Security and Risk Management

Learning Objectives:
This module will help you understand and apply fundamental principles of confidentiality, integrity, and availability in information security. Gain the skills to implement and manage security governance, address legal and regulatory issues, develop security policies and procedures, and identify and prioritize business continuity and disaster recovery requirements.

Topics:

- Understand and apply concepts of confidentiality, integrity, and availability.
- Implement and manage security governance principles.
- Understand legal and regulatory issues related to information security.
- Develop and implement security policies, standards, procedures, and guidelines.
- Identify, analyze, and prioritize business continuity and disaster recovery requirements.

Asset Security

Learning Objectives:
In this module, you will learn to identify and classify information assets, understanding their value and importance. You will also gain insights into ownership determination, privacy protection, data retention, and data security controls to safeguard these assets effectively.

Topics:

- Identify and classify information assets.
- Determine and maintain ownership.
- Protect privacy.
- Ensure appropriate data retention.
- Determine data security controls.

Security Architecture and Engineering

Learning Objectives:

In this module, you will implement and manage engineering processes using secure design principles, ensuring the application of effective security measures. You will also gain a solid understanding of security models, enabling you to select appropriate controls based on system security requirements. Additionally, you will learn to assess and mitigate vulnerabilities in systems and software, ensuring the overall security of information systems.

Topics:

- Implement and manage engineering processes using secure design principles.
- Understand the fundamental concepts of security models.
- Select controls based on systems security requirements.
- Understand the security capabilities of information systems.
- Assess and mitigate vulnerabilities in systems and software.

Communication and Network Security

Learning Objectives:

In this module, you will learn how to implement secure network architecture designs to ensure the integrity and confidentiality of network systems. You will gain knowledge in securing network components, implementing secure communication channels, and preventing or mitigating network attacks. Additionally, you will develop skills in managing identity and access management to control user privileges and enhance overall network security.

Topics:

- Implement secure network architecture designs.
- Secure network components
- Implement secure communication channels.
- Prevent or mitigate network attacks.
- Manage identity and access management.

Identity and Access Management (IAM)

Learning Objectives:
Learn to control access to assets physically and logically, manage identification and authentication, implement authorization mechanisms, prevent access control attacks, and manage the identity lifecycle.

Topics:

- Control physical and logical access to assets
- Manage identification and authentication of people and devices.
- Implement and manage authorization mechanisms.
- Prevent or mitigate access control attacks.
- Manage the identity lifecycle.

Security Assessment and Testing

Learning Objectives:
Learn how to design and validate assessment and test strategies to ensure the effectiveness of security controls. You will gain skills in conducting security control testing, collecting security process data, and analyzing and reporting test outputs. Additionally, you will develop knowledge in conducting or facilitating security audits to evaluate the overall security posture of an organization.

Topics:

- Design and validate assessment and test strategies.
- Conduct security control testing.
- Collect security process data.
- Analyze and report test outputs.
- Conduct or facilitate security audits.

Security Operations

Learning Objectives:

In this module, you will gain an understanding of how to support investigations and adhere to the requirements for physical and environmental security. You will learn how to implement and support patch and vulnerability management to maintain the security of systems. Additionally, you will develop the skills to implement and manage security operations and apply incident management concepts to effectively respond to security incidents.

Topics:

- Understand and support investigations.
- Understand requirements for physical and environmental security.
- Implement and support patch and vulnerability management.
- Implement and manage security operations.
- Understand and apply incident management concepts.

Software Development Security

Learning Objectives:

In this module, you will learn to understand the importance of integrating security throughout the Software Development Lifecycle (SDLC) and how to effectively apply security controls in software development environments. You will gain the skills to assess the effectiveness of software security and identify as well as mitigate vulnerabilities in software. Additionally, you will learn and implement secure coding practices to ensure the development of secure and resilient software applications.

Topics:

- Understand and integrate security throughout the Software Development Lifecycle (SDLC)
- Identify and apply security controls in software development environments.
- Assess the effectiveness of software security.
- Identify and mitigate vulnerabilities in software.
- Implement secure coding practices.

CISSP Exam Preparation

Learning Objectives:

Get introduced to computer adaptive testing (CAT) through our comprehensive guide to passing the CISSP exam. You will learn about the principles and benefits of CAT, explore the CISSP exam structure and content, and develop effective study strategies and exam preparation techniques. By the end of this module, you will be well-prepared to confidently and efficiently tackle the CISSP exam using CAT.

Topics:

- Introduction to Computer Adaptive Testing
- Guide to Passing CISSP Exam

Complementary Courses Worth US$ 10,000

1) Becoming a Cyber Security Professional - A Beginner's Career Guide *[On-Demand Course]*

Master the fundamentals of cybersecurity, explore diverse job roles, and gain comprehensive knowledge to kickstart your career in this high-demand field. Acquire the essential skills, certifications, and practical expertise needed to become a true cybersecurity expert. Uncover top job search sites and networking strategies to secure a rewarding career and excel in the cybersecurity industry.

- Course Duration: **2 Hours**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

2) Cyber Security for Absolute Beginners - 2022 Edition - Part 01 *[On-Demand Course]*

Master the art of cyber security and safeguard systems from relentless cyberattacks. Explore the world of hackers, their methods, and the tools to combat them. Gain comprehensive knowledge to become a skilled cyber security professional and defend against evolving digital threats.

- Course Duration: **3 Hours 28 Minutes**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

3) Cyber Security for Absolute Beginners - 2022 Edition - Part 02 *[On-Demand Course]*

Gain a strong foundation in cyber security, focusing on networking, privacy, and malware defense. Master TCP/IP, and DNS, and safeguard online privacy. Learn advanced techniques like VPNs, Tor, antimalware tools, backups, encryption, and social engineering defense to become a skilled cybersecurity professional.

- Course Duration: **6 Hours**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

4) Practical Cyber Hacking Skills for Beginners *[On-Demand]*

Master the art of cybersecurity, protecting computers and networks from digital threats. From Kali Linux to phishing techniques, gain hands-on skills in network security and scanning tools. Become an expert in incident response and data protection, forging a successful career in the ever-evolving world of cybersecurity.

- Course Duration: **8 Hours 20 Minutes**
- Author: **Alexander Oni**, Cyber Security Expert, Web Developer, and Instructor

5) Web Hacker's Toolbox - Tools Used by Successful Hackers *[On-Demand]*

Master the essential toolbox of ethical hackers and penetration testers. Learn to use SQL map for automated SQL injection, Google Hacking for web app security, and Burp Suite Intruder for fuzzing. Exploit race conditions with OWASP ZAP and elevate your penetration testing skills for real-world projects.

- Course Duration: **3 Hours**
- Author: **Dawid Czagan**, Founder and CEO at Silesia Security Lab, and Trainer

6) Web Hacking Expert – Full-Stack Exploitation Mastery *[On-Demand]*

Dive into full-stack exploitation to master modern web attacks. Learn to bypass Content Security Policy (CSP), hack through PDFs, images, and links, and steal secrets from AngularJS applications. Learn to exploit race conditions and discover powerful attacks like HTTP parameter pollution, subdomain takeover, and clickjacking.

- Course Duration: **4 Hours 46 Minutes**
- Author: **Dawid Czagan**, Founder and CEO at Silesia Security Lab, and Trainer

7) Linux Crash Course for Beginners – 2023 *[On-Demand]*

Master Linux's system administration, understand its open-source nature and navigate the file system with essential commands. Gain fundamental Linux command line skills and grasp the inner workings of this powerful operating system.

- Course Duration: **5 Hours 47 Minutes**
- Author: **Imran Afzal**, Systems Engineer, Entrepreneur, Instructor, and Public Speaker

8) Complete Python Course with 10 Real-World Projects *[On-Demand]*

Master Python programming from basics to advanced. Learn OOP, libraries like Matplotlib and Flask, and build ten practical applications. Gain proficiency to create executable Python programs independently.

- Course Duration: **27 Hours 7 Minutes**
- Author: **Ardit Sulce**, Python programmer, teacher, and founder of Python How