This course supports the assessments for LKT2. The course covers 3 competencies and represents 2 competency units.

**Introduction**

**Overview**
This course focuses on the practices of designing, maintaining, and securing computer networks. This component of your work at WGU is designed to help you gain a broad overview of the field of network management with a fundamental understanding of some key concepts and principles related to network security.

Building from your prior work in network architecture, network security, and wireless technologies, you will learn how security theory and network design are applied in real-world situations, the compromises that must be considered, and the inherent tradeoffs between security and ease-of-access that are made when applying a security theory and network design.

Network security specialists are in high demand and hold critical positions in organizations that require secured storage along with access to and availability of business's critical information and information assets. The content you learn and the competencies you demonstrate as you work through the course of study will be invaluable in your role in network security.

Watch the following video introduction for the course:

*Note: To download this video, right-click the following link and choose "Save as...": [download video]*

Watch the Getting Started video for this course:

*Note: To download this video, right-click the following link and choose "Save as...": [download video]*

**Competencies**
This course provides guidance to help you demonstrate the following 3 competencies:

- **Competency 426.1.3: Security Policy Evaluation**
  The graduate identifies and evaluates current federal security policies and demonstrates how these policies can be applied in an organizational setting.

- **Competency 426.1.7: Configuring Firewalls**
  The graduate analyzes and configures a firewall to protect against common threats.

- **Competency 426.1.8: Cryptography**
  The graduate evaluates common cryptology and encryption techniques for an encryption/decryption system.
Course Mentor Assistance
As you prepare to successfully demonstrate competency in this subject, remember that course mentors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course mentors are excited to hear from you and eager to work with you.

Successful students report that working with a course mentor is the key to their success. Course mentors are able to share tips on approaches, tools, and skills that can help you apply the content you're studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don't work out on your first try, course mentors act as a support system to guide you through the revision process. You should expect to work with course mentors for the duration of your coursework, and you are encouraged to contact them as soon as you begin. Course mentors are fully committed to your success!

Preparing for Success
The information in this section is provided to detail the resources available for you to use as you complete this course.

Learning Resources
The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

Automatically Enrolled Resources
You can access the learning resources listed in this section by clicking on the links provided throughout the course. You may be prompted to log in to the WGU student portal to access the resources.

SkillSoft and Books 24x7
You will access SkillSoft items at the activity level within this course. For more information on accessing SkillSoft items, please see the "Accessing SkillSoft Learning Resources" page.

The following Books24x7 e-texts will be used in this course:

Note: These e-texts are available to you as part of your program tuition and fees, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.

The following Books24x7 modules will be used in this course:

- Cisco ICND1 1.0: WAN Technologies and Routing
- Cisco IINS 1.0: Network Security Using Cisco IOS Firewalls

Pacing Guide

The pacing guide suggests a weekly structure to pace your completion of learning activities. It is provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.


Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.

Security Policy Evaluation

In this section you will learn how to analyze regulatory and policy entities. Network security has become an increasingly important part of network management, partially in response to post-9/11 governmental initiatives, and also as a result of organizations continuing to realize the costs of operating poorly secured network environments. Knowledge of the regulatory environment will help security managers perform required and recommended activities.

Security Policy

As you review the resources in this section, take notes and attempt to answer the following questions:

- What is the scope of each of the following regulations?
  - Federal Information Security Management Act (FISMA)
  - Homeland Security Presidential Directives (HSPDs)
  - North American Electrical Reliability Corporation (NERC) Cyber Security Standards
  - The USA PATRIOT Act
- How do the four regulations listed above interact with each other?
• What is the role of the National Security Agency in establishing and maintaining security policy for federal and private sector organizations?

This topic addresses the following competency:

• Competency 426.1.3: Security Policy Evaluation
  The graduate identifies and evaluates current federal security policies and demonstrates how these policies can be applied in an organizational setting.

**Reading: Compliance and Regulation**

Read the following sections in *The Complete Guide to Security and Privacy Metrics Measuring Regulatory Compliance, Operational Resilience and ROI*:

• sections 3.1, 3.10, 3.11, 3.12, and 3.14 of chapter 3 ("Measuring Compliance With Security and Privacy Regulation Standards")

These sections in chapter 3 address regulatory and policy entities for the Federal Information Security Management Act (FISMA), the Federal Office of Management and Budget (OMB), and the National Security Agency (NSA), and identifies policies related to completion and maintenance of accreditation or certification for federal information assurance requirements.

As you read through the assigned sections, keep in mind that you are preparing to discuss specific applications of FISMA and the roles the OMB and NSA play in creating and regulating policies related to federal information assurance.

**Hands-On: Quest for Reference URLs**

Conduct an internet search to locate and browse the websites of the following four agencies:

• FISMA
  • FAQs
  • Compliance
• Homeland Security
  • Presidential Directives
• NIST
  • NIST SP 800-59 Guideline for Identifying an Information System as a National Security System
  • NIST - NIST SP 800-37 Guide to Applying the Risk Management Framework
  • Six Step Risk Management Framework
  • NIST has a Risk management Framework training course
• NERC
  • Critical Infrastructure Protection
• OMB
  • CIRCULAR NO. A-130 Revised
  • OMB Memorandum M-10-15
Respond to the following questions in your notes:

- Why might you want to bookmark these websites?
- What type of information can you find there?
- How might familiarizing yourself with the agency websites help you with security policy evaluation?

**Establishing Organizational Policy and Guidelines**

Read the following section in *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI*:

- section 3.6 in chapter 3 ("Measuring Compliance with Security and Privacy Regulation Standards")

This section addresses the Organization for Economic Cooperation and Development (OECD) Privacy, Cryptography, and Security Guidelines adopted by nearly 30 different countries, including the United States.

As you read through the assigned sections, keep in mind that you are preparing to discuss specific policies and guidelines relevant to establishing compliance and/or accreditation related to information assurance.

Remember to use the message boards embedded in the course for additional feedback or to check your understanding with other students and the course mentor.

**Complete: RLKT Task 1 Performance Task**

Complete the following task in TaskStream:

- LKT2 Network Security: RLKT Task 1

For details about this performance assessment, see the "Assessment" tab in this course.

In this activity, you will submit a multimedia presentation in response to a scenario regarding Federal Regulations, Certification and Accreditation, and Compliance.

In your presentation, it is important that you

- analyze the applicable Federal regulations,
- discuss the relevance of agency policies,
explain the roles of relevant agencies, and
describe the process of certification and accreditation.

Configuration and Analysis of Firewalls

In this section you will learn that firewalls constitute the first line of defense when securing a network from malicious attacks, but even the best firewall will not be effective unless it is properly configured. Firewalls enhance network security by providing options a network administrator can configure using the virtual console that is hard-coded into the router device.

Configuring Firewalls

As you review the assigned reading and any outside references you identify, pay particular attention to the strengths and limitations of the various firewall features. Take note of the differences and similarities among the firewall features. Also, access your personal router/firewall and investigate the configuration.

Note: It is recommended that you DO NOT perform any investigation or make changes to production (i.e., live) firewalls. You should set up an area of your work or home network as test network. This will allow you to experiment and configure the network without worrying about crashing or compromising the current security features.

This topic addresses the following competency:

- Competency 426.1.7: Configuring Firewalls
  The graduate analyzes and configures a firewall to protect against common threats.

Reading: Understanding Firewalls and Proxy Servers

Read the following chapter in *Network + Study Guide & Practice Exams: Exam N10-003*:

- chapter 9 ("Network Infrastructure and Security")

In this chapter you will learn about configuring a firewall to perform network address translation (NAT), configuring a router to perform packet filtering, and configuring a router to act as a proxy server.

Additional SkillSoft Modules

The following SkillSoft course will help you review features and operations of WANS. It will also help you learn how to configure internet access using DHCP, NAT, and PAT on Cisco routers.

- ID: 254073_eng - Cisco ICND1 1.0: WAN Technologies and Routing
The following SkillSoft course will explain the operations of different types of firewall technologies that are embedded in Cisco routers and security appliances.

- ID: cc_iins_a04_it_enus - Cisco IINS 1.0: Network Security Using Cisco IOS Firewalls

Use the message boards embedded in the course for additional feedback or to check your understanding with other students and the course mentor.

**Complete: RLKT Task 2 Performance Task**

Complete the following task in [TaskStream](#):

- LKT2 Network Security: RLKT Task 2

For details about this performance assessment, see the "Assessment" tab in this course.

In this activity you will submit sections of a procedure manual in response to a scenario regarding support to remote users.

In your manual sections, it is important that you

- select specific network hardware and
- provide tutorials on Network Address Translation (NAT), packet filtering, and proxy server features of the device.

**Network Security**

Network planning and design is an integral part of reliable, scalable, and secure network environments.

**Network Infrastructure**

This section covers LAN technologies, network topologies, network devices, and network and protocol security mechanisms.

This topic addresses the following competency:

- Competency 426.1.7: Configuring Firewalls
  The graduate analyzes and configures a firewall to protect against common threats.

**Accountability, Attacks, Communications, and Countermeasures**

Read the following chapters in the *CISSP: Certified Information Systems Security Professional Study Guide*.
• chapter 1 ("Accountability and Access Control")
• chapter 2 ("Attacks and Monitoring")
• chapter 3 ("ISO Model, Protocols, Network Security, and Network Infrastructure")
• chapter 4 ("Communications Security and Countermeasures")

Access Control and Physical Security

This section covers the CIA triad, privacy, authentication, identification, encryption, and physical security.

This topic addresses the following competency:

• Competency 426.1.7: Configuring Firewalls
  The graduate analyzes and configures a firewall to protect against common threats.

Security Management and Concepts

Read the following chapters in the CISSP: Certified Information Systems Security Professional Study Guide:

• chapter 5 ("Security Management Concepts and Principles")
• chapter 19 ("Physical Security Requirements")

Use the message boards embedded in the course for additional feedback or to check your understanding with other students and the course mentor.

Public/Private Key Encryption

Public/private key encryption provides a secret handshake for communications between network nodes and preferential treatment for network traffic; it is a method to ensure that only the initiated computers can interpret the transmission and share the secret of the conversation. This type of encryption is more than a handshake, of course, and could be thought of as a fully disguised conversation across otherwise untrusted media.

In this section you will learn about data transmission security and how it is primarily possible due to encryption technologies that allow for private data to be securely transmitted across open, public networks. In order to encrypt and decrypt data, the end computers must share a code or key that allows only the receiving computer to decrypt the messages, while preventing other entities from reading the encoded message.

In order for two computers to exchange encrypted data, most networks use public/private key encryptions that allow two end computers to exchange secured data while simultaneously protecting them from unwanted access.

Cryptography
As you review this section's material, take notes and attempt to answer the following questions:

- What is the value of installing an SSL certificate on a web server?
- What is the value in using PKI over other forms of Key exchange?

Also, compare and contrast 40-, 128-, and 256-bit encryption.

This topic addresses the following competency:

- Competency 426.1.8: Cryptography
  The graduate evaluates common cryptology and encryption techniques for an encryption/decryption system.

**Encryption, and Public Key Infrastructures**

Read the following chapters in *User's Guide to Cryptography and Standards*:

- chapter 4 ("Encryption")
- chapter 13 ("Public Key Infrastructures")

As you progress through this material, pay particular attention in your notes to:

- differences between block ciphers, symmetric ciphers, and asymmetric ciphers;
- the process of creating or authenticating a public/private key policy; and
- the following terms: public key encryption, digital signatures, secure transmission, asymmetric key cryptography, and symmetric cryptography (private key).

Understanding the terms listed above will better prepare you to respond to the required tasks for this course.

Use the message boards embedded in the course for additional feedback or to check your understanding with other students and the course mentor.

**Developing the Performance Task: White Paper**

In this section you will develop a white paper for your third and final performance task. Review crucial concepts and skills associated with this course before you begin.

**Preparing for the Task**

Complete the following activities as you prepare to complete the performance task.

This topic addresses the following competencies:
• Competency 426.1.3: Security Policy Evaluation
The graduate identifies and evaluates current federal security policies and demonstrates how these policies can be applied in an organizational setting.
• Competency 426.1.7: Configuring Firewalls
The graduate analyzes and configures a firewall to protect against common threats.
• Competency 426.1.8: Cryptography
The graduate evaluates common cryptology and encryption techniques for an encryption/decryption system.

Review of Competencies and Associated Chapters

This course covers three competencies. The three competencies and their associated chapters are:

Competency 426.1.3: Security Policy Evaluation (p005241)
The graduate identifies and evaluates current federal security policies and demonstrates how these policies can be applied in an organizational setting.


Competency 426.1.7: Configuring Firewalls (p005245)
The graduate analyzes and configures a firewall to protect against common threats.


Competency 426.1.8: Cryptography (p005246)
The graduate evaluates common cryptology and encryption techniques for an encryption/decryption system.

- chapter 4 ("Encryption")

Complete: LKT Task 3 Performance Task

Complete the following task in TaskStream:

• LKT2 Network Security: LKT Task 3

For details about this performance assessment, see the "Assessment" tab in this course.
In this final activity you will submit a white paper, including a network diagram, in response to a scenario regarding the security challenges of combining two separate networks. The response will be submitted using TaskStream.

In your white paper, it is important that you

- diagram the existing networks and the potential combined network;
- summarize your plan for combining the resources;
- address the challenges inherent in your plan;
- discuss traffic routing on the new network (internal and Internet traffic); and
- provide mitigation for physical, logical, and information security threats in the newly combined environment.

**Final Steps**

Congratulations on completing the activities in this course! This course has prepared you to complete the assessments associated with this course. If you have not already been directed to complete the assessments, schedule and complete your assessments now.