# CIS 3368  Data Security & Governance

**Course Description:** This upper division course is for students majoring in Data Analytics. Students will gain an understanding of how analytics can be applied to a variety of security-related problems across organizations. In addition, students will explore various ethical, legal, and data governance issues that affect data analysts. (3 hr. lecture; 1 hr. lab)

<table>
<thead>
<tr>
<th>Course Competency</th>
<th>Learning Outcomes</th>
</tr>
</thead>
</table>
| **Competency 1:** Students will demonstrate an understanding of the R language for performing exploratory data analysis by: | • Critical thinking  
• Information Literacy  
• Cultural / Global Perspective  
• Social Responsibility  
• Ethical Issues  
• Computer / Technology Usage |
| 1. Performing installation of RStudio, and other important packages such as ggplot2 and dplyr for data preprocessing and manipulation.  
2. Managing the quality and integrity of the data;  
3. Visually inspecting for anomalies, strengths of relationships, or other aspects of the data for the purpose of understanding security and governance.  
4. Being able to communicate to non-analysts the story or the lack of story uncovered in the data.  
5. Formulating a research questions that serves as pivot points for decision or action | |
| **Competency 2:** The student will be able to understand the VERIS framework and how data analysts can use it to create visualizations, discover trends, and learn from data breaches by: | • Critical thinking  
• Information Literacy  
• Cultural / Global Perspective  
• Social Responsibility  
• Ethical Issues  
• Computer / Technology Usage |
| | |
1. Tracking the source of the incident, the incident itself and describe it.
2. Tackling conflation by separating the who from the event and what was affected.
3. Using VERIS to support and inform security decisions.
4. Understanding the threat actions and performing interpretation and classification.
5. Understanding the role of attributes and assets, as well as concepts such as confidentiality, integrity, and availability.
6. Understanding VERIS framework and its implementation in different sections such as discovery/response, impact and victim.

**Competency 3:** The student will demonstrate an understanding of machine learning techniques applications for information security by:

- Critical thinking
- Social Responsibility
- Ethical Issues
- Computer / Technology Usage

1. Using the R language for creating maps of security threats.
2. Using R language to create linear regression models to predict and understand the factors that affect infections.
3. Using the R language to create machine learning algorithms for classifying threats.

**Competency 4:** The student will understand how organizations should move toward a data-driven security program by:

- Critical thinking
- Information Literacy
- Cultural / Global Perspective
- Social Responsibility
- Ethical Issues
- Computer / Technology Usage

1. Understanding and updating the classic term Hacker in the context of security data science.
2. Learning the importance of combining coding and statistics skills to discover new ways to detect anomalous behavior in network data.
3. Understanding the different challenges that data scientists can find when making organizations data driven.
4. Learning how to work with others on gathering data and asking good questions.
5. Understanding the role and functioning of a real-life security data science team

**Competency 5:** The student will demonstrate an understanding of law and ethics in information security by:

- Critical thinking
- Information Literacy
- Cultural / Global Perspective
- Social Responsibility
- Ethical Issues
- Computer / Technology Usage

1. Learning to apply ethical and legal frameworks to initiatives in the data profession.
2. Investigating applied data methods for ethical and legal work in analytics.
3. Exploring practical approaches to data analytics problems posed by work in big data and data science.

**Competency 6:** The student will demonstrate knowledge of information governance key concepts and principles by:

- Critical thinking
- Information Literacy
- Cultural / Global Perspective
- Social Responsibility
- Ethical Issues
- Computer / Technology Usage

1. Defining information security governance.
2. Understanding how to improve data quality across an organization.
3. Learning how to improve data understanding and collaboration across organizations.
4. Understanding the role of machine learning in automating monitoring for non-compliance.
5. Learning the comprehensive power of metadata management and deriving valuables business insights.
6. Understanding the integration of data analytics and quality into comprehensive data governance solutions

Updated Spring 2021