that operational audit objectives include evaluating factors such as:
  - Effectiveness
  - Efficiency
  - Goal achievement

Module 1.2: IT Governance

A. Laws Governing Hacking and Other Computer Crimes
B. Corporate Auditing
C. Governance Frameworks
D. Risk Analysis

1.2.A: Computer Fraud and Abuse Act of 1986

- Federal regulation, USC Title 18, Section 1030
- Updates to USC title 18
  - National Information Infrastructure Protection Act of 1996
  - Homeland Security Act of 2002

Computer Fraud and Abuse Act

- Criminalizes intentional access of protected computers without authorization or in excess of authorization (Hacking)
- Criminalizes the transmission of a program, information, code, or command that intentionally causes damage without authorization of a protected computer (Denial-of-Service and Viruses)
- Punishment
  - For first offenses, usually 1-5 years; usually 10 years for second offenses
  - For theft of sensitive government information, 10 years, with 20 years for repeat offense
  - For attacks that harm or kill people, up to life in prison

Electronic Communications Privacy Act of 1986 (ECMA)

- U.S. C., Title 47
- Also referring as Federal Wiretapping Act
- Regulates interception and disclosure of electronic information

Digital Millennium Copyright Act (DMCA) of 1998

- Addresses copyright related issues
- Makes the following things illegal
  - Remove or alter copyright management information from digital copies of copyrighted works
  - Bypass technical measures used by copyright owners to protect their works
  - Manufacture or distribute technologies primarily designed to circumvent technical measures used by copyright owners to protect their works

Laws Around the World Vary

- The general situation: lack of solid laws in many countries
- Cybercrime Treaty of 2001
  - Signatories must agree to create computer abuse laws and copyright protection
  - Nations must agree to work together to prosecute attackers

1.2.B: Compliance Laws and Regulations

- Compliance laws and regulations create requirements for corporate security
  - Documentation requirements are strong
  - Identity management requirements tend to be strong
- Compliance can be expensive
- There are many compliance laws and regulations, and the number is increasing rapidly

The Sarbanes-Oxley Act of 2002 (1)

- Makes internal controls a legal requirement
- Affects corporate governance, financial disclosure and the practice of public accounting
- To restore the public's confidence in corporate governance by making chief executives of publicly traded companies personally validate financial statements and other information
  - After Enron/Worldcom
- http://www.aicpa.org/sarbanes/index.asp

The Sarbanes-Oxley Act of 2002 (2)

- Section 404 of the Sarbanes-Oxley Act mandates that all public organizations
  - demonstrate due diligence in the disclosure of financial information and
  - implement a series of internal controls and procedures to communicate, store and protect that data.
- Public organizations are also required under Section 404 to protect these controls from internal and external threats and unauthorized access, including those that could occur through online systems and networks
- Publicly traded companies need to file SOX reports to SEC
- Need to be certified by external auditors

Privacy Protection Laws (1)

- The European Union (E.U.) Data Protection Directive of 2002
- Many other nations have strong commercial data privacy laws
- The U.S. Gramm–Leach–Bliley Act (GLBA)
- The U.S. Health Information Portability and Accountability Act (HIPAA) for private data in health care organizations

Privacy Protection Laws (2)

- **Data Breach Notification Laws**
  - California's SB 1386
  - Requires notification of any California citizen whose private information is exposed
  - Companies cannot hide data breaches anymore
- **Federal Trade Commission (FTC)**
  - Can punish companies that fail to protect private information
  - Fines and required external auditing for several years

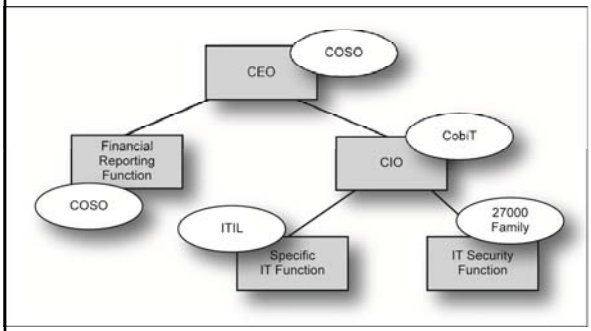
PCI-DSS

- Payment Card Industry–Data Security Standards
- Applies to all firms that accept credit cards
- Has 12 general requirements, each with specific subrequirements

FISMA

- Federal Information Security Management Act of 2002
- Processes for all information systems used or operated by a U.S. government federal agencies
- Also by any contractor or other organization on behalf of a U.S. government agency
- Certification, followed by accreditation
- Continuous monitoring
- Criticized for focusing on documentation instead of protection

1.2.C: Governance Frameworks



COSO - Background

- **Origins**
  - Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org)
  - Ad hoc group to provide guidance on financial controls
- **Focus**
  - Corporate operations, financial controls, and compliance
  - Effectively required for Sarbanes–Oxley compliance
  - Goal is reasonable assurance that goals will be met

COSO Components

- Control Environment
  - General security culture
  - Includes "tone at the top"
  - If strong, specific controls may be effective
  - If weak, strong controls may fail
  - Major insight of COSO
- Risk assessment
  - Ongoing preoccupation
- Control activities
  - General policy plus specific procedures
- Monitoring
  - Both human vigilance and technology
- Information and communication
  - Must ensure that the company has the right information for controls
  - Must ensure communication across all levels in the corporation

Enterprise Risk Management (COSO)

- Intent of ERM is to achieve all goals of the internal control framework and help the organization:
  - Provide reasonable assurance that company objectives and goals are achieved and problems and surprises are minimized.
  - Achieve its financial and performance targets.
  - Assess risks continuously and identify steps to take and resources to allocate to overcome or mitigate risk.
  - Avoid adverse publicity and damage to the entity's reputation.

CONTROL FRAMEWORKS

- Basic principles behind ERM:
  - Companies are formed to create value for owners.
  - Management must decide how much uncertainty they will accept.
  - Uncertainty can result in:
    - Risk
    - **Opportunity**

CONTROL FRAMEWORKS

- The ERM model is three-dimensional.
- Means that each of the eight risk and control elements are applied to the four objectives in the entire company and/or one of its subunits.

CONTROL FRAMEWORKS

- **ERM Framework Vs. the Internal Control Framework**
  - The internal control framework has been widely adopted as the principal way to evaluate internal controls as required by SOX. However, there are issues with it.
    - It has too narrow of a focus.
    - **Focusing on controls first has an inherent bias toward past problems and concerns.**

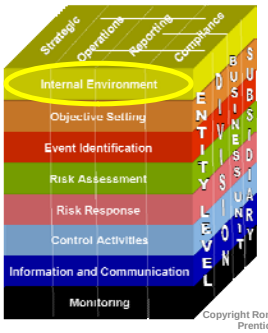
CONTROL FRAMEWORKS

- These issues led to COSO's development of the ERM framework.
  - Takes a risk-based, rather than controls-based, approach to the organization.
  - Oriented toward future and constant change.
  - Incorporates rather than replaces COSO's internal control framework and contains three additional elements:
    - Setting objectives.
    - Identifying positive and negative events that may affect the company's ability to implement strategy and achieve objectives.
    - Developing a response to assessed risk.

CONTROL FRAMEWORKS

- Controls are flexible and relevant because they are linked to current organizational objectives.
- ERM also recognizes more options than simply controlling risk, which include accepting it, avoiding it, diversifying it, sharing it, or transferring it.

INTERNAL ENVIRONMENT



- The most critical component of the ERM and the internal control framework.
- Is the foundation on which the other seven components rest.
- Influences how organizations:
  - Establish strategies and objectives
  - Structure business activities
  - Identify, access, and respond to risk
- A deficient internal control environment often results in risk management and control breakdowns.

INTERNAL ENVIRONMENT

- Internal environment consists of the following:
  - Management's philosophy, operating style, and risk appetite
  - The board of directors
  - Commitment to integrity, ethical values, and competence
  - Organizational structure
  - Methods of assigning authority and responsibility
  - Human resource standards
  - External influences

INTERNAL ENVIRONMENT

- The following policies and procedures are important:
  - Hiring
  - Compensating
  - Training
  - Evaluating and promoting
  - Discharging
  - Managing disgruntled employees
  - Vacations and rotation of duties
  - Confidentiality insurance and fidelity bonds

OBJECTIVE SETTING

- Objective setting is the second ERM component.
- It must precede many of the other six components.
- For example, you must set objectives before you can define events that affect your ability to achieve objectives

OBJECTIVE SETTING

- Objective-setting process proceeds as follows:
  - First, set strategic objectives, the high-level goals that support the company's mission and create value for shareholders.
  - To meet these objectives, identify alternative ways of accomplishing them.
  - For each alternative, identify and assess risks and implications.
  - Formulate a corporate strategy.
  - Then set operations, compliance, and reporting objectives.

EVENT IDENTIFICATION

- Events are:
  - Incidents or occurrences that emanate from internal or external sources
  - That affect implementation of strategy or achievement of objectives.
  - Impact can be positive, negative, or both.
  - Events can range from obvious to obscure.
  - Effects can range from inconsequential to highly significant.

EVENT IDENTIFICATION

- By their nature, events represent uncertainty:
  - Will they occur?
  - If so, when?
  - And what will the impact be?
  - Will they trigger another event?
  - Will they happen individually or concurrently?

EVENT IDENTIFICATION

- Management must do its best to anticipate all possible events—positive or negative—that might affect the company:
  - Try to determine which are most and least likely.
  - Understand the interrelationships of events.
- COSO identified many internal and external factors that could influence events and affect a company's ability to implement strategy and achieve objectives.

EVENT IDENTIFICATION

- Some of these factors include:
  - External factors:
    - Economic factors
    - Natural environment
    - Political factors
    - Social factors
    - **Technological factors**

EVENT IDENTIFICATION

- Some of these factors include:
  - Internal factors:
    - Infrastructure
    - Personnel
    - Process
    - **Technology**

EVENT IDENTIFICATION

- Companies usually use two or more of the following techniques together to identify events:
  - Use comprehensive lists of potential events
  - Perform an internal analysis
  - Monitor leading events and trigger points
  - Conduct workshops and interviews
  - Perform data mining and analysis
  - **Analyze processes**

RISK ASSESSMENT AND RISK RESPONSE

- The fourth and fifth components of COSO's ERM model are risk assessment and risk response.
- COSO indicates there are two types of risk:
  - **Inherent risk**

RISK ASSESSMENT AND RISK RESPONSE

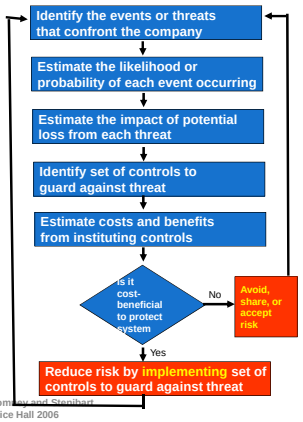
- The fourth and fifth components of COSO's ERM model are risk assessment and risk response.
- COSO indicates there are two types of risk:
  - Inherent risk
  - **Residual risk**

RISK ASSESSMENT AND RISK RESPONSE

- Companies should:
  - Assess inherent risk
  - Develop a response
  - Then assess residual risk
- The ERM model indicates four ways to respond to risk:
  - Reduce it
  - Accept it
  - Share it
  - **Avoid it**

RISK ASSESSMENT AND RISK RESPONSE

- Risks that are not reduced must be accepted, shared, or avoided.
  - If the risk is within the company's risk tolerance, they will typically accept the risk.
  - A reduce or share response is used to bring residual risk into an acceptable risk tolerance range.
  - An avoid response is typically only used when there is no way to cost-effectively bring risk into an acceptable risk tolerance range.



CONTROL ACTIVITIES

- Generally, control procedures fall into one of the following categories:
  - Proper authorization of transactions and activities
  - Segregation of duties
  - Project development and acquisition controls
  - Change management controls
  - Design and use of documents and records
  - Safeguard assets, records, and data
  - Independent checks on performance

CONTROL ACTIVITIES

- The following independent checks are typically used:
  - Top-level reviews
  - Analytical reviews
  - Reconciliation of independently maintained sets of records
  - Comparison of actual quantities with recorded amounts
  - **Double-entry accounting**

CONTROL ACTIVITIES

- The following independent checks are typically used:
  - Top-level reviews
  - Analytical reviews
  - Reconciliation of independently maintained sets of records
  - Comparison of actual quantities with recorded amounts
  - Double-entry accounting
  - **Independent review**

INFORMATION AND COMMUNICATION

- The seventh component of COSO's ERM model.
- The primary purpose of the AIS is to gather, record, process, store, summarize, and communicate information about an organization.
- So accountants must understand how:
  - Transactions are initiated
  - Data are captured in or converted to machine-readable form
  - Computer files are accessed and updated
  - Data are processed
  - Information is reported to internal and external parties

INFORMATION AND COMMUNICATION

- According to the AICPA, an AIS has five primary objectives:
  - Identify and record all valid transactions.
  - Properly classify transactions.
  - Record transactions at their proper monetary value.
  - Record transactions in the proper accounting period.
  - Properly present transactions and related disclosures in the financial statements.

MONITORING

- The eighth component of COSO's ERM model.
- Monitoring can be accomplished with a series of ongoing events or by separate evaluations.

MONITORING

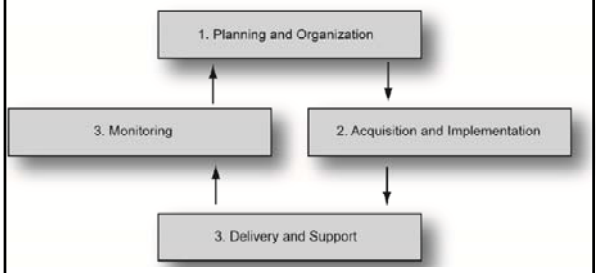
- Key methods of monitoring performance include:
  - Perform ERM evaluation
  - Implement effective supervision
  - Use responsibility accounting
  - Monitor system activities
  - Track purchased software
  - Conduct periodic audits
  - Employ a computer security officer and security consultants
  - **Engage forensic specialists**
  - Install fraud detection software
  - Implement a fraud hotline

CobiT

- Control Objectives for Information and Related Technologies
- CIO-level guidance on IT governance
- Offers many documents that help organizations understand how to implement the framework

The CobiT Framework

- Four major domains



The CobiT Framework

- Four major domains (Figure 2-26)
- 34 high-level control objectives
  - Planning and organization (11)
  - Acquisition and implementation (60)
  - Delivery and support (13)
  - Monitoring (4)
- More than 300 detailed control objectives

CobiT

- **Dominance in the United States**
  - Created by the IT governance institute
  - Which is part of the Information Systems Audit and Control Association (ISACA)
  - ISACA is the main professional accrediting body of IT auditing
  - Certified information systems auditor (CISA) certification

The ISO/IEC 27000 Family of Security Standards

- **ISO/IEC 27000**
  - Family of IT security standards with several individual standards
  - From the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- **ISO/IEC 27002**
  - Originally called ISO/IEC 17799
  - Recommendations in 11 broad areas of security management

The ISO/IEC 27000 Family of Security Standards

- **ISO/IEC 27002: Eleven Broad Areas**

Security policy	Access control
Organization of information security	Information systems acquisition, development and maintenance
Asset management	Information security incident management
Human resources security	Business continuity management
Physical and environmental security	Compliance
Communications and operations management	

The ISO/IEC 27000 Family of Security Standards

- **ISO/IEC 27001**
  - Created in 2005, long after ISO/IEC 27002
  - Specifies certification by a third party
    - COSO and CobiT permit only self-certification
    - Business partners prefer third-party certification
- **Other 27000 Standards**
  - Many more 27000 standards documents are under preparation

1.2.D: Risk Analysis

- Asset Value (AV)
- X Exposure Factor (EF)
  - Percentage loss in asset value if a compromise occurs
- = Single Loss Expectancy (SLE)
  - Expected loss in case of a compromise

Single Loss Expectancy (SLE)

- SLE
- X Annualized Rate of Occurrence (ARO)
  - Annual probability of a compromise
- = Annualized Loss Expectancy (ALE)
  - Expected loss per year from this type of compromise

Annualized Loss Expectancy (ALE)

Classic Risk Analysis Calculation

	Base Case	Countermeasure A	
Asset Value (AV)	$100,000	$100,000	
Exposure Factor (EF)	80%	20%	
Single Loss Expectancy (SLE): = AV*EF	$80,000	$20,000	
Annualized Rate of Occurrence (ARO)	50%	50%	
Annualized Loss Expectancy (ALE): = SLE*ARO	$40,000	$10,000	
ALE Reduction for Countermeasure	NA	$30,000	
Annualized Countermeasure Cost	NA	$17,000	
Annualized Net Countermeasure Value	NA	$13,000	

Countermeasure A should reduce the exposure factor by 75%

Classic Risk Analysis Calculation

Counter measure B should cut the frequency of compromises in half

	Base Case	Countermeasure B	
Asset Value (AV)	$100,000	$100,000	
Exposure Factor (EF)	80%	80%	
Single Loss Expectancy (SLE): = AV*EF	$80,000	$80,000	
Annualized Rate of Occurrence (ARO)	50%	25%	
Annualized Loss Expectancy (ALE): = SLE*ARO	$40,000	$20,000	
ALE Reduction for Countermeasure	NA	$20,000	
Annualized Countermeasure Cost	NA	$4,000	
Annualized Net Countermeasure Value	NA	$16,000	

Classic Risk Analysis Calculation

	Base Case	Countermeasure A	Countermeasure B
Asset Value (AV)	$100,000	$100,000	$100,000
Exposure Factor (EF)	80%	20%	80%
Single Loss Expectancy (SLE): = AV*EF	$80,000	$20,000	$80,000
Annualized Rate of Occurrence (ARO)	50%	50%	25%
Annualized Loss Expectancy (ALE): = SLE*ARO	$40,000	$10,000	$20,000
ALE Reduction for Countermeasure	NA	$30,000	$20,000
Annualized Countermeasure Cost	NA	$17,000	$4,000
Annualized Net Countermeasure Value	NA	$13,000	$16,000

Problems with Classic Risk Analysis Calculations

- **Uneven Multiyear Cash Flows**
  - For both attack costs and defense costs
  - Must compute the return on investment (ROI) using discounted cash flows
  - Net present value (NPV) or internal rate of return (ROI)

Problems with Classic Risk Analysis Calculations

- **Total Cost of Incident (TCI)**
  - Exposure factor in classic risk analysis assumes that a percentage of the asset is lost
  - In most cases, damage does not come from asset loss
  - For instance, if personally identifiable information is stolen, the cost is enormous but the asset remains
  - Must compute the total cost of incident (TCI)
  - Include the cost of repairs, lawsuits, and many other factors

Problems with Classic Risk Analysis Calculations

- **Many-to-Many Relationships between Countermeasures and Resources**
  - Classic risk analysis assumes that one countermeasure protects one resource
  - Single countermeasures, such as a firewall, often protect many resources
  - Single resources, such as data on a server, are often protected by multiple countermeasures
  - Extending classic risk analysis is difficult

Problems with Classic Risk Analysis Calculations

- **Impossibility of Knowing the Annualized Rate of Occurrence**
  - There simply is no way to estimate this
  - This is the worst problem with classic risk analysis
  - As a consequence, firms often merely rate their resources by risk level

Problems with Classic Risk Analysis Calculations

- **Problems with "Hard-Headed Thinking"**
  - Security benefits are difficult to quantify
  - If only support "hard numbers" may underinvest in security

Problems with Classic Risk Analysis Calculations

- **Perspective**
  - Impossible to do perfectly
  - Must be done as well as possible
  - Identifies key considerations
  - Works if countermeasure value is very large or very negative
  - But never take classic risk analysis seriously

2-16: Responding to Risk

- **Risk Reduction**
  - The approach most people consider
  - Install countermeasures to reduce harm
  - Makes sense only if risk analysis justifies the countermeasure
- **Risk Acceptance**
  - If protecting against a loss would be too expensive, accept losses when they occur
  - Good for small, unlikely losses
  - Good for large but rare losses

2-16: Responding to Risk

- **Risk Transference**
  - Buy insurance against security-related losses
  - Especially good for rare but extremely damaging attacks
  - Does not mean a company can avoid working on IT security
  - If bad security, will not be insurable
  - With better security, will pay lower premiums

2-16: Responding to Risk

- **Risk Avoidance**
  - Not to take a risky action
  - Lose the benefits of the action
  - May cause anger against IT security
- Recap: Four Choices when You Face Risk
  - Risk reduction
  - Risk acceptance
  - Risk transference
  - Risk avoidance

Module 1.3: Business Continuity Process

- The basic principle of BCP is to protect people first
  - Evacuation plans and drills
  - Never allow staff members back into unsafe environments
  - Must have a systematic way to account for all employees and notify loved ones
  - Counseling afterwards

Principles of Business Continuity Management

- People have reduced capacity in decision making during a crisis
  - Planning and rehearsal are critical
- Avoid rigidity
  - Unexpected situations will arise
  - Communication will break down and information will be unreliable
  - Decision makers must have the flexibility to act

Principles of Business Continuity Management

- Communication
  - Try to compensate for inevitable breakdowns
  - Have a backup communication system
  - Communicate constantly to keep everybody "in the loop"

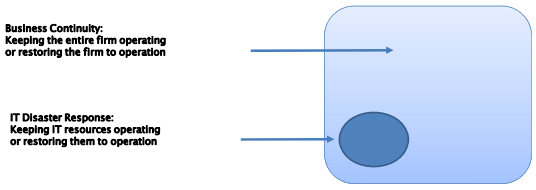
Business Process Analysis

- Identification of business processes and their interrelationships
- Prioritization of business processes
  - Downtime tolerance (in the extreme, mean time to belly-up)
  - Importance to the firm
  - Required by higher-importance processes
- Resource needs (must be shifted during crises)
  - Cannot restore all business processes immediately

Business Continuity Planning

- **Testing the Plan**
  - Difficult because of the scope of disasters
  - Difficult because of the number of people involved
- **Updating the Plan**
  - Must be updated frequently
  - Business conditions change and businesses reorganize constantly
  - People who must execute the plan also change jobs constantly
  - Telephone numbers and other contact information must be updated far more frequently than the plan as a whole
  - Should have a small permanent staff

Business Continuity versus Disaster Response



IT Disaster Recovery

- **IT Disaster Recovery**
  - IT disaster recovery looks specifically at the technical aspects of how a company can get its IT back into operation using backup facilities
  - A subset of business continuity or for disasters the only affect IT
  - All decisions are business decisions and should not be made by mere IT or IT security staffs

Types of Backup Facilities

- Hot sites
  - Ready to run (power, HVAC, computers): Just add data
  - Considerations: Rapid readiness at high cost
  - Must be careful to have the software at the hot site up-to-date in terms of configuration
- Cold sites
  - Building facilities, power, HVAC, communication to outside world only
  - No computer equipment
  - Less expensive but usually take too long to get operating
- Site sharing
  - Site sharing among a firm's sites (problem of equipment compatibility and data synchronization)
  - Continuous data protection needed to allow rapid recovery

IT Disaster Recovery

- **Office Computers**
  - Hold much of a corporation's data and analysis capability
  - Will need new computers if old computers are destroyed or unavailable
    - Will need new software
    - Well-synchronized data backup is critical
  - People will need a place to work

IT Disaster Recovery

- **Restoration of Data and Programs**
  - Restoration from backup tapes: Need backup tapes at the remote recovery site
  - May be impossible during a disaster
- **Testing the IT Disaster Recovery Plan**
  - Difficult and expensive
  - Necessary

AVAILABILITY

- Key components of effective disaster recovery and business continuity plans include:
  - Data backup procedures
  - Provisions for access to replacement infrastructure (equipment, facilities, phone lines, etc.)
  - Thorough documentation
  - Periodic testing
  - Adequate insurance

Module 3 – Protection of Information Assets

IT304 Internet and Network Security

04/21/2010

Agenda

- Information Assurance Career
  - IA job types & skill set
  - Scholarships
  - Certifications
  - IA Courses
- CISA exam six areas
  - Six areas
  - Topics in area 5
- Firewalls
- Virtual Private Networks
- Intrusion Detection

IA Job Types

- By contract type:
  - Full-time/In-House: typically recruited/promoted from within the company
  - Hired Guns: outside security contractors/consultants
- By position levels:
  - Security Engineers/Technicians: security in wired & wireless networks, firewall, intrusion detection & prevention, host security, (web) application security
  - Security Analysts: perform security audits and regulatory compliance checks
  - Security Architects: management-level position for designing and managing security infrastructure

IA Skill Set Requirements

- Hard Skills
  - Confidentiality:
    - working (but not necessarily expert) knowledge of encryption and cryptography, access control/authentication
    - → involves protecting the data from disclosure while stored or in transit
  - Integrity:
    - networking, hashing, public key infrastructure (PKI)
    - → ensures data stored or in transit cannot be corrupted or modified by unauthorized personnel without detection
  - Availability:
    - physical and network security, expert knowledge in Ethernet, Wifi, TCP/IP, FW/IDS/IPS, DDOS, etc
    - → requires not just technical know-how, but also physical construction and environment protections
  - Highly Marketable "Advanced skills":
    - expertise in penetration testing and code reviews, etc. Can really set the candidate apart
- Soft Skills
  - Communications skills, including technical writing and presentation skills, general management skills

Scholarships

- Department of Defense
  - DoD IA scholarship provides stipend and tuition
  - Will be required to serve a period of obligated service in DoD as a civilian employee or a member of one of the armed forces
- National Science Foundation
  - Federal Cyber Service: Scholarship for Service (SFS)
  - 2 years full scholarship
  - Will be required to work within the Federal Executive Branch at a Federal Agency, Independent Agency, Government Corporation, Commission, or Quasi-Official Agency, or at a National Laboratory
- Pace summer projects
  - Potential projects from Pace faculty

Industry certifications

- Information Systems Audit and Control Association, ISACA
  - Certified Information Security Auditor (CISA)
    - for professionals possessing information security audit and controls
  - Certified Information Security Manager (CISM)
    - for the individual who manages, designs, oversees and/or assesses an enterprise's information security
- The International Information Systems Security Certification Consortium, $(ISC)^2$
  - Certified Information Systems Security Professionals (CISSP)
    - for mid- and senior-level managers who are working toward or have already attained positions as Chief Information Security Officers or Senior Security Engineers

IA classes that you can take (for UG)

- CIT251 Computer Security Overview (originally IT300)
  - This course is usually offered in Fall
  - Wednesday 6:00-8:45PM
- CIT352 Network and Internet Security (originally IT304)
  - This course is usually offered in Spring
  - Wednesday 6:00-8:45PM
- CIT354 Computer Forensics (originally IT308)
  - This course is usually offered in Spring

MSIS or MSIT with a concentration on IA

- Introduction to Computer Security
- Information Security Management
- Web Security
- Network Security
- Security Forensics

Agenda

- Information Assurance Career
  - IA job types & skill set
  - Scholarships
  - Certifications
  - IA Courses
- CISA exam six areas
  - Six areas
  - Topics in area 5

CISA exam

- 200 multiple-choice questions that cover the six job practice areas
- The IS Audit Process (10%)
- IT Governance (15%)
- Systems and Infrastructure Life Cycle Management (16%)
- IT Service Delivery and Support (14%)
- Protection of Information Assets (31%)
- Business Continuity and Disaster Recovery (14%)

Importance of Information Security Management

- Key elements
- ISM Roles & responsibilities
- Inventory and classification of information assets
- System access permission
- Access control
- Privacy management and the role of IS auditor
- External parties and risks
- Addressing security when dealing with customers & 3rd party
- Human Resource Security
- Computer crimes & exposures
- Security incidence handling and responses

Logical Access

- Exposures
- Social engineering
- Logical access entry points
- Logical access control software
- Identification and authentication
- Authorization & access control lists
- Storing, retrieving, transporting and disposing of confidential information

Network Infrastructure Security

- LAN security
- Client-server security
- Wireless security
- Internet threat & security
  - IDS; firewalls/VPN
- Encryption
- Viruses
- Voice-over IP
- Private branch exchange

Auditing Information Security Management Framework

- Reviewing policies, procedures, and standards
- Logical access security policies
- Formal security awareness and training
- Data ownership; Documented authorization
- Terminate employee access; Security baseline
- Access standard
- Auditing logical access
- Testing tools & techniques

Auditing Network Infrastructure Security

- Auditing remote access
- Network penetration tests
- Full network assessment review
- Development and authorization of network changes
- Unauthorized changes
- Computer forensics

Environmental Exposures and Controls

- Environmental issues & exposures
  - Computer failure; power surge, etc
- Controls
- Fire suppression systems
- Location of computer rooms
- Emergency evacuation plan
- Power management

Physical Access Exposures and Controls

- Physical exposures
  - Blackmail; damage of equipments and documents
- Possible perpetrators
- Controls
- Auditing physical access

Mobile Computing

- WiFi security
  - Authentication; encryption; etc
- Laptop physical security

Firewall technology

IT304 Network and Internet security

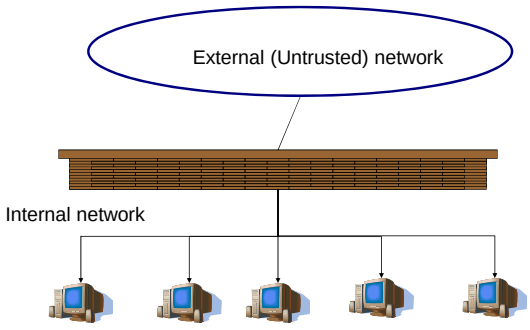
Li-Chiou Chen

03/12/2010

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN

Firewall as a chock point between two networks

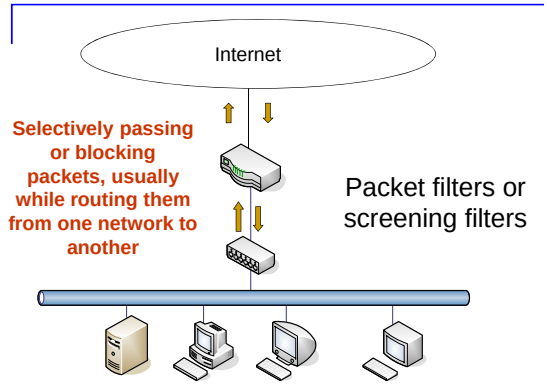


What is a firewall

- Firewall is a component that restrict traffic between external and internal networks
- Can be any device, software or arrangement or equipment that limits network access
- Sometimes it is bundled with other devices, such as routers, modems, and IP switches
  - Usually with limited functionality, such as packet filtering
- Some OS is bundled with simple software packet filters, such as Windows XP, Linux

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

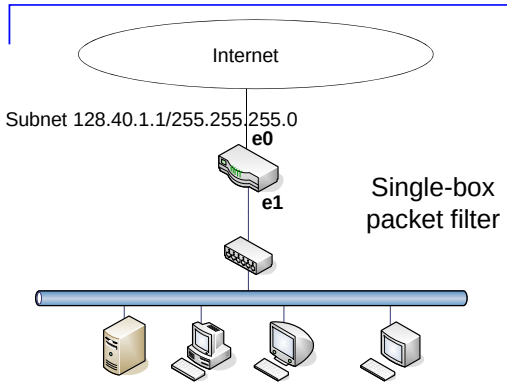


Data that a packet filter analyzes

- Device interface
  - The interface that the packet arrives on
  - The interface the packet will go out on
- Packet header
  - IP source & destination address
  - Protocol type
  - TCP/UDP source port and destination port
  - ICMP message type

Actions that a packet filter can take

- Block or send network traffic packet by packet
  - Accept the packet sent to its intended destination
  - Drop the packet without notifying the ender
  - Reject the packet with notification to the sender
- Log packet information
- Enforce security policy
  - Set off an alarm
  - Apply filtering rules
  - Send the packet to other server than its intended destination (e.g. or loaf balancing)
  - Modify a packet (e.g. NAT)



Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

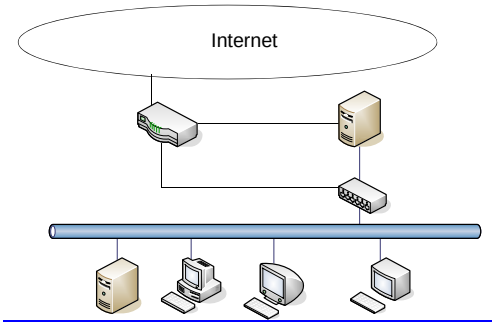
Stateful Inspection Firewalls

- State: whether the packet is part of an open connection.
- By default, permit connections openings from internal clients (on trusted network) to external servers (on untrusted network)
- By default, deny connection openings from the outside to inside servers
- These default behaviors can be changed with ACLs
- Accept future packets between hosts and ports in open connections with little or no more inspection

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Proxy server

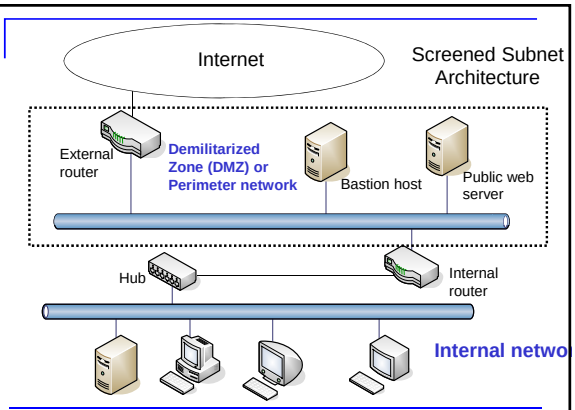


Proxy servers

- Specialized application or server programs that take users' requests for Internet services, such as telnet or http
- Proxy servers forward users' requests as appropriate according to the site's security policy
- Also known as "application-level gateway"

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall



Bastion host

- Main point of contact for incoming connections from external network
  - For FTP connections to the site's anonymous FTP server
  - For DNS queries about the hosts in the site
  - For SMTP sessions to deliver emails
- Outbound connections handled as one of the two methods
  - Through routers that allows direct internal to external connections
  - Through proxy server that runs on bastion host
- Must be highly secure because it is usually exposed to the Internet

Perimeter network

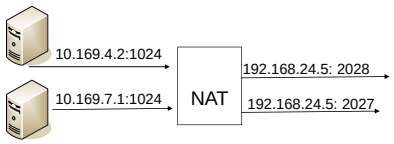
- A network added between an external network and an internal network in order to provide an additional layer of security
- Also called "demilitarized zone" (DMZ)
- No internal traffic is allowed
  - All traffic on the perimeter network should be to/from an external network or to/from bastion host

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Network Address Translation (NAT)

- Also called IP-masquerading
- Dynamically allocate external address and port for each connection initiated by an internal host
- Mainly used to multiplex numerous IP addresses over a few
- Enforces a firewall over outbound connections
- Helps to conceal internal network configuration



IPv4 Private IP Addresses

Name	IP address range	number of IPs	*classful* description	largest CIDR block
24-bit block	10.0.0.0 – 10.255.255.255	16,777,215	single class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65,535	256 continguous class Cs	192.168.0.0/16

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Keep the Rule Base Simple

- Keep list of rules as short as possible
  - About 30 and 50 rules
  - Shorter the rule base, faster the firewall will perform
- Firewalls process rules in a particular order
  - Usually rules are numbered starting at 1 and displayed in a grid
  - Most important rules should be at the top of the list
  - Make the last rule a cleanup rule
    - A catch-all type of rule

Restrict Subnets, Ports, and Protocols

- Filtering by IP addresses
  - You can identify traffic by IP address range
  - Most firewalls start blocking all traffic
    - You need to identify "trusted" networks
    - Firewall should allow traffic from trusted sources

Control Internet Services

- Web services
  - Employees always want to surf the Internet
- DNS
  - Resolves fully qualified domain names (FQDNs) to their corresponding IP addresses
  - DNS uses UDP port 53 for name resolution
  - DNS uses TCP port 53 for zone transfers
- E-mail
  - POP3 and IMAP4
  - SMTP
  - LDAP and HTTP

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Using VPNs with Firewalls

- VPNs do not reduce the need for a firewall
  - Always use a firewall as part of VPN security design
- Install VPN software on the firewall itself
  - Firewall allows outbound access to the Internet
  - Firewall prevents inbound access from the Internet
  - VPN service encrypts traffic to remote clients or networks

Install VPN software on the firewall itself

- Advantages
  - Control all network access security from one server
  - Fewer computers to manage
  - Use the same tools for VPN and firewall
- Disadvantages
  - Single point of failure
  - Must configure routes carefully
  - Internet access and VPN traffic compete for resources on the server

Set up VPN parallel to your firewall inside the DMZ

- Advantages
  - No need to modify firewall settings to support VPN traffic
  - Configuration scales more easily
  - Can deal with congested servers
- Disadvantages
  - VPN server is connected directly to the Internet
  - If VPN server becomes compromised, attacker will have direct access to your internal network
  - Cost of supporting a VPN increases with new servers

Set up VPN server behind the firewall connected to the internal network

- Advantages
  - VPN server is completely protected from the Internet
  - Firewall is the only device controlling access
  - VPN traffic restrictions are configured on VPN server
- Disadvantages
  - VPN traffic must travel through the firewall
  - Firewall must handle VPN traffic
  - Firewall might not know what to do with IP protocols other than ICMP, TCP, and UDP

PPTP Filters

- Might be only option when VPN connections pass through NAT
- PPTP uses two protocols
  - TCP
  - GRE

L2TP and IPSec Filters

- IKE uses protocol ID 171 and UDP on port 500
- ESP uses protocol ID 50
- AH uses protocol ID 51

Virtual Private Network

IT304 Internet and Network Security

Li-Chiou Chen

03/03/2010

Agenda

- VPN basics
  - Types of VPN
  - Encapsulation
  - Encryption in VPNs
  - Authentication in VPNs
  - Pros and Cons
- Configuration and Implementation
  - Design considerations
  - Configuration Options
  - Set up VPNs with firewalls
  - Guidelines for auditing VPNs and VPN policies
- Lab #7

What VPNs are

- A secure tunnel: enables computers to communicate securely over insecure channels such as the Internet
- Enables computers to exchange private encrypted messages that others cannot decipher
- Virtual network connection
- Extends an organization's network perimeter

Business incentives driving VPN adoption

- VPNs are cost-effective
- VPNs provide secure connection for remote users
  - Contractors
  - Traveling employees
  - Partners and suppliers
  - ……

VPN Components

- VPN server or host
  - Configured to accept connections from clients
- VPN client or guest
  - Endpoints connecting to a VPN
- Tunnel
  - Connection through which data is sent
- VPN protocols
  - Sets of standardized communication settings
  - Used to encrypt data sent along the VPN

Types of VPNs

- In terms of VPN implementation
  - Hardware VPN
  - Software VPN
- In terms of end points
  - End-point solutions
    - Site-to-site VPN
      - Gateway-to-gateway VPN
    - Client-to-site VPN
      - Remote access VPN
  - Infrastructure solution: MPLS VPN

Hardware-based VPNs

- Connect one gateway to another
- Routers at each network gateway encrypt and decrypt packets
- VPN appliance
  - Designed to serve as VPN endpoint
  - Join multiple LANs
- Benefits
  - Scalable
  - Better security

Software-based VPNs

- Integrated with firewalls
- Appropriate when participating networks use different routers and firewalls
- Benefits
  - More cost-effective
  - Offer maximum flexibility

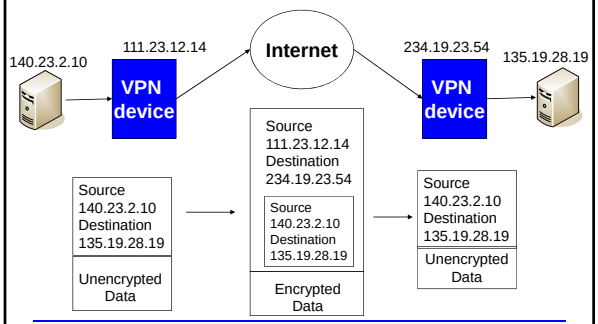
End point solutions

- Use tunneling protocols to encrypt and encapsulate IP packets
- Encrypted route through the Internet
  - Routes may be asymmetric as regular Internet routing
- Need VPN compliant routers
- Do not need to subscribe specific services from ISPs

Agenda

- VPN basics
  - Types of VPN
  - Encapsulation
  - Encryption in VPNs
  - Authentication in VPNs
  - Pros and Cons
- Configuration and Implementation
  - Design considerations
  - Configuration Options
  - Set up VPNs with firewalls
  - Guidelines for auditing VPNs and VPN policies
- Lab #7

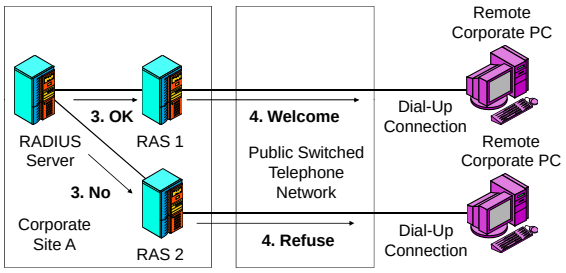
Encapsulation encloses a packet within another and assigns a different IP source and destination



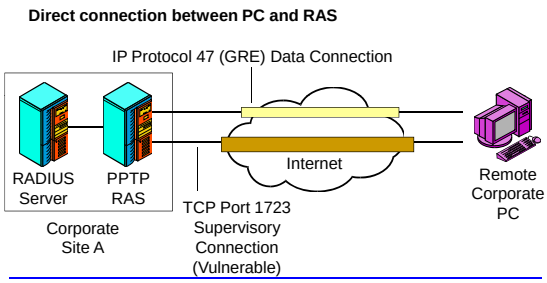
Tunneling protocols

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Both PPTP and L2TP operates at the data link layer

Point-to-Point Protocol (PPP) and RADIUS for Dial-Up Remote Access



Point-to-Point Tunneling Protocol (PPTP)



Point-to-Point Tunneling Protocol (PPTP)

- Encapsulates PPP data frames within IP packets for Internet
- Allow corporations that used PPP dialup systems to transform to VPN for remote access
- Header contains only information needed to route data from the VPN client to the server
- Uses Microsoft Point-to-Point Encryption (MPPE)
  - Encrypt data that passes between the remote computer and the remote access server

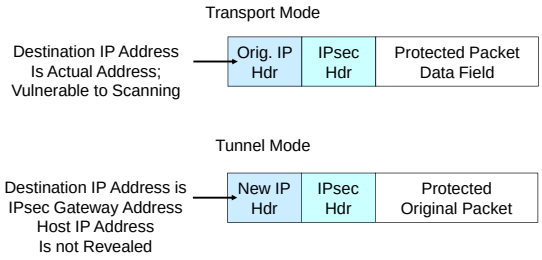
Layer 2 Tunneling Protocol (L2TP)

- Provides better security through IPSec
- IPSec encryption is more secure and widely supported
- IPSec enables L2TP to perform
  - Authentication
  - Encapsulation
  - Encryption

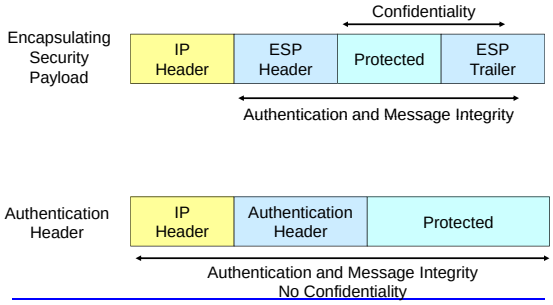
IPSec/IKE

- Internet Protocol Security (IPSec)
  - Set of standard procedures
  - Developed by the Internet Engineering Task Force (IETF)
  - Enables secure communications on the Internet
- Characteristics
  - Works at layer 3 (network layer, IP)
  - Can encrypt an entire TCP/IP packet
  - Originally developed for use with IPv6
  - Provides authentication of source and destination computers

IPsec Operation: Tunnel and Transport Modes



IPsec ESP and AH Protection



Authentication Header (AH)

- Provides authentication of TCP/IP packets
- Ensures data integrity
- Packets are signed with a digital signature
- Adds a header calculated by the values in the datagram
  - Creating a messages digest of the datagram
- AH in tunnel mode
  - Authenticates the entire original header
  - Places a new header at the front of the original packet
- AH in transport mode
  - Authenticates the payload and the header

Encapsulation Security Payload (ESP)

- Provides confidentiality for messages
- Encrypts different parts of a TCP/IP packet
- ESP in tunnel mode
  - Encrypts both the header and data part of each packet
  - Data cannot pass through a firewall using NAT
- ESP in transport mode
  - Encrypts only data portion of the packet
  - Data can pass through a firewall
- IPSec should be configured to work with transport mode

Other tunneling protocol listed in the textbook

- Considered as tunneling protocols (or VPN technology) from a pragmatic point of view
- Operate at the Application Layer. Do not provide encapsulation
- Secure Shell (SSH)
  - Provides authentication and encryption
  - Works with UNIX-based systems
    - Versions for Windows are also available
  - Uses public-key cryptography
- Socks V. 5
  - Provides proxy services for applications
    - That do not usually support proxying
  - Socks version 5 adds encrypted authentication and support for UDP

TLS (transport Layer Security)

- RFC 5246
- A session layer protocol (between application layer and transport layer)
- Largely used for Secure HTTP
- Build on TCP (not UDP)
- Ensure
  - Authentication of the server
  - Confidentiality of the communication
  - Integrity of the data

DTLS (Datagram TLS)

- RFC 4374, session layer protocol
- Similar to TLS but work on UDP
- Provide security for both UDP applications, such as IP phones and gaming programs
- Pace VPN client, CISCO AnyConnect uses DTLS

Intrusion Detection Systems

IT304 Internet and Network Security
Li-Chiou Chen
02/24/2010

Agenda

- Intrusion Detection Systems (IDS) basics
  - IDS components
  - Steps of intrusion detection
  - Options for implementing IDS
  - Evaluate different types of IDS products
- IDS configuration
  - Configure an IDS and develop filter rules
  - False alarms
  - Options for dealing with legitimate security alerts

What is an Intrusion Detection System (IDS)?

- A system that identifies intrusions by monitoring network traffic and/or host activities
- Intrusions
  - Misuse
  - Unauthorized use by authorized users
  - Unauthorized use by external advisories
- What the system is looking for
  - Malicious traffic
  - Unusual traffic, source, types
  - Unknown patterns
  - Reconnaissance activities
- Log and report the suspicious activity

Goals of IDS

- Detect a wide variety of intrusions
- Detect intrusions in a timely fashion
- Present the analysis in a simple and easy-to-understand format
- Be accurate: avoid false positives and false negatives

	Attack	No Attack
Detected	Attack detection	False positive
Not Detected	False negative	No attack

Intrusion Detection System Components

- Network sensors
- Alert systems
- Command console
- Response system
- Database of attack signatures or behaviors

Network Sensors

- Electronic "eyes" of an IDS
- Hardware or software that monitors traffic in your network and triggers alarms
- Sensors should be placed at common-entry points
  - Internet gateways
  - Connections between one LAN and another
  - Remote access server that receives dial-up connections from remote users
  - Virtual private network (VPN) devices
  - Sensors could be positioned at either side of the firewall
    - Behind the firewall is a more secure location
- Management program controls sensors

Alert Systems

- Trigger
  - Circumstances that cause an alert message to be sent
- Types of triggers
  - Detection of an anomaly
  - Detection of misuse

Command Console

- Provides a graphical front-end interface to an IDS
  - Enables administrators to receive and analyze alert messages and manage log files
- IDS can collect information from security devices throughout a network
- Command console should run on a computer dedicated solely to the IDS
  - To maximize the speed of response

Response System

- IDS can be setup to take some countermeasures
- Response systems do not substitute network administrators
  - Administrators can use their judgment to distinguish a false positive
  - Administrators can determine whether a response should be escalated
    - Increased to a higher level

Database of Attack Signatures or Behaviors

- IDSs don't have the capability to use judgment
  - Can make use of a source of information for comparing the traffic they monitor
- Misuse detection
  - References a database of known attack signatures
  - If traffic matches a signature, it sends an alert
  - Keep database updated
  - Passive detection mode
- Anomaly-based IDS
  - Store information about users in a database

Base-Rate Fallacy of Intrusion Detection Systems (IDS)

- IDS is useless unless accurate
  - Significant fraction of intrusions detected
  - False Alarms are suppressed significantly
- Suppose that an IDS can identify 99 intrusions out of 100 intrusions and generate one false alarm out of every 100 non-intrusions

	Attack	No Attack
Detected	Detection rate=99%	False positive rate = 1%
Not Detected	False negative rate =1%	True negative = 99%

An example: Base-Rate Fallacy of IDS

- IDS false positives and false negatives
  - An IDS can detect 99% of intrusions (false negative = 1%)
  - 1% of non-intrusions generate alarms (false positive = 1%)
- The IDS filters 100,000 events per hour
- When 10 in 100,000 events are really an intrusion; that is, 99990 in 100,000 are non-intrusions
- How many alarms that the systems will generate per hour?
  - The system will generate 999.90 false alarms in 99990 non-intrusion events (99990*1%)
  - The system will generate 9.9 real alarms in 10 intrusion events (10*99%)
  - The system will generate 999.9+9.9 = 1009.8 alarms
- What is the percentage of alarms that are real per hour?
  - only 9.9 in 1009.8 alarms are real, that is, ONLY about 1% of alarms are "real" (9.9/1009.8 ~ 1%)

Types of IDS

- Based on data
  - Network-based IDS
    - Monitors and inspects network traffic
  - Host-based IDS
    - Runs on a single host
- Based on detection techniques
  - Signature-based IDS
    - Uses pattern matching to identify known attacks
  - Anomaly-based IDS
    - Uses statistical, data mining or other techniques to distinguish normal from abnormal activities

Network-based IDS (NIDS)

- Can be a single monitor that looks for a specific network device
- Can locate at multiple machines across the network
- Advantages
  - Can monitor multiple machines from one location
  - Can test effectiveness of firewalls if it is configured properly
- Disadvantages
  - Cannot see through encrypted traffic or tunnels
  - Local view as monitored hosts
  - Require high performance to analyze fast links

Host-based IDS (HIDS)

- Centralized configuration
  - HIDS sends all data to a central location
  - Host's level of performance is unaffected by the IDS
  - Alert messages that are generated do not occur in real time
- Distributed configuration
  - Processing of events is distributed between host and console
  - Host generates and analyzes it in real time
  - Performance reduction in host

Advantages and disadvantages of HIDSs

- Advantages
  - Detect events on host systems
  - Can process encrypted traffic
  - Not affected by use of switched network protocols
  - Can compare records stored in audit logs
- Disadvantages
  - More management issues
  - Vulnerable to direct attacks and attacks against host
  - Susceptible to some denial-of-service attacks
  - Can use large amounts of disk space
  - Could cause increased performance overhead on host

Signature-based IDS

- Data available to the IDS
  - Packet header/data or log/audit trails
- Advantages
  - Widely available
  - Can be fairly fast
  - Easy to update and implement
  - Numerous commercial systems
- Disadvantages
  - Cannot detect attacks that have no known signatures
  - Must be updated for new attack or attack variants
  - Large rules base

Anomaly-based IDS

- Assumes that abnormal activities are intrusive
- Advantages
  - May be able to detect new attacks
- Disadvantages
  - What is the appropriate notion of normal?
  - Numerous research systems but few commercial systems
  - Can be computational intensive
  - Generally considered as high false positive
    - Think of a case with 0.001 false positives?

Hybrid IDS Implementations

- Hybrid IDS
  - Combines the features of HIDSs and NIDSs
    - Gains flexibility and increases security
- Combining IDS sensor locations
  - Put sensors on network segments and network hosts
  - Can report attacks aimed at particular segments or the entire network

Hybrid IDS Implementations (continued)

- Combining IDS detection methods
  - IDS combines anomaly and misuse detection
  - Database enables IDS to run immediately
  - Anomaly-based systems keep the alert system flexible
  - Can respond to the latest, previously unreported attacks
    - Both external and internal attacks
  - Administrators have more configuration and coordination work to do

Hybrid IDS Implementations (continued)

- Shim IDS
  - Acts like a type of NIDS
  - Involves sensors being distributed around a network
    - Data collected by sensors is sent to a central location
  - Sensors are installed in selected hosts and network segments
    - Those that require special protection

Hybrid IDS Implementations (continued)

- Distributed IDS
  - Multiple IDS devices are deployed on a network
  - Reduces response time
  - Two popular DIDSs
    - myNetWatchman
    - DShield

Hybrid IDS Implementations (continued)

- Advantages
  - Combine aspects of NIDS and HIDS configurations
  - Can monitor network as a whole
  - Can monitor attacks that reach individual hosts
- Disadvantages
  - Need to get disparate systems to work in coordinate fashion
  - Data gathered by multiple systems can be difficult to absorb and analyze

Evaluating Intrusion Detection Systems

- Survey various options and match them to your needs
- Review topology of your network identifying
  - Number of entry points
  - Use of firewalls
  - Number of network segments
- Evaluating IDSs can be time consuming

IDS Hardware Appliances

- Can handle more network traffic
  - Have better scalability than software IDSs
- Plug-and-play capabilities
  - One of its major advantages
  - Do not need to be configured to work with a particular OS
- You should create a custom configuration
  - To reduce the number of false positives and false negatives
- Upgrade appliances periodically
  - Can be complicated and expensive
- Examples
  - iForce, Intrusion SecureNet, StealthWatch G1

Agenda

- Intrusion Detection Systems (IDS) basics
  - IDS components
  - Steps of intrusion detection
  - Options for implementing IDS
  - Evaluate different types of IDS products
- IDS configuration
  - Configure an IDS and develop filter rules
  - False alarms
  - Options for dealing with legitimate security alerts
- Lab #5

Developing IDS Filter Rules

- IDS effectiveness depends on its database
  - Database should be complete and up to date
- IDS can have its own set of rules
  - You can edit it in response to scans and attacks
- IDS can be used proactively
  - Block attacks
  - Move from intrusion detection to intrusion prevention

Rule Actions

- IDS has a passive and reactive nature
- Configure IDS to take actions
  - Other than simply triggering alarms
  - Provides another layer of network defense
- IDSs include documentation for writing rules
- Customized rules can increase false positives during the learning process
  - Test your rules before using them in a real system

Rule Data

- Specify the action you want Snort to perform
- Specify the rest of the data that applies to the rule
  - Protocol
  - Source and destination IP addresses
  - Port number
  - Direction

Filtering Alerts

- To reduce false alarms adjust rules used by
  - Firewalls
  - Packet filters
  - IDSs
- Exclude specific signature from connecting to a selected IP address
  - Both internal and external addresses
  - Can even exclude an entire subnet or network

Dealing with Legitimate Security Alerts

- Determine whether the attack is a false alarm
  - Look for indications such as
    - You notice system crashes
    - New user accounts suddenly appear on the network
    - Sporadic user accounts suddenly have heavy activity
    - New files appear, often with strange file names
    - A series of unsuccessful logon attempts occurs
- Respond calmly and follow established procedures
- Call law enforcement personnel if necessary
  - To handle the intrusion

Assessing the Impact

- Was any host on your network compromised
- Determine the extend of the damage
- Determine the scope and impact of the problem
- Determine if the firewall was compromised
  - If firewall was compromised, computers on network could be accessed
  - Reconstruct firewall from scratch

Developing an Action Plan

- Action plan might involve the following steps:
  - Assess seriousness of the attack
  - Notify team leader immediately
  - Begin to document all actions
  - Contain the threat
  - Determine the extend of the damage
  - Make a complete bit-stream backup of the media
    - If you plan to prosecute
  - Eradicate the problem
  - Restore the system
  - Record a summary of the incident

Handling Internal Versus External Incidents

- Intrusions and security breaches often originate from inside an organization
- Your response needs to be more measured
- Avoid notifying the entire staff
- Human Resources and Legal departments should be made aware of the problem
- Notify the entire staff only when they need to know something serious happened

Taking Corrective Measures to Prevent Reoccurrences

- Take steps to prevent intrusions from recurring
- Set up intrusion rules that send alarms when the same intrusions are detected
- Notify others on the Internet about your attack

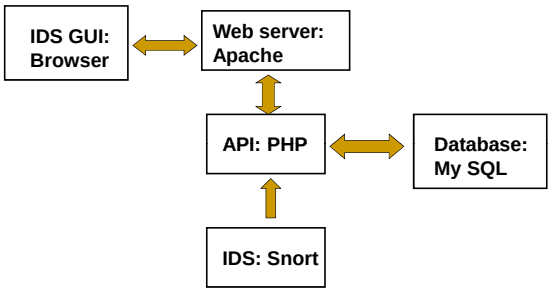
Gathering Data for Prosecution

- Rules to handle evidence
  - Make sure two people handle the data at all times
  - Write everything down
  - Lock it up!
- Chain of custody
  - Record of who handled an object to be used as evidence in court
  - Decide SIRT members that will handle the evidence
- Before an incident occurs, decide whether you will prosecute or not
  - Include this in your security policy

Steps for handling and examining hard disks and other computer data

- Secure the area
- Prepare the system
- Examine the system
- Shut down the system
- Secure the system
- Prepare the system for acquisition
- Examine the system
- Connect target media
- Secure evidence

BASE: a web GUI for Snort alerts



References

- Randy Weaver (2006). "Guide to Network Defense and Countermeasures," Second Edition, Thomson Course Technology. ISBN: 1418836796.
- William Stallings and Lawrie Brown (2008). "Computer Security: Principles and Practice," Prentice Hall. ISBN: 0106004245.
- Raymond R. Panko, Corporate Computer and Network Security, 2nd Edition, 2009, Pearson/Prentice Hall, ISBN: 0-13-185475-5.
- ISACA CISA Exam review Manual, ISACA