Course ITSS 4361-001 | Information Technology Cybersecurity
Instructor Dr. Mohammad Anwar Islam
Term Spring 2025
Meetings Thu 4:00 pm – 6:45 pm, Room: JSOM 2.717

Instructor:	Dr. Mohammad Anwar Islam
Email:	mohammad.islam@utdallas.edu
Office Hours:	By appointment via Teams
Teaching Assistant:	Akanhsha Katoch akanksha.katoch@utdallas.edu
Office Hours:	Tuesday and Wednesday: 10 am – 5 pm Office: TBD

Prerequisites: ITSS 4360

Course Description

To provide the student with an in-depth knowledge of IT Security as applicable to the eight security domains. This course allows students to master cybersecurity concepts and topics, including security and risk management (legal, regulatory compliance), asset security (data classification, ownership, data security, and privacy), security engineering (security architecture, design, and security models), telecommunication and network security (perimeter protection, network attacks, IDS, IPS, firewalls), identity and access management (authentication, authorization, identity as a service), security assessment and testing, security operations (business continuity, disaster recovery, incident management, vulnerability, and patch management), and software development security. This course is designed to prepare an individual with major concepts, topics, and applications as preparation for the CompTIA Security + exam and the Certified Information Systems Security Professional (CISSP) exam.

Student Learning Objectives/Outcomes

- Grasp cybersecurity principles, including the CIA triad (Confidentiality, Integrity, and Availability).
- Understand key cybersecurity threats, vulnerabilities, and risk management practices.
- Learn to identify and mitigate security vulnerabilities in IT systems and networks.
- Gain hands-on experience with cybersecurity tools like firewalls, intrusion detection systems, and encryption technologies.
- Understand principles of secure system architecture and design.
- Learn methods for implementing access control, authentication, and cryptographic techniques. Assess risks in IT systems and propose effective security solutions.
- Analyze and design secure systems to meet specific organizational needs.
- Use cybersecurity tools and techniques to secure IT systems effectively.
- Understand the role of cybersecurity policies, procedures, and frameworks (e.g., NIST, ISO 27001)
- Consider management, security, and business-related issues related to the field.

Texts & Resources

- CompTIA Security+ Study Guide by Mike Chapple, David Seidl. ©2023 | Sybex 9th Edition | ISBN: 978-1394211418
- Additional References: CISSP Study Guide, 4th Edition, Joshua Feldman, Seth Misenar, Eric Conrad, ©2023 | Syngress |ISBN: 978-0443187346 *

* This book is available as an online resource in UTD's library.

Textbooks and other bookstore materials can be ordered online or purchased at the University of Texas at Dallas Bookstore.

Technical Tools and Resources

- Students must have a computer for this course and bring their PC to every class.
- Students must have access to Microsoft Office applications – Excel, Word, PowerPoint – for classroom activities.
- Students will need to access and sometimes download other software on a trial basis for this course.
- Students are responsible for acquiring or using appropriate and usable technology equipment. If your personally owned devices and equipment are not compatible with the needs of this course, especially for assignments, students should use the computers available in the JSOM computer labs.
- In addition to a confident computer and Internet literacy level, minimum knowledge of broader information technology and systems must be met to enable a successful learning experience. Please review the essential technical requirements on the Getting Started with eLearning webpage.

Class Preparation and Materials

- The textbook materials will be covered in the class lectures and assignments. You must read the textbook chapters) before attending the class.
- The supplement lecture presentations will be posted in the eLearning under the Lectures folder.
- The additional materials will be posted in the eLearning for students.

Lecture Guidelines

- Students must be attentive, engaged, and participative during lectures.
- During the class, students **must not chat** with each other. However, students can raise their hands to ask any questions or clarifications.
- Students are expected to bring a personal computer to class.
- Electronic devices will not be allowed to distract the student, other students, or the instructor. The instructor may require a student to turn off an electronic device if it distracts others.
- Lectures will start on time and, most often, will use the entire class time duration. It is common courtesy and professional protocol to be seated and prepared to begin when the lecture starts and to stay in the classroom until the lecture is completed. If circumstances require you to arrive late or leave early, as a courtesy, please advise the instructor via email at least 15 minutes before class time.
- Students are responsible for all materials covered in a lecture, irrespective of their attendance. Neither the TA nor the instructor is required to cover lecture content one-on-one for students missing lectures. It is recommended that students use a "buddy system" to share lecture notes.
- Some lectures or parts of lectures may be video-recorded synchronously and/or asynchronously. Students are responsible for learning from the video content as it is covered in class.

Course Assessment

The students will be assessed through the following types of assignments:

- Weekly Quizzes
- Completion of all courses/modules of **Google Professional Cybersecurity Certificate** in Coursera.
- Exam I and Exam II – This course has no comprehensive exams.

No homework or project is required for this course.

Attendance and Quizzes Guidelines (20% of final grade calculation)

- Students are expected to attend all lectures. Attendance is a material part of the final grade calculation.
- For each session, a quiz will be taken on your laptop (Opens in eLearning) consisting of 15-20 questions of questions for 20 - 25 minutes.

- The questions will be relevant to the previous session's content, except for 1st session, in which the quiz will be based on your general knowledge.
- The quiz grade works toward your 20% portion of the overall grade.
- **NO** make-up for quizzes and thus for attendance.

Coursera Professional Cybersecurity Certificate (20% of final grade calculation)

Google Cybersecurity Professional Certificate
https://www.coursera.org/programs/career-academy-faculty-staff-2t8fy/professional-certificates/google-cybersecurity?authProvider=utdallas

Each student must use UTD credentials (ID) to log in to Coursera and enroll for the Google Cybersecurity Professional Certificate. This is a ***free*** *Coursera certificate for UTD students*. If you have any issues accessing this course, please reach out to UTD IT Support:

https://atlas.utdallas.edu/TDClient/30/Portal/Home/?ID=3142d75a-f646-4b7c-9b7d-c37bb8ad4fd8

The Google Cybersecurity Certificate helps prepare you for the CompTIA Security+ exam, the industry-leading certification for cybersecurity roles. You'll earn a dual credential when you complete both.

Outcomes: ***Prepare for a career in cybersecurity***

- Receive professional-level training from Google
- Demonstrate your proficiency in portfolio-ready projects
- Earn an employer-recognized certificate from Google
- Qualify for in-demand job titles: cybersecurity analyst, security analyst, security operations center (SOC) analyst

There are **eight courses (modules)** in the Google Cybersecurity Professional Certificate. You have to complete all eight courses to get a full score. Almost every alternate week, you must complete one course and upload the course completion certificate in eLearning.

All course (module) completion assignments will be submitted via eLearning. I do not accept assignments via email. If you submit an incorrect assignment or need to resubmit it in eLearning, you can resubmit one more time, as long as it is before the due date. You will be granted only one attempt to resubmit the assignment before the due date, and this will be automatically available to you in learning when the instructor creates the assignment.

Every module/course of this certificate must be completed per the assignment schedule. Under extraordinary circumstances, you ask for instructor approval if you cannot complete the course/module on time. **There will be a late penalty (20% + 5% incremental per day)** for any submission after the due date.

Exam Guidelines (60% of final grade calculation)

- Exams are scheduled well in advance. Missing an exam results in a score of zero.
- Make-up exams will be given only for justified situations; discuss it with the instructor **BEFORE** the scheduled exam. If you contact the instructor after the exam, it is considered missing the exam, and no credit will be given for missed exams.
- The exams may include multiple-choice, fill-in-the-blank, or short essay questions. The final exam is **NOT** comprehensive.
- Exams will be administrated via the testing center. Make sure to register for all two exams after the first session.

Grading

This course will feature a mix of activities and written assignments that may be in class or on campus. Homework will include readings from the text, Coursera Professional Certificate courses, and activities that usually require the student to complete a task. The instructor will provide detailed instructions and the grading criteria for each assignment. Please consult the course schedule for deadlines. Please be advised that if you have a question or issue with your assignment grade, your entire assignment is subject to re-grading, which could lead to the addition or deduction of points.

Grading Scheme

Grade Component	Percentage
Google Cybersecurity Certificate	20%
Quizzes	20%
Exam 1	30%
Exam 2	30%
Total	100%

Scoring

Final % Total	Letter Grade
>=93	A+
>=90 and < 93	A
>=86 and < 90	A-
>=82 and < 86	B+
>=78 and < 82	B
>=74 and < 78	B-
>=70 and < 74	C+
>=66 and < 70	C
>=62 and < 66	C-
>=58 and < 62	D+
>=54 and < 58	D
< 54	F

Miscellaneous Course and Instructor Policies

The following guidelines and policies describe how the course will be managed. Situations and issues not covered will be resolved at the instructor's discretion. Changes to the guidelines will be posted in syllabus updates on eLearning. Students will be notified via eLearning announcements when syllabus changes occur.

- **Special note:** Employ the following assignment file naming conventions to maximize clarity (attachment files not named in the required manner may not be graded):
  Surname Course First few words of the assignment title - Filename Example: *Smith ITSS4361-001 Essay*
  All course-related emails must include ***ITSS 4361-001 <subject>*** in the subject line. This triggers an alert to draw your instructor's attention to your email. You should expect a response within 48 hours. Please let me know if this standard is not being met.

- **Late submission of the assignments**: All assignments are due at 3:59 pm on the specified date mentioned in the course calendar. I do not accept late assignments unless prior arrangements have been made with me. A penalty of 25% will be assessed on late assignments for up to one day after the due date, after which late submissions will not be accepted. No exceptions. No extra credit or make-up work will be given. If there are genuine/ extenuating circumstances, I will make exceptions on a case-to-case basis.

- **Extra Credit:** Getting the following certifications during the semester will earn you extra credit:
    - **Network+**: 5%
    - **CompTIA Security+** : 10%
    - **CISSP**: 15%

  Certificate(s) earned before the first day of the class or after the last day of class do(es) not qualify for the extra credit.

- **Timing of Scoring / Timing of Score Reviews:** Scoring of assignments and exams is targeted to be completed 7 days after the work is due (the Scoring Period). It is the student's responsibility to check their scores. Questions about scores and requests for Score Reviews will be accepted during the Score Review Period, which is the 7 days after the scoring was scheduled to be completed. After the Score Review Period, the instructor will not address score questions**.**
    - ***If you do not see a score in eLearning for work that you believe you have turned in and for which the Scoring Period has passed, you must ask the TA or instructor about it via email during the Score Question Period, or you will receive a zero.***

- **Score Reviews:** Requests to review a score for an assignment should be submitted in writing via email to the Teaching Assistant (TA). If a student is not satisfied with the TA's explanation, the student may appeal to the instructor via email.

- **eLearning:** eLearning will be used for all graded items and recording scores/grades. eLearning will be used to access all class content not covered in the online website resource (e.g., additional lecture preparation resources, lecture slides, exams, etc.). Class announcements (e.g., changes in assignment dates, course calendar adjustments, etc.) also will be posted on eLearning.

- **Instructor Response Policy:** For any questions for which you expect a formal (actionable) response, you must submit the question in writing from your The University of Texas at Dallas email to the instructor's or TA's UT Dallas email. Neither the instructor nor the TA is responsible for questions submitted orally (e.g., after class or in the hallway) or via any other communication medium. The instructor / TA will respond to all student emails within 48 hours or less (excluding holidays and weekends).

- **Academic Integrity**: The University and the instructor are committed to academic excellence and expect academic honesty from all University community members. We believe that academic honesty is essential for academic excellence and integrity. Academic honesty includes adherence to guidelines established by the instructor in a particular course. It prohibits representing the work of others to be one's own (plagiarism), receiving unauthorized aid on an assignment (cheating), and using similar papers or other work products to fulfill the obligations of different classes without the instructor's permission. Penalties for academic dishonesty will be assessed per the policies and precedents of The University of Texas at Dallas Office of Community Standards and Conduct (OCSC). Penalties may include a score of zero on the work in question or for the entire course. In addition, any student engaged in academic dishonesty will be subject to The University of Texas at Dallas disciplinary action. Please refer to the General Policies website (see below) for detailed information pertaining to academic dishonesty, including procedures for determining disciplinary action.

- **Working Together** on Individual Assignments: This course will have considerable computing work for application assignments. Each student is expected to work on the "individual" assignments. Copying another student's work (computer files) or having another person do your work is academic dishonesty and will be dealt with accordingly.

Comet Creed: This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:
"As a Comet, I pledge honesty, integrity, and service in all that I do."

General The University of Texas at Dallas Policies & Procedures

For information regarding general University policies and procedures, please go to http://go.utdallas.edu/syllabuspolicies. These policies include the following:

- Technical Support
- Field Trip Policies, Off-Campus Instruction, and Course Activities
- Student Conduct and Discipline, Academic Integrity, Avoiding Plagiarism
- Copyright Notice
- Email Use
- Withdrawal from Class
- Student Grievance Procedures
- Incomplete Grade Policy
- Disability Services
- Religious Holy Days

Tentative Class Schedule

This is a tentative class schedule; changes to the schedule will be posted in eLearning. The following gives a tentative outline and sequence of the topics to be covered or the activities to take place (exams or assignments) in these meetings. Assignments are due at the beginning of class; for example, an assignment due in Class 2 should be submitted through eLearning before the start of Class 2. The agenda, topics, and Coursera course (Google Cybersecurity Professional Certificate) for each meeting will be posted before or shortly after the class.

Week	Date	Topics	Reading	Coursera Google Certificate Course/Due
Week 1	01/23/2025	Review of Syllabus Overview of Cybersecurity Cybersecurity career Chapter 1 Today's Security Professional Chapter 2 Cybersecurity Threat Landscape	Chapter 1 Chapter 2	
Week 2	01/30/2025	Chapter 3 Malicious Code Chapter 4 Social Engineering and Password Attacks Quiz 1	Chapter 3, Chapter 4	Course1 Foundations of Cybersecurity
Week 3	02/06/2025	Chapter 5 Security Assessment and Testing Quiz 2	Chapter 5	Course 2 Play It Safe: Manage Security Risks
Week 4	02/13/2025	Chapter 6 Application Security Quiz 3	Chapter 6	
Week 5	02/20/2025	Chapter 7 Cryptography and the PKI Quiz 4	Chapter 7	Course 3 Connect and Protect: Networks and Network Security
Week 6	02/27/2025	Chapter 8 Identity and Access Management Quiz 5	Chapter 8	
Week 7	03/06/2025	Chapter 9 Resilience and Physical Security Exam Review Quiz 6	Chapter 9	Course 4 Tools of the Trade: Linux and SQL
Week 8	03/13/2025	**Exam I**	Testing Center	
Week 9	03/20/2025	Spring Break (3/17/25 – 3/23/25)		No Class

Week 10	03/27/2025	Chapter 10 Cloud and Virtualization Security Quiz 7 (Chapter 9)	Chapter 10	Course 5 Assets, Threats, and Vulnerabilities
Week 11	04/03/2025	Chapter 11 Endpoint Security Quiz 8	Chapter 11	
Week 12	04/10/2025	Chapter 12 Network Security Quiz 9	Chapter 12	Course 6 Sound the Alarm: Detection and Response
Week 13	04/17/2025	Chapter 13 Wireless and Mobile Security Quiz 10	Chapter 13	
Week 14	04/24/2025	Chapter 14 Monitoring and Incident Response Chapter 15 Digital Forensics Quiz 11	Chapter 14 Chapter 15	Course 7 Automate Cybersecurity Tasks with Python
Week 15	05/01/2025	Chapter 16 Security Governance and Compliance Quiz 12	Chapter 16	
Week 16	05/08/2025	Chapter 17 Risk Management and Privacy Exam Review Quiz 13 (Covers Chapters 16 &17)	Chapter 17	Course 8 Put It to Work: Prepare for Cybersecurity Jobs
Week 17	05/12/2024 05/16/2024	**Exam II**	Testing Center	