NATIONAL UNIVERSITY OF ENGINEERING
COLLEGE OF INDUSTRIAL AND SYSTEMS ENGINEERING
SYSTEMS ENGINEERING PROGRAM

SYLLABUS - ST275 INFORMATION SYSTEMS AUDITING

I. GENERAL INFORMATION

CODE	:	ST275
SEMESTER	:	10
CREDITS	:	3
HOURS PER WEEK	:	4 (Theory – Practice)
PREREQUISITES	:	ST215 Information Security
CONDITION	:	Compulsory
INSTRUCTOR	:	Humberto Arteaga, Nelly Huarcaya
INSTRUCTOR E-MAIL	:	ahuarcaya@gmail.com

II. COURSE DESCRIPTION

This course is divided in two parts. In the first part, students are given knowledge about audit, techniques, methods and others to integrate audit teams, so that they can carry out systems audit work, mainly from the audit planning to the handing over and formulation of the audit report. In the second part, students are trained in all basics so that they are capable of implementing information systems and good practices.

III. COURSE OUTCOMES

1. Planning – For an audit work and/or security, a proper drawing up of information must be carried out according to proposed objectives, and it should allow perform works and planning, for both audit and information security.
2. Analysis – Allows to apply all the knowledge students acquired so far in a proper system audit work or information security works. .
3. Apply Internal Control criteria in all processes / activities in the professional career. As well as the application of ITIL and Cobit good practices.
4. Manage main risks in the enterprise information integrity, confidentiality and availability, on the basis of risks analysis.
5. Propose alternatives based on cases involving design and implementation of protection mechanisms against main computer crime techniques.

IV. LEARNING UNITS

1. BASIC CONCEPTS AND PREVIOUS DEFINITIONS / 4 HOURS
Introduction to the course / Basic concepts for the course performance / Legal aspects of computing / Governmental audit.

2. TOOLS AND AUDIT SYSTEMS DEFINITIONS / 2 HOURS
Systems audit definition / Computer assisted audit techniques – CAAT and general techniques.

3. FUNDAMENTALS FOR A SYSTEM AUDIT PLANNING / 6 HOURS

ISACA and Cobit / Internal Control System / Internal Control Questionnaire / Methodology for a system audit work / Formulation of an audit plan / Resolution of proposed cases.

4. PLANNING AND EXECUTION OF A SYSTEMS AUDIT WORK

Audit program formulation / Audit findings formulation / Study of audit cases / Remarks, conclusions and recommendations formulation / Resolution of proposed cases.

5. AUDIT REPORTS / 3 HOURS

Formulation of a technical audit report / Formulation of an audit report / Audit work documents / Resolution of proposed cases.

6. INFORMATION SECCURUTY AND IT RISKS ASSESSMENT / 6 HOURS

Information security, basic principles / Risks management and risk matrix / CISO (Chief Information Security Officer) certifications and basics for the implementation of a Information Security Management System model – ISMS, based on Series 2700X ISO standards.

7. ISMS MODEL IMPLEMENTATION – PART I / 9 HOURS

Domain 01: Security policy / Domain 02: Security organization / Information security organization / Domain 03: Assets administration / Assets management / Domain 04: Human resources security / Domain 05: environmental and physical security / Domain 06: Operation and communication management / Domain 07: Access control system / Access control.

8. ISMS MODEL IMPLEMENTATION – PART II / 6 HOURS

Domain 08: Information system acquisition, development and maintenance / Domain 09: Administration / Information security incidents management / Domain 10: Business continuity planning / Business continuity management / Domain 11: Fulfillment.

V. LABORATORIES AND PRACTICAL EXPERIENCES:

Lab 1: Formulation of the audit planning based on certain objective.
Lab 2: Audit findings formulation.
Paper 1: Handing over of audit report.
Lab 3: Functions of Information security area.
Lab 4: Carrying out of actions, proceedings and/or processes to implement ISMS domains.
Paper 2: Complete handing over of the information security management system.

VI. METHODOLOGY

This course is carried out in theory, practical and lab sessions. In theory sessions, the instructor introduces concepts, fundamentals and applications. In practical sessions, several exercises, cases and problems are solved, and their solutions are analyzed. In lab sessions, real application cases are studied for the carrying out of an audit work from the planning to the audit report handing over. Likewise, the progressive handing over of the implementation of an information security management system based on Information security ISO standards. Labs are graded and students must hand in an integrator project or paper. In all sessions students' active participation is encouraged.

VII. EVALUATION FORMULA

The average grade PF is calculated as follows:

PF = [EP+EF+3(L1 + L2 + TF1) + 3(L3 + L4 + TF2)] / 22

EP: Mid-Term Exam EF: Final Exam TF#: Final paper
T#: Quizzes L#: Laboratories

VIII. BIBLIOGRAPHY

1. **PIATTINI, MARIO AND DEL PESO, EMILIO (Coordinators)**
   Information Technology Audit, A Practical Approach (Spanish)
   Alfaomega-Rama Editorial, 2nd Edition, revised and expanded, 2005
2. **DERRIEN, YANN**
   Information Technology Audit Techniques (Spanish)
   Alfaomega-Rama Editorial, 2005
3. **JOSÉ ANTONIO ECHENIQUE**
   Information technology Audit (Spanish)
   Ed. Mc-Graw Hill
4. **COBIT STEERING COMMITTEE AND THE IT GOVERNANCE INSTITUTE**
   COBIT Management Guidelines 4.1, 2008