Syllabus
BIS3111 Information Security Assurance: Principles& Practices
Visiting Prof. Dr. Garry L. White, CCP, CISSP (Texas State University)
Summer Semester 2023

Level	Bachelor		
Credits	3		
Student Contact Hours	Equivalent to 2 x 45min / week ("2 SWS") - compressed mode, see online time table LSF)		
Workload	90 hours - 30 hours within class and 60 hours for self-study		
Prerequisites	Proof of level B2 in English		
Time	further details, see: LSF		
Room	further details, see: LSF		
Start Date	March 13, 2023		
Lecturer	**Name**	Garry White, CCP, CISSP, PhD	
	Office	W2.2.23	
	Virtual Office	Monday	12:30 to 13:45
		Tuesday	12:30 to 15:30
	Office Hours	Monday	9:00 to 11:00; 12:30 to 13:45
		Tuesday	9:00 to 11:00; 12:30 to 15:30
	Phone	-	
	Email	gw06@txstate.edu	

Outline of the Course

Information Security

This course will provide a foundation for information security. Information security is an ever-evolving field, requiring constant vigilance and technological adaptation to stay ahead of malicious actors. This lecture explores the various approaches for safeguarding digital assets, with a focus on mechanisms as well as general strategies. Special attention is paid to common attacks and lessons learnt from known security breaches.

We will also shed light into legal and ethical considerations. This includes an analysis of differences in law and security standards in the United States, Germany, and the European Union. Finally, we will also examine the role of the user in information security, including best practices for password hygiene and authentication processes.

Part of the course will involve a project to do a root cause analysis of the target breach and what countermeasures are needed. Four key questions will be answered throughout the course:

1) Why is cybercrime so successful?
2) What are the worst cyber threats and vulnerabilities? What can be done about them?
3) What are the differences between security and assurance?
4) Why is assurance replacing security?

Course Contents

Class/hr	Ch	Topics
1-1	Intro to course,	Intro topics
1-2	RCA Sec Br topic	Target Breach Intro Project – RCA
1-3	Ch 1	Security Systems
2-1	Ch 2	Changing technologies
2-2	Supplement	Physical security, Mindsets, DatBr, N.AmCySum,Trends,Privacy, 800-33
2-3	Ch 3	Risks, Threats, Vulnerabilities
2-4	Ch 7	Cryptography; Pub/Pri keys & DigSig
2-5	**Project RCA lab**	**Lab to work on Project – RCA**
3-1	**Exam #1, Ch 1-3, 7, supp**	**EXAM #1 essay, partner**
3-2	Ch 4, Ch 5	Bus. Drivers, Risk Manag, Net & Tele- tech
3-3	Ch 5 & Cloud	Cloud (tech)
4-1	Ch 6	Access controls
4-2	Ch 6, 8	Access controls, Malicious Software, Attack Vectors
4-3	Ch 8	Malicious Software, Attack Vectors
4-4	Ch 9	Operations & Admin., SDLC
4-5	**Exam #2, Ch 4,5,6,8,9**	**EXAM #2 essay, partner**
5-1	Ch 10	Auditing, testing, monitoring
5-2	Ch 11	Contingency Planning, Digital Forensics

Class/hr	Ch	Topics
5-3	**Exam #3 Ch 10, 11**	**EXAM #3 essay partner.** **Due _Project RCA_**
6-1	Ch 13, 14	Security Standards
6-2	Ch 14, 15	Security Certifications, Compliance Laws
6-3	CASE Studies	CASE studies
6-4	CASE Studies	CASE studies
6-5	**Exam #4, Ch 13-15, Case Studies, Pub/Pri, Dig Sig, Practice Exercise,**	**EXAM #4 varies, individual**

Course Intended Learning Outcomes and their Contribution to Program Intended Learning Outcomes / Program Goals

Program Intended Learning Outcomes		Course Intended Learning Outcomes	Assessment Methods		
	After completion of the program the students will be able…	After completion of the course the students will be able…	Project Work	3 Written Exams	Written Exam
			20%	45%	35%
			Collective	Collective	Individual
1	**Expert Knowledge**				
1.1	…to demonstrate their distinguished and sound competencies in General Business Administration.	To define and explain the components of security and assurance.		X	X
1.2	...to demonstrate their distinguished and sound competencies in Economics.	To explain the impact of security breaches.		X	X
1.3	...to have command of legal methodology for case solutions on basis of claims.	To understand due care and due diligence and forensics.	X	X	
1.4	...to solve business problems based on profound data research skills and by applying quantitative methods.	To be able to calculate loss and risk levels		X	X
1.5	...to demonstrate profound expert knowledge in their field of specialization.	To be able to analytical thinking in solving security threats	X	X	
2	**Digital Skills**				
2.1	...to know and understand relevant IT software tools used in business and their features and have a solid understanding of digital technologies.	To be able to use encryption and hashing calculations.		X	X
2.2	...to effectively use and apply information systems to develop solutions in business settings.	To develop safeguards and countermeasures for threats and vulnerabilities	X	X	X
2.3	...to effectively use digital technologies to interact, to collaborate and to communicate.	To collaborate in solving security threats and vulnerabilities	X	X	
2.4	...to handle the professional use of digital technologies in a responsible manner.	To know and apply the security policies of an organization.		X	X
3	**Critical Thinking and Analytical Competence**				
3.1	...to implement adequate methods in a competent manner and to apply them to complex problems.	To know and use root cause analysis to resolve security breaches and to develop countermeasures.	X		
3.2	...to critically reflect and interpret findings and to develop comprehensive solutions for complex problems.	To evaluate case studies of security breaches			X
4	**Ethical Awareness**				
	...to develop sound strategies in the areas of ethics, sustainable development and social responsibility and are able to apply them to typical economic decision-making problems.	To know the ethics of security professionals		X	

Program Intended Learning Outcomes		Course Intended Learning Outcomes	Assessment Methods		
5	**Communication and Collaboration Skills**				
5.1	...to express complex issues effectively in writing.	To write about complex issues for the essay exams and RCA project report	X	X	X
5.2	...to demonstrate their oral communication skills in presentations.	This is done through working with a partner for the RCA project and three essay exams.	X	X	
5.3	...to work successfully in a team by performing practical tasks.	This is done through working with a partner for the RCA project and three essay exams.	X	X	
6	**Internationalization**				
6.1	...to understand and explain business challenges in an international context.	To understand how the globalization of the Internet makes cybercrime hard to stop		X	
6.2	...to articulate themselves in a professional manner in international business.	To know the differences with privacy laws between the USA and Europe.		X	
6.3	...to successfully demonstrate awareness of cross-cultural differences.	To know the differences between national laws and standards.		X	

Assessment

The course is graded through a project and four essay exams. The Root Cause Analysis project and three of the essay exams may be done with a partner.

RCA Project	partner	20%
Exam 1 essay	partner	15%
Exam 2 essay	partner	15%
Exam 3 essay	partner	15%
Exam4 varies	individual	35%

The following evaluation scheme is used: 'Very good' means exceptional performance that is far above the average. 'Good' means good performance that is above the average. 'Satisfactory' means average performance, which certainly has shortcomings, but basically complies with the requirements. 'Adequate' means underperformance with conspicuous defects. 'Poor' means not acceptable performance, which no longer complies with the requirements.

Academic Integrity and Student Responsibility

In general, I expect that you will be using code, examples, and ideas from many different websites and resources for your exercises. This is allowed within reason. Wholesale copying of entire projects is definitely not allowed. Using code to round out a feature is allowed. If you ever have a question about what is or is not appropriate, ask first!

In all cases, you need to cite all sources at the top of the file where the code or algorithm was used, and you should note all sources in your documentation. Failure to properly attribute your sources will result in failing the complete lecture.

Code of Conduct

In this course, there will be a focus on working well together and learning about the development process. A large portion of that process involves interpersonal skills and conflict management. Students and staff are all expected to treat each other with respect. This includes, but certainly is not limited to:

- Excessive web browsing during class
- Disrespectful language
- Promptness for all deadlines and class meetings

- Quality work
- Not working well with your partner
- Collaborating with other teams
- Be fair to the other students!
- Be punctual and do not leave early!

The number one problem with professionalism in class is the overuse of laptops and mobile devices. Taking notes on a laptop and following along with the slides is welcome and encouraged. Doing work for other classes, watching videos, chatting, or anything else that distracts from your ability to learn and follow along (or anyone around you), will result in a professionalism penalty. Students can and will be penalized for unprofessional behavior.

Your class work might be used for research purposes. For example, we may use anonymized student assignments to design algorithms or build tools to help programmers. Any student who wishes to opt out can contact the instructor or do so after final grades have been issued. This has no impact on your grade in any manner.

In addition, please be aware and follow rules as explained in the University's online code of conduct:

Code of Conduct for online Teaching

Teaching Philosophy

I am always happy to serve as conversation partner and support you with advice. Please contact me during the lecture or via e-mail or during my office hours.

I am willing to contribute to your successful learning and provide an understanding of the practical impacts of the learning content. Comprehension questions should, if possible be equated during the lessons. Your comments, which serve the progress of all others are also welcome. Also, suggestions for improvements, and constructive criticism are very welcome. My goal is that you can successfully pass the exam, however a major part of the work is up to you.