

MIS 5208 – Data Analytics for IT Auditors

Introduction & Course Overview

Week 1: Introductions, Course Outline, Reading, Tools and Other Administration Issues

Ed Ferrara, MSIA, CISSP

eferrara@forrester.com

Agenda

- Introductions
- Course Description
- Tools
 - Audit Control Language (ACL)
 - Splunk
 - Excel
- Schedule
 - Syllabus
 - Reading List
- Grades and Grading
 - Labs
 - Quizzes
 - Mid-term
 - Final exam
 - Class Participation Blog

Edward S. Ferrara



- Chief Information Security Officer, CSL Behring
 - Cybersecurity services
 - Cloud
 - Metrics
 - Enterprise cybersecurity information architecture
- CISSP #316968
- B.A. Franklin & Marshall College (Economics)
- M.A. University of Delaware (Educational Studies, Computer Science, Cognition)
- M.S. Norwich University (Cybersecurity)
- Twitter: @eferrara
- LinkedIn: [Ed Ferrara](#)

Introductions

- Who am I?
 - Share my interest in this topic with you and help you apply data analytics to IT auditing and cybersecurity
 - West Chester, Pennsylvania
 - I really like sailing
- Who are you?
 - **In your first blog** – please write a brief description of yourself.
 - Please tell us your goals and objectives for this class
 - Please tell us your goals and objectives for the program
 - Please tell us where you are from
 - Please tell us one thing you want us all to know about



Course Description

- MIS 5208 examines the use and power of data for both fraud detection but also for cybersecurity incident investigation
- You get what you measure.
- The course presents:
 - Basic data analysis concepts and then applies these techniques to cybersecurity and fraud detection problems.
- **Tools:**
- **Audit**
 - Audit Control Language (ACL)
 - Excel
- **Cybersecurity**
 - Bash Shell Commands
 - Splunk

Course Schedule

Course Schedule

Week	Meeting Date	Topic	Comments	WEBEX	Reading	Deliverables / Quizzes / Tests Due
1	Tuesday 01.12.2016	Introduction to the Course Introduction to Fraud and Forensic Investigations ACL Tool installation Demonstration	<p>V9.0 Desktop EDUC Non-Unicode (Windows Only). If you have a Mac or Linux machine you will need to run Windows in a VM to use this software.</p> <p>Temple students are entitled to one copy each of the following software:</p> <ul style="list-style-type: none"> Windows 8.1 Microsoft Office <p>See the following Temple Website: Microsoft Work At Home</p> <p>If you are not using Windows as your primary operating system (e.g. Mac or Linux) you will need to install a virtual windows machine in order to run windows. There is no version of VMware Player for OS X. VMware sells a Mac version of their product called VMware Fusion. You may use it as trial version 30 days for free. There is a free version of VMWare Player for Linux</p>	WEBEX		
2	Tuesday 01.19.2016	Fraud Detection and Prevention	Tools needed: ACL Quiz 1 Available Lab 1 Available	WEBEX	Coderre - 1, 2, 3 Appendix C ACL In Practice Tutorial - 1, 2	Lab 01: Frauds of Note
3	Tuesday 01.26.2016	Introduction to ACL -	Tools needed: ACL	NONE Please work on Lab and Quiz.	Coderre - 4, 5 ACL In Practice Tutorial - 3, 4	Quiz 1
4	Tuesday 02.02.2016	Fraud in Cyberspace	Special Guest Speaker: Mr. Mike Green, Head of IT Security, Risk, and Governance, Mars Inc. - Quiz 2 Available	WEBEX	None.	Lab - 02 - Using ACL to Examine Expense Patterns
5	Tuesday 02.09.2016	Overview of the Data and Working with Data	Tools needed: ACL	WEBEX	Coderre - 6, 7 ACL In Practice Tutorial - 5, 6	Quiz 2
6	Tuesday 02.16.2016	Analyzing Trends in the Data and Known Symptoms of Fraud	Tools needed: ACL / EXCEL	WEBEX	Coderre - 8, 9	Lab - 03 - Using ACL to Analyze Transactions
7	Tuesday 02.23.2016	Unknown Symptoms of Fraud, Automating the Detection Process, Verifying the Results	Tools needed: ACL / EXCEL Mid-Term Exam Available Install Splunk Community Enterprise or Community Edition to be ready for the next half of class over Spring Break.	WEBEX	Appendix A - Fraud Investigation Plans	MID-TERM EXAM

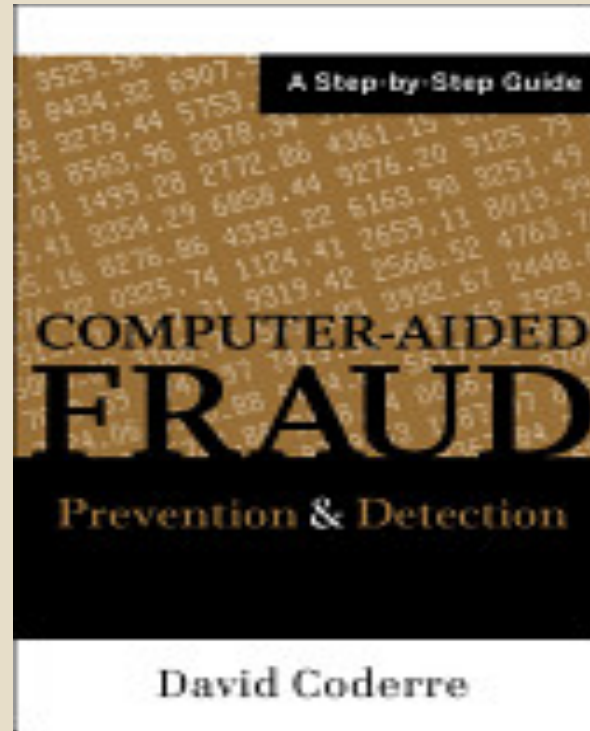
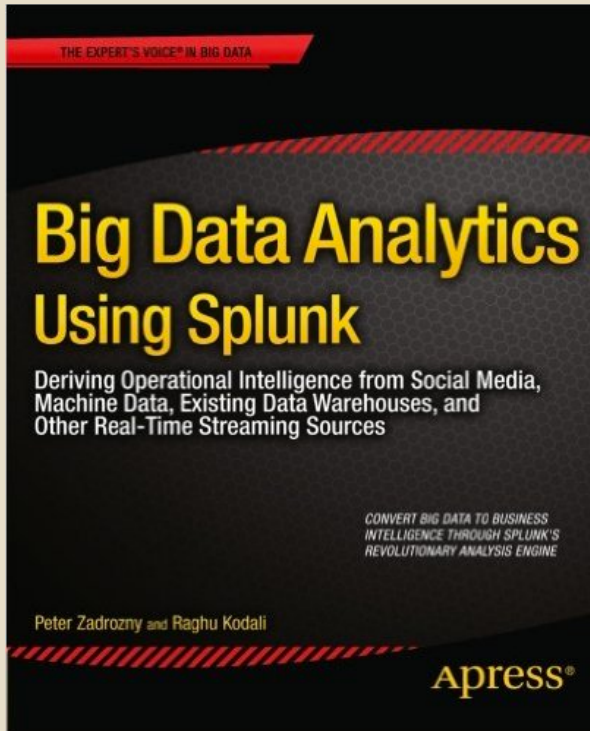
Course Schedule

SPRING BREAK (February 29 – March 6)					
8	Tuesday 03.08.2016	Introduction to Cybersecurity Investigations - The Kill Chain	Install Splunk Community Enterprise or Community Edition	WEBEX	
9	Tuesday 03.15.2016		Tools: Splunk	WEBEX	Zadrozni and Kodalli – 1, 2
10	Tuesday 03.22.2016		Tools: Splunk	WEBEX	Zadrozni and Kodalli – 3 Lab 04 – Getting Data into Splunk and Processing the Data Quiz 3
11	Tuesday 03.29.2016	Processing and Analyzing Data	Tools: Splunk	WEBEX	Zadrozni and Kodalli – 4
12	Tuesday 04.05.2016		Tools: Splunk	WEBEX	Zadrozni and Kodalli – 5 Quiz 4
13	Tuesday 04.12.2016	Defining Alerts	Tools: Splunk	WEBEX	Prepare for Final Exam Lab 05 – Visualizing the Results and Defining Alerts
14	Tuesday 04.19.2016			NONE.	FINAL EXAM

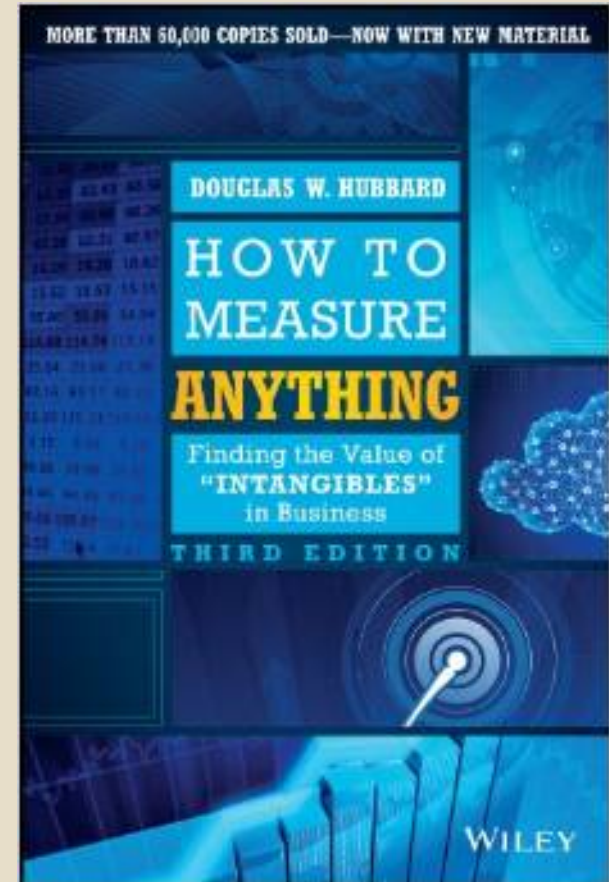
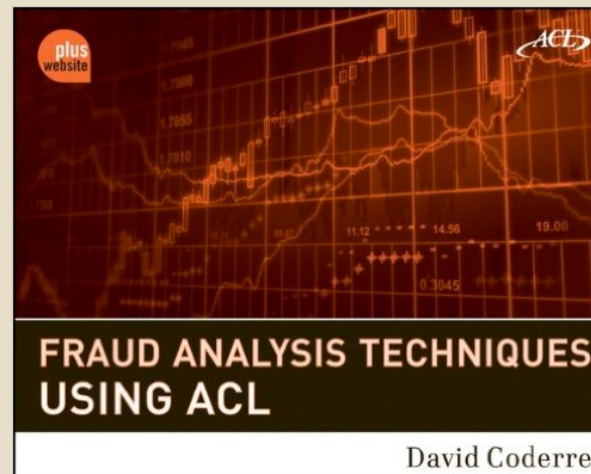
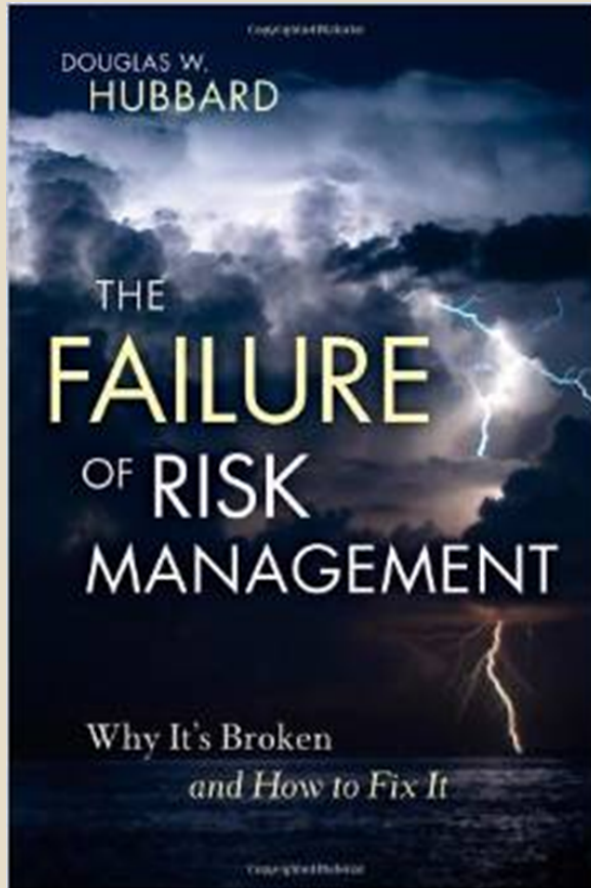
Mission and Learning Objectives

- Understand how to organize and analyze control data
- Understand the principles of transaction-oriented data, and how to store and retrieve data for data sources.
- Understand methods to identify ways in which perpetrators compromise data to affect fraud.
- Identify and compare sources and methods of capturing data throughout a business process.
- Use data mining techniques to identify associations and trends among data.
- Apply data mining techniques to examine control efficacy.
- Integrate data across multiple sources, transforming it into a single view.
- Understand and select appropriate data visualization techniques to effectively communicate the results of an analysis effort.
- Communicate analysis results to stakeholders for ongoing quality assurance and process improvement.

Required Texts



Optional Texts (Future Reading)



Presentations and Lab 01

- Later in the course you will be asked to present your lab findings on a selective basis – either individually or as a group
- Ideas and proposals in business are now typically communicated via “[decks](#)”. Often these decks are not even presented in the formal sense, they just get emailed to the recipient. You need to learn how to communicate your ideas using decks. This is an important skill. You can be the best analyst in the world but if you cannot get your ideas across...
- Writing skills are important but we tend to overemphasize correct grammar and form – not necessarily simple and direct communication – the essence of creating good decks.
- Each slide in your deck should be crafted just like you would craft a canvas of a painting!
- The Cognitive Style of PowerPoint by Edward Tufte (34 Pages)
- Presentation Skills Video: <https://www.youtube.com/watch?v=ayxfblOyUBY> (3:56)
- Presentation Skills Video: <https://www.youtube.com/watch?v=VVP8UGjECt4> (5:20)
- Presentation Skills Video: <https://www.youtube.com/watch?v=whTwjG4ZIJg> (7:18)

Thank you.