A Complete Cutting-Edge & Interactive Curriculum Solution

For Student-Centered Information System Security Programs

- Authoritative TextBooks Written by Leading Experts
- Fully Scoped & Sequenced Interactive Online Courses
- State-of-the-Art Virtual Cloud Labs

www.issaseries.com
Prepare Students for Careers in IT Security, Cybersecurity, Information Assurance and Information Systems Security

By 2018, the need for qualified information security professionals is expected to grow by nearly 30%, much faster than most other occupations. To help meet the need for more information security professionals, Jones & Bartlett Learning has developed the first comprehensive program solution designed to prepare students for success in IT Security, Cybersecurity, Information Assurance, and Information System Security. This innovative curriculum, developed by certified IT professionals, combines first-of-its kind technology, student-friendly texts, and complete instructor support to facilitate seamless implementation, ensure improved student outcomes, and increased retention rates.

The Jones & Bartlett Learning Information System Security & Assurance Curriculum delivers fundamental IT security principles packed with real-world applications, innovative hands-on labs, and a wealth of examples and assessments. The flexible and interactive curriculum solution includes:

- 13 custom information systems security textbooks/e-books each with content divided into 15 chapters.
- 13 classroom-based courses with accompanying instructor guides. Each course includes scenario based problems where students role-play an IT security practitioner as well as homework assignments, quizzes, exams, and detailed instructor guides and lab manuals.
- 13 courses developed for online delivery featuring scenario-based learning activities throughout. Each course is SCORM compliant and developed using multi-media/flash-based animation interaction.
- 120 total hands-on Applied Labs that provides a unique, scenario-based learning experience.

Innovative Labs with Mock IT Infrastructure Provide Real-World Experiential Learning

The Information Systems Security & Assurance Curriculum is available with online Virtual Security Cloud Labs, delivered in a first-of-its-kind cloud computing environment. These hands-on labs provide a fully immersive mock IT infrastructure enabling students to test their skills with realistic security scenarios; scenarios they will encounter in their future careers.
Teaching and Learning Tools to Support the Program:

Jones & Bartlett Learning understands that the key to success for any school, college, or university is to build and offer high enrollment degree programs that lead to job work force readiness in high-demand careers. We believe that one of the common business challenges to solve by the organization is to properly prepare its instructors for delivery operational readiness.

The Information Systems Security & Assurance Series includes the following ancillary support to provide a complete teaching and learning curriculum solution:

- Textbook available in print or eBook format
- Lab Manual available in print or eBook format
- Virtual Security Cloud Labs
- Navigate Learning Management System
- Video Demo Labs
- Case Scenarios and Handouts
- Instructor’s Manual
- Test Questions
- PowerPoint Lecture Outlines
- Sample Syllabus

A Complete Learning, Homework Assignment, and Assessment Solution

Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System. All material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution. With JBL Integrate™, we can deliver specific course assets or complete course curricula in formats compatible with most learning management systems.

Customized Course Material Made Easy!

Jones & Bartlett Learning is pleased to offer PUBLISH, a new service that lets instructors and other curriculum developers build customized course materials to fit their precise curriculum needs. Using a simple, easy-to-navigate web-based interface, instructors can quickly search and select content from the Jones & Bartlett Learning content library, and build a textbook to meet their specific course objectives using chapters from as many titles as necessary.

Contact Your Account Specialist Regarding Cost-Saving Bundling Opportunities.

Visit www.issaseries.com to Learn More
### The Complete Curriculum Solution for Your InfoSec Program!

<table>
<thead>
<tr>
<th>TEACHING RESOURCES</th>
<th>COURSEWARE</th>
<th>APPLIED LABS</th>
</tr>
</thead>
</table>

- **Kim, Fundamentals of Information Systems Security**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Weiss, Auditing IT Infrastructures for Compliance**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Harwood, Security Strategies in Web App. & Social Networking**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Stewart, Network Security, Firewalls, and VFNs**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Vacca, System Forensics, Investigation and Response**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Oriyano, Hacker Techniques, Tools, and Incident Handling**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Ballad, Access Control, Authentication, and Public Key Infrastructure**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Johnson, Security Policies and Implementation Issues**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Solomon, Security Strategies in Windows Platforms and Applications**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Jang, Security Strategies in Linux Platforms and Applications**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Grama, Legal Issues in Information Security**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- **Gibson, Managing Risk in Information Systems**  
  - PowerPoints
  - Test Questions
  - Instructor's Manual
  - Lab Instructor Manual
  - Syllabus
  - Case Scenarios & Handouts
  - eBook (via CourseSmart)
  - Navigate
  - Paper-based Labs
  - Video Demo Labs

- Available on Secure Site
- Demo Available on [www.issaserics.com](http://www.issaserics.com)
Innovative Labs Providing Hands-On Experiential Learning

The Information Systems Security & Assurance Curriculum is available with the new online Virtual Security Cloud Labs, delivered in a first-of-its-kind cloud computing environment using cutting-edge technology. These hands-on labs provide a fully immersive mock IT infrastructure enabling students to test their skills with realistic security scenarios, scenarios they will encounter in their future careers.

- This “Virtual Sandbox” provides students with instant, unscheduled access to 65 virtual labs from a fully hosted environment.
- Allows student to practice “white hat” hacking on an actual IT infrastructure.
- Unlike simulations, the Jones & Bartlett Learning Virtual Security Cloud Labs reproduce the complex challenges of the real-world without putting an institution’s IT assets at risk.
- As part of a blended solution, these labs are an essential tool for catalyzing key course concepts through hands-on training.
- This style of engaging experiential learning is proven to deliver the highest retention among all training methodologies.

Students can gain up to 200 hours of hands-on experience as part of a curriculum that is mapped to popular industry certifications, including the Certified Information Systems Security Professional (CISSP), CompTIA Security +, and Systems Security Certified Practitioner (SSCP). Providing “virtual internships” that provide students with real-world experience while they are still in school increases student engagement, retention and motivation.


Visit www.issaseries.com to Learn More
Teaching Information Security Has Never Been Easier


Complete Learning, Homework Assignment, and Assessment Solution

USER-FRIENDLY TEACHING TOOLS

- Each course in the complete program is comprised of 15 lessons and all content is pre-populated in the course shell for immediate use. Instructors can also upload custom content.
- Robust grade book enables detailed reporting on students’ progress or overall class statistics. It can be configured to add weighted grading, custom scales, or generate statistical item analyses on quiz questions.
- User-friendly control panel lets instructors easily deploy & track online quizzes and homework.
- Includes optional web hosting and technical support—no need to involve your IT department.

INTERACTIVE LEARNING

- Using a proven model that focuses on the natural, active processes of learning, Navigate: Information System Security & Assurance embodies a “Discover-Apply-Create” method of instruction that helps students process and retain critical information more effectively and in less time than traditional teaching methods.
- Numerous exercises, including multiple choice, fill-in-the-blank questions, matching, and drag-and-drop, help assess comprehension.
- The curriculum has been developed to present students with engaging, relevant, real-world information security system roles and challenges, as well as the basics skills and knowledge required to enter the job force.

Navigate incorporates a collaborative learning environment through:

- Discussion Forums
- Instant Chat
- Instructor and Student Blogs
- Single Question Polling
- Community Glossary Building
- Community Wiki
- Matching textbook
- Syllabus
- Assignment activities focused on information security challenges
- Instructor Guides
- Assessment quizzes and exams (with answer keys)
- Discussion Questions
- Interactive Discover-Apply-Create tools for each lesson of study
- Critical Thinking Applications highlights the Challenge, Resources to Use, and Course of Action
- Practice Activities
- Handouts
- PowerPoints
- Student Study Guide
- Virtual Hands-on Labs *(hosted in a cloud environment or provided in video simulation)

Visit www.issaseries.com to Learn More
Jones & Bartlett Learning is pleased to offer PUBLISH—a new service that lets instructors and other curriculum developers build customized course materials to fit their exact curriculum needs. Using a simple, easy-to-navigate web-based interface, instructors can quickly search and select content from the Jones & Bartlett Learning content library, and include as many chapters from any number of titles as necessary to meet specific course objectives.

After selecting a range of content, PUBLISH lets instructors:
- Arrange chapters in any order
- Upload and include their own material
- Customize a cover

Once the project is complete, instructors simply:
- Preview their custom content
- Review the instant price quote
- Submit the order online

Jones & Bartlett Learning will do the rest, including processing the order and shipping copies directly to college bookstores or other retail outlets.

PUBLISH Your Custom Course Content Today!
- PUBLISH editions are priced by the page—publish as many pages as needed
- Minimum of 25 books per order
- Minimum of 10 books on reprints per order
- Customize front and back covers
- Upload your own content

Visit www.issaseries.com to Learn More
Fundamentals of Information Systems Security

David Kim and Michael G. Solomon

Fundamentals of Information System Security provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)² SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Applied Labs:
- Lab #1: Perform Reconnaissance & Probing Using ZenMap GUI (Nmap)
- Lab #2: Perform a Vulnerability Assessment Scan Using Nessus®
- Lab #3: Enable Windows Active Directory and User Access Controls
- Lab #4: Configure Group Policy Objects and Microsoft Baseline Security Analyzer
- Lab #5: Perform Protocol Capture & Analysis Using Wireshark & Netwitness Investigator
- Lab #6: Perform Business Continuity Plan Implementation Planning
- Lab #7: Relate Windows Encryption and Hashing to Confidentiality & Integrity
- Lab #8: Perform a Website & Database Attack by Exploiting Identified Vulnerabilities
- Lab #9: Perform a Virus Scan and Malware Identification Scan and Eliminate Threats
- Lab #10: Craft an Information Systems Security Policy

Courseware:

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning's customizable course content delivery solution.
Textbook Table of Contents:

Part 1: The Need for Information Security
- Chapter 1: Information Systems Security
- Chapter 2: Changing the Way People and Businesses Communicate
- Chapter 3: Malicious Attacks, Threats, and Vulnerabilities
- Chapter 4: The Drivers of Information Security Business

Part 2: The Systems Security Certified Practitioner (SSCP®) Professional Certification from (ISC)²
- Chapter 5: Access Controls
- Chapter 6: Security Operations and Administration
- Chapter 7: Auditing, Testing, and Monitoring
- Chapter 8: Risk, Response, and Recovery
- Chapter 9: Cryptography
- Chapter 10: Networks and Telecommunications
- Chapter 11: Malicious Code and Activity

- Chapter 12: Information Security Standards
- Chapter 13: Information Security Education and Training
- Chapter 14: Information Security Professional Certifications
- Chapter 15: US Compliance Laws

Key Features:
- Focuses on new risks, threats, and vulnerabilities associated with the transformation to a digital world.
- Presents a high-level overview of each of the seven domains within the Systems Security Certified Practitioner certification.
- Provides a resource for readers and students desiring more information on information security standards, education, professional certifications, and recent compliance laws.
- Features an SSCP practice exam as well as a coupon offer for an SSCP Review Seminar.

About the Authors:

David Kim is president and chief security officer for Security Evolutions, Inc. (SEI). SEI provides IT security training and consulting services for organizations around the world. SEI has specific expertise and experience in VoIP and SIP layered security solutions where privacy data may encompass both data and voice communications. Mr. Kim’s IT and IT security experience encompasses more than 20 years of technical engineering, technical management, and sales and marketing management. This experience includes LAN/WAN, internetworking, enterprise network management, and IT security for voice, video, and data networking infrastructures. Previously, Mr. Kim was chief operating officer of (ISC)² Institute located in Vienna, Virginia, where he was responsible for content development, educational products, and educational delivery for (ISC)² (www.isc2.org) and its IT security professional certifications.

Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University's Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.
Legal Issues in Information Security

Joanna Lyn Grama

Legal Issues in Information Security provides a unique, in-depth look at the major federal and state laws that regulate information security and data privacy practices. Written by an industry expert, this book provides a comprehensive explanation of the most pertinent regulatory laws; discussing key concepts common to information security, data privacy, and the American legal system. Using examples and exercises, this book incorporates hands-on activities to walk the reader through the entire process of creating an information security program.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Courseware:
The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.

Paper-based Applied Labs:
- Lab #1: Create an IT Infrastructure Asset List & Identify Where Privacy Data Resides
- Lab #2: Case Study for Activity on Veteran Affairs and Loss of Private Information
- Lab #3: Case Study on PCI DSS Non-Compliance: CardSystems SolutionsM
- Lab #4: Analysis and Comparison of GLBA and HIPAA
- Lab #5: Case Study on Issues Related to Sharing Consumers’ Confidential Information
- Lab #6: Identify the Scope of Your State’s Data & Security Breach Notification Law
- Lab #7: Digital Millennium Copyright Act
- Lab #8: Cyber Stalking or Cyber Bullying and Laws to Protect Individuals
- Lab #9: Recommend IT Security Policies to Help Mitigate Risk
- Lab #10: Case Study in Computer Forensics – Pharmaceutical Company
Textbook Table of Contents:

Part 1: Fundamental Concepts
Chapter 1: Information Security Overview
Chapter 2: Privacy Overview
Chapter 3: The American Legal System

Part 2: Laws Influencing Information Security
Chapter 4: Security and Privacy of Consumer Financial Information
Chapter 5: Security and Privacy of Information Belonging to Children and Educational Records
Chapter 6: Security and Privacy of Health Information
Chapter 7: Corporate Information Security and Privacy Regulation
Chapter 8: Federal Government Information Security and Privacy Regulation
Chapter 9: State Laws Protecting Citizen Information and Breach Notification Laws
Chapter 10: Intellectual Property Law
Chapter 11: The Role of Contracts
Chapter 12: Criminal Law and Tort Law Issues in Cyberspace

Part 3: Security and Privacy in Organizations
Chapter 13: Information Security Governance
Chapter 14: Risk Analysis, Incident Response, and Contingency Planning
Chapter 15: Computer Forensics and Investigations

Key Features:

- Introduces federal information security requirements, including: the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).
- Illustrates how to create an organizational information security program that addresses compliance requirements.
- Discusses information security risk management and business continuity planning.
- Identifies legal issues surrounding the collection, handling, and use of digital evidence.

Visit www.issaseries.com to Learn More

About the Author:

Joanna Lyn Grama, (JD, CISSP, CIPP/IT) serves as the information security policy and compliance director for Purdue University, where she creates the university’s IT security policy and is responsible for compliance governance and activities. She is a member of the Information Systems Audit and Control Association, the organization for IT governance professionals; the American Bar Association, Section of Science and Technology Law, Information Security Committee; EDUCAUSE; and the Indiana State Bar Association. Joanna graduated from the University of Illinois College of Law with honors, and was the editor-in-chief of The Elder Law Journal. She is a frequent speaker on a variety of IT security topics, including identity theft, personal information security, and university compliance issues.
Managing Risk in Information Systems

Darril Gibson

Managing Risk in Information Systems provides a unique, in-depth look at how to manage and reduce IT-associated risks. Written by an industry expert, this book provides a comprehensive explanation of the SSCP Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Using examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Courseware:
The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Paper-based Applied Labs:
Lab #1: How to Identify Threats and Vulnerabilities in an IT Infrastructure
Lab #2: Align Threats & Vulnerabilities to the COBIT P09 Risk Management Controls
Lab #3: Define the Scope & Structure of an IT Risk Management Plan
Lab #4: Perform a Qualitative Risk Assessment for an IT Infrastructure
Lab #5: How to Identify Threats & Vulnerabilities in Your IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus®
Lab #6: Develop a Risk Mitigation Plan for Prioritized Threats & Vulnerabilities
Lab #7: Perform a Business Impact Analysis for an IT Infrastructure
Lab #8: Develop an Outline for a Business Continuity Plan for an IT Infrastructure
Lab #9: Develop Disaster Recovery Back-up Procedures and Recovery Instructions
Lab #10: Create a CIRT Response Plan for a Typical IT Infrastructure

Instructor’s Material:
- PowerPoint Lectures
- Instructor's Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: Risk Management Business Challenges
Chapter 1: Risk Management Fundamentals
Chapter 2: Managing Risk: Threats, Vulnerabilities, and Exploits
Chapter 3: Maintaining Compliance
Chapter 4: Developing a Risk Management Plan

Part 2 Mitigating Risk
Chapter 5: Defining Risk Assessment Approaches
Chapter 6: Performing a Risk Assessment
Chapter 7: Identifying Assets and Activities to Be Protected
Chapter 8: Identifying and Analyzing Threats, Vulnerabilities, and Exploits
Chapter 9: Identifying and Analyzing Risk Mitigation Security Controls
Chapter 10: Planning Risk Mitigation Throughout the Organization
Chapter 11: Turning Your Risk Assessment into a Risk Mitigation Plan

Part 3: Risk Mitigation Plans
Chapter 12: Mitigating Risk with a Business Impact Analysis
Chapter 13: Mitigating Risk with a Business Continuity Plan
Chapter 14: Mitigating Risk with a Disaster Recovery Plan
Chapter 15: Mitigating Risk with a Computer Incident Response Team Plan

Key Features:

- Introduces the fundamentals of risk and risk management.
- Illustrates how to identify and analyze threats and vulnerabilities as well as evaluate security controls to mitigate risk.
- Discusses how to translate a risk assessment into a risk management plan.
- Identifies how to perform a business impact analysis and the differences between business continuity plans and disaster recovery plans.

About the Author:

Darril Gibson is an IT trainer who regularly teaches security topics to Air Force personnel. An adjunct professor, he’s written or co-authored several IT books, including CompTIA Security+: Get Certified Get Ahead, and Mastering Windows Server 2008 R2. In addition, he’s also created training videos on multiple topics for Keystone Learning. Mr. Gibson holds numerous certifications, including (ISC)2 CISSP and CompTIA Security+. He’s also been a Microsoft Certified Trainer since 1999.
The study of information system security concepts and domains is an essential part of the education of computer science students and professionals alike. *Security Policies and Implementation Issues* offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building, to the psychology of implementation. It presents an effective balance between technical knowledge and soft skills, and introduces many different concepts of information security in clear, simple terms such as governance, regulator mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of security policies and frameworks.

The Complete Curriculum Solution!

The *Information Systems Security & Assurance Course Curriculum* provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certificate level.

Courseware:
The *Information System Security & Assurance Curriculum* offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning's Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning's customizable course content delivery solution.

Paper-based Applied Labs:
Lab #1: Craft an Organization-Wide Security Management Policy for Acceptable Use
Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan
Lab #3: Define an Information Systems Security Policy Framework for an IT Infrastructure
Lab #4: Craft a Layered Security Management Policy - Separation of Duties
Lab #5: Craft an Organization-Wide Security Awareness Policy
Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics
Lab #7: Identify Necessary Policies for Business Continuity – BIA & Recovery Time Objectives
Lab #8: Craft a Security or Computer Incident Response Policy – CIRT Response Team
Lab #9: Assess and Audit an Existing IT Security Policy Framework Definition
Lab #10: Align an IT Security Policy Framework to the 7 Domains of a Typical IT Infrastructure
Textbook Table of Contents:

**Part 1: The Need for IT Security Policy Frameworks**
- Chapter 1: Information Systems Security Policy Management
- Chapter 2: Business Drivers for Information Security Policies
- Chapter 3: U.S. Compliance Laws and Information Security Policy Requirements
- Chapter 4: Business Challenges Within the Seven Domains of IT Responsibility
- Chapter 5: Information Security Policy Implementation Issues

**Part 2: Types of Policies and Appropriate Frameworks**
- Chapter 6: IT Security Policy Frameworks
- Chapter 7: How to Design, Organize, Implement, and Maintain IT Security Policies
- Chapter 8: IT Security Policy Framework Approaches
- Chapter 9: User Domain Policies
- Chapter 10: IT Infrastructure Security Policies
- Chapter 11: Data Classification and Handling Policies and Risk Management Policies
- Chapter 12: Incident Response Team (IRT) Policies

**Part 3: Implementing and Maintaining an IT Security Policy Framework**
- Chapter 13: IT Security Policy Implementations
- Chapter 14: IT Security Policy Enforcement
- Chapter 15: IT Policy Compliance Systems and Emerging Technologies

Key Features:
- Offers a comprehensive, end-to-end view of information security policies and framework.
- Addresses the technical knowledge and software skills required for policy implementation.
- Covers governance, regulator mandates, business drivers, legal considerations, and much more.
- Provides an excellent starting point for the creation of an effective IT security policy framework

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

About the Author:

**Robert Johnson** (CISA, CGEIT, CISM, CISSP) has 20 years’ experience dealing with all aspects of information security, IT audit, risk management, and privacy compliance. His diverse background includes hands-on operational experience as well as providing strategic risk assessment and scoring for leadership and board-level audiences. Currently he works in the security risk management division of a large financial services insurance company. Previously he worked as a first vice president and IT audit and security advisory director at Washington Mutual.

Available as an eTextbook through VitalSource and CourseSmart!
Auditing IT Infrastructures for Compliance

Martin Weiss and Michael G. Solomon

Auditing IT Infrastructures for Compliance provides a unique, in-depth look at recent U.S. based information systems and IT infrastructure compliance laws in both the public and private sector. Written by industry experts, this book provides a comprehensive explanation of how to audit IT infrastructures for compliance based on the laws, and the need to protect and secure business and consumer privacy data. Using examples and exercises, this book incorporates hands-on activities to prepare readers to skillfully complete IT compliance auditing.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Courseware:
The Information System Security & Assurance Curriculum offers lab manuals available in print and online, which allow students to put their classroom skills to work on numerous laboratory exercises.

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.

Paper-Based Applied Labs:
Lab #1: Assess the Impact of Sarbanes-Oxley (SOX) Compliance Law on Enron
Lab #2: Align Auditing Frameworks for a Business Unit within the DoD
Lab #3: Define a Process for Gathering Information Pertaining to a HIPAA Compliance Audit
Lab #4: Align an IT Security Assessment to Achieve Compliance
Lab #5: Define a Process for Gathering Information Pertaining to a GLBA Compliance Audit
Lab #6: Auditing the Workstation Domain for Compliance
Lab #7: Auditing the LAN-to-WAN Domain for Compliance
Lab #8: Auditing the Remote Access Domain for Compliance
Lab #9: Auditing the Systems/Application Domain for Compliance
Lab #10: Professional Information Systems Security Certifications—Charting Your Career Path
Textbook Table of Contents:

Part 1: The Need for Compliance
Chapter 1: The Need for Information Systems Security Compliance
Chapter 2: Overview of U.S. Compliance Laws
Chapter 3: What Is the Scope of an IT Audit for Compliance?

Part 2: Auditing for Compliance: Frameworks, Tools, and Techniques
Chapter 4: Auditing Standards and Frameworks
Chapter 5: Planning an IT Infrastructure Audit for Compliance
Chapter 6: Conducting an IT Infrastructure Audit for Compliance
Chapter 7: Writing the IT Infrastructure Audit Report
Chapter 8: Compliance Within the User Domain
Chapter 9: Compliance Within the Workstation Domain
Chapter 10: Compliance Within the LAN Domain
Chapter 11: Compliance Within the LAN-to-WAN Domain
Chapter 12: Compliance Within the WAN Domain
Chapter 13: Compliance Within the Remote Access Domain
Chapter 14: Compliance Within the System/Application Domain

Part 3: Ethics, Education, and Certification for IT Auditors
Chapter 15: Ethics, Education, and Certification for IT Auditors

Key Features:
- Identifies and explains today's U.S. compliance laws.
- Reviews compliance frameworks, tools, and techniques.
- Provides real-world examples to help readers gain a better understanding of key concepts.
- Discusses how to achieve compliance within the IT infrastructure.
- Identifies ethics, education, and certification for IT auditors.

About the Authors:

Martin Weiss is a manager of information security gurus at RSA, The Security Division of EMC, which helps organizations accelerate their business by solving their most complex and sensitive security challenges. He is also on the board of directors for the Connecticut chapter of ISSA and has written several books. He holds a number of certifications, including Security+, CISSP, MCSE: Security, and RSA CSE. Marty received his MBA from the Isenberg School of Management at the University of Massachusetts and currently lives in New England with his wife and three sons.

Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University's Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.
Access Control, Authentication, and Public Key Infrastructure

Bill Ballad, Tricia Ballad, and Erin K. Banks

Access Control, Authentication, and Public Key Infrastructure provides an accessible and comprehensive look at how access controls protect resources against unauthorized viewing, tampering, or destruction and serves as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Written by industry experts, this book defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs, before looking at risks, threats, and vulnerabilities prevalent in information systems and IT infrastructure and ways of handling them. Using examples and exercise, this book incorporates hands-on activities to prepare readers to successfully put access control systems to work as well as test and manage them.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certificate level.

Applied Labs:
- Lab #1: Assess the Impact on Access Controls for a Regulatory Case Study
- Lab #2: Design Infrastructure Access Controls for a Network Diagram
- Lab #3: Identify & Classify Data for Access Control Requirements
- Lab #4: Implement Organizational-Wide Network and WLAN Access Controls
- Lab #5: Enhance Security Controls for Access to Sensitive Data
- Lab #6: Enhance Security Controls Leveraging Group Policy Objects
- Lab #7: Design a Multi-factor Authentication Process
- Lab #8: Align Appropriate PKI Solutions Based on Remote Access and Data Sensitivity
- Lab #9: Apply Encryption to Mitigate Risk Exposure
- Lab #10: Use Reconnaissance, Probing, & Scanning to Identify Servers and Hosts

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Courseware:

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: The Need for Access Control Systems
Chapter 1: Access Control Framework
Chapter 2: Assessing Risk and Its Impact on Access Control
Chapter 3: Business Drivers for Access Controls
Chapter 4: Access Control Policies, Standards, Procedures, and Guidelines
Chapter 5: Unauthorized Access and Security Breaches

Part 2: Mitigating Risk with Access Control Systems, Authentication, and PKI
Chapter 6: Mapping Business Challenges to Access Control Types
Chapter 7: Human Nature and Organizational Behavior
Chapter 8: Access Control for Information Systems
Chapter 9: Physical Security and Access Control
Chapter 10: Access Control in the Enterprise

Part 3: Implementing, Testing, and Managing Access Control Systems
Chapter 11: Access Control System Implementations
Chapter 12: Access Control Solutions for Remote Workers
Chapter 13: Public Key Infrastructure and Encryption
Chapter 14: Testing Access Control Systems
Chapter 15: Access Control Assurance

Key Features:
- Provides a real-world view of access controls and systems.
- Examines both technical and business considerations.
- Explains why and how to implement an access control system.
- Uses a simple approach to presenting complex access control concepts.

About the Authors:

**Bill Ballad** has been active in the IT security community since the mid-1990s. He is the co-author and SME for *Securing PHP Web Applications* (Addison-Wesley Professional, 2008) and wrote the security chapters for *PHP & MySQL Web Development All-in-One Desk Reference for Dummies* (For Dummies, 2008). Bill is a senior systems engineer working with mission-critical Windows networks.

**Tricia Ballad** spent several years as a Web applications developer before becoming a full-time freelance writer and technical editor. She has written online courseware on various consumer electronics and computing subjects and has co-authored *PHP & MySQL Web Development All-in-One Desk Reference for Dummies* (For Dummies, 2008) and *Securing PHP Web Applications for Mere Mortals*.

**Erin Banks** (CISSP) is a technical writer and editor. She has been in the network and security industry for more than 15 years in support, management, and technical sales roles in Fortune 500 and not-for-profit organizations. She has contributed quarterly articles to EMC-Now print magazine, provided technical editing for On Magazine, written monthly and quarterly newsletters for a Fortune 25 company, and has been a writer and contributor to a weekly corporate marketing/technical blog. Erin is an avid runner and lover of technology.

Available as an eTextbook through VitalSource and CourseSmart!
Security Strategies in Windows Platforms and Applications

Michael G. Solomon

The majority of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Written by an industry expert, Security Strategies in Windows Platforms and Applications focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and step-by-step examples, this must-have resource will ensure readers are educated on the latest Windows security strategies and techniques.

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certificate level.

Applied Labs:
- Lab #1: Configure Active Directory and Implement Departmental and User Access Controls
- Lab #2: Implement Access Control Lists to Secure Folders and Read/Write/Access to Files
- Lab #3: Enable Encryption on a Microsoft Server to Ensure Confidentiality
- Lab #4: Identify, Remove, and Verify Malware and Malicious Software on a Microsoft Workstation
- Lab #5: Configure Access Rights to Folder & Files Using Microsoft GPO Manager & Enable Microsoft BSA to Define a Security Baseline Definition
- Lab #6: Perform a Microsoft Windows Server & Workstation Backup and Restoration
- Lab #7: Harden a Microsoft Workstation Using Security Configuration Wizard & Manual Configurations
- Lab #8: Apply Security Hardening on Windows Microsoft Server & Microsoft Client Applications
- Lab #9: Perform Digital Evidence Collection & Documentation Aligned with the Chain of Custody
- Lab #10: Perform a Security Baseline Definition Using MBSA to Harden a Microsoft Server


Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: The Microsoft Windows Security Situation
- Chapter 1: Windows and the Threat Landscape
- Chapter 2: Security in Microsoft Windows OS

Part 2: Managing and Maintaining Microsoft Windows Security
- Chapter 3: Access Controls in Microsoft Windows
- Chapter 4: Microsoft Windows Encryption Tools and Technologies
- Chapter 5: Protecting Microsoft Windows Against Malware
- Chapter 6: Group Policy Controls in Microsoft Windows
- Chapter 7: Microsoft Windows Security Profile and Audit Tools
- Chapter 8: Microsoft Windows Backup and Recovery Tools
- Chapter 9: Microsoft Windows Network Security
- Chapter 10: Microsoft Windows OS Security Administration

Part 3: Microsoft Windows OS and Application Security Trends and Directions
- Chapter 11: Hardening the Windows OS
- Chapter 12: Microsoft Application Security
- Chapter 13: Microsoft Windows Incident Handling and Management
- Chapter 14: Microsoft Windows and the Security Lifecycle
- Chapter 15: Best Practices for Microsoft Windows and Application Security

Key Features:
- Discusses the Microsoft Windows threat landscape.
- Highlights Microsoft Windows security features.
- Covers managing security in Microsoft Windows.
- Explains hardening Microsoft Windows operating systems and applications.
- Reviews security trends for Microsoft Windows computers.

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

About the Author:

Michael G. Solomon, CISSP, CISM, TICSA, is a full-time security speaker, consultant, and trainer, and a former college instructor who specializes in development and assessment security topics. As an IT professional and consultant since 1987, he has worked on projects or trained for over 60 major companies and organizations including EarthLink, Nike Corporation, Lucent Technologies, BellSouth, UPS, the U.S. Coast Guard, and Norrell. From 1998 until 2001, he was an instructor in the Kennesaw State University’s Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications.
Security Strategies in Linux Platforms and Applications

Michael Jang
ISBN: 978-0-7637-9189-6 • Paperback • 512 pages • © 2011

Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system, using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Applied Labs:
- Lab #1: Install a Core Linux Operating System on a Server
- Lab #2: Configure Basic Security Controls on a Fedora Linux Server
- Lab #3: Apply Hardened User Account Management & Security Controls
- Lab #4: Apply Hardened Linux File System Security Controls
- Lab #5: Apply Hardened Security for Linux Services & Applications
- Lab #6: Apply Hardened Security for Controlling Access
- Lab #7: Apply Hardened Security for the Linux Kernel
- Lab #8: Implement Best Practices for Secure Software Management
- Lab #10: Define Linux OS & Application Backup & Recovery Procedures

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Courseware:


Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: Is Linux Really Secure?
Chapter 1: Security Threats to Linux
Chapter 2: Basic Components of Linux Security

Part 2: Layered Security and Linux
Chapter 3: Basic Security: Facilities Through the Boot Process
Chapter 4: User Privileges and Permissions
Chapter 5: Filesystems, Volumes, and Encryption
Chapter 6: Every Service Is a Potential Risk
Chapter 7: Networks, Firewalls, and More
Chapter 8: Networked Filesystems and Remote Access
Chapter 9: Networked Application Security
Chapter 10: Kernel Security Risk Mitigation

Part 3 Building a Layered Linux Security Strategy
Chapter 11: Managing Security Alerts and Updates
Chapter 12: Building and Maintaining a Security Baseline
Chapter 13: Testing and Reporting
Chapter 14: Detecting and Responding to Security Breaches
Chapter 15: Best Practices and Emerging Technologies

Key Features:

- Focuses on Linux as a server operating system.
- Covers every major aspect of security on a Linux system.
- Explores open source and proprietary tools when building a layered security strategy for your Linux operating system.
- Offers step-by-step instructions for identifying weaknesses and creating more secure systems.

About the Author:

Michael Jang (RHCE, LPIC-2, UCP, Linux+, MCP) has been a freelance technical writer since 1998. He had previously worked for more than 10 years as a specialist engineer at Boeing Commercial Airplane Group. Michael has written white papers on new products and processes. He’s also the author of more than two-dozen IT books, including LPIC-1 In Depth (2009) and Ubuntu Server Administration Course (for VTC in 2009). Finally, Michael travels overseas extensively to troubleshoot IT issues and manage projects.
Network Security, Firewalls, and VPNs

J. Michael Stewart

Network Security, Firewalls, and VPNs provides a comprehensive and accessible look at the major business challenges and threats that are introduced when an organization’s network is connected to the public Internet. Written by an industry expert, this book provides an in-depth explanation of network security basics, including how hackers access online networks, and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

Applied Labs:
- Lab #1: Analyze Essential TCP/IP Networking Protocols
- Lab #2: Network Documentation
- Lab #3: Network Discovery & Security Scanning using ZenMap GUI (Nmap)
- Lab #4: Perform a Software Vulnerability Scan & Assessment with Nessus® (Nessus is a Registered Trademark of Tenable Network Security, Inc.)
- Lab #5: Configure a Microsoft Windows Workstation Internal Firewall
- Lab #6: Design a De-Militarized Zone (DMZ) for a LAN-to-WAN Ingress/Egress
- Lab #7: Implement a VPN Tunnel for Secure Remote-Access
- Lab #8: Design a Layered Security Strategy for an IP Network Infrastructure
- Lab #9: Construct a Linux Host Firewall and Monitor for IP Traffic
- Lab #10: Design and Implement Security Operations Management Best Practices

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Courseware:

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: Foundations of Network Security
- Chapter 1: Fundamentals of Network Security
- Chapter 2: Firewall Fundamentals
- Chapter 3: VPN Fundamentals
- Chapter 4: Network Security Threats and Issues

Part 2: Technical Overview of Network Security, Firewalls, and VPNs
- Chapter 5: Network Security Implementation
- Chapter 6: Network Security Management
- Chapter 7: Exploring the Depths of Firewalls
- Chapter 8: Firewall Deployment Considerations
- Chapter 9: Firewall Management and Security Concerns
- Chapter 10: Using Common Firewalls
- Chapter 11: VPN Management
- Chapter 12: VPN Technologies

Part 3: Implementation, Resources, and the Future
- Chapter 13: Firewall Implementation
- Chapter 14: Real-World VPNs
- Chapter 15: Perspectives, Resources, and the Future

Key Features:
- Introduces the basics of network security—exploring the details of firewall security and how VPNs operate.
- Illustrates how to plan proper network security to combat hackers and outside threats.
- Discusses firewall configuration and deployment as well as managing firewall security.
- Identifies how to secure local and Internet communications with a VPN.

Visit www.issaseries.com to Learn More

About the Author:

James Michael Stewart has been working with computers and technology for more than 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job-skill and certification courses such as CISSP, CEH, and Security+. He is the primary author of the CISSP Study Guide 4th Edition and the Security+ 2008 Review Guide. In addition, Michael has written numerous books on other security and Microsoft certification and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, iNet+. He graduated in 1992 from the University of Texas at Austin with a bachelor’s degree in Philosophy.
Computer hacking is a damaging and dangerous crime that information systems security professionals have to understand and prepare for. Written by industry experts, *Hacker Techniques, Tools, and Incident Handling* examines the landscape, key terms, and concepts that security professionals need to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It provides a technical overview of hacking and reviews the various methods attackers use, including footprinting, postscanning, enumeration, malware, sniffers, and denial of service. The book closes with an overview of incident response and defensive technologies, discussing how to respond to hacking attacks and how to fend them off.

The Complete Curriculum Solution!

The *Information Systems Security & Assurance Course Curriculum* provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor’s or certificate level.

**Applied Labs:**
- Lab #1: Develop an Attack & Penetration Test Plan
- Lab #2: Implement Hashing & Encryption for Secure Communications
- Lab #3: Perform Data Gathering and Foot-printing on a Targeted Website
- Lab #4: Compromise and Exploit a Vulnerable Microsoft Workstation/Server
- Lab #5: Perform a Website & Database Attack by Exploiting Identified Vulnerabilities
- Lab #6: Identify & Mitigate Malware & Malicious Software on a Windows Server
- Lab #7: Conduct a Network Traffic Analysis & Baseline Definition
- Lab #8: Audit and Implement a Secure WLAN Solution
- Lab #9: Perform Incident Response for Linux and Microsoft Workstations
- Lab #10: Design and Implement SNORT as an Intrusion Detection System (IDS)

**Instructor’s Material:**
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

**Courseware:**


**Learning Management System Options:**
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning’s Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning’s customizable course content delivery solution.
Textbook Table of Contents:

Part 1: Hacker Techniques and Tools
Chapter 1: The Evolution of Hacking
Chapter 2: TCP/IP Review
Chapter 3: Cryptographic Concepts
Chapter 4: Physical Security

Part 2: A Technical Overview of Hacking
Chapter 5: Footprinting Tools and Techniques
Chapter 6: Portscanning
Chapter 7: Enumeration and Computer System Hacking
Chapter 8: Wireless Vulnerabilities
Chapter 9: Web and Database Attacks
Chapter 10: Trojans and Backdoors
Chapter 11: Malware, Worms, and Computer Viruses
Chapter 12: Sniffers, Session Hijacking, and Denial of Service
Chapter 13: Linux, Live CDs, and Automated Assessment Tools

Part 3: Incident Response and Defensive Technologies
Chapter 14: Incident Response
Chapter 15: Defensive Technologies

Key Features:

- Examines the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals.
- Covers the history of hacking and the standards of ethical hacking.
- Examines the technical overview of hacking: how attacks target networks and the methodology they follow.
- Reviews incident response and defensive technologies: how to respond to hacking attacks and how to fend them off.

About the Authors:

Sean-Philip Oriyano has been actively working in the IT field since 1990. Throughout his career, he has held positions as support specialist to consultants and senior instructor. Currently he is an IT instructor who specializes in infrastructure and security topics for various public and private entities. Sean has instructed for the US Air Force, Navy, and Army at locations both in North America and internationally.

Michael Gregg, CISSP, is the president of Superior Solutions, Inc., a Houston based training and consulting firm. He has more than 20 years experience in the IT field. He holds two associate's degrees, a bachelor's degree, and a master's degree. He has consulted and taught for many organizations, and he is a 9-time winner of Global Knowledge's Perfect Instructor Award.
Security Strategies in Web Applications and Social Networking

Mike Harwood

Security Strategies in Web Applications and Social Networking provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercise, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certificate level.

Applied Labs:
Lab #1: Evaluate Business World Transformation – Impact of the Internet and WWW
Lab #2: Engage in Internet Research to Obtain Useful Personal Information
Lab #3: Perform a Post-Mortem Review of a Data Breach Incident
Lab #4: Exploit Known Web Vulnerabilities on a Live Web Server
Lab #5: Apply OWASP to a Web Security Assessment
Lab #6: Align Compliance Requirements to FISMA, SOX, HIPAA, GLBA, PCI DSS and AICPA
Lab #7: Perform Dynamic and Static Quality Control Testing
Lab #8: Perform an IT & Web Application Security Assessment
Lab #9: Recognize Risks & Threats Associated with Social Networking & Mobile Communications
Lab #10: Build a Web Application & Security Lifecycle Plan

Instructor's Material:
- PowerPoint Lectures
- Instructor's Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Courseware:

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning's Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning's customizable course content delivery solution.
Textbook Table of Contents:

Part 1: Evolution of Computing, Communications, and Social Networking
Chapter 1: From Mainframe to Client-Server to World Wide Web
Chapter 2: From Brick-and-Mortar to E-commerce to E-business Transformation
Chapter 3: Evolution of People-to-People Communications
Chapter 4: From Personal Communication to Social Networking

Part 2: Secure Web-Enabled Application Deployment and Social Networking
Chapter 5: Mitigating Risk When Connecting to the Internet
Chapter 6: Mitigating Web Site Risks, Threats, and Vulnerabilities
Chapter 7: Introducing the Web Application Security Consortium (WASC)
Chapter 8: Securing Web Applications
Chapter 9: Mitigating Web Application Vulnerabilities
Chapter 10: Maintaining PCI DSS Compliance for E-commerce Web Sites
Chapter 11: Testing and Quality Assurance for Production Web Sites
Chapter 12: Performing a Web Site Vulnerability and Security Assessment

Part 3: Web Applications and Social Networking Gone Mobile
Chapter 13: Securing End-Point Device Communications
Chapter 14: Securing Personal and Business Communications
Chapter 15: Web Application Security Organizations, Education, Training, and Certification

Key Features:
- Addresses Web security issues and solutions from administrator, developer, and user perspectives.
- Provides comprehensive coverage of Web attacks.
- Covers penetration testing of production Websites.
- Examines mobile devices and connectivity security.

About the Author:
Mike Harwood (MCT, MCSE, A+, Network+, Server+, Linux+) has more than 15 years experience working in information technology and related fields. In that time, he’s held a number of roles within IT, including network administrator, instructor, technical writer, Web site designer, consultant, and online marketing strategist. He’s been a regular on-air technology contributor for CBC Radio and has written numerous computer books, including the best-selling Network+ Exam Cram for Que Publishing and the A+ Faster Smarter title for Microsoft. Currently Mike is employed as the new editor and writer for the yoursecondfifty.com/magazine.
System Forensics, Investigation, and Response

John R. Vacca and K Rudolph

Computer crimes call for forensics specialists, people who know how to find and follow the evidence. System Forensics, Investigation, and Response begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field.

Visit www.issaseries.com to Learn More

The Complete Curriculum Solution!

The Information Systems Security & Assurance Course Curriculum provides a flexible, interactive curriculum solution with complete courseware, covering all the essential topics needed to support a variety of Information Security programs at the associate, bachelor's or certificate level.

Applied Labs:
- Lab #1: Perform a Byte-Level Computer Audit
- Lab #2: Apply the Daubert Standard on the Workstation Domain
- Lab #3: Create a Mock Forensic System Image for Analyzing Forensic Evidence
- Lab #4: Uncover New Digital Evidence Using Bootable Utilities
- Lab #5: Automate Digital Evidence Discovery Using Paraben's P2 Commander
- Lab #6: Apply Steganography to Uncover Modifications to an Image File
- Lab #7: Monitor & Define a Baseline Definition for Network Traffic
- Lab #8: Automate Image Evaluations and Identify Suspicious or Modified Files
- Lab #9: Craft an Evidentiary Report for a Digital Forensics Case
- Lab #10: Perform an Incident Response Investigation for a Suspicious Login

Instructor’s Material:
- PowerPoint Lectures
- Instructor’s Guide
- Test and Quiz Items
- Sample Syllabus
- Case Scenarios/Handouts

Courseware:

Learning Management System Options:
- Deliver your course in our LMS through Navigate™, Jones & Bartlett Learning's Premier Teaching and Learning System.
- All resources and course material can be fully integrated into your current LMS using JBL Integrate™, Jones & Bartlett Learning's customizable course content delivery solution.
Textbook Table of Contents:

**Part 1: The System Forensics Landscape**
- Chapter 1: System Forensics Fundamentals
- Chapter 2: Overview of Computer Crime
- Chapter 3: Challenges of System Forensics
- Chapter 4: Forensics Methods and Labs

**Part 2: Technical Overview: System Forensics Tools, Techniques, and Methods**
- Chapter 5: System Forensics Technologies
- Chapter 6: Controlling a Forensic Investigation
- Chapter 7: Collecting, Seizing, and Protecting Evidence
- Chapter 8: Understanding Information-Hiding Techniques
- Chapter 9: Recovering Data
- Chapter 10: Investigating and Scrutinizing E-mail
- Chapter 11: Performing Network Analysis
- Chapter 12: Searching Memory in Real Time with Live Systems Forensics

**Part 3: Incident Response, Future Direction, and Resources**
- Chapter 13: Incident/Intrusion Response
- Chapter 14: Trends and Future Directions
- Chapter 15: System Forensics Resources

Key Features:

- Examines the fundamentals of system forensics: what forensics is, an overview of computer crime, the challenges of system forensics, and forensics methods and labs.
- Addresses the tools, techniques, and methods used to perform computer forensics and investigation.
- Discusses collecting evidence, investigating information-hiding, recovering data, scrutinizing e-mail, and searching memory in real time.
- Explores incident and intrusion response, emerging technologies and future directions of this field, and additional system forensics resources.

About the Authors:

**John Vacca** is an information technology consultant and internationally known best-selling author based in Pomeroy, Ohio. Since 1982, John has authored 62 books and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA’s space station program (Freedom) and the International Space Station Program from 1988 until his retirement from NASA in 1995. In addition, John is also an independent online book reviewer. Finally, John was also one of the security consultants for the MGM movie, “AntiTrust,” which was released in 2001.

**K. Rudolph** (CISSP) has given numerous presentations and taught courses on computer security during her career. She’s been a speaker on security awareness at events held by the Internal Revenue Service, Defense Logistics Agency, Census Bureau, National Oceanic and Atmospheric Administration, and more. Ms. Rudolph has also been the primary author of a chapter on security awareness in the *Computer Security Handbook, Vol. 5* as well as for the *Handbook of Information Security*. The Federal Information Systems Security Educators’ Association named her its Security Educator of the Year in 2006.