ITT Technical Institute

IS4680

Security Auditing for Compliance

SYLLABUS

Credit hours: 4.5

Contact/Instructional hours: 60 (30 Theory Hours, 30 Lab Hours)

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS3350 Security Issues in Legal Context or equivalent

Course Description:

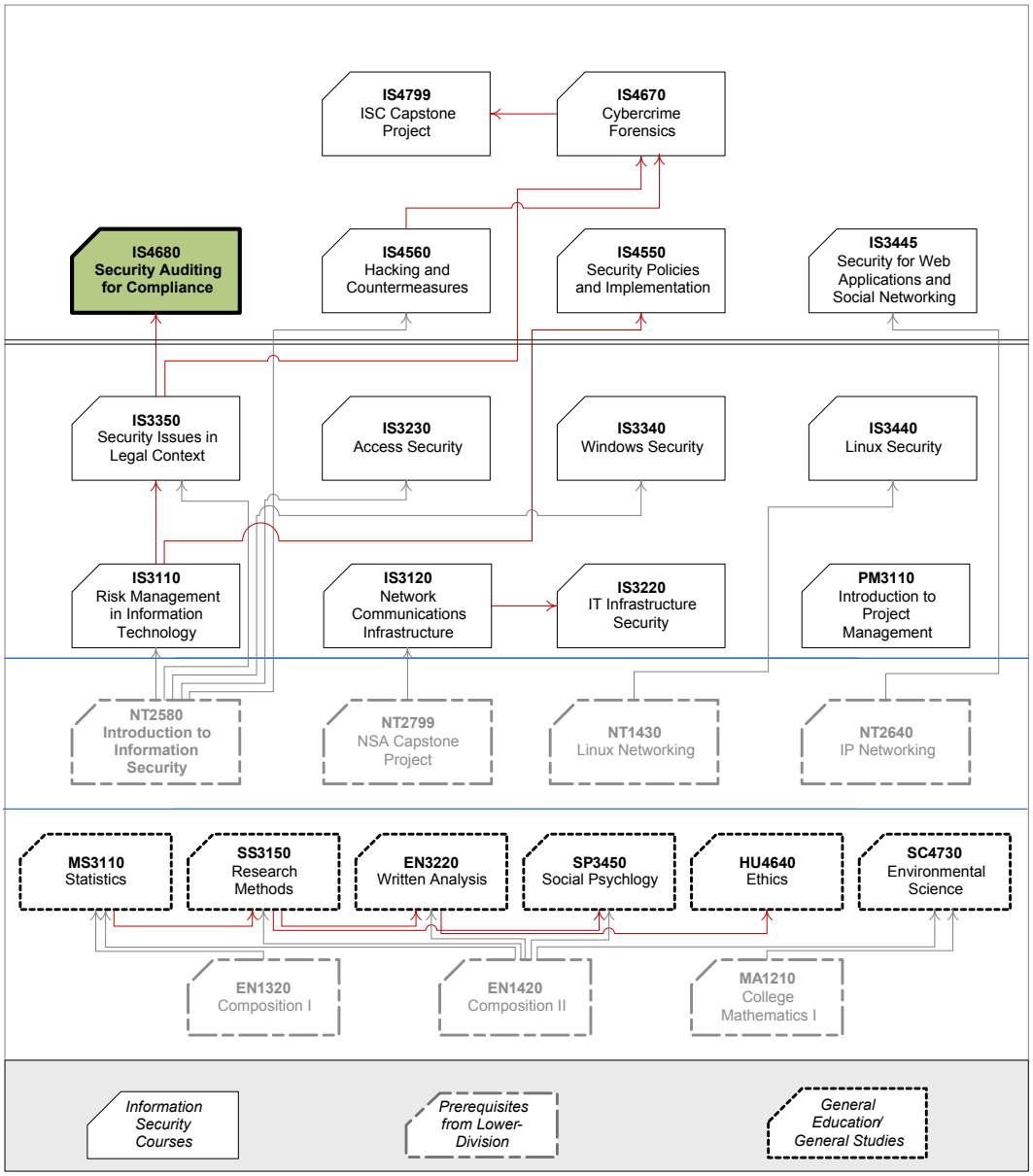
This course examines principles, approaches and methodology used in auditing information systems security to ensure processes and procedures are in compliance with pertinent laws and regulatory provisions.

Where Does This Course Belong?

This course is required for the Bachelor of Science in Information Systems Security (BSISS) program. This program covers the following core instructional areas:

- Foundational Courses
- Technical Courses
- BSISS Project

The following diagram demonstrates how this course fits in the program:



Course Summary

Major Instructional Areas

1. ISS compliance
2. The standards and the frameworks in the compliance audit of an information technology (IT) infrastructure
3. The components and the basic planning requirements of an IT infrastructure audit for compliance
4. The parameters for conducting and reporting on a compliance audit of an IT infrastructure
5. ISS compliance within the User Domain, Workstation and Local Area Network (LAN) Domains, LAN-to-Wide Area Network (WAN) and WAN Domains, Remote Access Domain, and System/Application Domain
6. Qualifications, ethics, and certification organizations for IT auditors

Course Objectives

1. To describe the role of ISS compliance in relation to U.S. compliance laws.
2. To explain the use of standards and frameworks in a compliance audit of an IT infrastructure.
3. To describe the components and basic requirements for creating an audit plan to support business and system considerations.
4. To describe the different parameters required to conduct and report on IT infrastructure audit for organizational compliance.
5. To describe information security systems compliance requirements within the User Domain.
6. To describe information security systems compliance requirements within the Workstation and LAN Domains.
7. To use an appropriate framework to implement ISS compliance within the LAN-to-WAN and WAN Domains.
8. To describe information security systems compliance requirements within the Remote Access Domain.
9. To describe the information security systems compliance requirements within the System/Application Domain.
10. To describe the qualifications, ethics, and certification organizations for IT auditors.

Course Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Weiss, Martin, and Michael G. Solomon. *Auditing IT Infrastructures for Compliance.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	■		
Printed IS4680 Student Lab Manual	■		
ISS Mock IT Infrastructure (1) – Cisco Core Backbone Network consisting of Cisco 2811 routers, 2950/2960 catalyst switches, ASA 5505s for classroom hands-on labs that require a live, IP network. (For onsite only)	■	■	■
ISS Mock IT Infrastructure (2) – VM Server Farm (2 Microsoft Windows Servers and 2 Ubuntu Linux Servers) for classroom hands-on VM labs. (For both onsite and online)	■	■	■
ISS Mock IT Infrastructure (2) – VM Workstation (Microsoft Windows XP Professional Workstation with Core ISS Apps and Tools) for classroom hands-on VM labs. (For both onsite and online)	■	■	■

(1) The following presents the core ISS Cisco core backbone network components needed for some of the hands-on labs for onsite delivery only. (Note: video labs will be used for online delivery):

- Cisco 2811 Routers
- Cisco 2950/2960 Catalyst Switches
- Cisco ASA 5505 Security Appliances
- Simulated WAN Infrastructure
- EGP using BGP4 or IGP using EIGRP
- Layer 2 Switching with VLAN Configurations
- Telnet and SSH version 2 for Remote Access
- Inside and Outside VLANs
- DMZ VLAN

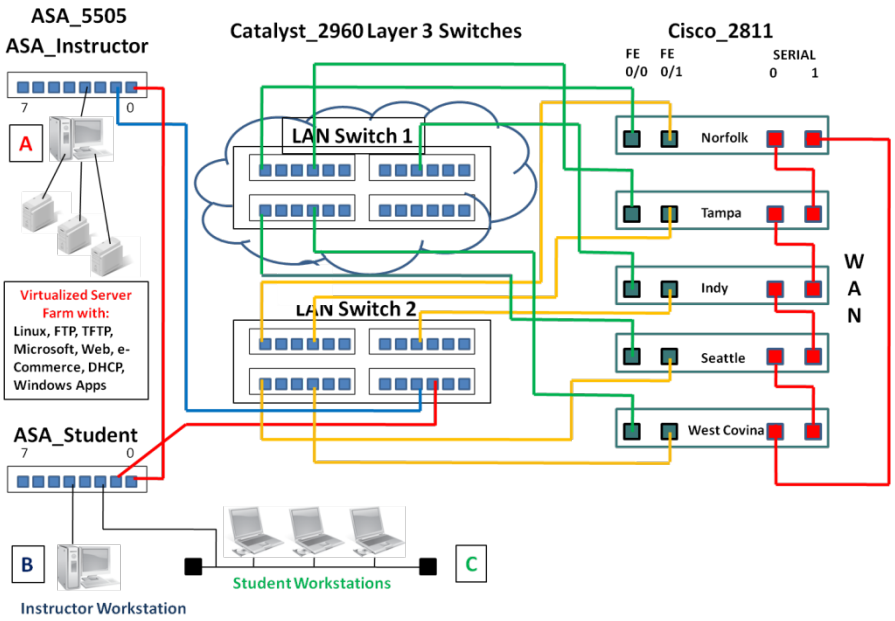


Figure 1 – ISS Cisco Core Backbone Network

(2) The following lists the core ISS VM server farm and VM workstation OS, applications, and tools required for this course for both onsite and online course deliveries:

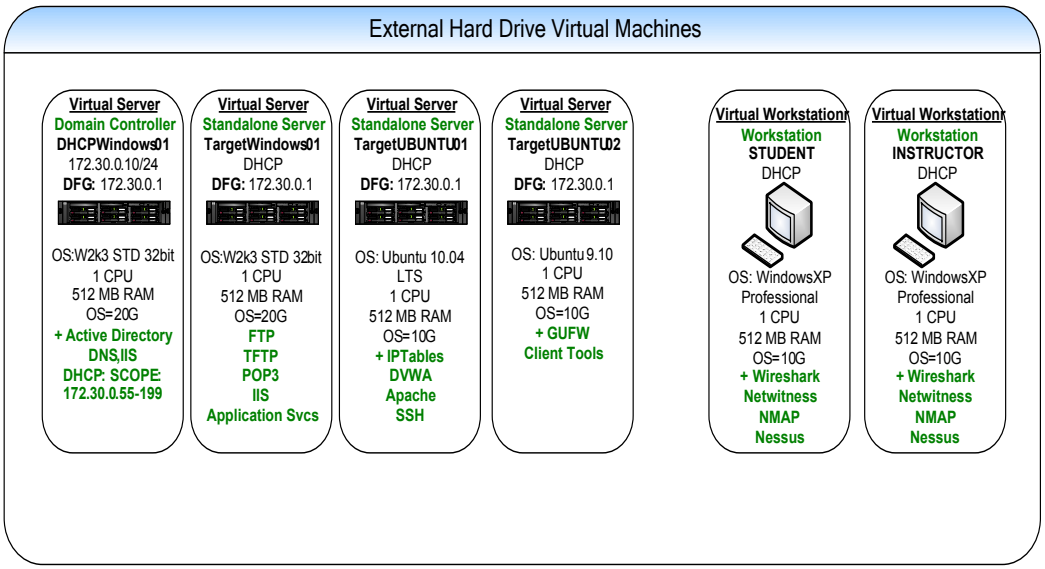


Figure 2 – ISS Core VM Server Farm & VM Workstations

Note #1: ISS onsite students can obtain their removable hard drive directly from their ITT campus. ISS online students will be required to download the core ISS VM server farm and VM workstations directly to their personal computer for installation. The ITT Onsite or Online Instructor will provide students with the specific instructions and procedures for how to obtain the core ISS VM server farm and workstation image files during the first week of class.

(3) The following lists the new VMs, applications, and tools required to perform the hands-on labs for this course for both onsite and online deliveries:

1. New VM for server farm: “VulnerableXP01”. This VM is a vulnerable Microsoft Windows Server 2003 Standard Edition used for performing attacks.

2. New VM for server farm: “Backtrack01”. A Backtrack 4 Ubuntu Server pre-loaded with the following applications and tools:

   a. Metasploit with required plug-ins
   b. Kismet
   c. Aircrack-ng
   d. Airsnort
   e. Snort
   f. MySQL
   g. BASE

3. New VM that Replaces the Old “TargetUbuntu01” VM on the VM server farm. An Ubuntu Server 10.4 VM pre-loaded with the following applications and tools:

   a. Damn Vulnerable Web App (DVWA)
   b. ClamAV Installed
   c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
   d. Chrootkit: http://www.chkrootkit.org/
   e. Appropriate rootkit tools can be found at: http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html
   f. Infected with EICAR
   g. tcpdump
   h. Common Linux tools such as strings, sed and grep

4. Tools Directory: A directory called "tools" which contains the binary installation files for each tool covered in the course, including:

   a. Infected with EICAR
   b. ClamAV Installed
   c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
   d. Chrootkit: http://www.chkrootkit.org/
   e. Appropriate rootkit tools can be found at: http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html
   f. Wireshark
   g. Netwitness Investigator
   h. FileZilla FTP client/Server
   i. Putty SSH client
   j. Nessus®[1]

[1] Nessus® is a Registered Trademark of Tenable Network Security, Inc.

k. Zenmap
l. MD5sum
m. SHA1sum
n. GnuPG (Gnu Privacy Guard)
o. OpenSSL
p. VMware Player

Note #2: Installation instructions for installing these new VMs, applications and tools will be provided by the ISS onsite or online Instructor during day 1/ week 1 of the course.

Recommended Resources

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

Books

Periodicals

EbscoHost

Books24X7

- Arnason, Sigurjon Thor, and Keith D. Willett. *How to Achieve 27001 Certification: An Example of Applied Compliance Management.* (Chapter 3)

- Bacik, Sandy. *Building an Effective Information Security Policy Architecture*. (Chapters 1,2,7)

- Davis, Chris, Mike Schiller, and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets*. (Chapters 1,5,14)

- Killmeyer, Jan. *Information Security Architecture: An Integrated Approach to Security in the Organization*. (Chapter 9, Appendix A-6)

- Tipton, Harold F., and Micki Krause. *Information Security Management Handbook*. (Chapters 2,4,18,19,26,32,41,42)

- "Domain expert user development: The Smartgov Approach." By: Lepouras, George, Costas Vassilakis, Constantin Halatsis, and Panagiotis Georgiadis. *Communications of the ACM*, Sep2007, Vol. 50 Issue 9, p79-83.

- "Work-Domain Experts as Evaluators: Usability Inspection of Domain-Specific Work-Support Systems." By: Følstad, Asbjørn. *International Journal of Human-Computer Interaction*, 2007, Vol. 22 Issue 3, p217-245, 29p, 10 Charts; DOI: 10.1080/10447310701373048; (*AN 25264815*)

- "An Approach to Formulation of Professional Standards for Internal Auditors." By: Campfield, William L. *Accounting Review*, Jul60, Vol. 35 Issue 3, p444, 5p; (*AN 7062080*)

- "The Identification and Categorization of Auditors' Virtues." By: Libby, Theresa; Thorne, Linda. *Business Ethics Quarterly*, Jul2004, Vol. 14 Issue 3, p479-498, 20p, 2 Diagrams, 7 Charts; (*AN 13801301*)

Professional Associations

- CERT
  This Website provides assistance in understanding and handling security vulnerabilities. It also provides the research tools on long-term changes in the networked systems and gives training assistance to improve security.
  http://www.cert.org/ (accessed April 26, 2010).

- Foundation for Information Policy Research (FIPR)
  This Website provides information on policy research and the impacts of formulated policies on society.
  http://www.fipr.org/index.html (accessed April 26, 2010).

- ISACA
  This Web site provides access to original research, practical education, career-enhancing certifications, industry-leading standards, and best practices. It also provides a network of like-minded colleagues, and it contains professional resources and technical/managerial publications.
  http://www.isaca.org/template.cfm?section=home (accessed April 22, 2010).

- National Institute of Standards and Technology (NIST)
  This Website provides access to the subject matter experts, and it facilitates in the area of research. It also provides career-building resources and opportunities.
  http://www.nist.gov/index.html (accessed April 26, 2010).

- National Security Agency/Central Security Service (NSA/CSS)
  This Website provides guidance on information assurance security solutions and provides insights on risks, vulnerabilities, mitigations, and threats. It also provides information on cryptologic support.
  http://www.nsa.gov/index.shtml (accessed April 26, 2010).

- SANS: Computer Security Training, Network Research & Resources

This Website provides information on computer security training through several delivery methods such as live and virtual conferences, mentors, and online and/or onsite training. It also provides certification and numerous free security resources.
http://www.sans.org/ (accessed April 26, 2010).

Other References

- Paulding, Mark. “Department of Defense Proposes New Information Security Requirements for Contractors.” *HL Chronicle of Data Protection*, (Mar30, 2010).
  http://www.hhdataprotection.com/articles/information-security/ (accessed April 26, 2010).

- May, Chris, Marie Baker, Derek Gabbard, Travis Good, Galen Grimes, Mark Holmgren, Richard Nolan, Robert Nowak, and Sean Pennline. *Advanced Information Assurance Handbook*. PA: CERT®/CC Training and Education Center, 2004.
  http://www.cert.org/archive/pdf/aia-handbook.pdf (accessed April 26, 2010).

NOTE: All links are subject to change without prior notice.

Keywords:
Information systems security (ISS)
Information assurance
U.S. compliance laws
Information systems security (ISS) audits
Public sector regulatory requirements
Private sector regulatory requirements
Governance
IT Security Audit
Security Control Assessment
DOD-related systems
DoD laws and policies
Public sector compliance requirements
Private sector compliance requirements
Security controls
Auditing standards
Auditing frameworks
Security control points
Organizational compliance
Local Area Network (LAN)

Wide Area Network (WAN)
Remote Access Domain
System/Application Domain

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and to support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group-learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to the development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and as a member of a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and the instructor, to work collaboratively on projects and team assignments, to raise critical questions, and to provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment

DO	DON'T
and your own experiences	components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Information Security Compliance	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 1 ▪ Chapter 2	Discussion	1.1	Public and Private Sector Regulatory Requirements	1
			Lab	1.2	Assess the Impact of Sarbanes-Oxley (SOX) Compliance Law on Enron	2
			Assignment	1.3	Compliance Laws	2
2	Information Security Compliance Audit—Standards and Frameworks	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 3 ▪ Chapter 4	Discussion	2.1	Organizational Barriers to IT Compliance	1
			Lab	2.2	Align Auditing Frameworks for a Business Unit within the DoD	2
			Assignment	2.3	Frameworks—Role in IT Security Domains and Auditing Compliance	2
3	Information Security Policy Audit Tools	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 5	Discussion	3.1	Information Gathering	1
			Lab	3.2	Define a Process for Gathering Information Pertaining to a HIPAA Compliance Audit	2
			Assignment	3.3	Analyzing the Critical Security Control Points	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
4	Conducting and Reporting an IT Infrastructure Compliance Audit	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 6 ▪ Chapter 7	Discussion	4.1	The Importance of Job Role Separation in Organizations	1
			Lab	4.2	Align an IT Security Assessment to Achieve Compliance	2
			Assignment	4.3	IT Security Controls and Countermeasure Gap Analysis	2
5	Creating Compliance Within the User Domain	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 8	Discussion	5.1	Separation of Duties, Least Privilege, and Need-to-Know	1
			Lab	5.2	Define a Process for Gathering Information Pertaining to a GLBA Compliance Audit	2
			Assignment	5.3	Best Practices for User Domain Compliance	2
6	Compliance Within the Workstation and LAN Domains	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 9 ▪ Chapter 10	Discussion	6.1	Vulnerability Management in Workstation and LAN Domains	1
			Lab	6.2	Auditing the Workstation Domain for Compliance	2
			Assignment	6.3	Best Practices for LAN Domain Compliance	2
7	Compliance Within the LAN-to-WAN and WAN Domains	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 11 ▪ Chapter 12	Discussion	7.1	Vulnerability Management in LAN-to-WAN and WAN Domains	1
			Lab	7.2	Auditing the LAN-to-WAN Domain for Compliance	2
			Assignment	7.3	Best Practices for LAN-to-WAN and WAN Domain Compliance	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
8	Compliance Within the Remote Access Domain	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 13	Discussion	8.1	Virtual Private Network (VPN) Tunneling and Performance	1
			Lab	8.2	Auditing the Remote Access Domain for Compliance	2
			Assignment	8.3	Best Practices for Remote Access Domain Compliance	2
9	Compliance Within the System/Application Domain	*Auditing IT Infrastructures for Compliance*: ▪ Chapter 14	Discussion	9.1	Maximizing Availability, Integrity, and Confidentiality (A-I-C) for System/Application	1
			Lab	9.2	Auditing the Systems/Application Domain for Compliance	2
			Assignment	9.3	Best Practices for System/Application Domain Compliance	2
10	Qualifications, Ethics, and Certifications for IT Auditors	*Auditing IT Infrastructures for Compliance* ▪ Chapter 15	Discussion	10.1	Acceptable Use Policy (AUP)	1
			Lab	10.2	Professional Information Systems Security Certifications—Charting Your Career Path	2
			Assignment	10.3	Codes of Conduct for Employees and IT Auditors	2
11	Course Review and Final Examination	N/A	Project	11.1	Project†	25
			Exam	11.2	Final Exam	25

† Candidate for ePortfolio

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Assignment	20
Lab	20
Project	25
Discussion	10
Exam	25
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage	Credit
A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5
D	60–64%	1.0
F	<60%	0.0

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)