NATIONAL UNIVERSITY OF ENGINEERING
COLLEGE OF SCIENCES

COMPUTER SCIENCE PROGRAM

CC0A6 – INFORMATION SYSTEMS AUDITING

I. GENERAL INFORMATION

CODE	: CC0A6 Information Systems Auditing
SEMESTER	: 8-10
CREDITS	: 4
HOURS PER WEEK	: 6 (Theory, Practice)
PREREQUISITES	: CC411 Computer and Information Security
CONDITION	: Elective

II. COURSE DESCRIPTION

The course prepares students for understanding and applying the methods and techniques for the auditing of information systems and technologies, the examination of the management controls within an information technology infrastructure. Students learn to select, analyze and evaluate pertinent evidences for determining if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization goals and objectives. The evaluation includes system internal control design and effectiveness, efficiency and security protocols, development processes, and information technology governance and oversight. The COBIT model is analyzed and applied for the auditing of a real information systems and technology company.

III. COURSE OUTCOMES

At the end of the course students:

1. Understand and apply the methods for information systems and technologies monitoring and control commonly used in business and enterprises.
2. Evaluate the operativeness of computer-based systems, as well as the reliability and security of information systems and technologies.
3. Know and properly apply the information systems and technology auditing software applications available in different business settings.
4. Elaborate complete and well-supported auditing appraisals, opinions and documents.

IV. LEARNING UNITS

1. GENERAL CONCEPTS

Introduction to auditing. Evaluation, control and monitoring. Auditing types and forms. Systems auditing: concepts, objectives and scope. System auditing classes. Revision of information system concepts. Auditing systemic and integral approach. Development of technological innovation projects. Organization, management and functioning of computing-based business. Control systems: concepts and types. Analysis of practical case.

2. INFORMATION TECHNOLOGY CONTROL SYSTEMS
Auditing steps and process. Information technology control structure. Norms and standards. Software applications for each auditing step. Analysis of a practical case.

3. INFORMATION TECHNOLOGY MANAGEMENT EVALUATION
Systems management. Information systems management. Control systems. Organization controls and administration controls. Operational controls regarding computing resources usage. Operational controls regarding information use and information reliability. Applicable norms and standards. Analysis and solution of a practical case.

4. INFORMATION SECURITY EVALUATION
Evaluation of information security system. Revision of computing security concepts and norms. NTP ISO-17799 norm. ISO 27001 Norm. Plan-Do-Check-Act PDCA cycle. Analysis and solution of a practical case: systems auditing techniques, check list, sampling, wrong transactions, security violation.

5. ISO 27001 NORM. INFORMATION SECURITY
Information security policies. Organization of information security (7 controls). Human resource security. Asset management. Access control. Cryptography. Physical and environmental security. Operational security. Communications security. System acquisition, development and maintenance. Supplier relationships. Information security incident management. Information security aspects of business continuity management. Compliance with internal (policies) and external (law) requirements.

6. APPLICATION SYSTEMS EVALUATION
Application systems auditing. Input-output control. Process control. Library control. Logic and physical access control. Use of software application and tools. Revision of applicable norms. System and operating procedures analysis. Internal control weakness and strengths. Security systems weakness and strengths. Analysis and solution of a practical case.

7. INFORMATION PROJECTS EVALUATION
Information projects auditing. Project life-cycle. Planning stage controls. Execution stage controls. Deployment stage controls. Administration and follow-up controls. Determination of applicable criteria.

8. COBIT MODEL
Control Objectives for Information and Related Technologies. Information technology management and governance. COBIT components: framework, process descriptions, control objectives, management guidelines, maturity models. Processes: Evaluate, Direct and Monitor (EDM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). Analysis and solution of practical case. Audit opinion elaboration, following and control. Monitoring corrective and improvement actions.

9. QUALITY ASSURANCE EVALUATION
Preventive auditing. Information technologies quality assurance. Information systems quality assurance. ISO norms application.

V. METHODOLOGY

The course takes place in theory and practice sessions. In theory sessions, the instructor presents the concepts, methodologies, processes and models for information systems and information technology auditing. In practice sessions, instructor and students work together for analyzing and proposing solutions to different problems related information systems and technology auditing in different types of companies and operation environments. At the end of the course, each student group present and defend the final project report.

VI. EVALUATION FORMULA

The final grade PF is calculated as follows:

$$PF = 0.20\ EP + 0.3\ EF + 0.20\ PR + 0.30\ TF$$

where:

PF: Final grade EP: Mid-term exam EF: Final exam
PR: Practice work: TF: Final project report and defense

VII. BIBLIOGRAPHY

1. Information Systems Auditing
   Jack Champlain
   Wiley Editions, 2018.
2. Information Systems Control and Audit
   Ron Weber
   Pearson Editions, 2016
3. COBIT 5 Framework
   ISACA, 2015