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
<table>
<thead>
<tr>
<th>Week</th>
<th>Meeting Date</th>
<th>Topic</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tuesday 01.12.2016</td>
<td>Introduction to the Course, Introduction to Fraud and Forensic Investigations, ACL Tool installation Demonstration</td>
<td>WEBEX</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tuesday 01.19.2016</td>
<td>Fraud Detection and Prevention</td>
<td>Coderre - 1, 2, 3 Appendix C, ACL In Practice Tutorial 1, 2, Quiz 1 Available, Lab 1 Available</td>
</tr>
<tr>
<td>3</td>
<td>Tuesday 01.26.2016</td>
<td>Introduction to ACL</td>
<td>Coderre - 4, 5 Quiz 1, ACL In Practice Tutorial 3, 4, None.</td>
</tr>
<tr>
<td>4</td>
<td>Tuesday 02.02.2016</td>
<td>Fraud in Cyberspace</td>
<td>Lab 01: Frauds of Note</td>
</tr>
<tr>
<td>5</td>
<td>Tuesday 02.09.2016</td>
<td>Overview of the Data and Working with Data</td>
<td>Lab 02 - Using ACL to Examine Expense Patterns</td>
</tr>
<tr>
<td>6</td>
<td>Tuesday 02.16.2016</td>
<td>Analyzing Trends in the Data and Known Symptoms of Fraud</td>
<td>Quiz 2</td>
</tr>
<tr>
<td>7</td>
<td>Tuesday 02.23.2016</td>
<td>Unknown Symptoms of Fraud, Automating the Detection Process, Verifying the Results</td>
<td>Appendix A - Fraud Investigation Plans, MID-TERM EXAM</td>
</tr>
</tbody>
</table>

**WEBEX**

- **WEBEX**
- **WEBEX**
- **WEBEX**
- **WEBEX**
- **WEBEX**
- **WEBEX**
- **WEBEX**

**Reading**

- Microsoft Work At Home
- Temple Website: Microsoft Work At Home

**Deliverables / Quizzes / Tests Due**

- Install Splunk Community Enterprise or Community Edition to be ready for the next half of class over Spring Break.

**ACL Tool installation Demonstration**

- 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. Temple students are entitled to one copy of the following software:
  - Windows 8.1
  - Microsoft Office

- See the following Temple Website: Microsoft Work At Home
- 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. VM ware 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.
## Course Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Tools</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>03.08.2021</td>
<td>Introduction to Cybersecurity Investigations</td>
<td>Install Splunk Community Enterprise or Community Edition</td>
<td>WEBEX</td>
<td>Zadrozni and Kodalli – 1, 2</td>
</tr>
<tr>
<td>9</td>
<td>03.15.2021</td>
<td>The Kill Chain</td>
<td>Tools: Splunk</td>
<td>WEBEX</td>
<td>Lab 04 – Getting Data into Splunk and Processing the Data Quiz 3</td>
</tr>
<tr>
<td>10</td>
<td>03.22.2021</td>
<td>Getting Data Into Splunk</td>
<td>Tools: Splunk</td>
<td>WEBEX</td>
<td>Zadrozni and Kodalli – 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab 04 – Getting Data</td>
<td>Tools: Splunk</td>
<td>Zadrozni and Kodalli – 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>into Splunk and Processing the Data Quiz 3</td>
<td>Tools: Splunk</td>
<td>Quiz 3</td>
<td>Quiz 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quiz 4</td>
<td>Tools: Splunk</td>
<td>Quiz 4</td>
<td>Quiz 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quiz 5</td>
<td>Tools: Splunk</td>
<td>Quiz 5</td>
<td>Quiz 6</td>
</tr>
<tr>
<td>12</td>
<td>04.05.2021</td>
<td>Visualizing The Results</td>
<td>Tools: Splunk</td>
<td>WEBEX</td>
<td>Quiz 6</td>
</tr>
<tr>
<td>13</td>
<td>04.12.2021</td>
<td>Defining Alerts</td>
<td>Tools: Splunk</td>
<td>WEBEX</td>
<td>Quiz 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab 05 – Visualizing the Results and Defining Alerts</td>
<td>Tools: Splunk</td>
<td>Prepare for Final Exam</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>04.19.2021</td>
<td>Final Exam</td>
<td>Tools: Splunk</td>
<td>Final Exam</td>
<td></td>
</tr>
</tbody>
</table>
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

Big Data Analytics Using Splunk
Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources

Peter Zadrozny and Raghu Kodali

Computer-Aided Fraud Prevention & Detection

David Coderre
Optional Texts (Future Reading)

- The Failure of Risk Management: Why It's Broken and How to Fix It
  - By Douglas W. Hubbard
- Fraud Analysis Techniques Using ACL
  - By David Coderre
- How to Measure Anything: Finding the Value of "Intangibles" in Business
  - Third Edition
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.