Assurance of Student Learning Report
2023-2024

Gordon Ford College of Business	*Department of Analytics and Information Systems*
Cybersecurity Data Analytics Certificate (1754)	
Dr. Mark Ciampa	
Is this an online program? X Yes □ No	Please make sure the Program Learning Outcomes listed match those in CourseLeaf . Indicate verification here □ Yes, they match! (If they don't match, explain on this page under **Assessment Cycle)**

***** Please include Curriculum Map as part of this document (at the end), NOT as a separate file.**

Use this page to list learning outcomes, measurements, and summarize results for your program. Detailed information must be completed in the subsequent pages. Add more Outcomes as needed.			
Program Student Learning Outcome 1: Students will understand the fundamentals of cybersecurity from a data analytics perspective.			
Instrument 1	**Project**		
Instrument 2			
Instrument 3			
Based on your results, check whether the program met the goal Student Learning Outcome 1.		□ **Met**	□ **Not Met**
Program Student Learning Outcome 2: Students will understand the applicable policies, laws, and regulations in cybersecurity.			
Instrument 1	**Project**		
Instrument 2			
Instrument 3			
Based on your results, check whether the program met the goal Student Learning Outcome 2.		□ **Met**	□ **Not Met**
Program Student Learning Outcome 3: Students will be able to perform vulnerability management activities and analyze output from common vulnerability tools.			
Instrument 1	**Capstone course artifact**		
Instrument 2			
Instrument 3			
Based on your results, check whether the program met the goal Student Learning Outcome 3.		□ **Met**	□ **Not Met**
Assessment Cycle Plan:			
Student data will be collected and assessed during the 2024-2025 Academic Year.			

Program Student Learning Outcome 1			
Program Student Learning Outcome	**Identify the fundamentals of cybersecurity from a data analytics perspective**		
Measurement Instrument 1	(Direct) Students will examine in detail data that has been generated from applying data analytics and artificial intelligence (AI) to cybersecurity. They will then make conclusions regarding the viability of the results and determine how (and if) it can be applied to cybersecurity defenses.		
Criteria for Student Success	The overall score on the activity must equal or exceed 70%		
Program Success Target for this Measurement	70% of students will achieve Capable or Advanced level	**Percent of Program Achieving Target**	
Methods			
Based on your results, highlight whether the program met the goal Student Learning Outcome 1.	□ **Met**	□ **Not Met**	
Results, Conclusion, and Plans for Next Assessment Cycle (Describe what worked, what didn't, and plan going forward)			
Results: **Conclusions**: ****IMPORTANT - Plans for Next Assessment Cycle**: Student data will be collected and assessed during the 2024-2025 Academic Year.			

Program Student Learning Outcome 2	
Program Student Learning Outcome	Apply policies, laws, and regulations in cybersecurity.
Measurement Instrument 1	(Direct) Students will review in detail the 16 WKU Information Technology policies and generate a report based on the review of the policies
Criteria for Student Success	The overall score on the activity must equal or exceed 70%.

Program Success Target for this Measurement	70% of students will achieve Capable or Advanced level	**Percent of Program Achieving Target**	
Methods			
Based on your results, circle or highlight whether the program met the goal Student Learning Outcome 2.		□ **Met**	□ **Not Met**
Results, Conclusion, and Plans for Next Assessment Cycle (Describe what worked, what didn't, and plan going forward)			
Results: **Conclusions**: **Plans for Next Assessment Cycle**: Student data will be collected and assessed during the 2024-2025 Academic Year.			

Program Student Learning Outcome 3			
Program Student Learning Outcome	Demonstrate the ability to perform vulnerability management activities.		
Measurement Instrument 1	(Direct) Students will use cybersecurity data to create a data analytics model and then apply that model to the data. They will make conclusions regarding the results to determine the predictive nature of a future cybersecurity incident.		
Criteria for Student Success	The overall score on the activity must equal or exceed 70%.		
Program Success Target for this Measurement	70% of students will achieve Capable or Advanced level	**Percent of Program Achieving Target**	
Methods			
Methods			
Based on your results, circle or highlight whether the program met the goal Student Learning Outcome 3.		□ **Met**	□ **Not Met**
Results, Conclusion, and Plans for Next Assessment Cycle (Describe what worked, what didn't, and plan going forward)			
Results: **Conclusions**: **Plans for Next Assessment Cycle**: Student data will be collected and assessed during the 2024-2025 Academic Year.			

SLO 1 Rubric

Program Student Learning Outcome 1 – Identify the fundamentals of cybersecurity from a data analytics perspective.

Measurement Instrument 1 - (Direct) Students will examine in detail data that has been generated from the application of data analytics and artificial intelligence (AI) to cybersecurity. They will then make conclusions regarding the viability of the results and determine how (and if) it can be applied to cybersecurity defenses.

Criteria for Student Success - 70% of students will achieve Capable or Advanced level.

Activity	Weight	Developing	Capable	Advanced
Analyze the paper *Predicting Cyber-Attacks Using Publicly Available Data*.	25%	Analysis is incomplete and does not explain the paper's aim, research design, or limitations.	Analysis is complete and explains the problem the paper is focusing on and describes data used and data sources.	Review reflects depth of analysis and reveals insights into the research by describing the types of attacks being researched and research design.
The file *Cisco Large Scale Brute Force Activity* is data accumulated from a recent large-scale brute force activity targeting services with commonly used login credentials (courtesy Cisco). Explain how you could use this data using a Naïve Bayes Classifier for predicting a brute force cyberattack.	25%	Unable to explain how data could be used or determine what additional data would be needed.	Describes how data could be used in predicting an attack and what additional data is needed to combine with it for a Naïve Bayes Classifier analysis.	Provides an in-depth description of how the data can be used and clearly articulates additional data sources necessary along with alternative classifiers.

Evaluate an analysis of different cybersecurity data (see below). Analyze each of these four attack types and explain for each type which could be a reliable predictor (and why) and which could not be a reliable predictor (and why not).	25%	Incorrectly or incompletely identifies attack types as unreliable predictors.	Correctly designates all attack types as reliable predictors and explains why they are reliable.	Analyzes why the attack types could be used as reliable predictors based on F-measure within the context of cybersecurity attacks.
Write a memo to your CISO explaining why AI can be used to predict attacks. Include what you have learned from analyzing the paper *Predicting Cyber-Attacks Using Publicly Available Data.*	25%	Memo lacks depth explaining why AI can be used and does not include information from analysis of paper.	Memo gives strong reasons why AI can be used in predicting attacks and leverages analysis of paper to bolster reasoning.	Memo explains in depth why AI can be used and gives in-depth analysis of paper.

Attack Type	**Precision**	**Recall**	**F-Measure**	**ROC Area**
Attack on Internet-facing Web Server	0.63	0.74	0.68	0.72
Malware	0.82	0.93	0.88	0.78
Malicious Email	0.71	0.98	0.82	0.76
Distributed Denial of Service (DDoS)	0.84	1.00	0.91	0.91

SLO 2 Rubric

Program Student Learning Outcome 2 – Apply policies, laws, and regulations in cybersecurity.

Measurement Instrument 1 - (Direct) Students will review in detail the 16 WKU Information Technology policies and generate a report based on the review of the policies.

Criteria for Student Success - 70% of students will achieve Capable or Advanced level.

Activity	Weight	Developing	Capable	Advanced
Analyze the 16 WKU Information Technology policies and assess each as to whether it follows the CAI model and discuss each of the areas as related to WKU policies.	25%	Analysis is incomplete and does not analyze the policies in regard to CAI.	Analysis is complete and answers all appropriate questions while defining C (Confidentiality) I (Integrity), and A (Availability).	Analysis reflects depth and reveals insights into the areas related to WKU policies.
Assess how the WKU IT policies are organized. Determine if they use plain language to make the policies clear and understandable. Evaluate if the policy supports the WKU mission and goals.	25%	Assessment is limited and does not analyze their organization, language, or support of WKU mission and goals.	Assessment is sufficient in describing the organization, language, and support.	Description is in depth regarding organization, language, and support.
Evaluate each of the WKU IT individual policies to determine their consistency with policy document components.	25%	Incomplete evaluation or missing evaluation of document components or their consistency or inconsistency.	Assessment determines whether consistency or inconsistency with policy document components is complete while covering Version control, Introduction, Policy heading, Policy goals and objectives, and Policy statements.	Provides advanced description and analysis of document components including Policy exceptions, Policy enforcement

				clause, Administrative notations, and Policy definitions.
Analyze WKU IT policies to determine if they include specific topics related to policy examples and discuss each area that need improvement.	25%	Unable to analyze policies or incomplete analysis.	Provides accurate analysis and discussion of areas of improvement.	Gives in-depth analysis and discussion.

SLO 3 Rubric

Program Student Learning Outcome 3 – Demonstrate the ability to perform vulnerability management activities.

Measurement Instrument 1 - (Direct) Students will use cybersecurity data to create a data analytics model and then apply that model to the data. They will make conclusions regarding the results to determine the predictive nature of a future cybersecurity incident.

Criteria for Student Success - 70% of students will achieve Capable or Advanced level.

Activity	**Weight**	**Developing**	**Capable**	**Advanced**
Using the enclosed cybersecurity data set create a model to analyze the data.	50%	Unable to complete a workable model for analysis.	The model is complete and appropriate for analysis.	The model depth of analysis and reveals insights into the model creation.
Create a video that discusses the model created, its strengths and weaknesses, and how it can be applied to cybersecurity data analytics.	50%	Description is shallow with limited insight into how it can be applied.	Description is sufficient in describing the model and its application.	Description is in depth regarding the choice and construction of the model and its application.

CURRICULUM MAP TEMPLATE

Program name:	Cybersecurity Data Analytics
Department:	Analytics and Information Systems
College:	Gordon Ford College of Business
Contact person:	Dr. Mark Ciampa
Email:	mark.ciampa@wku.edu

KEY:

I = Introduced

R = Reinforced/Developed

M = Mastered

A = Assessed

			Learning Outcomes		
			LO1:	**LO2:**	**LO3:**
			Identify the fundamenals of cybersecurity from a data analytics perspective	Apply policies, laws, and regulations in cybersecurity	Demonstrate the ability to perform vulnerability management activities
Course Subject	**Number**	**Course Title**			
CYSA	520	Principles of Cybersecurity for Data Analytics	I	I	
	522	Cybersecurity Risk and Compliance	R	M/A	
	524	Cybersecurity Orchestration Using Data Analytics	M/A	R	
BDAN	513	Contemporary Business Analytics			I
CYSA	599	Cybersecurity Data Anlytics Portfolio			