Hello, and welcome!

Every day, we hear about security breaches. They can impact government agencies, hospitals, and companies of all sizes. Keeping information safe can seem like a never-ending battle! In this course, you will learn information security terms. You will explore the principles, processes, and best practices for protecting data. In addition, you will study security weaknesses that can affect everyone. Along the way, you will discover strategies for combatting cyberattacks.

We invite you to take a minute to learn about the course by reviewing the information that follows. This way, you will be better able to understand the expectations of the course as a whole. Then you can determine how to manage your time and efforts as you navigate through it.

You are in the right place. You belong here. You can do this!
Course Description and Competencies

What to Expect

This course is divided into four modules, focusing on various concepts. These are Access, Accountability, Security, and Devices and Testing. The course materials include readings, practice quizzes, videos, and lab activities. These will help prepare you to demonstrate your achievement of three competencies.

There is no prerequisite for this course and there is no specific technical knowledge needed.

This course covers the following competencies:

1. The learner identifies security principles, policies, practices, and methods for asset protection and cyber defense.
2. The learner identifies security requirements based on principles of confidentiality, integrity, and availability.
3. The learner identifies cybersecurity guidelines in privacy and compliance.

The objective assessment allows you to demonstrate three core competencies from the course. You will have two attempts to pass the exam.

• 1 final exam • 3 competency units
# Course Outline

<table>
<thead>
<tr>
<th>Module</th>
<th>Upon completion of this module, you will be able to:</th>
</tr>
</thead>
</table>
| **1. Access** | A. Define information security and the risk management process and stages.  
B. Classify cybersecurity concepts and tools according to the type of vulnerability they find, identify, and protect.  
C. Define compliance, including regulatory and industry compliance.  
D. Compare identification, identity verification, and authentication.  
E. Explain authorization and access control and the considerations for which systems to use. |
| **2. Accountability** | A. Explain how to use accountability techniques to trace the activities of users and then use auditing to ensure accuracy.  
B. Describe how to use modern cryptography techniques to enhance information security.  
C. Categorize cybersecurity principles and defense concepts according to area of impact.  
D. Differentiate between privacy and regulatory and industry compliance.  
E. Define FISMA, HIPAA, SOX, FERPA, and GLBA, including their purpose and main components. |
B. Explain how physical security and network security are used to protect people, equipment, and data.  
C. Identify the six main ways to decrease attack surface through hardening and how can they be used to prevent attacks.  
D. Explain how to determine if security measures are protecting assets.  
E. Identify the main software development vulnerabilities and how you can use applications security to account for them. |
4. Devices & Testing

A. Identify security issues particular to mobile devices, embedded devices, and IoT.
B. Identify mobile device management, deployment models, and areas of embedded security.
C. Explain how to determine if security measures are protecting assets.
D. Explain how to conduct a vulnerability assessment, penetration testing, and realistic testing.

Technology Requirements

We want you to have the tools to succeed! Since this course includes at least one proctored test, please be sure to have a working microphone, speakers, and an external webcam. Unfortunately, an internal webcam (built into many laptops) is not acceptable. (Note: The external webcam is required only for exams that have proctors. You do not need one for practice tests and other non-proctored assessments.) For other details about the technology you’ll need, review the Computer System and Technology Requirements. If you have questions about your setup, contact support@academy.wgu.edu.

You will need Adobe Acrobat Reader DC. If you haven’t already, download this free software. You may encounter an interactive form that contains fields that you can select or fill in. Review how to fill in a PDF form.

Key Contacts

Your Fellow Learners

Check out the Fundamentals of Information Security Lobby in the course site! In this online community, you can ask questions and explore ideas. You can connect with your fellow learners. When you use this site, you will realize that other learners may have the same questions you have. You can all benefit from learning together!

Technical Support

If you encounter technical issues, be sure to contact the Help Desk. Just submit a Support Request for assistance.
Do you have questions about your account? Student Support has answers. They can help with billing, switching courses, and other requests. You can contact them at (888) 320-0540 or support@academy.wgu.edu.

Accommodations

WGU provides compliant and accessible learning experiences. If you require accommodation, please contact us at the start of the course. You can email StudentAffairs@academy.wgu.edu or call (888) 320-0540. We are committed to ensuring that all students with disabilities have equal access to WGU's services and materials. We strive to use best practices for accessibility. Our goal is to conform to existing U.S. laws. These include the Americans with Disabilities Act and Section 504 and Section 508 of the Rehabilitation Act. Our learning management system (LMS) platform is Open edX. Open edX's commitment to accessible content is published on their Website Accessibility Policy.