**Course Syllabus**
**IDS 520: Enterprise Information Infrastructure Planning & Security**

## Course Overview

Enterprises rely on a complex infrastructure of applications, systems, software, database and networking technologies to provide the services and information required to achieve business objectives. While this infrastructure is a means to an end, most businesses recognize that competitiveness is manifested in how a firm integrates and delivers commercially available information technology (IT) into an infrastructure that successfully achieves business application requirements. This is evidenced by many firms seeking IT individuals not only with pure technical skills, but with more rounded planning and management skills so that IT planning can add true business value.

To this end, this course introduces students with methods and practices involved in the planning, design and security of information infrastructure commonly found in large and medium enterprises. The course blends concepts and techniques found in project planning, system design and development, technology planning, and security technology with those found in enterprise architecture planning, with the goal of providing students with the ability and understanding of how to plan and design a secure information infrastructure for a firm.

The course will be divided into two modules. The first module will focus on enterprise information infrastructure planning techniques and processes. The second module will focus on information infrastructure security, protection and management. Students will be organized into work teams that will work on both assignments and a term project. For assignments, students are encouraged to work with their team to review and discuss solutions and help each other learn. Each team will also be required to produce a term project on a case study that will reflect application of the techniques learned in class, to be turned in and presented in two parts: mid-term and at the conclusion of class. To master the material in this course, students are advised to utilize the text books that are assigned to complete assignments and quizzes on time. Students will be required to read the assigned sections in the textbooks prior to class each week. Students will be required to take the on-line quiz based on the reading assignment to certify that they have read and understood the material. The grade in the course will be determined on the basis of class participation, team project, assignments and quizzes.

## Learning Outcomes

The course is an introduction to current practices and decision-making relative to information systems infrastructure, recognized by today's business enterprises for competing in today's global economy driven by electronic commerce and online business. It is intended to provide students an introduction to key functional areas, provide them with sufficient knowledge to make decisions and introduce terminology and concepts useful for communicating with operating personnel.

**Method of Instruction**
Each week, readings will be assigned in preparation for the next week. Students will take an-online quiz to certify understanding and the reading of the material. Each class session will be divided into two parts. The first part will be a lecture which will review and summarize concepts and techniques covered in the readings. The second part will be an open lab session in which students will work with their teams on their class assignment and/or project.

**Prerequisites**
IDS and University requirements apply. Courses or equivalent training and/or experience in management information systems, information systems analysis and design are a plus.

**Course Requirements:**
- Assignments: 25%
- Term project: 25%
- On-line Quizzes: 25%
- Attendance & Participation: 25%

**Policies:**
- Attendance and tardiness are expected. Attendance will be taken into account for borderline students.
- Late assignments will not be accepted without instructor consent
- Class participation is required and considered in the overall grade

**Honor Code:**
The CBA Honor Code will be in effect. (Refer to: http://www.uic.edu/cba/Faculty/academicaffairs/honorcode.html for more information)

**Course Texts**
Note: Readings, assignments and quizzes will be directly taken from texts listed as "Required." Texts listed as "Optional" provide supplemental information that may be useful to students for fulfilling course requirements, but are not required to do so. The text titles are listed for each of the two modules.

**Schedule of Course Topics (Tentative):**
Note: This course syllabus provides a general plan for the course; deviations may be necessary. It is the student's responsibility to stay apprised of changes in assignments, due dates, material to be covered, etc. The dates on which the following topics are covered are contained in the file named *IDS 520 Class Schedule and Assignments* that is posted on the course Blackboard Web site under the *Course Information* folder.

**MODULE 1:**
**ENTERPRISE INFORMATION ARCHITECTURE PLANNING**

Required text:

- *Network Analysis, Architecture and Design, 3rd Edition*. James D. McCabe, Morgan Kaufman, 2007, ISBN 978-0-12-370480-1.

Optional texts and readings:

- *A Practical Guide to Federal Enterprise Architecture*, CIO Council, Feb. 2001.
- *Enterprise Architecture at Work: Modeling, Communication and Analysis*, Springer 2nd ed. Sept, 2009, ISBN-10: 3642013090, ISBN-13: 978-3642013096.
- *Mission-Critical Network Planning*, Matthew Liotine, Artech House, 2003, ISBN 158053516-X.

**Course Introduction, Enterprise Infrastructure Project Development**

- Course requirements
- Definition & mission of successful infrastructure projects.
- Overview of Analysis, Architecture, and Design Processes
- Systems Methodology Overview
- System Description & Characterization
- Service Description & Characterization
- Performance Characteristics
- Network Supportability

**Infrastructure Requirements & Design**

McCabe: Chpts. 1, 2, 3

- Requirements and Features
- User Requirements
- Application Requirements
- Device Requirements
- Network Requirements
- Other Requirements
- Gathering and Listing Requirements
- Developing Service Metrics
- Characterizing Behavior
- Developing RMA Requirements
- Developing Delay Requirements
- Developing Capacity Requirements
- Environment-Specific Thresholds and Limits
- Requirements for Predictable and Guaranteed Performance
- Requirements Mapping
- Developing the Requirements Specification

**Data & Information Architecture & Flow Analysis**

McCabe: Chpts. 4, 5

- Flow Characterization
- Identifying and Developing Flows
- Data Sources and Sinks
- Flow Models
- Flow Prioritization
- The Flow Specification
- Architecture and Design
- Component Architectures
- Reference Architecture
- Architectural Models
- Systems and Network Architectures

**Addressing & Routing**

McCabe: Chpts. 6

- Addressing Mechanisms
- Routing Mechanisms
- Addressing Strategies
- Routing Strategies

**Infrastructure Performance & Management Planning**

McCabe: Chpts. 7, 8

- Network Management Mechanisms
- Architectural Considerations
- Developing Goals for Performance
- Performance Mechanisms

**Technology Design & Procurement**

McCabe: Chpts. 10

- Design Concepts
- Design Process
- Vendor, Equipment, and Service-Provider Evaluations
- Network Layout & Diagramming
- Design Traceability
- Design Metrics

**Module 1 Case Study Project Presentation**

Student teams will each present and review their infrastructure case study projects to the class.

**MODULE 2:**
**ENTERPRISE INFORMATION ARCHITECTURE SECURITY & PROTECTION**

Required text:

- *Management of Information Security , 3rd Edition*, Michael E. Whitman & Herbert J. Mattord, Delmar, Cengage Learning 2010, ISBN-10: 1-4354-8884-9 ISBN-13: 978-1-4354-8884-7.

Optional texts and readings:

- *Readings and Cases in the Management of Information Security, 1st Edition,* Michael E. Whitman & Herbert J. Mattord, Course Technology, 2006, ISBN-10: 0619216271 ISBN-13: 9780619216276.
- *Information Security: Principles and Practices,* Mark Merkow & James Breithaupt, Prentice Hall, 2006, ISBN-10: 0131547291, ISBN-13: 9780131547292.

**Information Infrastructure Security Overview**

McCabe: Chpts. 9

Whitman & Mattord: Chpts. 1

- Principles of Information Security
- CNSS Security Model
- Security and Privacy Administration & Mechanisms
- Physical Security and Awareness
- Protocol and Application Security
- Network Perimeter Security
- Remote Access Security
- Information Security Project Management

**Information Security & Continuity Planning**

Whitman & Mattord: Chpts. 2, 3

- Strategic Planning
- Information Security Governance
- Planning for Information Security Implementation
- Introduction to the Security Systems Development Life Cycle
- Components of Contingency Planning
- Business Impact Analysis
- Disaster Recovery Plan
- Business Continuity Plan
- Business Resumption Planning
- Testing Contingency Plans

**Information Security Policy & Programs**

Whitman & Mattord: Chpts. 4, 5

- Need for Policy, Standards, and Practices
- Enterprise Information Security Policy (EISP)
- Issue-Specific Security Policy (ISSP)
- System-Specific Security Policy (SysSP)
- Guidelines for Effective Policy
- Developing Information Security Policy
- Policy Compliance & Enfprcement

- Automated Tools
- Defining a Framework for Policies
- Preparing a Coverage Matrix,
- SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems
- Organizing for Security
- Placing Information Security within an Organization
- Components of the Security Program
- Information Security Roles and Titles
- Implementing Security Education, Training, and Awareness Programs

**Security Management Models**

Whitman & Mattord: Chpts. 6

- Blueprints, Frameworks, and Security Models
- Access Control Models
- Security Architecture Models
- Trusted Computing Base
- ITSEC
- The Common Criteria
- Bell-LaPadula Confidentiality Model
- Biba Integrity Model
- Clark-Wilson Integrity Model
- Graham-Denning Access Control Model
- Harrison-Ruzzo-Ullman Model
- The ISO 27000 Series
- NIST Security Models
- SP 800-53A
- Information Security Governance Framework

**Security Management Practices**

Whitman & Mattord: Chpts. 7

- Benchmarking Recommended Security Practices
- The Gold Standard
- Limitations to Benchmarking and Recommended Practices
- Support for Baselining and Recommended Practices
- Performance Measures in Information Security Management
- InfoSec Performance Management & Metrics
- Reporting InfoSec Performance Measures
- Emerging Trends in Certification and Accreditation
- SP 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
- SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations

**Risk Management**

Whitman & Mattord: Chpts. 8, 9

- Risk Identification
- Creating an Inventory of Information Assets
- Threat Identification
- The TVA Worksheet
- Risk Assessment
- Assessing Potential Loss
- Risk Determination
- Access Controls
- Documenting Risk Assessment
- Risk Control Strategies
- Feasibility and Cost-Benefit Analysis
- Recommended Risk Control Practices
- Qualitative and Hybrid Measures
- The OCTAVE Methods
- Microsoft Risk Management Approach
- FAIR
- ISO 27005 Standard for Information Security Risk Management

**Security Protection Mechanisms**

Whitman & Mattord: Chpts. 10

- Access Controls
- Identification, Authentication & Authorization
- Evaluating Biometrics
- Firewalls
- Intrusion Detection and Prevention Systems (IDPS)
- Remote Access Protection
- RADIUS and TACACS
- Wireless Networking Protection
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Max & Bluetooth Access
- Scanning and Analysis Tools
- Cryptography

**Personnel Security & Security Law and Ethics**

Whitman & Mattord: Chpts. 11, 12

- Staffing the Security Function
- Information Security Professional Credentials
- Employment Policies and Practices
- Information Security and the Law
- Ethics in Information Security
- Professional Organizations and their Codes of Ethics
- Organizational Liability and the Need for Counsel
- Key Law Enforcement Agencies
- Managing Investigations in the Organization

**Module 2 Project Presentations**

Student teams will each present and review their security case study plans to the class.