This course supports the assessments for Cyberlaw, Regulations, and Compliance. The course covers 6 competencies and represents 3 competency units.

Introduction

Overview
Cyberlaw can be defined as the legal doctrines and principles applying to the operation and development of computer technology and the Internet. Due to the rapid advancement of technology during the last century, what was once viewed as science fiction has now become a part of daily life.

This course of study will prepare you to

- participate in relevant cyberlaw rules and regulations, and
- address governance standards, policies, and legislation pertaining to information security and assurance.

The proliferation of innovative technology has necessitated new legislation and judicial response to resolve evolving legal problems. This emerging area of law will impact you every day. The regulations and laws are ever changing; you must be aware of the steps necessary to research what currently governs the areas in which you work. Penalties for violation of these regulations and laws range from fines to imprisonment.

Watch the following video for an introduction to this course:

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

View the video in fullscreen at 720p for best results.

Competencies
This course provides guidance to help you demonstrate the following 6 competencies:

- **Competency 423.1.1: Standards & Legal Issues**
  The graduate develops a legal analysis addressing legal issues, standards, policies, legislation, and governance related to cybercrimes for enterprise systems.

- **Competency 423.1.3: Cyberterrorism & Homeland Security**
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.

- **Competency 423.1.4: Cyberagreements**
  The graduate explains the underlying principles governing e-commerce third-party vendor agreements and translates them into practical recommendations for the implementation of such agreements.
- **Competency 423.1.5: Regulatory Requirements & Standards**
  The graduate ensures alignment of regulatory requirements and standards with appropriate information security and assurance controls for organizations that process or hold privacy, financial, or medical information electronically.

- **Competency 423.1.6: Intellectual Property**
  The graduate selects appropriate business practices that ensure the protection of intellectual property.

- **Competency 423.1.7: Cybercrimes**
  The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.

**Course Instructor Assistance**

As you prepare to successfully demonstrate competency in this subject, remember that course instructors 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 instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors 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 instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are welcome to contact them as soon as you begin. Course instructors 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.

**VitalSource E-Text**

The following textbook is available to you as an e-text within this course. You will be directly linked to the specific readings required within the activities that follow.


Note: These e-texts are available to you as part of your program tuition and fees, but you may purchase a hard copy at your own expense through VitalSource or 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 sites provide instruction on how to create a VitalSource account, use features such as downloading your e-texts for offline use, and purchase a print-on-demand option, if available.

VitalSource Navigational Video

Print-On-Demand Option

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.

ANSI - ISO/IEC 27002 Standard

Log into the American National Standards Institute (ANSI) portal using the login credentials provided below to download the following documents.


***IMPORTANT - PLEASE READ BEFORE DOWNLOADING***

You can access this resource using the following information:

ANSI (ISO 27001/27002) Standards login instructions

ALL USERS must complete a one-time Standards Connect user registration.

Click on the following link to the Standards Connect user registration page:

http://asc.ansi.org/User/Register.aspx?rt=6a30e9c1-14e1-45bc-9704-011d86269f68

The required fields are marked with a "***", including the creation of a unique username and password known only to you and managed by you.

After you click REGISTER, you will automatically be logged into the Western Governors University account on Standards Connect.

View a results listing of your licensed content by clicking the VIEW MY DOCUMENTS link

LOGOUT: After 90 minutes of inactivity, you will be prompted to log in to Standards Connect again, which you can do at https://asc.ansi.org

TIP: Bookmark STANDARDS CONNECT https://asc.ansi.org in your web browser for quick login access to your content.

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.

- Pacing Guide: Cyberlaw

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.

Cyberlaw: Regulatory Requirements and Standards

Different types of information are protected by different regulatory requirements. Different categories of enterprises (e.g., insurance companies, financial institutions, educational institutions) have different regulatory requirements.

Introduction to Cyberlaw

This topic will introduce you to
- history of cyberlaw,
- content regulation in cyberspace,
- internet governance and regulation, and
- enterprise information security.

This topic addresses the following competencies:

- Competency 423.1.5: Regulatory Requirements & Standards
  The graduate ensures alignment of regulatory requirements and standards with appropriate information security and assurance controls for organizations that process or hold privacy, financial, or medical information electronically.

**Introduction to Cyberlaw**

Read the following chapter in *Cyberspace Law: Cases and Materials*:

- **chapter 1** ("Introduction to the Study of Cyberspace Law")

**Internet Governance and Regulation**

Read the following sections in *Cyberspace Law: Cases and Materials*:

- **section 2A** ("Cyberanarchy vs. Cyberorder") in **chapter 2** ("Regulating Cyberspace")
- **section 2B** ("Personal Jurisdiction") in **chapter 2** ("Regulating Cyberspace")
- **section 2C** ("Regulatory Authority") in **chapter 2** ("Regulating Cyberspace")

**Content Regulation in Cyberspace**

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 115 - 147 in **chapter 3** ("Speech in Cyberspace")

This reading will introduce you to cyberspace content regulation.

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 148 - 173 in **chapter 3** ("Speech in Cyberspace")

This reading covers information on CIPA and Internet filtering.

**Why Controls and Audits are Important**

Read the following chapter in *Information Technology Control and Audit*:

- **chapter 1** ("Information Technology Environment-Why Are Controls and Audit Important?")

As you read through the chapter, think about implementing a good computer security policy.
Information Security Management

Download the following documents if you have not already done so:

- ISO/IEC 27001  Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002  Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 27005  Information technology - Security techniques - Information security risk management

Read the following text in the ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management document:

- chapter 1
- pages 2 - 4 in section 5

This provides some guidance regarding how to write and implement a good computer security policy. The guidelines recommend procedures for security policy creation that will ultimately adhere to the ISO 27001 standard.

Write your own security policy for your current organization.

- What might your policy include?
- How might it be different depending on the type of organization, or individual needs?
- What regulations (federal or otherwise) might guide what is included in the security policy?
- How does the policy align with the ISO 27001 standards? In which part of the standard are the policy guidelines located?

Note: Creating your own security policy (or policies) now will help you prepare for the Security Policies course toward the end of your program.

Standards and Legal Issues in Cyberspace

Corporations must comply with

- Federal and State statutes and regulations,
- court decisions,
- government agency decrees, and
- the laws of other countries.

Missteps can be extremely costly.

Speech in Cyberspace

Cyberlaw covers broad territory. Topics such as intellectual property, privacy, and freedom of expression are almost daily entries in the news.
This topic addresses the following competencies:

- Competency 423.1.1: Standards & Legal Issues
  The graduate develops a legal analysis addressing legal issues, standards, policies, legislation, and governance related to cybercrimes for enterprise systems.

**Anonymous Communications in Cyberspace**

Read the following sections in *Cyberspace Law: Cases and Materials*:

- section 3C (“Anonymous Communications”) in [chapter 3 (“Speech in Cyberspace”)]
- section 3D (“Access to Cyberspace”) in [chapter 3 (“Speech in Cyberspace”)]

**ISP Liability for Speech**

Read the following section in *Cyberspace Law: Cases and Materials*:

- section 3E (“Internet Service Provider Liability for Speech”) in [chapter 3 (“Speech in Cyberspace”)]

**Communications Decency Act**

Review the following pages in *Cyberspace Law: Cases and Materials*:

- pages 243 - 262 (“Liability after the Communications Decency Act”) in [chapter 3 (“Speech in Cyberspace”)]

**Code as Speech**

Read the following section in *Cyberspace Law: Cases and Materials*:

- section 3F (“Code as Speech”) in [chapter 3 (“Speech in Cyberspace”)]

**Privacy of Communications**

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 575 - 594 (“Privacy of Communications”) in [chapter 5 (“Privacy”)]

**Encryption**

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 631 - 635 (“Technological Measures to Maintain Privacy: Encryption”) in [chapter 5 (“Privacy”)]

**Interception of Communications**

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 594 - 630 (“Intercepting Communications”) in [chapter 5 (“Privacy”)]

**Data Privacy**
Websites and web-based applications have the ability to collect personal information. Legal conflicts may arise if personal information, collected in cyberspace, is not protected.

This topic addresses the following competencies:

- Competency 423.1.1: Standards & Legal Issues
  The graduate develops a legal analysis addressing legal issues, standards, policies, legislation, and governance related to cybercrimes for enterprise systems.

Data Privacy

Read the following section in *Cyberspace Law: Cases and Materials*:

- section 5B ("Data Privacy") in [chapter 5 ("Privacy")](#)

Privacy Act of 1974

Read the following page on the U.S. Department of Justice website:

- [The Privacy Act of 1974](#)

Legal Practice on the Internet

Read the following website about legal practice on the Internet:

- [Digital-Lawyer.com](#)

This website has a great reference section that discusses laws as they relate to information technology; it also has great information that will help you to

- involve clients in the delivery of legal services,
- create new law firm structures, and
- think about new ways of practicing law using information technology proactively to re-design the delivery of legal services.

Cybercourts and Online ADR

The following article contains two parts.

- Part 1 discusses the nature of the Internet, problems with online disputes, and suggests creating a Cybercourt system.
- Part 2 discusses legal, technological, practical, and political issues in a future Cybercourt.

Download and read the following parts of the "Cybercourts, the future of governmental online disputes resolution?" article:

- [Cybercourts, the future of governmental online dispute resolution? Part 1](#)
- [Cybercourts, the future of governmental online dispute resolution? Part 2](#)

Legal Implications
In an information security role, you may be required to defend or oppose different regulations.

Create a new discussion thread on the message boards and respond to the following prompt:

- Proponents of HIPAA/HITECH believe that it enhances effective prosecution of individuals or groups that cause or could cause a breach of protected information. These individuals or groups are classified as cybercriminals or perpetrators of cybercrimes. Choose to defend or oppose this belief and describe how the federally mandated response requirements for breaches described in HIPAA/HITECH enhance or inhibit the effective prosecution and conviction of cybercriminals.


**Security Breaches**

As an information security professional, you need to be aware and prepared to handle different types of security breaches.

An excellent example of a security breach can be found in the following document from Verizon:

- "International Retailer Contains Security Breach with Verizon Business Computer Forensic Services"

In this particular case, it was determined that employee fraud was not the cause of the suspicious credit card activity noted by customers.

Consider the following questions:

- What if the cause of the suspicious credit card activity was indeed caused by employee fraud?
- What would you have recommended Verizon do to prevent fraud?
- What type of security measures could potentially be put in place that may not have been there before?
- What kinds of laws or standards might guide the types of security measures implemented?

**Information Categories and Relevant Requirements and Standards**

This section helps you apply your cyberlaw knowledge.

This topic addresses the following competencies:

- Competency 423.1.1: Standards & Legal Issues
  The graduate develops a legal analysis addressing legal issues, standards, policies, legislation, and governance related to cybercrimes for enterprise systems.

**U.S. Federal Regulatory Requirements**
Create a table with the following information:

- type of information
- regulation(s) that govern that type of information
- relevant details pertaining to information security you should pay attention to (i.e., the reason that particular regulation is applicable)

A few examples of information types are listed below:

- individual privacy
- personal health
- financial
- credit

Aspects of Cyberlaw, Part 1

Define the differences between the following terms. You can create flash cards or write them in your notebook.

- standards
- guidelines
- frameworks
- best practices

In cyberlaw, it is important to understand the difference between these technical terms, as they exist to assist companies in ensuring that information security assurance concerns are being appropriately addressed.

*Note: Use chapter 7 ("The Role of Standards") of the Information Security Law: The Emerging Standard for Corporate Compliance text from Books24x7 as a reference for this activity.*

ISO/IEC 27002 Mind Map

Access the following web page on the ISO 27001 Security website:

- [ISO/IEC Code of Practice](#)

Scroll down to "Content of ISO/IEC 27002:2015" and print the outline mind map.

The image will give you an excellent perspective of each of the main policy sections of the ISO 27002.

ISO 27002 Controls

You should have downloaded the following ISO standards:

- ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27002  Information technology - Security techniques - Code of practice for information security management
ISO/IEC 27005  Information technology - Security techniques - Information security risk management

Familiarize yourself with these standards and use them throughout your information security and assurance studies. You will be taking an assessment toward the end of your program that will emphasize these standards. Now is a good time to take some notes and get a sense of how the three documents work together.

Quick Reference Chart

Create a quick reference chart outlining different standards, guidelines, frameworks, and best practices.

The following column titles may prove helpful in completing this assignment:

- category (standard guideline, framework, best practice)
- title
- relevance to information security and assurance and/or legal impact

Look at such categories as the following:

- NIST
- COBIT
- ISF
- Payment Card Industry Data

Complete: RTFT Performance Tasks

Complete the following tasks:

- TFT2 Cyberlaw: RTFT Task 1
- TFT2 Cyberlaw: RTFT Task 2

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

Trademarks and Content Ownership on the Internet

The Internet fosters the dissemination and sharing of content. How do trademark and copyright laws work in Cyberspace? The upcoming activities will expose you to some of the challenges of protection of intellectual property on the Internet.

SLA Agreements

Service level agreements can be used to reduce some of the risks associated with outsourcing
resources, including those that reside in Cyberspace. With the increase of pushing resources to the cloud, service level agreements are becoming more and more necessary.

This topic addresses the following competencies:

- **Competency 423.1.4: Cyberagreements**
  The graduate explains the underlying principles governing e-commerce third-party vendor agreements and translates them into practical recommendations for the implementation of such agreements.

- **Competency 423.1.6: Intellectual Property**
  The graduate selects appropriate business practices that ensure the protection of intellectual property.

### Service Level Agreements:

Read the following chapters in *Service Level Agreements: A Legal and Practical Guide*:

- chapter 1 ("Why Do You Need a Service Level Agreement?")
- chapter 2 ("Where Slas Go Wrong")
- chapter 3 ("Building the Foundation for the Sla")
- chapter 4 ("Drafting the Sla and Key Clauses")

### Trademark Basics

At the start of companies scrambling to have an online presence, cybersquatting was born. Cybersquatters would buy domain names that had not yet been purchased by the company whose name actually matched the domain name. The new problems created by Internet technology required new laws to be passed.

This topic addresses the following competencies:

- **Competency 423.1.4: Cyberagreements**
  The graduate explains the underlying principles governing e-commerce third-party vendor agreements and translates them into practical recommendations for the implementation of such agreements.

- **Competency 423.1.6: Intellectual Property**
  The graduate selects appropriate business practices that ensure the protection of intellectual property.

### Domain Names, Meta Tags, and Keyword Buys

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 271 – 322 ("Domain Names and Trademark Infringement") in chapter 4 ("Content as Property in Cyberspace")
Copyright Basics, Copyright Infringement
Accessibility to information provided by the Internet has somewhat blurred society’s understanding of the Fair Use Doctrine and copyright laws.

This topic addresses the following competencies:

- Competency 423.1.4: Cyberagreements
  The graduate explains the underlying principles governing e-commerce third-party vendor agreements and translates them into practical recommendations for the implementation of such agreements.
- Competency 423.1.6: Intellectual Property
  The graduate selects appropriate business practices that ensure the protection of intellectual property.

Copyright Infringement

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 355 - 440 from section 4B ("Copyright in Cyberspace") in chapter 4 ("Content as Property in Cyberspace")

Fair Use

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 440 - 478 from section 4B ("Copyright in Cyberspace") in chapter 4 ("Content as Property in Cyberspace")

The DMCA

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 478 - 503 from section 4B ("Copyright in Cyberspace") in chapter 4 ("Content as Property in Cyberspace")

The Private Ordering of Cyberspace

Conducting business using the Internet has influenced government regulations, departments, and federal laws.

This topic addresses the following competencies:

- Competency 423.1.4: Cyberagreements
  The graduate explains the underlying principles governing e-commerce third-party vendor agreements and translates them into practical recommendations for the implementation of such agreements.
• Competency 423.1.6: Intellectual Property
  The graduate selects appropriate business practices that ensure the protection of intellectual property.

The Private Ordering of Cyberspace

Read the following chapter in *Cyberspace Law: Cases and Materials*:

• chapter 7 ("Private Ordering of Cyberspace")

E-Commerce: Electronic Signatures and Secure Online Transactions, E-Sign, FERPA

Access the following web pages and read through the information found there:

• [Electronic Signatures in Global and National Commerce Act](https://example.com)
• [Family Educational Rights and Privacy Act](https://example.com)

Complete: RTFT Task 3 Performance Task

Complete the following task in:

• TFT2 Cyberlaw: RTFT Task 3

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

Cybercrimes and Cyberterrorism

Innovative opportunities in education, medicine, and business were generated by the Internet. Unfortunately, criminals and terrorist also learned how innovative the Internet can be.

The rapid increase of new forms of crime and terrorism has necessitated changes to our laws.

Spam, Phishing, Spear Phishing, IVR, and Communications Fraud

Unsuspecting users of the Internet, without an IT background, are protected by laws against spam and fraud. You will learn the legal reasons why it is not the fault of naïve users when they fall prey.

This topic addresses the following competencies:

• Competency 423.1.3: Cyberterrorism & Homeland Security
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.
• Competency 423.1.7: Cybercrimes
  The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.

Spam, Phishing, Spear Phishing, IVR, and Communications Fraud

Read the following section in *Cyberspace Law: Cases and Materials*:
Jurisdiction in Cyberspace

The Internet spans the globe. You will learn how it is handled when a cybercrime originates in another country and if copyright laws can really be enforced in cyberspace.

This topic addresses the following competencies:

- Competency 423.1.3: Cyberterrorism & Homeland Security
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.

- Competency 423.1.7: Cybercrimes
  The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.

Jurisdiction in Cyberspace

Read the following pages in Cyberspace Law: Cases and Materials:

- pages 19 – 58 of chapter 2 (“Regulating Cyberspace”)

In Rem Jurisdiction, Forum Selection, and Choice of Law in Cyberspace

Read the following pages in Cyberspace Law: Cases and Materials:

- pages 58 – 72 of chapter 2 (“Regulating Cyberspace”)

International Jurisdiction Issues

Read the following pages in Cyberspace Law: Cases and Materials:

- pages 90 – 113 of chapter 2 (“Regulating Cyberspace”)

Cybercrime and Network Access

The Internet is comprised of many computers and networks. The potential of trespassing by accessing a computer or network without authorization is possible.

This section covers the various laws that are broken when cybercrime involves unauthorized access.

This topic addresses the following competencies:

- Competency 423.1.3: Cyberterrorism & Homeland Security
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.

- Competency 423.1.7: Cybercrimes
  The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.
Cybercrime and Network Access

Read the following pages in *Cyberspace Law: Cases and Materials*:

- pages 687 – 708 of chapter 6 (“Network Ownership and Access”)

Computer Fraud and Abuse Act

Access the following web page and read through the information found there:

- [Fraud And Related Activity In Connection With Computers](#)

Investigating and Trying Cybercrimes

Criminal investigations and forensics must be conducted within the body of the law. The same is true while investigating cybercrimes.

This topic addresses the following competencies:

- Competency 423.1.3: Cyberterrorism & Homeland Security
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.
- Competency 423.1.7: Cybercrimes
  The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.

Forensic Investigations, Chain of Custody, and Evidence

Access the following web page and read through the information found there:

- [The Role of Computer Forensics in Stopping Executive Fraud](#)

Civil Discovery of Electronic Evidence

Access the following web page and read through the information found there:

- [Federal Rules of Civil Procedure: Rule 34](#)

Enterprise Continuity

Security and privacy problems, brought on by the Internet, impact private and public organizations. Appropriate security controls and auditing requirements are sometimes cited in security laws and regulations.

This topic addresses the following competencies:

- Competency 423.1.3: Cyberterrorism & Homeland Security
  The graduate evaluates the application of current laws and regulations in situations involving constitutional controversy and authority, deterring terrorism, ethical implications, or cybercrime.
- Competency 423.1.7: Cybercrimes
The graduate analyzes cybercrime scenarios to determine potential implications to enterprise continuity.

**Enterprise Continuity**

Read the following chapters of *Information Technology Control and Audit*:

- chapter 1 ("Information Technology Environment – Why Are Controls and Audits Important?")
- chapter 2 ("The Legal Environment and Its Impact on Information Technology")

**Complete: TFT Task 4 Performance Task**

Complete the following task in:

- TFT2 Cyberlaw: TFT Task 4

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

**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.