# FLORIDA ATLANTIC UNIVERSITY™

## Graduate Programs—COURSE CHANGE REQUEST[1]

UGPC APPROVAL _____
UFS APPROVAL _____
SCNS SUBMITTAL _____
CONFIRMED _____
BANNER POSTED _____
CATALOG _____

| | |
|---|---|
| DEPARTMENT<br>ITOM | COLLEGE<br>BUSINESS |
| COURSE PREFIX AND NUMBER<br>ISM 6328 | CURRENT COURSE TITLE<br>INFORMATION SECURITY MANAGEMENT |
| CHANGE(S) ARE TO BE EFFECTIVE (LIST TERM) SPRING 2016 | ____ TERMINATE COURSE (LIST FINAL ACTIVE TERM) |
| CHANGE TITLE TO: MANAGEMENT OF INFORMATION ASSURANCE AND SECURITY<br><br>CHANGE PREFIX FROM: TO:<br><br>CHANGE COURSE NO. FROM: TO:<br><br>CHANGE CREDITS[2] FROM: TO:<br><br>CHANGE GRADING FROM: TO:<br><br>CHANGE DESCRIPTION TO:<br><br>AN INTRODUCTION TO THE ORGANIZATIONAL, COMPLIANCE, AND TECHNICAL ASPECTS OF INFORMATION SECURITY AND INFORMATION ASSURANCE MANAGEMENT. REVIEW OF PROGRAMS, STANDARDS, AND PRACTICES. | CHANGE PREREQUISITES/MINIMUM GRADES TO*:<br><br>CHANGE COREQUISITES TO*:<br><br>CHANGE REGISTRATION CONTROLS TO:<br><br>*Please list both existing and new pre/corequisites, specify AND or OR, and include minimum passing grade. |
| **Faculty contact, email and complete phone number:**<br>**DR. T. DINEV, TDINEV@FAU.EDU, 561-297-3181** | **Attach syllabus for ANY changes to current course information.** |
| Should the requested change(s) cause this course to overlap any other FAU courses, please list them here:<br>**N/A** | Please consult and list departments that might be affected by the change(s) and attach comments.[3]<br>**CEECS** |

| *Approved by:* | *Date:* |
|---|---|
| Department Chair: Tamara Dinev | 8/31/16 |
| College Curriculum Chair: Wm R McDaniel | 9-13-2016 |
| College Dean: [illegible] | 9-13-2016 |
| UGPC Chair: Wm R McDaniel | 10-12-2016 |
| Graduate College Dean: Deborah Ahern | 10-13-16 |
| UFS President: | |
| Provost: | |

1. **Syllabus** must be attached; see guidelines for requirements: *www.fau.edu/provost/files/course syllabus.2011.pdf*

2. Review **Provost Memorandum: Definition of a Credit Hour** *www.fau.edu/provost/files/Definition_Credit_Hour_Memo_2012.pdf*

3. **Consent** from affected departments (attach if applicable)

Email this form and syllabus to *UGPC@fau.edu* **one week before** the University Graduate Programs Committee meeting.

Florida Atlantic University
COLLEGE OF BUSINESS

**ISM 6328 – Section 001**
**CRN 13067**
**Management of Information Assurance and Security**
**Fall 2017**
**FL 401**
**Tuesday 6:30-9:20 pm**

## Professor Information

**Dr. Oge Marques**
**Department:** CEECS (College of Engineering & CS)
**Office:** EE 441 (bldg. 96), Boca campus
**Email:** omarques@fau.edu
**Phone:** (561) 297-3857
**Web:** http://www.eng.fau.edu/directory/faculty/marques/

## Office Hours (subject to change)

Wednesdays 11:00 am – 1:00 pm, Thursdays 2:00-3:00 pm, or by appointment

## Required Text and Materials

- Whitman and Mattord, *Principles of Information Security*, 5th Edition, CENGAGE Learning, ISBN-13: 978-1285448367

## Course Description

An introduction to the organizational, compliance, and technical aspects of information security and information assurance management. Review of programs, standards, and practices.

## Course Prerequisites, Credit Hours, and Class Time Commitments

Completion of undergraduate degree in a related field.

This course is worth 3 credit hours.

According to Florida State Statute 6A-10.033, students must spend a minimum 37.5 hours of **in class** time during a 3-credit course. Additionally, students enrolled in a 3-credit course are expected to spend a minimum of 75 hours of **out-of-class-time** specifically working on course-related activities (i.e., reading assigned pieces, completing homework, preparing for exams and other assessments, reviewing class notes, etc.) and fulfilling any other class activities or duties as required.

Florida Atlantic University
COLLEGE OF BUSINESS

**Supplemental Course Description**

This course provides a comprehensive review of contemporary topics in the field of Information Security Management. Various Information Security Management models and organizations providing governance in this arena are examined. In addition, there are extensive discussions of technologies used to safeguard information as well as methods used to effectively select, design, and deploy Information Security System programs for various size organizations.

Topics include: Risk Assessment and Mitigation, Access Control Strategies, File-Level Security, People Authentication, Encryption Methods, Network Security, Enterprise-Level Security Methods and Policies, and Contingency Planning.

This course discusses theoretical concepts of information security and introduces several practical and hands-on approaches, in order to better understand and to devise strategies related to security policy development and enforcement.

**Course Learning Objectives**

This course is graduate level and the following learning outcomes are expected of students:

1. Students will demonstrate the ability to conduct research and to utilize analytical skills in articulating information technology investment strategies that align with business strategies. Understanding elements of organizational function processes, work practices and human resource capital as integrated components to address technical, logistical and business challenges and to provide paradigm shift in IT service delivery and to explore alternative opportunities to contain cost without impacting organizational mission.
2. Students will demonstrate effective oral and writing communication skills necessary to be effective and to compete in global business environment.
3. Students will demonstrate an ability to understand sourcing issues involving global IT providers and terms. Students will apply this knowledge for selecting and evaluating information technology vendors, partners and service providers to augment in-house skills.
4. Students will demonstrate understanding various aspects of information security management including planning, process, policy, procedure and security model as well as hardware and software technologies to safeguard organizational assets.
5. Students will develop the necessary skills to examine security management progression within an organization including training, policy development, governance, organizational model, risk assessment and mitigation, security management models as well as integration of project management techniques.

Florida Atlantic University
COLLEGE OF BUSINESS

**Course Resources**

This course will use the Blackboard course management tool, and changes will be announced on the course web site. Several lectures might be delivered via Blackboard as well as Blackboard collaboration as needed.

Students are expected and required to have Internet access for this course.

It is the student's responsibility to check their FAU email regularly. The instructor will assume that all announcements or updates sent out to the students' FAU email address are received, read, and acted upon accordingly.

**Grading Scale**

| | |
|---|---|
| *92-100 = A* | *70-72 = C* |
| *88-91 = A–* | *66-69 = C–* |
| *84-87 = B+* | *61-65 = D+* |
| *80-83 = B* | *56-60 = D* |
| *77-79 = B–* | *50-55 = D–* |
| *73-76 = C+* | *0-49 =* |

*** Graduate level courses below B may have to be repeated ***

**Course Evaluation Method**

| | |
|---|---|
| (1) Midterm | 25% |
| (2) Final Exam | 25% |
| (3) Reference paper (and presentation) | 25% |
| (4) Current Event Analysis: group paper and Presentation | 25% |

EXAMS
The midterm will cover the materials presented in class up to that point. The final exam is not comprehensive and will only cover materials from the midterm through the end of the semester.

REFERENCE PAPER (AND PRESENTATION)
Each student will research a specific topic related to information security or security management and present an analysis using concepts learned throughout the semester. *The resulting paper and/or presentation may be used to fulfill the GEB 6215 requirements*. Students will present their analysis and recommendations to the class at the end of the term.

CURRENT EVENT ANALYSIS: PROJECT AND PRESENTATION
Students will form *groups* of 3-4 to provide an analysis of a current event using concepts learned in class. Students will assess the business and technical risks related to information security, conduct a financial analysis related to the current event, and recommend a solution. Students will present their findings to the class before the beginning of each class, starting on the third week of the term.

## Additional Course Policies

Exam and Assignment Make-up Policy
Students are responsible for arranging to make up work missed because of legitimate reasons, such as illness, family emergencies, military obligation, court-imposed legal obligations or participation in University-approved activities. Examples of University-approved reasons to request make up work include participating on an athletic or scholastic team, musical and theatrical performances and debate activities. It is the student's responsibility to give the instructor notice prior to any such event, whenever possible. The instructor will then provide opportunities to prepare and submit make up work, without any reduction in the student's final course grade as a direct result of such events.

Late Assignments

All assignments are due by 11:59 PM on the due date indicated in the course schedule.
***Late assignments will be graded with a penalty of 10% of the grade for each day after the assignment's due date, up to a maximum of 3 days late (i.e., 30% penalty), beyond which the assignment will receive a grade 0 (zero).***
No extra assignments are permitted for additional credit in this course unless assigned by the instructor to the entire class.

Attendance Policy

Each student is responsible for keeping up with the class schedule, checking FAU email, and checking the course web site in Blackboard.

Academic Irregularities

It is valuable to work with a friend or classmate when working out a problem. However, the work that you perform for a grade must be your own work. Please note that none of the exams are collaborative, and any cheating attempts will be dealt with harshly and swiftly.

Cheating, plagiarism, copying, unauthorized collaboration, and hiring another person to do your assignments are unacceptable, and are subject to disciplinary actions, including, but not limited to, an "F" in the course, a letter of fact on your student record, and a notation on your transcript in accordance with the policies of FAU and the College of Business. In cases where this has occurred, both the person who cheats/plagiarizes/copies/collaborates/hires another person AND the originator of the work will be punished.

For information about the University's Honor Code, please refer to the policy statement under the section titled Selected College and University policies.

Anti-plagiarism Software

Written components of any assignment or project may be submitted to anti-plagiarism software to evaluate the originality of the work. Any students found to be submitting work that is not their own will be deemed in violation of the University's honor code discussed above.

Email

Students are required to have an email account for this course, and it is your responsibility to ensure that your email address listed on Blackboard is the one that you check regularly (you can always change it on Blackboard or set up auto-forward or POP download if not).

The best way to reach me is through sending an email message or visiting my office during office hours. Additionally, you are strongly encouraged to use Blackboard's Discussion Boards for questions of general interest.

ALL emails should:

- Have "ISM 6328" at the beginning of the subject line, so that I recognize that it is from one of you, and so that my spam filters do not accidentally delete your message.
- Include your name in the body of the message, since email addresses do not always identify the sender.
- Use proper salutations and signatures.
- Use the same type of language and manners that you would use in a formal, business setting.
- Ask specific questions which are not answered through Blackboard.

*If you do not follow these guidelines, I reserve the right to request a revised email with appropriate changes before addressing your questions or issues.*

Florida Atlantic University
COLLEGE OF BUSINESS

Course Outline (Tentative schedule)

[Classes marked with * will start with a group Current Event Analysis presentation]

| Week | Date | Plan | Assignments due |
|---|---|---|---|
| **1** | Aug 23 | Introduction to course contents, goals, and methodology<br>Introduction to Information Security (Chapter 1) | |
| | | **Aug 26: Last day to drop a course or withdraw without receiving a "W"** | |
| **2** | Aug 30 | Introduction to Information Security (Chapter 1) (cont'd)<br>The need for security (Chapter 2) | |
| **3** | Sep 6* | Legal, Ethical, and Professional Issues (Chapter 3) | |
| **4** | Sep 13* | Planning for security (Chapter 4) | |
| **5** | Sep 20* | Risk management (Chapter 5) | |
| **6** | Sep 27* | Security Technology (Chapters 6-7) | Deadline to select reference paper topic |
| **7** | Oct 4 | **Midterm Exam (online – Blackboard)**<br>**Guest speaker: TBA** | |
| **8** | Oct 11 | **Fall Break (no classes)** | |
| **9** | Oct 18* | Cryptography (Chapter 8) | |
| **10** | Oct 25* | **Guest speaker: TBA**<br>Physical security (Chapter 9) | |
| **11** | Nov 1* | Implementing Information Security (Chapter 10) | |
| **12** | Nov 8* | Security and Personnel (Chapter 11) | |
| **13** | Nov 15* | Information Security Maintenance (Chapter 12) | **Draft reference paper due today** |
| | | **Nov 18: Last day to drop a course or withdraw without receiving an "F"** | |
| **14** | Nov 22 | **Research (*individual*) presentations (6-8 min) [Part I]** | **Slides due on Nov 22, 11:59 pm** |
| **15** | Nov 29 | **Research (*individual*) presentations (6-8 min) [Part II]** | |
| **16** | Dec 7 | **Reading day – no classes** | **Final reference paper due today** |
| **17** | Dec 14 | **Final Exam (online – Blackboard)** | |

Florida Atlantic University
COLLEGE OF BUSINESS

**Selected University and College Policies**

Code of Academic Integrity Policy Statement
Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see University Regulation 4.001.

Disability Policy Statement
In compliance with the Americans with Disabilities Act Amendments Act (ADAAA), students who require reasonable accommodations due to a disability to properly execute coursework must register with Student Accessibility Services (SAS)—in Boca Raton, SU 133 (561-297-3880); in Davie, LA 131 (954-236-1222); or in Jupiter, SR 110 (561-799-8585) —and follow all SAS procedures. Their web site is: https://fau.edu/sas.

Religious Accommodation Policy Statement
In accordance with rules of the Florida Board of Education and Florida law, students have the right to reasonable accommodations from the University in order to observe religious practices and beliefs with regard to admissions, registration, class attendance and the scheduling of examinations and work assignments. For further information, please see Academic Policies and Regulations.

University Approved Absence Policy Statement
In accordance with rules of the Florida Atlantic University, students have the right to reasonable accommodations to participate in University approved activities, including athletic or scholastics teams, musical and theatrical performances and debate activities. It is the student's responsibility to notify the course instructor at least one week prior to missing any course assignment.

College of Business Minimum Grade Policy Statement
The minimum grade for College of Business requirements is a "C". This includes all courses that are a part of the pre-business foundation, business core, and major program. In addition, courses that are used to satisfy the university's Writing Across the Curriculum and Gordon Rule math requirements also have a minimum grade requirement of a "C". Course syllabi give individualized information about grading as it pertains to the individual classes.

Incomplete Grade Policy Statement

A student who is passing a course, but has not completed all work due to exceptional circumstances, may, with consent of the instructor, temporarily receive a grade of incomplete ("I"). The assignment of the "I" grade is at the discretion of the instructor, but is allowed only if the student is passing the course.

The specific time required to make up an incomplete grade is at the discretion of the instructor. However, the College of Business policy on the resolution of incomplete grades requires that all work required to satisfy an incomplete ("I") grade must be completed within a period of time not exceeding one calendar year from the assignment of the incomplete grade. After one calendar year, the incomplete grade automatically becomes a failing ("F") grade.

Withdrawals

Any student who decides to drop is responsible for completing the proper paper work required to withdraw from the course.

Grade Appeal Process

A student may request a review of the final course grade when s/he believes that one of the following conditions apply:

- There was a computational or recording error in the grading.
- Non-academic criteria were applied in the grading process.
- There was a gross violation of the instructor's own grading system.

The procedures for a grade appeal may be found in Chapter 4 of the University Regulations.

Disruptive Behavior Policy Statement

Disruptive behavior is defined in the FAU Student Code of Conduct as *"... activities which interfere with the educational mission within classroom."* Students who behave in the classroom such that the educational experiences of other students and/or the instructor's course objectives are disrupted are subject to disciplinary action. Such behavior impedes students' ability to learn or an instructor's ability to teach. Disruptive behavior may include, but is not limited to: non-approved use of electronic devices (including cellular telephones); cursing or shouting at others in such a way as to be disruptive; or, other violations of an instructor's expectations for classroom conduct.

**Faculty Rights and Responsibilities**

Florida Atlantic University respects the right of instructors to teach and students to learn. Maintenance of these rights requires classroom conditions which do not impede their exercise. To ensure these rights, faculty members have the prerogative:

- To establish and implement academic standards
- To establish and enforce reasonable behavior standards in each class
- To refer disciplinary action to those students whose behavior may be judged to be disruptive under the Student Code of Conduct.

## Bibliography

1. Gikas, 2015 “Information Systems Security: A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards.” File : FISMA GLBA HIPAA/Information_Security_White_Paper.pdf

2. National Science Foundation Cybersecurity Ideas Lab, “Interdisciplinary Pathways Toward a More Secure Internet” (2014) (focus on p. 20-41). File: future of security/CybersecurityIdeasLab_July2014.pdf

3. IEEE-USA Committee on Communications Policy, “Risking It All: Unlocking the Backdoor to the Nation’s Cybersecurity.” (2014). File: Future of Security/backdoors.IEEE.pdf

4. Addressing Cyber Security Through Public Private Partnership: An Analysis of Existing

5. Models, Intelligence and National Security Alliance, 2009

6. Howard, Michael; LeBlanc, David; & Viega, John. 19 Deadly Sins of Software Security. New York, NY: McGraw-Hill Osborne Media, 2005 (ISBN 0072260858).

7. Allen, Julia H., Barnum, Sean, Ellison, Robert J., McGraw, Gary, and Mead, Nancy R. Software Security Engineering: A Guide for Project Managers. Boston, MA: Addison-Wesley, 2008 (ISBN 032150917X).

8. Mark Weiser, “The Computer for the 21st Century.” Scientific American. Sep 2011, Vol. 265 Issue 3, p94. 8p. File: Argumented Reality/weiser-orig.pdf

9. Federal Trade Commission, “Financial Institutions and Customer Information: Complying with the Safeguards Rule.” File: FISMA GLBA HIPAA/GLBA safeguarding-customers-personal-information-requirement-financial-institutions copy

10. University of Minnesota, “GLBA Safeguards Rule Reference Guide.” File: FISMA GLBA HIPAA/glba_reference.uminn

11. Federal Financial Institutions Examination Council, “Authentication in an Internet Environment” (read text plus appendix). File: FISMA GLBA HIPAA/FFIEC authentication_guidance copy

12. Federal Financial Institutions Examination Council, "Supplement to Authentication in an Internet Banking Environment." File: FISMA GLBA HIPAA/FFIEC Supplement

13. D.J. Solove, "HIPAA Turns 10: Analyzing the Past, Present, and Future Impact." File: FISMA GLBA HIPAA/HIPAA Turns 10.pdf

14. C.J. Wang & D.J. Huang, "The HIPAA Conundrum in the Era of Mobile Health and Communications." File: FISMA GLBA HIPAA/The HIPAA Conundrum in the Era of Mobile Health and Com.pdf

15. M. Butler, "Top HITECH-HIPAA Compliance Obstacles Emerge." File: FISMA GLBA HIPAA/Top HITECH-HIPAA Compliance Obstacles Emerge.pdf

16. Z.A. Collier, D. DiMase, S. Walters, M. Tehranipoor, J.H. Lambert, I. Linkov, "Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities." File: Risk-Based Cybersecurity Standards – Policy Challenges and Opportunities.pdf

17. National Institute of Standards and Technology, 2014 "Framework for Improving Critical Infrastructure Cybersecurity." URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

18. "All Bill Information for S. 2588, Cybersecurity Information Sharing Act of 2014." File: Cyber Security Information Sharing/CISA Bill Details.pdf

19. Steven Norton, "Former NSA Director: Better Information Sharing Needed on Cybersecurity" Dec. 1, 2014. File: Cyber Security Information Sharing/Former NSA Director_ Better Information Sharing Needed on Cybersecurity – The CIO Report – WSJ.pdf

20. Global Internet Policy Initiative, "Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime" (2005). File: cybercrime/ Trust and Security in Cyberspace.pdf

21. R. Clarke, "Securing Cyberspace Through International Norms Recommendations for Policymakers and the Private Sector." File: SecuringCyberspace_web

22. Brian Harley, "A Global Convention on Cybercrime?" Columbia Science & Technology Law Review (2010). File: cybercrime/ A Global Convention on Cybercrime?

23. B. Elgin & M. Riley, “Now at the Sands Casino: An Iranian Hacker in Every Server” Bloomberg, Dec. 11, 2014. File: cyberwar/ Iranian Hackers Hit Sheldon Adelson’s Sands Casino in Las Vegas – Businessweek.pdf

24. Ernst & Young, “Bring your own device: Security and risk considerations for your mobile device program” (2013). File: security vs usability/ Bring_your_own_device.pdf

25. D. Norman, “When Security Gets in the Way” (2009). File: security vs usability/When Security Gets In the Way.pdf

26. R. Kainda, I. Flechais, A.W. Roscoe, “Security and Usability: Analysis and Evaluation” (2010). File: security vs usability/Security and Usability Analysis and Evaluation.pdf

27. T. Gonen, “Why Security Without Usability Leads To Failure” Forbes 2014. File: security vs usability/ Why Security Without Usability Leads To Failure – Forbes.pdf

28. R.L. Rutledge, A.K. Massey, A.I.Antón, and P.P. Swire, “Clarifying the Internet of Things by Defining the Internet of Devices,” ACM Computing Surveys, Currently under review. (Do not cite or circulate.) (pages 4 to 8, 18 to 31; optional 8-18] File: iod-survey-akm-15dec2014 copy

29. Paul Brody and Veena Pureswaran. “Device Democracy: Saving the future of the Internet of Things.” IBM Global Business Services Executive Report. URL: http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03620usen/GBE03620USEN.PDF

30. Burstein, 2015. “Conducting Cybersecurity Research Legally and Ethically” file: security ethics/Conducting Cybersecurity Research Legally and Ethically.pdf

31. P. Swire, “Going Dark vs. the Golden Age of Surveillance” (2011). URL: https://cdt.org/blog/‘going-dark’-versus-a-‘golden-age-for-surveillance’/

**Books**

[1] Whitman and Mattord, *Principles of Information Security*, 5th Edition, CENGAGE Learning, ISBN-13: 978-1285448367 (*current textbook*)
[2] Richard E. Smith, *Elementary Information Security*, 2nd Edition, Jones & Bartlett, ISBN-13: 978-1284055931
[3] Mjolsnes, *A Multidisciplinary Introduction to Information Security*, Chapman and Hall/CR, ISBN-13: 978-1420085907
[4] Bidgoli, Hossein, ed. Handbook of Information Security. Hoboken, NJ: Wiley, 2005.
[5] Boone, J. V. A Brief History of Cryptology. Annapolis, MD: Naval Institute Press, 2005.
[6] Bosworth, Bruce. Codes, Ciphers, and Computers: An Introduction to Information Security. Rochelle Park, NJ: Hayden Book Co., 1982.
[7] Bruen, Aiden A. and Mario Forcinito. Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. Hoboken, NJ: Wiley-Interscience, 2005.
[8] Calabrese, Thomas. Information Security Intelligence: Cryptographic Principles and Applications. Clifton Park, NY: Delmar Learning, 2004.
[9] Easttom, Chuck. Computer Security Fundamentals. Upper Saddle River, NJ: Pearson Prentice Hall, 2006.
[10] Erbschloe, Michael. Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code. Boston: Elsevier Butterworth Heinemann, 2005.
[11] Fugini, Mariagrazia, and Carlo Bellettini. Information Security Policies and Actions in Modern Integrated Systems. Hershey, PA: Idea Group Pub., 2004.
[12] Kairab, Sudhanshu. A Practical Guide to Security Assessments. Boca Raton, FL: Auerbach Publications, 2005.
[13] Kruegel, Christopher, Fredrik Valeur, and Giovanni Vigna. Intrusion Detection and Correlation: Challenges and Solutions. Advances in Information Security; 14. New York: Springer, 2005.
[14] Merkow, Mark S. and Jim Breithaupt. The Complete Guide to Internet Security. New York, NY: AMACOM, 2000.
[15] Peltier, Thomas R. Information Security Policies and Procedures: A Practitioner's Reference. 2nd ed. Boca Raton, FL: Auerbach Publications, 2004.
[16] Peltier, Thomas R., Justin Peltier, and John Blackley. Information Security Fundamentals. Boca Raton, FL: Auerbach Publications, 2005.
[17] Purser, Steve. A Practical Guide to Managing Information Security. Artech House Technology Management and Professional Development Library. Boston, MA: Artech House, 2004.
[18] Tipton, Harold F. and Micki Krause. Information Security Management Handbook. 5th ed. Boca Raton, FL: Auerbach, 2003. (Volume 1)
[19] Tipton, Harold F. and Micki Krause. Information Security Management Handbook. 5th ed. Boca Raton, London: Auerbach, 2005. (Volume 2)
[20] Wylder, John. Strategic Information Security. Boca Raton, FL: Auerbach Publications, 2004.

**Scholarly articles**

[1] Trim, Peter R.J. "Managing Computer Security Issues: Preventing and Limiting Future Threats and Disasters." *Disaster Prevention & Management* 14, no. 4 (2005): 493-505.

[2] Ryan, Julie J.C.H. "Information Security Tools and Practices: What Works?" IEEE Transactions on Computers 53, no. 8 (2004):1060-1063

[3] Ruiu, Dragos. "Learning From Information Security History." IEEE Security & Privacy 4, no. 1 (2006):77-79

[4] Jain, Anil K., Arun Ross, and Sharath Pankanti. "Biometrics: A Tool for Information Security." IEEE Transactions on Information Forensics and Security 1, no. 2 (2006):125-143

[5] Chesla, Avi. "Information Security: A Defensive Battle." Information Systems Security 12, no. 6 (2004): 24-32

Gmail

D Huang <dr.dhuang@gmail.com>

# Fwd: ITOM courses - title changes

1 message

**Tamara Dinev** <tdinev@fau.edu> Tue, Aug 30, 2016 at 5:31 PM
To: Jahyun Goo <jgoo@fau.edu>, Chiang-Sheng Huang <dhuang@fau.edu>

Hi Goo, Derrick, we received all the approvals we needed, both accounting and engineering
Please proceed. Thanking for checking the syllabi too!
Tamara

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: Hari Kalva <hari.kalva@fau.edu>
Date: 8/30/16 4:24 PM (GMT-05:00)
To: Tamara Dinev <tdinev@fau.edu>, Mihaela Cardei <mcardei@fau.edu>
Cc: Nurgun Erdol <erdol@fau.edu>
Subject: RE: ITOM courses - title changes

Dear Tamara, Our graduate and undergraduate program committees have reviewed the proposed changes and we do not have any objections.

Thank You,

Hari

---

**From:** Tamara Dinev
**Sent:** Thursday, August 25, 2016 4:53 PM
**To:** Mihaela Cardei <mcardei@fau.edu>; Hari Kalva <hari.kalva@fau.edu>
**Subject:** RE: ITOM courses - title changes
**Importance:** High

Dear Dr. Kalva, Dr. Cardei:

I know Dr. Erdol is out of the country so she will probably not checking her email. I am asking for your approval per my request below, the changes of the course titles below are quite trivial and the main purpose is to align the terms with the current name of our joint Big Data certificate. We are not changing any content.

I will be very thankful for your prompt response, we want to process fast for the first councils.

Thank you so much!

Best Regards:

Tamara

==========

Tamara Dinev, Ph.D.

Department Chair and Professor

Dean's Research Fellow

Department of Information Technology and Operations Management

College of Business

Florida Atlantic University

Boca Raton, Florida 33431

OFFICE: Fleming Hall, 219

TEL: (561) 297-3181

FAX: (561) 297-3043

e-mail: tdinev@fau.edu

---

**From:** Tamara Dinev
**Sent:** Wednesday, August 24, 2016 7:37 AM
**To:** Nurgun Erdol <erdol@fau.edu>
**Subject:** ITOM courses - title changes
**Importance:** High

Dear Nurgun:

I am seeking your approval on the proposed title (and course description in some) changes (see below) of our courses related to the Business Analytics and Information Security.

The reason for the title changes is to align the course titles and descriptions with the current terminology in the business discourse and the current FAU strategic plan for Data analytics. When ITOM created its concentration and courses back in 2004, the predominant term for analyzing data for knowledge discovery was "business intelligence". Recently, this term is less and less used in the public discourse and I find it difficult in explaining to students and constituents. They think about more investigation rather than analysis. Nationwide MIS programs with Business Analytics also moved away from this term as well as the general textbooks about Information Systems, such as for ISM 3011. Computer Science has already renamed/created their courses to include terms such as "Big Data" and "Data Analytics"

Likewise, Information Security Management outlets, the NIST standards and the NSA vocabulary moved toward the term "Information Assurance". In light of the NSA educational certification we are all seeking the overarching term used is Information Assurance.

For these reasons, the proposed changes are as follows:

| Course | Old Title (Description given if changed) | New Title and Description |
|---|---|---|
| ISM 4332 | Information Security Management | Management of Information Assurance and Security |
| ISM 6328 | Information Security Management<br><br>An introduction to the various technical and administrative aspects of information security. Emphasis is on the management of information security efforts. | Management of Information Assurance and Security<br><br>An introduction to the organizational, compliance, and technical aspects of information security and information assurance management. Review of programs, standards, and practices. |
| ISM 3116 | Introduction to Business Intelligence<br><br>Provides an understanding of the business intelligence processes and techniques used in transforming data to knowledge and value in organizations. Students also develop skills to analyze data using generally available tools (e.g., Excel) | Introduction to Business Analytics and Big Data<br><br>Provides an understanding of the business intelligence and business analytics processes and techniques used in transforming data to knowledge and value in organizations. Students also develop skills to analyze data using generally available tools (e.g., Excel) |
| ISM 6404 | Introduction to Business Intelligence<br><br>This course provides an understanding of the business intelligence processes and techniques used in transforming data to knowledge and value in organizations. Students also develop skills in analyzing data using generally available tools, e.g., Excel. | Introduction to Business Analytics and Big Data<br><br>This course provides an understanding of the business intelligence and business analytics processes and techniques used in transforming data to knowledge and value in organizations. Students also develop skills in analyzing data using generally available tools, e.g., Excel. |
| ISM 4403 | Advanced Business Intelligence | Advanced Business Analytics |
| ISM 4117 | Data Mining and Data Warehousing | Data Mining and Predictive Analytics |
| ISM 6136 | Data Mining and Data Warehousing | Data Mining and Predictive Analytics |

Please give your feedback so I can prepare presenting the changes to the councils

Best Regards:

Tamara

==========

Tamara Dinev, Ph.D.

Department Chair and Professor

Dean's Research Fellow

Department of Information Technology and Operations Management

College of Business

Florida Atlantic University

Boca Raton, Florida 33431

OFFICE: Fleming Hall, 219

TEL: (561) 297-3181

FAX: (561) 297-3043

e-mail: tdinev@fau.edu