MARYMOUNT UNIVERSITY

School of Business Administration
2018-19 Summer Semester

COURSE SYLLABUS

Course Number	**Course Title**		
IT-727-A & IT-727-OL	Managing Cybersecurity Risk		
Fall Semester	**Spring Semester**	**Summer Semester**	**Credit Hours**
2019		XXX	3
Name of Instructor: Dr. Ibrahim Waziri Jr.			
Meeting Day, Time, and Room Number **In Class:** Thursdays 6:30PM – 9:15PM Ballston Room 4064 | **Online:** Details on Canvas			
Final Exam Day, Time, and Room Number Online – Exams opens Monday 12/09 at 12:00 am and closes Friday 12/13 at 11:59pm.			
Office Hours, Location, Phone: Available by e-mail or appointment as needed			
E-mail/Phone: [redacted]			
Course Description: This doctoral-level course covers all aspects of the management of the risk of cyber-attack and covers the foundations for the thoughtful and purposeful development of cyber defense strategies in any organization. In general, there are too many threats and potential vulnerabilities but not enough money and resources to protect all the digital assets in organizations, particularly those connected to the Internet. This course covers the strategic decision-making process, including formal methodologies, as to which assets to defend and why.			

UNIVERSITY STATEMENTS

ACADEMIC INTEGRITY

By accepting this syllabus, you pledge to uphold the principles of Academic Integrity expressed by the Marymount University Community. You agree to observe these principles yourself and to defend them against abuse by others. Items submitted for this course may be submitted to TurnItIn.com for analysis.

STUDENT COPYRIGHT INFORMATION

For the benefit of current and future students, work in this course may be used for educational critique, demonstrations, samples, presentations, and verification. Outside of these uses, work shall not be sold, copied, broadcast, or distributed for profit without consent.

ACCOMMODATIONS AND ACCESSIBILITY CONCERNS

Please address any special challenges or needs with the instructor at the beginning of the semester.

Students with Disabilities

If you are seeking accommodations (class/course adjustments) for a long-term or short-term (less than 6 months) disability, you must do the following:

- Register as a student with a disability with Student Access Services (SAS) in the Center for Teaching and Learning. This process takes time, so you should engage it as early as possible.
- Once registered with SAS, you may be approved for accommodations by SAS. Approved accommodations will be listed on a "Faculty Contact Sheet" (FCS). This is important because not all accommodation requests are approved.
- After receiving the FCS, meet with each of your instructors as soon as possible to review your accommodations, and have them sign the FCS. This document will help you and your instructors develop a plan for providing the approved accommodations.
- Let SAS know if there are any concerns about the way your accommodations are being implemented by your instructors.

Please remember that:

- Accommodations for disabling conditions cannot be granted if you do not follow the above steps.
- Accommodations are not retroactive. That is, accommodations can only be applied to a course *after* they have been approved by SAS and put into motion by *you* through working with your instructors.
- Appointments with the SAS staff are scheduled through the Starfish "Success Network" tab in Canvas. For more information, check the SAS website, e-mail access@marymount.edu, or call 703-284-1538.

Students with Temporary Challenges: Temporary challenges due to accident, illness, etc. that may result in missing class or navigating general campus access do not fall under the purview of SAS. If you experience something of this nature, please start by alerting your instructors. The Dean of Student Success may be involved in alerting instructors in extreme cases.

EMERGENCY NOTIFICATION POLICY

When students are absent due to a crisis situation or unexpected, serious illness and unable to contact their individual instructors directly, the Division of Student Affairs can send out an Emergency Notification. To initiate an Emergency Notification, students should contact the **Division of Student Affairs 703-284-1615** or studentaffairs@marymount.edu. Emergency Notifications are **NOT** appropriate for non-emergency situations (e.g. car problems, planned absences, minor illnesses, or a past absence); are **NOT** a request or mandate to excuse an absence, which is at the sole discretion of the instructor; and are **NOT** a requirement for student absences. If a student contacts instructor about an emergency directly, it is not necessary to involve the Division of Student Affairs as arrangements are made to resolve the absence. For non-emergency absences, students should inform their instructors directly.

ACCESS TO STUDENT WORK

Copies of your work in this course including copies of any submitted papers and your portfolios may be kept on file for institutional research, assessment and accreditation purposes. All work used for these purposes will be submitted anonymously.

UNIVERSITY POLICY ON WEATHER AND EMERGENCY CLOSINGS

Weather and Emergency closings are announced on Marymount's web site: **www.marymount.edu**, through **MUAlerts**, area radio stations, and TV stations. You may also call the **Weather and Emergency Hotline at (703) 526-6888** for current status. Unless otherwise advised by local media or by official bulletins listed above, students are expected to report for class as near normal time as possible on days when weather conditions are adverse. Decisions as to inclement closing or delayed opening are not generally made before 6:00 AM and by 3:00 PM for evening classes of the working day. Emergency closing could occur at any time making **MUAlerts** the timeliest announcement mechanism. **Students are expected to attend class if the University is not officially closed.** If the University is closed, course content and assignments will still be covered as directed by the course instructor. Please look for communication from course instructor (e.g., Canvas) for information on course work during periods in which the University is closed.

DESIGNATION

Marymount University is designated as a National Center of Academic Excellence for Cyber Defense Education (CAE/CDE) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). The course has been developed following applicable government and industry guidelines including mapping to the National Initiative for Cybersecurity Education (NICE) framework.

HOW TO GET STARTED WITH THIS COURSE, WHERE TO FIND VARIOUS COURSE COMPONENTS, AND EXPECTED TECHNICAL COMPETENCIES

To get started with this course, be sure you are familiar with the Canvas components we will be using in this course including:

- ANNOUNCEMENTS: current information, updates, and any changes to the syllabus. Please check it often.
- DISCUSSIONS: takes you to the discussion forums where you will interact with the professor or and your fellow students on a continuing basis. Discussions may also be linked from the PAGES described above when they are tied to specific modules.
- MODULES: all work in each unit is outlined in the Modules tab.
- GRADES: all grades and corresponding feedback will be posted to the GRADES folder. The grades are updated after each deliverable, so you need to check and make sure it is an accurate reflection of your work. If you have some questions, contact the professor.
- PEOPLE: lists contact information for your fellow students: contact them separately or communicate with the entire class.

Learners are expected to be familiar with Canvas and Zoom, as well as with the use of the Marymount Library Tools and the Internet.

For technical assistance, contact the Marymount University Help Desk:
Email: itshelp@marymount.edu
Telephone: 703-526-6990

For assistance with literature research contact the department's library liaison, Mason Yang.
Email: hyang@marymount.edu
Telephone: 703-526-6844

For Canvas support, there are a variety of options, accessible through the Help (?) button at the bottom of the menu on the left, including Live Chat for online chat with Canvas Support
Hotline for voice conversations (24 by 7) at 844-408-6459

The following links will provide detailed information on available resource.

Academic Integrity	**Plagiarism; Academic Offenses** http://www.marymount.edu/Student-Life/Student-Affairs-Administration/Student-Conduct/Academic-Integrity

	https://my.marymount.edu/Offices-Resources/Academic-Affairs/Academic-Integrity/Academic_Integrity_Code
Student Access Services	**Students with disabilities** http://www.marymount.edu/Academics/Services-Resources/Student-Access-Services
Tutoring and Writing Services	**Content tutors and writing consultants** http://www.marymount.edu/Academics/Services-Resources/Center-for-Teaching-Learning/Tutoring-Writing-Assistance
Library Services	**Library and Research services** http://www.marymount.edu/academics/lls The Library Liaison contact information: Professor Mason Yang, E-mail: mason.yang@marymount.edu
Financial Aid	**Scholarships, Grants, Loans** http://www.marymount.edu/financialAid
Bookstore	**Text Books, School supplies, Clothing** http://marymountu.bncollege.com/webapp/wcs/stores/servlet/BNCBHomePage?storeId=47053&catalogId=10001&langId=-1
Computer Help	**Canvas Access, Passwords, Marymount Commons** http://www.marymount.edu/its
Student Privacy Rights	**Family Educational Rights and Privacy Acts** http://www.marymount.edu/marymount.edu/media/Home/Notices-to-Students.pdf
TurnItIn	**Online writing feedback** www.turnitin.com
Brainfuse	**Online Tutoring** Go to Canvas and it is a menu tab on the top
Purdue Owl	**Assistance with citations and paper formats** http://owl.english.purdue.edu/owl/
Starfish	**Attendance policy and Contact Information** **Go to my.marymount portal and it is a menu tab on the left**
Student Health Center	**The Student Health Center (SHC) provides diagnosis and treatment of illnesses and injuries. They provide many of the routine services offered at primary healthcare offices. Healthcare services are available to all students who are actively enrolled in classes.** **https://www.marymount.edu/Student-Life/Health-Wellness/Student-Health-Center**
Student Counseling Services	**Student Counseling Services (SCS) provides supportive, confidential, empowering services to help all students thrive at Marymount.** **https://www.marymount.edu/Student-Life/Health-Wellness/Counseling-Center**

1. BROAD PURPOSE OF COURSE

This doctoral-level course covers all aspects of the management of the risk of cyber-attack and covers the foundations for the thoughtful and purposeful development of cyber defense strategies in any organization. In general, there are too many threats and potential vulnerabilities but not enough money and resources to protect all the digital assets in organizations, particularly those connected to the Internet. This course covers the strategic decision-making process, including formal methodologies, as to which assets to defend and why.

2. COURSE OBJECTIVES: Upon successful completion of this course students will be expected to:

- Perform a cybersecurity risk assessment for an organization;
- Use risk management as a foundational tool to facilitate the development of thoughtful and purposeful defense strategies;
- Analyze formal cybersecurity risk management models, frameworks, and tools to determine the most applicable to government and business;
- Apply qualitative and quantitative risk assessment methods, determining their applicability under certain circumstances;
- Articulate information security risks as business consequences in written and oral reports;
- Work with state-of-the-art governance, risk management, and compliance tools; and
- Communicate the consequences of cybersecurity risk to business managers, C-suite executives and the board.

3. TEACHING METHOD

This course is designed as an in-class/online doctoral-level seminar. This means that the emphasis is on enabling considerable interaction between the professor and the students and between the students in the class who bring different backgrounds to the program. The approach engages the students in research, analysis, and writing assignments on a weekly basis. The professor suggests readings (mainly freely available on the internet or available through the Canvas site), however the student is expected to identify additional applicable materials based on their own experience or research. In addition to the weekly activities (posed as a series of research questions and submitted through the discussion board), there are additional scenario-based written analyses, news reporting, a critical review by each student on a different topic, a presentation, and a final exam. Communications (oral and writing) are an important component of the course and the weekly activities will include tailoring your material to a specific audience (e.g., the Board, a professional conference). The professor will provide limited lecture on certain topics, but most activities will be to probe, ask questions, provide detailed feedback, challenge, model, and critique to help each student understand, research and to integrate and critically evaluate information.

This course is being taught in class and online. In class sessions will be live streamed using Zoom every Thursday beginning at 6:30 PM. Active participation is an integral part of the educational experience in the course. It is expected that you log on at least 2 times per week and participate meaningfully based on detailed research. This course will require 7 to 10 hours of your time each week, some weeks being more than others, such as when you are assigned to do the critical review. As your professor, it is my responsibility to present learning opportunities through the various components outlined in the course syllabus. As the student, it is your responsibility to do the learning by completing the assigned work, by participating in individual and group activities with energy, enthusiasm and relevant content. You will also be asked to provide a critical review of the work of other students.

Quizzes: There will be four (4) quizzes provided throughout the semester, one per lecture. The questions will be multiple choice or fill in the blank. The content of each quiz will be focused on its corresponding lecture. Quizzes constitute **20%** of your grade. Students must complete every quiz in one sitting. Student will NOT be able to retake an attempted quiz.

NIST RMF Activities: There will be six (6) activities provided throughout the semester. The activities will be based on the NIST Risk Management Framework. Each activity will include filling in a risk management deliverable template provided by the professor. Submission will be shared with the entire class, to enable learning from each other. Activities will constitute **30%** of your grade. To ensure fairness, every student must submit by the deadline. Student will NOT be allowed to submit at a later day unless an exception has been given by the professor.

Weekly Discussions: Course participation and interaction in the weekly activities are one of the keys to the community learning experience in this course. There will be weekly questions/issues relevant to risk management asked by the professor (posted on canvas), and these questions are based on a topic from the weekly learning outcomes. Students (excluding reviewers) are expected to begin their research early in the week and submit their response by the end of the week. All responses should be based on independent research using both academic and industry sources, available through the library or the Internet.

Each student is expected to do their own research on the question each week. Their initial posting should be **150 - 200 words** and should be directed at the specified audience. The text must be associated with at least **3 citations; at least one must be academic reference**

and one must be a commentary from an expert in the field in the last twelve months. The text must also be geared to senior management audience (e.g. the Board/CEO). The postings will be made to the discussion board; to ensure equal effort, students will not be able to see other student's posting until they have posted their response, also students will also not be able to edit their responses after posting. Students are then expected to review other's postings and comment accordingly, highlighting important points. All comments are due the following **Monday at 12:00PM.** This is to allow the reviewer sometime to review and document their assigned detailed report. In a situation where a student cannot submit by the said deadline, students can reach out to the reviewer(s) to work out a convenient time. There will be ten (10) discussion sessions throughout the semester, however because each student will be a reviewer at some point, students will be expected to participate in nine (9) discussions sessions. Due to the number of students, there will be sessions that includes two (2) discussions boards with different topics. Discussions will constitute **9%** of your grade.

Discussions Report: Each week, selected student(s) will be tasked to critically review **all** the discussion response/postings and prepare a detailed report. The report should be professionally prepared (like submission to a magazine, blog or journal) and be around **1,300 to 1,500 words (excluding citations and including an abstract).** It should include a complete bibliography of the citations presented in the postings in **APA format**, (removing duplicate citations). The detailed report will be due **before the beginning of the next class**. Students are expected to read the detailed reported after its final submission because final exams will include the discussion reports. There will ten (10) discussion reports sessions throughout the semester, however students are only expected to review and report only once (on their assigned date). Discussion report will constitute **5%** of your grade. **Reviewers are expected to give a 10 mins briefing of their reports.**

- **IT 727A** – The briefing will be given in class following an in-person set up. (No presentation required)
- **IT 727OL** – The briefing should be audio recorded and posted to Canvas, and every other student is expected is expected to listen and comment. (No presentation required)

News: Cybersecurity is a fast-changing field and it is imperative that students keep up to date with relevant cybersecurity incidents, new legislation and policy, and new tools and techniques, **all in relation to risk management**. Students will be assigned as the primary news reporter(s) for one week and will be expected to be a secondary reporter on the remaining weeks.

- Primary news reporter(s) initiate the news alert process on the discussion board by summarizing the news (between 75 to 100 words) and providing links to the detailed news. Primary news reporter(s) are also responsible for moderating and responding to every secondary reporter's comment/question. Primary news report will constitute **5%** of your final grade. Primary news reporter should report initial news the following **Friday before 6:00PM**
- Secondary reporter(s) are expected to read the detailed news provided by primary news reporter(s), comment and ask questions. Secondary news report will constitute **9%** of your final grade.

Invited Guest Report: Towards the end of the semester, an invited guest will be delivering a lecture in-person class (for online class, the lecture will be live-streamed and students will be provided with an opportunity to ask questions – a recording of the lecture will be uploaded to canvas for online who could not join the live-stream). All students are expected to write a report based on the lecture. The report should be around 1,300 to 1,500 words (excluding citations and including an abstract). It should include a complete bibliography of the citations presented in the postings in APA format. Invited guest report will constitute **10%** of your final grade.

Final Exam: Students will be expected to take a comprehensive final examination that will draw from material presented in the course as well as the individual assignments and discussions conducted throughout the course. The final exams will be open book (notes, electronic devices etc.) and will consist of a series of challenging essay questions that require high-level thinking, knowledge, skills and abilities expected of doctorate-level students. Final exams will constitute **10%** of your final grade.

All activities are expected to be submitted to Canvas. Unless an exception is given, the Professor will not grade late submission/email deliverables. Students can swap their activity dates with other students (by coordinating between themselves) if needs be. **All submissions will be uploaded to Turn it in for plagiarism detection.**

Participation: Active participation is expected of all students. Active participation will constitute 2% of your final grade.

4. GRADING POLICY

Central to the assessment process is quality and personal analysis. Focal doctoral level work principles include:

- Critical thinking and personal conclusions;
- Depth and accuracy of synthesis and analysis;
- Determination of advantages and disadvantages of multiple solutions;
- Professionalism and creativity in a variety of formal and ad-hoc presentations;
- Articulation of practical applications and strategies, including to non-technical persons;

- Higher-level research/writing skills; and reflection of the various activities

Grade	Grade Range		Deliverable Grade	% of Final Grade
A	95 – 100%		Quizzes (4 @ 5% each)	20%
B+	87 – 89.9%		NIST RMF Activities (6 @ 5% each)	30%
B	83 – 86.9%		Weekly Discussions (9 @ 1% each)	9%
B-	80 – 82.9%		Weekly Discussion Report (1 @ 5%)	5%
C+	77 – 79.9%		News (Secondary) (9 @ 1% each)	9%
C	70 – 76.9%		News - Primary (1 @ 5%)	5%
F	Below 70%		Invited Guest Report	10%
			Final Exams	10%
			Participation	2%
			TOTAL	**100%**

5. CLASS SCHEDULE

Module	Topics (instructor to deliver)	Task (student to-do)
Kick-Off 08/29	Introductions IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Get textbooks. • Introduce yourself. • Familiarize yourself with class expectations. • Know how to use Canvas
Module 1 09/05	Lectures: • Security and Risk Management – Intro • IT Risk Identification – Chapter 1 – ISACA Book IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Quiz – (Canvas)
Module 2 09/12	Lectures • IT Risk Assessment – Chapter 2 – ISACA Book • IT Risk Response & Mitigation – Chapter 3 – ISACA Book IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Quiz – (Canvas)
Module 3 09/19	Lectures • Risk & Control Monitoring and Reporting – Chapter 4 – ISACA Book IT 727-A - (No in-person session, watch video online) IT 727-OL - (watch video online)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Quiz – (Canvas)
Module 4 09/26	Lectures – NIST Framework – I IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Quiz – (Canvas)
Module 5 10/03	Activity – NIST Framework – Applying Step 1 IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 6 10/10	Activity – NIST Framework – Applying Step 2 IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 7 10/17	Activity – NIST Framework – Applying Step 3 IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 8 10/24	Activity – NIST Framework – Applying Step 4 IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 9 10/31	Activity – NIST Framework – Applying Step 5 IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion – (Discussion Board) • Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 10	Activity – NIST Framework – Applying Step 6	• Discussion – (Discussion Board)

11/07	IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Discussion Report & Briefing – (Upload in pdf or word) • News (Primary & Secondary) – (News Board) • Activity – (Upload)
Module 11 **11/14**	Invited Guest IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Upload Report
11/28	Thanksgivings Break	
Module 12 **12/05**	Review IT 727-A - (meet in-person) IT 727-OL - (Live stream and video to be uploaded)	• Extra credit activity (if any)
Module 13 **12/12**	Finals IT 727-A - (on canvas) IT 727-OL - (on canvas)	Take exams before due date Exams opens Monday 12/09 at 12:00 am and closes Friday 12/13 at 11:59pm.

6. SUGGESTED READINGS

Materials used for this course include:

Books

- ***ISACA CRISC: Review Manual, 6th Edition, Certified in Risk and Information Systems Control. An ISACA® Certification. (2015) - Required***
  ISACA
  ISBN-13: 978-1604203714
  ISBN-10: 1604203714

- ***Official (ISC)2 Guide to the CAP CBK, 2nd Edition* - (Optional)**
  Patrick D. Howard
  ISBN-13: 978-1439820759
  ISBN-10: 1439820759

Articles & Open Source Documents:

- Baldridge Performance Excellence Program: Baldridge Cybersecurity Excellence Builder, September 2016, National Institute for Standards and Technology, September 2016, available from Canvas
- Dempsey, K et al: SP800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST, September 2011, available from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
- Global Institute for Risk Management Standards: G31000, available from http://worldviewmission.nl/wp-content/uploads/2012/09/WM-G31000-Brochure-24-Jan-2013.pdf
- ISACA: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, available from Canvas
- ISACA the Risk IT Framework, Excerpt available from
- http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf
- Klein, P: How to read and academic article, 2010, available from https://organizationsandmarkets.com/2010/08/31/how-to-read-an-academic-article/
- NIST, Managing Information Security Risk Organization, Mission, and Information System View, Special Publication 800-39, 2011, available from http://dx.doi.org/10.6028/NIST.SP.800-39
- NIST: FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, 2011, available from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- NIST, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37 Revision 1, 2014 available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Updated 2015 and available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- North, G: How to Read a Textbook, available from http://www.garynorth.com/public/1899.cfm
- SANS: Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It, available from
- https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030

- SANS: Quantitative Risk Analysis Step-By-Step, SANS Reading Room, available at https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849
- Other readings and videos will be provided through the Canvas site, the Marymount library, and publicly available Web sites.

Additional Books

- Dhillon, G.: Principles of Information Systems Security: Text & Cases. Edition 1.1. Prospect Press. (2017)
- Freund, J. and Jones, J.: Measuring and Managing Information Risk: A FAIR Approach, B&H, 2015
- Gibson, D.: Managing Risk in Information Systems. Jones & Bartlett Learning: Information Systems Security & Assurance Series. (2011)
- Hubbard, Douglass W.: How to Measure Anything in Cybersecurity Risk, Wiley, 2016
- Hubbard, Douglass W.: The Failure of Risk Management: Why It's Broken and How to Fix It, Wiley, 2009 (Chapter 2 on Canvas)
- Peltier, Thomas R.: Information Security Risk Analysis, 2nd Edition. 2005
- Talabis, Mark Ryan M. and Martin, Jason L., Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress, 2013
- Wheeler, E.: Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngress, 2011
- Whitman, Dr. Michael E. and Mattord, Herbert J.: Readings and Cases in the Management of Information Security, Thomson Course Technology, 2006