IS536 - Information Security Governance
Second Semester, Academic Year 1439/1440 - Credit Hours: 3 hours
Section 194: Meeting Time: Monday (4:00PM-6:50PM)

Instructor	**Dr. Ahmad Alhamed**
E-mail	**aalhamed@ksu.edu.sa**
Course website	**KSU LMS**
Room No	**2053, CCIS, KSU**
Office Hours	**Monday 10:00am – 1:00pm**
	Tuesday 10:00am – 2:00pm
	or *other times by appointment*.
Office Telephone	
Course Coordinator	This course is designed by **Dr. Saad Saleh Alaboodi** and **Dr. Sk Md Mizanur Rahman**

Course Description

   This course first introduces the full spectrum of basic information security concepts necessary for establishing governance program in computing environments, i.e., technological, administrative, and physical, including security fundamentals, security in programs, operating systems, networks, and databases, cryptography, and security auditing. It then explores security governance domain, covering its objectives, metrics, roles and responsibilities, and risk management. Students completing this course should be better able to develop and evaluate security governance program using structured and widely-accepted methodologies.

Intended audience

   Upper year undergrad or graduate students.

Prerequisites

Fundamentals of operating systems (e.g., CSC227), computer networks (e.g., IS370), and database management systems (e.g., IS335).

Main textbook

Information Security Governance: A Practical Development and Implementation Approach, by Krag Brotby, ISBN: 978-0-470-13118-3.

Additional textbooks

1) Principles of Information Security, Fourth Edition by Michael E. Whitman and Herbert J. Mattord
2) Security in Computing, 4th Edition by Charles P. Pfleeger
3) Computer Security, 3rd Edition by Dieter Gollmann, Wiley, 2011
4) Information Security: Principles and Practice, Second Edition, Wiley-Inter Science, 2011, by Mark Stamp

Extra reading

1) Security Engineering, Ross Anderson, Wiley, 2001, http://www.cl.cam.ac.uk/~rja14/book.html
2) Computer Security: Principles and Practice by William Stallings and Lawrie Brown
3) Matt Bishop Computer Security, Art and Science Addison-Wesley, 2003.
book info @ http://nob.cs.ucdavis.edu/book/book-aands/index.html
4) Handbook of Information and Communication Security, Springer, Peter Stavroulakis and Mark Stamp (Editors): Electronic copy available.

Other Resources

- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.
- The RISKS Digest, http://catless.ncl.ac.uk/Risks. A forum on risks to the public in computers and related systems.
- BugTraq, http://www.securityfocus.com/archive/1. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.

Modes of study

Lectures, research work, presentations, and discussions.

Outline

The deliverables of this course consists of three main parts:

Part I: Introductory lectures (selective topics)		
Seq #	Subject	Resource type
1	Introduction to information security: its definition, the history of computer security, define key terms and critical concepts of information security, the phases of the security systems development life cycle, and information security roles of professionals within an organization.	ppt slides available in LMS
2	The business need for information security, explanation of why a successful information security program is the responsibility of both an organization's general management and IT management	
3	Describe the functions and relationships among laws, regulations, and professional organizations in information security; differentiate between laws and ethics, identify major national laws and explain the role of culture as it applies to ethics in information security	
4	Understanding elementary cryptography and basics of program security, operating system security, database security and privacy and network security	

Part II: Security governance program		
Each student (or a group of students) will present and discuss in class one section from the main textbook (or additional course materials as indicated).		
Seq #	**Subject**	**Distribution**	**Resource**
1	CH1: GOVERNANCE OVERVIEW	By instructor	Main textbook chapters "Information Security Governance: A Practical Development and Implementation Approach"
2	CH2: WHY GOVERNANCE?		
3	CH3: LEGAL AND REGULATORY REQUIREMENTS		
4	CH4: ROLES & RESPONSIBILITIES	By students	
5	CH5: STRATEGIC METRICS		
6	CH6: INFORMATION SECURITY OUTCOMES		
7	CH7: SECURITY GOVERNANCE OBJECTIVES		
8	CH8: RISK MANAGEMENT OBJECTIVES		
9	CH9: CURRENT STATE		
10	CH10: DEVELOPING A SECURITY STRATEGY		
11	CH11: SAMPLE STRATEGY DEVELOPMENT		
12	CH12: IMPLEMENTING STRATEGY		
13	CH13: SECURITY PROGRAM DEVELOPMENT METRICS		
14	CH14: INFORMATION SECURITY MANAGEMENT METRICS		
15	CH15: INCIDENT MANAGEMENT AND RESPONSE METRICS		
	ISO27001	By Instructor	ISO documents

Part III: Project or topic research and presentation		
Seq #	**Paper**	**Domain**
1	Organized in groups of Single/TWO students, each group will choose to either work on a project or topic research. The group will submit a project/topic report, and present and discuss their work and findings in class.	**Project:** information security governance. **Topic research:** any area under/related to security and privacy—subject to prior approval.

Grading Policy

Grades will be calculated as follows: (Open Book Exam)
- Midterm exam: 20%   (*week 9th or 10th*)
- Final exam: 40%
- Module assignment and presentation (Part II): 20%
- Project/topic research and presentation (Part III): 20%

Attending Policy: Attendance will be recorded during each class meeting and KSU rules will be implemented concerning the absence. Also, your grade may be affected for absence without accepted excuse.

General Policy: Assignments are due at the announced due date. Late assignments will only be accepted in extenuating circumstances.

Students with Disabilities:
If you need assistance, pleases contact the department officials. If you feel that you need special accommodations, due to the physical or other situation, pleases let me know at the beginning of the semester.