

# ECONOMIC CRIME FORENSICS, M.S.

## Program Description

The goal of this program is to prepare students to enter the field of economic crime in careers such as internal and external fraud auditors, criminal and economic crime investigators, litigation support analysts and anti-money laundering investigators. The program prepares individuals to detect, deter, and investigate instances of economic crime, misconduct, and abuse.

The M.S. in ECF incorporates key components from La Salle's graduate programs in Computer Information Science and Master of Business Administration. The program adds additional theory in areas of criminal justice, litigation preparation, and corporate ethics. The program also provides an additional path for technology managers interested in pursuing a leadership career by integrating financial compliance with corporate business goals. Students complete a capstone experience which integrates theory and practice through either an industry specific research project or a program-related experiential position.

The program is offered in an online format and follows the traditional academic calendar of a fall and spring semester and a shorter summer semester. The fall and spring semesters are divided into two 8 week terms. A full-time graduate student carries a minimum of 6 semester credit hours. Some courses may require more hours per week in some areas of instruction. All courses are online and 3 credits in length. The courses will meet both synchronously (optional) and asynchronously. Students are required to participate in chat sessions and/or discussion boards, which will take the place of classroom meetings. Synchronous sessions will be recorded for students who are not able to attend the actual session. Students who are not able to attend the synchronous sessions will be asked to complete a short assignment related to the recorded session. Depending on their personal schedules, students may elect to take courses every term or wait for the next term to continue studies. Courses in the summer are also 8 weeks in length. If a student decides to take two courses during the summer session, they will overlap in the time frame.

The M.S. in ECF focuses on a set of theoretical core competencies which include the following:

- Economic crime definition, analysis, and prevention;
- Legal and corporate compliance and ethical issues;
- Economic risk analysis and mitigation; and
- Investigative practices, principles, and prosecution.

## Mission

The M.S. in Economic Crime Forensics augments students' background, to acquire both practical and theoretical knowledge in their chosen field, and to enhance their professional competence. Students who earn a M.S. in Economic Crime Forensics will be prepared to advance in their professional careers while completing a graduate degree.

## Program Specific Information

### Progression through the Program

Ten courses (30 credits) are required for the degree. Each student is required to satisfy all six required courses (which includes the capstone), and a grouping of 4 additional courses.

## Degree or Certificate Earned

Master of Science (M.S.)

## Required for Program Completion

- Courses
  - 10
- Credits
  - 30
- GPA
  - 3.0

## Program Goals

- Prepare students to participate ethically and professionally in a global market.
- Prepare students to enter the field of economic crime prevention and detection and investigation.
- Prepare students to apply standards and best practices of forensics and litigation support.
- Prepare students to be corporate leaders in fraud prevention and deterrence.
- Prepare students to participate ethically and professionally in a global market.

## Student Learning Outcomes

1. Propose business law standards, standards of ethics, and professional codes of conduct related to corporate leadership.
2. Evaluate and support accounting and auditing concepts related to the causation of corporate economic crime.
3. Develop standards of conduct relative to litigation services, including conflicts of interest and background considerations.
4. Develop managerial and communication skills to measure and support fraud deterrence.

Students are required to complete a specialization by selecting 4 courses from either group. If a student does not wish to consider a specialization, they may select any four courses from the groupings.

*All students complete a capstone project.*

## Academic Requirements

Code	Title	Credits
<b>Core Courses</b>		
ECF 610	Criminal Justice and Legal Concepts	3
FACC 702	Financial Statement Fraud	3
FACC 703	Occupational Fraud and Abuse	3
FACC 704	The Computer and Internet Fraud	3
FACC 705	Fraud Detection and Prevention: Special Cases	3
<b>Specialization Courses</b>		
Students select a series of 4 courses from one of the following groups:		12

*IT and Cybersecurity Policy Specialization*

ECF 625	Litigation Support Practices and Procedures
CYB 612	Ethics, Issues, and Government Regulations
CYB 644	Information Security
CYB 652	Leadership Assessment and Evaluation
CIS 619	Crisis Management and Business Continuity

*Data Science Specialization*

CIS 523	Data Processing and Database Management
CIS 658	Data Mining
CIS 633	Data Analysis with R
CIS 654	Artificial Intelligence

**Capstone Project**

ECF 880	Integrative Capstone	3
---------	----------------------	---

<b>Total Credits</b>		<b>30</b>
----------------------	--	-----------

## Course Sequence

### Tentative Schedule

Course	Title	Credits
<b>First Year</b>		
<b>First Semester</b>		
ECF 610	Criminal Justice and Legal Concepts	3
FACC 702	Financial Statement Fraud	3
<b>Credits</b>		<b>6</b>
<b>Second Semester</b>		
FACC 703	Occupational Fraud and Abuse	3
FACC 704	The Computer and Internet Fraud	3
<b>Credits</b>		<b>6</b>
<b>Third Semester</b>		
FACC 705	Fraud Detection and Prevention: Special Cases	3
Group 1 or Group 2 Course		3
<b>Credits</b>		<b>6</b>
<b>Second Year</b>		
<b>First Semester</b>		
Group 1 or Group 2 Course		3
Group 1 or Group 2 Course		3
<b>Credits</b>		<b>6</b>
<b>Second Semester</b>		
Group 1 or Group 2 Course		3
ECF 880	Integrative Capstone	3
<b>Credits</b>		<b>6</b>
<b>Total Credits</b>		<b>30</b>

## Course Descriptions

### Computer Information Science

#### CIS 523 Data Processing and Database Management

This course entails analysis and evaluation of database designs in relation to the strategic mission of the project. Topics include database systems, database architectures, and data-definition and data-manipulation languages. Also included are logical and physical database design, database models (e.g., entity-relationship, relational), normalization, integrity, query languages including SQL, and relational algebra, in addition to social and ethical considerations and privacy of data. This course incorporates case studies and a project using a relational DBMS.

#### CIS 619 Crisis Management and Business Continuity

This course explores the area of Risk Management with particular emphasis on Business Continuity Management. Risk Management involves assessing threats which may lead to disastrous events, evaluating control alternatives and implementing solutions. Potential threats include terrorist, criminal, industrial, natural, technological, environmental, economic and political. Practical solutions to enable an organization to protect assets, mitigate risk, manage crisis and recover after a disaster will be discussed. The role of business and government will be explored, as well as professional practices, standards and strategies. The course is designed to expose the student to all aspects of a holistic Business Continuity & Crisis Management program and to determine the most appropriate requirements.

#### CIS 654 Artificial Intelligence

This course introduces students to the field of artificial intelligence (AI). Students will learn how big data and data mining techniques are utilized by machines to create the AI models used by autonomous aircraft and automobiles, personal assistants, IT security software, fraud investigations and credit bureaus. The course will review the history, present day use, and future of artificial intelligence. Through case studies and current events, students will examine the benefits and risks associated with AI. The course will cover issues related to AI and privacy, ethics, and machine bias. Neuromorphic computing, the Open Neural Network Exchange (ONNX), and data analytics will also be discussed.

#### CIS 658 Data Mining

This course introduces the field of data mining, with specific emphasis on its use for Machine Learning algorithms. Techniques covered may include conceptual clustering, learning decision rules and decision trees, case-based reasoning, Bayesian analysis, genetic algorithms, and neural networks. The course covers data preparation and analysis of results. Skills in Microsoft Excel are useful. Prerequisite(s): CIS 523

## Cybersecurity

#### CYB 540 Network Theory

Lecture/theory course considers the current methods, practices, and standards used to enable communication on computer and voice networks. This includes a study of the physical layers, architectural layers, design, operation, management, and ISO standards, with particular and telephony technologies. Both local and wide area networks are examined.

#### CYB 612 Ethics, Issues, and Government Regulations

This course considers privacy both on- and off-line; legal background of intellectual property and e-mail; ethics and codes of ethics; effects of computers on work and society; and responsibilities and risks of computing, including topics such as accuracy of information, e-waste, and multitasking. This course includes an examination of government policies and regulations related to data security and information assurance.

#### CYB 628 Cybercrime, Cyber Warfare and Cyber Espionage

This course introduces students to the differences between cybercrime, cyber espionage, and cyber warfare by discussing the relationship of cyber intrusions and cybersecurity to nations, businesses, society, and people. Students will use case studies to analyze the threats, vulnerabilities and risks present in these environments, and develop strategies to reduce the breaches and mitigate the damages.

**CYB 644 Information Security**

This course explores all aspects of computing and communications security, including policy, authentication, authorization, administration, and business resumption planning. It examines key security technologies, such as encryption, firewalls, public-key infrastructures, smart cards, and related technologies that support the development of an overall security architecture. Coursework includes plans for developing and implementing a technology security strategy focused on business needs. Prerequisite(s): CIS 540

**CYB 652 Leadership Assessment and Evaluation**

This experiential course emphasizes the importance of feedback and self-assessment for leadership development. It includes extensive assessment of each participant's management style and skills based on self-evaluations (using structured questionnaires) and feedback from coworkers, faculty, and other participants. Leadership development experiences emphasize time and stress management, individual and group problem-solving, communication, power and influence, motivation, conflict management, empowerment, and team leadership. Each participant identifies skills he or she needs to develop and reports on efforts to develop those skills.

**CYB 665 Computer Digital Forensics**

This course examines techniques used to conduct computer crime investigations and gather probative evidence to secure a conviction under state and federal laws. Students will simulate a computer forensic investigation: developing an investigation plan, securing the crime scene, analyzing evidence, preparing the case for court, and testifying in a moot court situation.

**CYB 668 Computer and Network Security**

Students will study and implement basic computer and network security strategies on Window and Linux networks. Students examine and analyze network traffic, including investigating wireless transmission, install firewalls and define Internet Protocol Security Controls (IPSEC). Labs include system hardening, dissecting network packet structure and creating encryption formats; managing authentication and access controls. Students study implementing a public key infrastructure and best strategies for using intrusion detection systems.

**CYB 880 Integrative Capstone**

The capstone project is an opportunity to pursue an independent learning experience focused on a specific aspect of economic crime forensics based on the student interest. The capstone is intended to extend students beyond the coursework and cases to apply knowledge in ways that are relevant to their professional goals. Students will work on a research project or in an experiential learning environment. Each student will be required to present his/her capstone both as an oral presentation and a summary written document. Students are expected to complete the capstone with a grade of B or better in order to graduate from the program.

**Econ Crime Forensics****ECF 610 Criminal Justice and Legal Concepts**

The course provides an overview of the legal systems and expertise required for fraud risk professionals. The course enables participants to deepen their knowledge of the U.S. legal system by acquiring a broader understanding of processes and procedures that focus on fraud investigation, prosecution, and civil remedies. The course covers knowledge of law enforcement agencies, federal rules and regulations and evidence management, and expert testimony.

**ECF 625 Litigation Support Practices and Procedures**

Learners will explore white collar misconduct that constitutes civil and/or criminal fraud in a corporate setting, including but not limited to: (1) falsification of business records; (2) false billing; (3) forgery of documents or signatures; (4) embezzlement; (5) creation of false companies; (6) false insurance claims; (7) bankruptcy fraud; (8) investment frauds (such as Ponzi schemes); (9) tax fraud; and (10) securities fraud. Students will develop processes and procedures for proper evidence management as well as learn how to prepare to serve as an expert witness and write legally sound expert reports. Prerequisite(s): ECF 610

**ECF 880 Integrative Capstone**

The capstone project is an opportunity to pursue an independent learning experience focused on a specific aspect of economic crime forensics based on the student interest. The capstone is intended to extend students beyond the coursework and cases to apply knowledge in ways that are relevant to their professional goals. Students will work on a research project or in an experiential learning environment. Each student will be required to present his/her capstone both as an oral presentation and a summary written document. Students are expected to complete the capstone with a grade of B or better in order to graduate from the program.

**Fraud and Forensics Accounting****FACC 702 Financial Statement Fraud**

Financial statement fraud involves intentional misstatements or omissions of financial statement amounts or disclosures to deceive users of the statements. This topic, commonly known as "cooking the books," will introduce students to management's motives and pressures to achieve desired financial results as opposed to true economic financial results. This course will enable students to both understand and detect the creative accounting methods management employs to "cook the books," along with related fraud prevention strategies.

**FACC 703 Occupational Fraud and Abuse**

Occupational fraud and abuse is described as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of one's employing organization's resources or assets. Through the use of real-life case examples, this course will focus on the types of persons most likely to perpetrate occupational fraud, the conditions under which fraud might be committed, and the specific schemes used to defraud organizations of amounts ranging from hundreds to millions of dollars.

**FACC 704 The Computer and Internet Fraud**

Computers have made organizations easier to run. All accounting information, inventory records, customer data, and intellectual property that an organization possesses is contained somewhere in an electronic file. As such, these electronic files are vulnerable to attacks from both employees and outsiders from around the world. This course will provide the student with an understanding of how computer fraud and manipulation is accomplished and what security measures should be instituted to prevent it.

#### FACC 705 Fraud Detection and Prevention: Special Cases

The opportunity to commit and conceal fraud exists only when there are assets susceptible to misappropriation and a lack of internal controls to prevent or detect fraud. This course will focus on the high-risk fraud environments wherein assets are more vulnerable to misappropriation and fraud because of either a lack of, or non-functioning of, internal controls. The study of various fraud investigative methods and the process for communicating an expert report will be an essential part of this course.

## Faculty

Associate Professors: Redmond

Assistant Professors: McCoey

Lecturers: Casey, Monaghan, Smith, Walters, Zikmund

## Program Contact Information

Holroyd 129

[ecf@lasalle.edu](mailto:ecf@lasalle.edu)

(215)951-1136

## Staff Contact Information

Margaret McCoey, Program Director

Holroyd 129

[mccoey@lasalle.edu](mailto:mccoey@lasalle.edu)

(215)951-1136