# CompTIA Security+ SY0-601 Exam Prep

## Florida Cybersecurity Training Program

## Offered by the University of West Florida Center for Cybersecurity

## Course Overview

**Course / Cyber Skills Exercise Dates:** 05 Feb. – 05 Apr. 2024

**Cyber Skills Exercise Times:** N/A

**Duration:** 8 weeks + 1 test week

**Estimated Time Commitment:** 20 hours per week for individuals with pre-requisite knowledge; 20+ hours per week for individuals with no prior professional experience or technical education.

**Instructional Hours:** 40 contact hours

**Delivery Format:** Asynchronous online with weekly instructor Zoom sessions.

**Target Audience:** Early career IT practitioners with a security function 1+-years' experience recommended, college graduates with hands-on cybersecurity course backgrounds, uniformed and civilian personnel subject to DoD Regulation 8570/8140.

**Required Prerequisites / Background:** Recommended (CompTIA) minimum 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts and networking. Network+ certification or equivalent is highly recommended.

**CEU's:** 4.0, **CPE's:** 48

**Course Instructor**

| Instructor | Email Address |
|---|---|
| Guy Garrett, M.S., M.B.A. | ggarrett@uwf.edu |

## Course Description

This course has one purpose – preparing you to take and pass the CompTIA Security+ exam. The goal is mastering concepts, terminology, processes, and procedures to the point that you can accurately apply them to various situations.

**What is Sec+?**
Sec+ is a global industry certification that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career.

**What should a successful candidate know and be able to do?**

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

**How to succeed in this course.**

- Manage your time. Most students average 20-30 hours/week for exam prep.
- Actively engage your instructor.
- Do the labs and watch the demonstrations. This test is performance-based. Hands-on work is the key to conquering situation-based questions.

## NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

**Cybersecurity Work Roles and Categories:**
**Operate and Maintain**

- Technical Support Specialist (OM-STS-001)
- Network Operations Specialist (OM-NET-001)
- System Administrator (OM-ADM-001)

**Securely Provision**

- Security Control Assessor (SP-RSK-002)

**Oversee and Govern**

- Information Systems Security Manager (OV-MGT-001)

## Course Information

**Materials**

- Course organization, including assignments, grading, and instructor-student communication will be done through the Canvas learning management system (LMS).

- This course uses a variety of materials, including the official curriculum from CompTIA-TestOut. Students will be given access codes and instructions on the first day of class to access these resources and connect to the correct class.

**Technical Specifications**

- Reliable high speed Internet connection | Computer with up-to-date browser.
- Students should have a computer with microphone, speakers, camera (optional), capable of running Zoom sessions.

**Student Accessibility Resources:**

If you have a disability that impacts your full participation in this course, please email Student Accessibility Resources at 850.474.2387 or by email, sar@uwf.edu.

**Grading**

This course is designed for workforce development and focuses on concept and task mastery learning. Students are required to complete 70% of all assigned material in order to pass the course and receive a digital badge. **Doing only 70% of the assignments is not sufficient to pass the certification exam.**

**Assignments are rated based on the following scale.**

| Rating | Requirements | Progress |
|---|---|---|
| 4 | Scored 90% or higher on the assignment | Likely to pass cert exam |
| 3 | Scored 80%-89% on the assignment | Possibly pass cert exam |
| 2 | Scored 70%-79% on the assignment | Requires remediation to pass cert exam |
| 1 | Scored >70% on the assignment | Unlikely to pass cert exam |
| 0 | Failed to complete the assignment | Will not pass cert exam |

**Course Outline**

**Assessments: PBQs, Labs, Practice Exams, Certification Exam**

**Module 1 – Domain 5 Governance, Risk, and Compliance**

1. Compare and contrast various types of controls
2. Explain applicable regulations, standards, or frameworks to that impact organizational security posture
3. Explain the importance of policies to organizational security
4. Summarize risk management processes and concepts
5. Explain privacy and sensitive data concepts in relation to security

**Module 2 -- Domain 1 Threats, Attacks, and Vulnerabilities**

1. Compare and contrast different types of social engineering techniques
2. Given a scenario, analyze potential indicators to determine the type of attack
3. Given a scenario, analyze potential indicators associated with application attacks

4. Given a scenario, analyze potentail indicators associated with network attacks
5. Explain different threat actors, vectors, and intelligence sources
6. Explain security concerns associated with various types of vulnerabilties
7. Summarize the techniques used in security assessments
8. Explain techniques used in penetration testing

**Module -- 3 Domain 2 Architecture & Design**

1. Explain the importance of security concepts in an enterprise environment
2. Summarize virtualization and cloud computing concepts
3. Summarize secure application development, deployment, and automation concepts
4. Summarize authentication and authorization design concepts
5. Given a scenario, implement cybersecurity resilience
6. Explain the security implications of embedded and specialized systems
7. Explain the importance of physical security controls
8. Summarize the basics of cryptographic concepts

**Module -- 4 Domain 3 Implementation**

1. Given a scenario, implement secure protocols
2. Given a scenario, implement host or application security solutions
3. Given a scenario, implement secure network designs
4. Given a scenario, install and configure wireless security settings
5. Given a scenario, implement secure mobile solutions
6. Given a scenario, apply cybersecurity solutions to the cloud
7. Given a scenario, implement identity and account management controls
8. Given a scenario, implement authentication and authorization solutions
9. Given a scenario, implement public key infrastructure

**Module -- 5 Operations and Incident Response**

1. Given a scenario, use the appropriate tool to assess organizational security
2. Summarize the importance of policies, processes, and procedures for incident response
3. Given an incident, utilize the appropriate data sources to support an investigation
4. Given an incident, apply migitation techniques or controls to secure an environment
5. Explain the key aspects of digital forensics