COASTLINE
COLLEGE

CIS Computer Information Systems
CST Computer Service Technology

Advisory Board Meeting Minutes 05/17/19

Department Chairs

Professor Michael Warner
Professor Tobi West, CISSP, GCFE

The purpose of the meeting is to gain feedback from industry, government, and academic professionals working in the areas of computer networking, cybersecurity, data analytics, programming, and other related professions.

Attendees:

- Aaron Voelcker - Dean of Institutional Effectiveness, Rancho Santiago CC
- Aeron Zentner - Dean of Research and Institutional Effectiveness, Coastline
- Adrian Lucero - Asst. Principal, La Quinta High School
- Brandon Brown - Full-time faculty, Coastline
- Christine Kirkpatrick - San Diego Supercomputer Center, UC San Diego
- Dante Bui - CyberPatriot Teacher, Early College High School
- David Martinez - Principal, Early College High School
- Dwight Osborne - Cisco/Computer Networking Teacher - Valencia HS
- Gora Datta - IEEE
- Mohammad Husain - Tenured Computer Science Professor, Cal Poly Pomona
- Rebecca Barber - Arizona State University
- Ron Pike - Tenured Computer Info Systems Professor, Cal Poly Pomona
- Terry Ginsburg - CA State

Meeting minutes:

- Covered an overview of the CIS and CST programs
    - CAE Re-designation
    - NSF Grant - Cyber Up! Digital Forensics & Incident Response
    - NSF Grant - GenCyber 07/15/19-07/19/19
    - K-12 Pathways
    - Military/distance learning
- Covered the advisory board responsibilities
- Reviewed current curriculum

START HERE
IDENTIFY your assets
PROTECT your assets
DETECT incidents
RESPOND with a plan
RECOVER normal operations
THE 5-STEP APPROACH

- ★ Computer Networking: Cisco
- ★ Computer Networking: Microsoft
- ★ Cybersecurity

- Reviewed pending curriculum
  - ★ Data Analytics
  - ★ Intro to Programming
- Reviewed proposed curriculum & supporting frameworks
  - ★ Digital Forensics and Incident Response
    - CyberSeek
    - SANS GIAC
    - NICE Cybersecurity Workforce Framework
- Discussion questions and program recommendations
  - ★ Overall recommendations
    - Move forward with all curriculum and programs outlined, including AS in Digital Forensics and Incident Response, and Data Analytics programs
    - Create a multi-purpose room where cyber and data analytics students can work on projects and research to build hands-on skills
    - Create a student Security Operations Center (multi-purpose room)
    - Develop programs in Artificial Intelligence and Blockchain technologies
    - Develop a program in audit & forensics for cloud
    - Develop course that addresses cybersecurity for various industries to help non-IT/non-cyber employees
    - Develop a program in Homeland Security / Cybersecurity
    - Develop a course for cybersecurity awareness (non-credit)
    - Need to better balance out the suggested schedule for Data Analytics courses
  - ★ Christine
    - Data carpentry
    - Add elective: cyber at scale
    - Modeling for 100GB flows
    - Add elective: Data Analytics / Cyber mashup
    - Will tell people about our programs to help market/promote
    - Employers need qualified people for data analytics
    - Not a lot of openings for less than Bachelor's degrees
    - In the 90's they didn't have computing courses
    - Help high school diploma people get the data analytics jobs by continuing to develop out the data analytics program at Coastline
    - Encourage students to create portfolios of their work to show employers
    - Helping employers to restructure work strains, distinguish ethics and privacy in course work
  - ★ Adrian
    - Students already have too much on the high school level, need to move the basic computing down to the lower levels, before high school.

  - Good opportunity for data analytics, how can we fit Data Analytics into the HS schedule?
  - Students take Net+ and Sec+ after AP Comp Sci Principles
- Aeron
  - There is a great need for data analytics professionals, not so much for the Data Science side
  - Develop a course in data visualizations, perhaps an elective on the DA program
  - Create an apprenticeship for Data Analytics to go with CCAP
  - CIS - Data Analysts - cross-over to Business Intelligence
- Ron
  - Challenges are that organizations have a range of needs but they don’t know how to fill it, so they start with the most highly qualified person
- Brandon
  - Across all organizations and fields they are looking to massage data, manipulate data
- Rebecca
  - The public is not ready to see AI & machine learning within data analytics
  - Organizations need innovative thinking, business intelligence, and data analytics
  - Employers need employees to have some tech skills, yet more analytical
- Gora
  - Look at the course names, how can we show more
  - Make them generic like cybersecurity
  - Use naming conventions on the courses
- Mohammad
  - Add SIEM tools to the DFIR program
  - Create a student Security Operations Center (multi-purpose room)
- Dwight
  - Computer Science AP class is now lab science and math class according to LQHS
  - Not enough room for Data Analytics at the HS level because they already have a lot with forensics, computer networking, and others
  - Too many students are using Google docs and can’t save a file, can’t keyboard, can’t find a file

COASTLINE
COLLEGE

CIS Computer Information Systems
CST Computer Services Technology

Degrees and Certificates

Advisory Board Meeting 05/17/19

Computer Information Systems (CIS)			
Pending – Fall 2019			
Certificate of Achievement	Data Analytics	20 units	MATH C160 Introduction to Statistics PSYC Introduction to Research Methods in Psychology CST C157 SQL Database Development *OR* CIS C240 SQL Database Development CIS C250 Data Analytics 1 – Introduction to Data Analytics CIS C260 Data Analytics 2 – Systems Analysis and Design CIS C270 Data Analytics 3 – Applied Predictive Analytics
Certificate of Accomplishment	Introduction to Programming	12 units	CIS C111 Introduction to Information Systems & Programming CIS C155 Introduction to Programming Using Java CIS C156 Web Development with JavaScript and Cloud Services CIS C157 Introduction to Python Programming

Computer Service Technology (CST)

Active

Associate in Science	**Computer Networking: Cisco**	**60 units**	**CST C116 A+ Essentials Hardware** **CST C128 Network+** **CST C177 Configuring Microsoft Windows 8** **CST C191 Linux+** **CST C201C CCNA 1: Introduction to Networks** **CST C202C CCNA 2: Routing and Switching Essentials** **CST C203C CCNA 3: Scaling Networks** **CST C204C CCNA 4: Connecting Networks** **CST C230 Introduction to Security**
Certificate of Achievement	Computer Networking: Cisco	27 units	CST C116 A+ Essentials Hardware CST C128 Network+ CST C177 Configuring Microsoft Windows 8 CST C191 Linux+ CST C201C CCNA 1: Introduction to Networks CST C202C CCNA 2: Routing and Switching Essentials CST C203C CCNA 3: Scaling Networks CST C204C CCNA 4: Connecting Networks CST C230 Introduction to Security
Certificate of Accomplishment	Cisco Certified Networking Administrator (CCNA)	12 units	CST C201C CCNA 1: Introduction to Networks CST C202C CCNA 2: Routing and Switching Essentials CST C203C CCNA 3: Scaling Networks CST C204C CCNA 4: Connecting Networks

Certificate of Specialization	Cisco Certified Networking Professional (CCNP)	9 units	CST C205 CCNP: Implementing Cisco IP Routing CST C207 Building Multilayer Switched Networks/CCNP 3 CST C208 CCNP: Troubleshooting and Maintaining Cisco IP Networks
Associate in Science	**Cybersecurity**	**60 units**	***Required:*** **CST C128 Network+** **CST C230 Introduction to Security** **CST C158 Server+** **CIS C157 Introduction to Python Programming** ***Choose 3 electives:*** **CST C191 Linux+** **CST C231 CompTIA Advanced Security Practitioner** **CST C232 Ethical Hacking** **CST C242 PenTest+** **CST C245 Computer Forensics** **CST C253 Cisco ASA, PIX, and Network Security** **CST C255 Cybersecurity Analyst+** **CST C258 Linux Networking & Security** **CST C260 CISSP**

Certificate of Achievement	Computer Networking: Cybersecurity	27 units	*Required:* CST C116 A+ Essentials Hardware CST C128 Network+ CST C177 Configuring Microsoft Windows 8 CST C191 Linux+ CST C201C CCNA 1: Introduction to Networks CST C230 Introduction to Security *Choose 3 electives:* CST C231 CompTIA Advanced Security Practitioner CST C232 Ethical Hacking CST C245 Computer Forensics CST C248 Wireless Networking CST C253 Cisco ASA, PIX, and Network Security CST C260 CISSP
Certificate of Accomplishment	Cybersecurity Fundamentals	12 units	CST C128 Network+ CST C230 Introduction to Security CST C158 Server+ CIS C157 Introduction to Python Programming
Certificate of Accomplishment	CompTIA	15 units	CST C116 A+ Essentials Hardware CST C117 A+ Essentials Software CST C128 Network+ CST C191 Linux+ CST C230 Introduction to Security
Certificate of Accomplishment	Penetration Testing	12 units	CST C230 Introduction to Security CST C191 Linux+ CST C232 Ethical Hacking CST C242 PenTest+

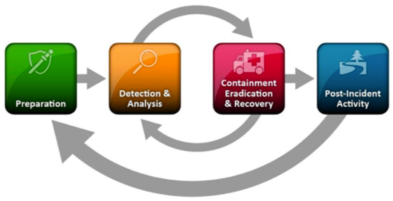
Certificate of Accomplishment	IT Foundation	12 units	CST C104 IT Fundamentals CST C116 A+ Essentials Hardware CST C117 A+ Essentials Software CST C128 Network+
Associate in Science	**Computer Networking: Microsoft**	**60 units**	***Required:*** **CST C116 A+ Essentials Hardware** **CST C128 Network+** **CST C177 Configuring Microsoft Windows 8** **CST C191 Linux+** **CST C201C CCNA 1: Introduction to Networks** **CST C230 Introduction to Security** ***Choose 3 electives:*** **CST C172 SQL Server Design and Implementation** **CST C173 MCTS – Microsoft Exchange Server – Configuration** **CST C184 Microsoft Server 2008 Active Directory Configuration** **CST C185 Microsoft Server 2008 Network Infrastructure** **CST C186 Microsoft Server 2008 Applications Infrastructure Config** **CST C222 Installing/Configuring Windows Server 2012** **CST C223 Administering Windows Server 2012** **CST C224 Configuring Advanced Windows Server 2012 Services**

Certificate of Achievement	Computer Networking: Microsoft	27 units	*Required:* CST C116 A+ Essentials Hardware CST C128 Network+ CST C177 Configuring Microsoft Windows 8 CST C191 Linux+ CST C201C CCNA 1: Introduction to Networks CST C230 Introduction to Security *Choose 3 electives:* CST C172 SQL Server Design and Implementation CST C173 MCTS – Microsoft Exchange Server – Configuration CST C184 Microsoft Server 2008 Active Directory Configuration CST C185 Microsoft Server 2008 Network Infrastructure CST C186 Microsoft Server 2008 Applications Infrastructure Config CST C222 Installing/Configuring Windows Server 2012 CST C223 Administering Windows Server 2012 CST C224 Configuring Advanced Windows Server 2012 Services
Certificate of Accomplishment	Windows Server 2008	12 units	CST C177 Configuring Microsoft Windows 8 CST C184 Microsoft Server 2008 Active Directory Configuration CST C185 Microsoft Server 2008 Network Infrastructure CST C186 Microsoft Server 2008 Applications Infrastructure Config
Certificate of Specialization	MCSA: Windows Server 2012	9 units	CST C222 Installing/Configuring Windows Server 2012 CST C223 Administering Windows Server 2012 CST C224 Configuring Advanced Windows Server 2012 Services
Certificate of Specialization	MCSA: Windows 8	6 units	CST C177 Configuring Microsoft Windows 8 CST C178 Managing and Maintaining Windows 8

Computer Service Technology (CST)			
Pending for Fall 2019/Spring 2020			
Certificate of Accomplishment	Cybersecurity and Computer Networking	15 units	*Required:* CST C128 Network+ CST C230 Introduction to Security *Choose 3 electives:* CST C231 CompTIA Advanced Security Practitioner CST C232 Ethical Hacking CST C242 PenTest+ CST C245 Computer Forensics CST C248 Wireless Networking CST C253 Cisco ASA, PIX, and Network Security CST C255 Cybersecurity Analyst+ CST C258 Linux Networking & Security CST C260 CISSP

Certificate of Achievement	Cybersecurity	21 units	*Required:* CST C128 Network+ CST C230 Introduction to Security CST C158 Server+ CIS C157 Introduction to Python Programming *Choose 3 electives:* CST C191 Linux+ CST C231 CompTIA Advanced Security Practitioner CST C232 Ethical Hacking CST C242 PenTest+ CST C245 Computer Forensics CST C248 Wireless Networking CST C253 Cisco ASA, PIX, and Network Security CST C255 Cybersecurity Analyst+ CST C258 Linux Networking & Security CST C260 CISSP
Certificate of Achievement	Cybersecurity Apprenticeship Program	24 units	CST C128 Network+ CST C230 Introduction to Security CST C158 Server+ CIS C157 Introduction to Python Programming CST C191 Linux+ *CST C232 Ethical Hacking (change to* CST C242 PenTest+) CST C245 Computer Forensics CST C255 Cybersecurity Analyst+
Certificate of Specialization	MCSA: Windows Server 2012	9 units	CST C222 Installing/Configuring Windows Server 2012 CST C223 Administering Windows Server 2012 CST C224 Configuring Advanced Windows Server 2012 Services

COASTLINE COLLEGE



Cyber Up! DFIR

Course & Program Catalog Descriptions

Course Title	Course Description
Intro to Digital Forensics	Students will explore an introduction to digital forensics using open source applications. Topics covered include chain of custody, forensic acquisition of data, forensic evidence reporting, expert witness testimony, timeline analysis, and anti-forensic techniques. Hands-on assignments will be used to develop introductory technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.
Intro to Incident Response	Students will explore an introduction to laws relevant to cybercrime and the roles of the Cyber Security Incident Response Team (CSIRT). Topics covered include incident response case studies, incident response tools used in industry, advanced persistent threats, documentation and technical reporting, timeline analysis, case management, and hunting, gathering, and foraging for cyber threats. Hands-on assignments will be used to help students develop introductory technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.
Cybercrime and CSIRT Coordination	Students will explore an introduction to cyber incident response using industry-recognized tools. Topics covered include international, federal, and state laws relevant to cybercrime, an overview of the U.S. court system and jurisdictions, CSIRT coordination within the team and with stakeholders internal to the organization, ethics pertaining to cyber professionals, project management, technical writing, countermeasures, and compliance. This course is intended for students with an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.
Intermediate Digital Forensics	Students will explore digital forensic techniques using industry-recognized tools. Topics covered include an introduction to network forensics and mobile device forensics, investigative and extraction tools, live acquisition data, evidence reporting, time-stomping and anti-forensic techniques, and the significance of time zones for forensic case analysis. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.
Intermediate Incident Response / PenTest+	Students will explore incident response techniques using industry-recognized tools. Topics covered include planning and scoping a cyber incident, information gathering for vulnerability assessment, network exploitation and summarization reporting, report writing and best practices, obfuscation techniques, forensic artifacts, social media forensics, memory forensics, ethics and compliance issues. Hands-on assignments will be used to develop technical skills relevant to entry-level cybersecurity professionals. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.
Advanced DFIR Capstone	Students will explore advanced digital forensics and incident response techniques using industry-recognized tools. Hands-on projects will be used to demonstrate technical skills relevant to entry-level cybersecurity professionals. Students will analyze a mock case and report findings through technical documents and presentation. This course is intended for students with computer experience and an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated.

Description requirements:

- Include the main competencies students will have achieved that are required for a specific occupation.
- At a minimum, clearly indicate the specific occupation(s) or field(s) the program will prepare students to enter the basic occupational competencies students will acquire.

Program Title	Catalog Description
Certificate of Achievement in Digital Forensics and Incident Response	The Certificate of Achievement in Digital Forensics and Incident Response will provide students with a solid foundation in the field of cybersecurity with specialization in cyber defense techniques. The program is designed to prepare students for entry-level cyber jobs, or to help them advance into mid-level cyber careers, such as cybercrime analyst, cyber incident analyst, cyber incident responder, digital forensic examiner, digital forensic technician, and vulnerability tester. Topics covered include planning and scoping a cyber incident, domestic and international cyber laws, ethics, chain of custody, incident detection and analysis, anti-forensic techniques, timeline analysis, incident containment, eradication, recovery, report preparation, and expert testimony. The program includes hands-on and technical writing assignments to help students develop their skills for the cybersecurity workforce. **18 units** (6 courses listed above) Upon completion of the program, students will be able to: • Given a lab scenario, demonstrate the appropriate use of tools to identify security gaps and develop a response plan. • Given a mock case, analyze and organize digital evidence to produce a report of findings using appropriate, industry-recognized terminology. • Apply diverse viewpoints to ethical dilemmas in the cybersecurity field and recommend appropriate actions.
Associate of Science in Digital Forensics and Incident Response	The Associate of Science in Digital Forensics and Incident Response will provide students with a solid foundation in the field of cybersecurity with specialization in cyber defense techniques The program is designed to prepare students for entry-level cyber jobs, or to help them advance into mid-level cyber careers, such as cybercrime analyst, cyber incident analyst, cyber incident responder, digital forensic examiner, digital forensic technician, and vulnerability tester. Topics covered include planning and scoping a cyber incident, domestic and international cyber laws, ethics, chain of custody, incident detection and analysis, anti-forensic techniques, timeline analysis, incident containment, eradication, recovery, report preparation, and expert testimony. The program includes hands-on and technical writing assignments to help students develop their skills for the cybersecurity workforce. **60 units** (6 courses listed above plus 42 units of general education) Upon completion of the program, students will be able to: • Given a lab scenario, demonstrate the appropriate use of tools to identify security gaps and develop a response plan. • Given a mock case, analyze and organize digital evidence to produce a report of findings using appropriate, industry-recognized terminology. • Apply diverse viewpoints to ethical dilemmas in the cybersecurity field and recommend appropriate actions.

COASTLINE COLLEGE

DFIR Program Course List

Seq	Course Title	Skills/Modules	Student Learning Outcomes
1	Intro to Digital Forensics	● Chain of Custody with regard to digital evidence ● Forensic Data Acquisitions (live memory dump & dead box) ● Evidence Collection - Windows artifacts ● Windows Registry and OS file systems ● Windows-based tools (EnCase, FTK, Autopsy, & other tools) ● Reporting ● Expert Testimony ● Forensic Specializations ● Digital forensics process and procedures ● Steganography ● Intro to timeline analysis/significance of time zone & time stamps ● Intro to anti-forensics ● Legal authority; scope of collection ● Intro to forensics; mobile, cloud, etc. ● Hash values ● Intro to encryption	a. Identify and collect digital evidence in an organized manner for reporting. b. Demonstrate an understanding of chain of custody with regard to digital forensics. c. Recognize the various professional specializations of cybersecurity, incident response, and digital forensics.
2	Intro to Incident Response	● Incident Response process and procedures ● Threat hunting security posture ● IR case studies ● IR case review (hands-on exercises) ● APTs ● Hunting, gathering, and foraging ● Tools ● Documentation/reporting ● Intro to timeline analysis (eg using plaso) ● Case management ● Intro to incident response	a. Identify common resolutions to basic cybersecurity incidents. b. Given an incident response case study, analyze to identify attack patterns based on the kill chain process. c. Demonstrate an understanding of the incident response process.

*red text denotes 04/19/19 advisory board suggestions; *blue text denotes 05/14/19 Ginsburg suggestions

3	Cybercrime and CSIRT Coordination	● Federal and State Laws ● US Court system / jurisdictions (federal, state, local & civil vs. criminal) ● Relevance to collection & identification of evidence ● IR team collaboration (relevance of evidence, collection, collaboration, preparing for court) ● Define CSIRT roles ● Review case studies related to issues of integrity to understand ethical behaviors ● Project management ● Technical writing (procedural tasks, active/passive voice, avoiding negative writing, creating an index) ● IR Team dynamics and interactions with external stakeholders ● International laws: GDPR, Russian laws, Privacy laws, CCPA ● Countermeasures ● Compliance	a. Demonstrate an understanding of the typical roles and interactions of a Cyber Security Incident Response Team (CSIRT). b. Apply diverse viewpoints to ethical dilemmas in the cybersecurity field and recommend appropriate actions. c. Develop a technical report using appropriate, industry-recognized terminology.
Seq	**Course Title**	**Skills/Modules**	**Student Learning Outcomes**
4	Intermediate Digital Forensics	● Investigative/extraction tools (Linux-based tools; SIFT workstation) ● Comprehensive mock case (Windows evidence) ● Live data acquisition ● Mobile device forensics (assignment) ● Network forensics (assignments) ● Evidence report development (full report) ● Mock testimony (webex / video recording) ● Anti-forensics/red team artifacts ● Time-stomping ● Significance of time zones for analysis ● Checklist for entry-level analysts ● Memory forensics ● Tools: Wireshark; packet analysis ● Mac/Apple forensics	a. Evaluate a collection of digital evidence to distinguish and extract relevant items. b. Given a mock case, use a forensic framework or methodology to analyze and reconstruct the electronic events of the scene. c. Given a mock case, produce a report to describe evidence and present findings.

*red text denotes 04/19/19 advisory board suggestions; *blue text denotes 05/14/19 Ginsburg suggestions

5	Intermediate Incident Response / PenTest+	● Explain the importance of planning and scoping ● Gather info to prepare for exploitation then perform a vulnerability scan and analyze results ● Exploit network and summarize results ● Conduct information gathering exercises with various tools ● Utilize report writing and handling best practices ● Obfuscation techniques ● Forensic artifacts from red team activity ● Social media forensics ● Memory forensics ● Payment Systems (POS usually based on Android tablet) ● Ethics and compliance ● Civil/divorce/family law cases ● Independent security researcher (Twitter, social media) ● Tools: Cobalt Strike, Metasploit; SIFT workstation ● Pivot point ● Time anchor ● Linux forensics	a. Given a lab scenario, plan and scope an assessment. b. Demonstrate the use of appropriate tools and techniques to perform vulnerability scanning and penetration testing. c. Analyze penetration test results to provide practical recommendations for management.
6	Advanced DFIR Capstone	● Project management and team coordination ● Capstone team project (industry project like ITC at CPP or like SANS bootcamp exercise) ● Individual presentations ● Individual report of findings ● Field trip to RCFL or local industry partners ● Timeline analysis ● Case management tools ● Red team artifacts ● Case studies such as Casey Anthony ● Sandboxing/reverse-engineering ● Gathering indicators of compromise	a. Given a lab scenario, demonstrate the appropriate use of tools to identify security gaps and develop a response plan. b. Given a mock case, analyze and organize digital evidence to produce a report of findings using appropriate, industry-recognized terminology. c. Understand the qualifications and certifications of the incident response career path. d. Understand the qualifications and certifications of the digital forensics career path.
	Electives to consider	1. ICS/SCADA 2. Mobile device forensics; IoT forensics	

*red text denotes 04/19/19 advisory board suggestions; *blue text denotes 05/14/19 Ginsburg suggestions

Coastline College: Certificate of Achievement in Data Analytics

Program Start: Fall 2019
Units: 20
Courses: 6
Program Length: 1 year (Fall, Spring, Summer)
Course Format: Online
Course Term Length: 8 weeks and 16 weeks
Associated Occupations: Business Analytics Specialist, Data Analyst, Data Visualization Developer, Operations Research Analyst, and Market Research Analyst
Median Salary: $77,485

Course Sequence:

Fall (16 weeks) (11 Units)

- MATH C160 - Introduction to Statistics
- PSYC C280 - Introduction to Research Methods in Psychology
- CIS C240 - SQL Database Development

Spring (16 weeks) (6 Units)

- CIS C250 Data Analytics 1 - Introduction to Data Analytics
- CIS C260 Data Analytics 2 - Systems Analysis & Design

Summer (8 weeks) (3 Unit Capstone)

- CIS C270 Data Analytics 3 - Applied Predictive Analytics

Courses:

MATH C160 - Introduction to Statistics (4 Units)
Catalog Description: Topics covered include collecting of data, sampling, probability, hypothesis testing, analyzing of variance, correlation and regression, nonparametric testing, and correlating for application in the natural sciences, social sciences, business, and management. Use of statistical technology will be introduced.

PSYC C280 - Introduction to Research Methods in Psychology (4 Units)
Catalog Description: This course introduces to students psychological research methods and critical analysis techniques that may be applied to diverse research studies and issues.

CIS C240 - SQL Database Development (3 Units)
Catalog Description: Students will explore an introduction to relational database fundamentals and SQL programming skills in the Microsoft environment. Topics covered include relational database architecture, database design techniques, data retrieval, data integrity, and simple and complex query skills. This course is intended for students new to the SQL programming language. Careers and emerging trends in the field will be evaluated.

CIS C250 Data Analytics 1 - Introduction to Data Analytics (3 Units)
Catalog Description: Students will explore the topics of data analytic thinking and its applicability to the business world. The practical application of business intelligence and data analysis will be experienced in hands-on projects. The process of business decision-making will be applied with an emphasis on data mining. Careers and emerging trends in the field will be evaluated.

CIS C260 Data Analytics 2 - Systems Analysis & Design (3 Units)
Catalog Description: Students will explore the topics of systems analysis and design and its applicability to the business world. The practical application of systems analysis and design will be experienced in hands-on projects. The process of business decision-making will be applied with an emphasis on the systems development life cycle. Careers and emerging trends in the field will be evaluated.

CIS C270 Data Analytics 3 - Applied Predictive Analytics (3 Units)
Catalog Description: Students will gain a fundamental understanding of the art and science of predictive analytics as it relates to improving organizational performance. The course will cover the key concepts necessary to extract stored data elements, understand what they mean from a business perspective, and transform their formats and derive new relationships among them to produce a dataset suitable for analytical modeling. After successful completion of the course, students will be able to use these skills to produce fully processed datasets that are compatible for building predictive models that can be deployed to increase organizational effectiveness.

COASTLINE COLLEGE

Field Test: Certificate of Achievement in Data Analytics

During the fall 2018 term Coastline College conducted a field test survey using a random selection of professionals and faculty in the field of data science and data analytics from private industry and universities. A survey was distributed electronically via LinkedIn to approximately 50 professionals that held titles directly related to the data analytics field. There was a 60% response rate to the survey.

Prior to taking the survey, participants were asked to review the proposed framework for the Certificate of Achievement in Data Analytics, which was a link to a PDF stored on a Coastline College Google Drive. After reviewing the proposal, participants were asked to specify their level of agreement to a series of statements related to the framework. Table 1 provides a summary of the findings.

Table 1 *Field Test Results*

Framework Assessment	Total	Strongly Agree	Agree	Disagree	Strongly Disagree
There is industry demand for entry-level data analytics-related positions.	30	63.3%	33.3%	3.3%	0.0%
There is a need for data analytics career development for working professionals.	30	63.3%	36.7%	0.0%	0.0%
The proposed program supports career development for individuals seeking to enter the data analytics field.	29	37.9%	62.1%	0.0%	0.0%
The course sequence provides a clear pathway leading to entry-level positions in the data analytics field.	30	40.0%	50.0%	10.0%	0.0%
12 months is a reasonable time for program completion.	30	46.7%	30.0%	20.0%	3.3%
The course descriptions are relevant to entry-level positions in the data analytics field.	29	31.0%	58.6%	10.3%	0.0%

The majority of all participants felt that that there was an emerging demand for entry-level positions and career development in the field of data analytics. Additionally, over 90% percent of respondents agreed that the proposed framework provides a clear and relevant pathway into the field of data analytics. While overall, the field study affirmed the program as an opportunity to meet job and skill market demand, only 77% indicated that 12-monthes was a reasonable timeframe. While this response was the lowest outcome on the assessment, it was not below a threshold which would be a cause for concern.

Finally, 57% of respondents indicated that they would be interested to participate on a program advisory board.