

# UCI Extension

Information Technologies Programs

## Information Systems Security Certificate Program

**Accelerate Your Career**

[extension.uci.edu/infosec](http://extension.uci.edu/infosec)

University of California, Irvine





## Improve Your Career Options with a Professional Certificate

**University of California, Irvine Extension's professional certificate and specialized studies programs** help you increase or enhance your current skills or prepare for a new career. Courses are highly practical and instructors are qualified leaders in their field. Convenient online courses make it easy to learn on your own time, in your own way. A certificate bearing the UC seal signifies a well-known, uncompromising standard of excellence.



## Information Systems Security Certificate Program

Corporations have been put on alert to heighten their infrastructure and data security due to threats from hackers and cyber-terrorists. As information security threats and high visibility breaches have skyrocketed in the past few years, government agencies and customers have dramatically increased their requirements and scrutiny of corporate security process and procedures. UC Irvine Extension's Certificate program in Information Systems Security prepares professionals within a wide range of career levels to develop the skills they need to succeed in this rapidly expanding, dynamic field.

The curriculum focuses on developing a comprehensive understanding of the underlying principles for designing, engineering, and managing secure information systems environments. Core topic areas include: access control; application development security; business continuity; disaster recovery planning; cryptography; information security governance; risk management; legal; regulations; investigations and compliance; operations security; physical (environmental) security; security architecture; design and telecommunications; and network security. Learn how to effectively combat external attacks that can compromise data and business operations through our cyber security track of elective courses. This program will help prepare you to sit for the Certified Information Systems Security Professional (CISSP®) exam administered by the International Information Systems Security Certification Consortium, Inc., (ISC)²®.

**For More Information:**  
Julie Pai  
Program Representative  
julie.pai@uci.edu  
(949) 824-6333

## Who Should Enroll?

This program has been designed to benefit security professionals who require CISSP® certification and work on software development and information technology infrastructure teams, security technicians working with Internet service providers, application service providers, systems integrators, and security auditors. Business professionals who must combat potential cyber-threats and attacks that endanger their organizations' data will also benefit from this program.

The program also includes courses that expand technical skills and enable security professionals and those training to be security professionals to pursue and maintain a variety of industry certifications. The courses include current findings from academic and technological research and state-of-the-art practice.

## Program Benefits:

- Develop key knowledge of information systems security, including access control, administration, audit and monitoring, risk, response, and recovery
- Protect the confidentiality, integrity, and availability (CIA) of stored information
- Implement government and customer imposed security requirements
- Develop best practices for business continuity planning
- Broaden your knowledge to include the implementation of multiple technologies, including client/server, Web, mainframe, and wireless
- Identify and apply industry standards at the physical, personal, and organizational level
- Design, diagnose, implement, manage, and resolve complex computer security threats
- Gain the knowledge required to obtain your CISSP® certification.



# Curriculum

## Program Fees

Course Fees:	\$4,865
Candidacy Fee:	\$ 125
Textbooks and Materials:	\$ 700
<hr/>	
Total Estimated Cost:	\$5,690

## Certificate Requirements

A certificate is awarded upon completion of: three (3) required courses and six (6) units of elective courses; totaling minimum of fifteen (15) units or 150 hours of instruction with a grade point average of 'B' or better.

To become an official candidate in the program, students pursuing the certificate must submit a Declaration of Candidacy. To receive the certificate after completing all program requirements, students must submit a Request for Certificate. All requirements must be completed within five (5) years after the student enrolls in his/her first course. Students not pursuing the certificate program are welcome to take as many individual courses as they wish.

## Transfer Credit

Graduates from UC Irvine Extension's Information Systems Security Certificate program are eligible to transfer credits to University of Wisconsin-Platteville, Master of Science in Criminal Justice and University of Maryland, Baltimore County (UMBC), Master in Professional Studies (MPS): Cybersecurity programs.

## Onsite Training

Our Corporate Training specialists can deliver this program or a customized one that fits your organization's specific needs. Visit [extension.uci.edu/corporte](http://extension.uci.edu/corporte) or call (949) 824-1847 for information.

## Required Courses

### Introduction to Information Systems Security

I&CSCI X465.00 (3.0 units)

Focus is on basic computer security concepts including logical and physical security at corporate and remote workforce locations. This introductory course will expose you to various design principles of trusted computing bases, legal regulations, investigation, and compliance requirements. Also learn about secure computing concepts including security protocols and principles. Networking security methodologies, an introduction to business continuity and disaster recovery concepts, will also be covered in this course.

### Secure Systems

I&CSCI X465.01 (3.0 units)

Learn design principles of trusted computing bases (TCB). Issues regarding: authentication; access control and authorization; introductory cryptography; controls categories; media; backups and change control management; discretionary and mandatory security policies; secure kernel design; application development security; secure operating systems (patching and vulnerability management); and secure databases will be covered from a systems architecture perspective. Emphasis will be on the design of security measures for critical information infrastructures.

### Security Architecture & Design

I&CSCI X465.02 (3.0 units)

Increase your knowledge of the principles and benefits of security architecture. This course will cover trusted systems and computing bases, system and enterprise architecture, and information security evaluation (e.g. PCI-DSS). Additional topics include an overview of security capabilities, vulnerabilities, threats, and an in-depth introduction to countermeasure and defense.



## Elective Courses (Choose 6 units)

### Host and OS Security

I&CSCI X465.03 (3.0 units)

Learn the security aspects of Windows Vista, MAC, and Apple OS technology as it applies to home and mobile user configurations. This course will also cover the most prominent networking and stand-alone OS's vital to company client server operations as well as information security governance and risk management.

### Database Security

I&CSCI X465.05 (3.0 units)

This course will focus on issues related to the design and implementation of secure data stores. Emphasis will be placed on multilevel security in database systems, covert channels, and security measures for relational and object-oriented database systems.

### Network Security: Concepts & Technologies

I&CSCI X465.06 (3.0 units)

Fundamental concepts, principles, networking and inter-networking issues relevant to the design, analysis, and implementation of enterprise-level networked systems are covered in this course. Topics include networking and security architectures, techniques, and protocols at the various layers of the Internet model. Security problems will be analyzed, discussed, and implemented.

## Cyber Security Track

### Introduction to Computer Forensics

I&CSCI X465.07

This hands-on computer forensics training course offers practical experience in a wide array of computer forensics situations that are applicable to the real world. Learn how to analyze data held on or retrieved from computer storage media to uncover misuse or possible criminal activity. The course provides you with the knowledge to systematically and impartially approach the preservation and extraction

of relevant digital evidence from computers, computer systems, and computer networks (including the Internet) using appropriate tools and techniques. This process will include the preservation of volatile data and the forensic analysis of memory, registries, and files.

### Ethical Hacking

I&CSCI X465.09

Explore hacking techniques and counter-measures focusing on techniques used by malicious, black hat hackers. Topics include: network systems penetration tools, techniques for identifying vulnerabilities and security holes in operating systems, and software applications. Learn how perimeter defenses work, how to scan and attack your own network, how intruders escalate privileges, and the steps that need to be taken to secure a system. Intrusion detection, policy creation, social engineering, DDoS attacks, buffer overflows and virus creation will also be covered.

### Reverse Engineering

I&CSCI X465.10

Understanding and analyzing malware through the process of reverse engineering is a key methodology to stop malware attacks. Learn how to use this process to discover vulnerabilities in binaries in order to properly secure your organization from ever evolving threats. This class covers a wide variety of malware, from native Windows executables, to web-based malware with numerous types of obfuscation. Take a hands-on approach to learn how to reverse-engineer malicious code using system/network monitoring utilities, debuggers, disassemblers, and a handful of scripts.



### Advisory Committee

**Leo A. Dregier III**, CISSP®, CEH™, CHFI™, CISM®, CEO,  
The Security Matrix, LLC

**Tony Gaidhane**, MBA, M.S., CISSP®, CISM®, CISA®, PMP,  
Senior Manager, Information Security, WellPoint Inc.

**Ian Harris, Ph.D.**, Associate Professor, Donald Bren  
School of Information and Computer Science, University  
of California, Irvine

**Terry House, Ph.D.**, Assistant Professor of Computer  
Science, Methodist University

**Barbara Johnson**, CISA®, CISSP®, ISSMP®, CBCP, MBCI,  
Information Security and Business Continuity Consultant,  
Member of the (ISC)²® Common Body of Knowledge (CBK)  
Committee

**David M. Mahoney**, MBA, CISSP®, PMP®, Manager  
Infrastructure Services, Information Systems Sector, Civil  
Systems Division, Northrop Grumman Corporation

**Pramod Pandya**, Ph.D., Professor and Director,  
Information Technologies, California State University  
Fullerton

**Debbie Rodriguez**, MBA, CISSP®, CISA®, System Analyst,  
Intuit Financial Services

**Maria Suarez**, Information Security Officer, The City  
of Hope

### Academic Management

Dave Dimas, Ph.D., Director, Engineering, Sciences and Information Technologies

## Information Systems Security Certificate Program

Julie Pai ■ (949) 824-6333 ■ [julie.pai@uci.edu](mailto:julie.pai@uci.edu)

**UCI** Extension