



COURSE SYLLABUS

**Course Name: NITA 422:
End-User systems planning and design**

Instructor:

Office Hours:

Office: Telephone:

Internet/E-Mail Address:

Course Description: This course focuses on planning and designing end-user systems that deliver information services and resources. Emphasis is on end-user needs assessment, alternative system designs, security planning, support issues, and training and development. Topics include analyzing the business case, requirements modeling, enterprise modeling and development strategies. Students also learn about data design, the user interface, input and output design, system architecture, systems implementation and systems operations and support. Students will develop a proposal for a new or revised end-user system that reflects the principles covered in the course.

Purpose: The purpose of this course is to provide undergraduate level students with an educational experience in the application of Systems Analysis techniques to Network and Information Security projects. The student will apply theory and principles to network security policy, information systems computer and network facilities, and the life cycle development process.

Scope: The scope of the material to be covered includes the demonstrate knowledge of the principles and practices of the following information technology disciplines:

- Information security
- Business communication
- End user need assessment
- Technology support best practice
- Disaster recovery and business continuity
- Information technology measuring, reporting and controlling
- Information technology strategy

Course Objectives: Upon successful completion of this course, students will be able to:

- Describe the fundamental systems development life cycle
- Recognize the various roles on a project team
- Create a system request
- Assess technical, economic and organizational feasibility
- Perform a feasibility analysis
- Create a project work plan

- Use techniques for staffing a project
- Recognize how to reduce risk on a Information Assurance project
- Recognize when to use various business process analysis strategies
- Use various methods for gathering information
- Create Data Flow Diagrams
- Create Entity Relationship Diagrams
- Develop a design plan using appropriate design strategies
- Differentiate between server-based, client-based and client-server base computing Create a network model
- Develop hardware and software specifications
- Create a information Security plan
- Design user interfaces using proper design principles
- Write program specifications
- Create a structure chart
- Develop documentation
- Develop Change Management plan

Required Texts and Handouts: Students will receive reading assignments that may include handout material, and/or research searches, and is responsible to read and act on the material as directed. The required texts are:

Textbook: Systems Analysis and Design, Seventh Edition

Author: Shelly Cashman Rosenblatt

Publisher: Thompson, 2008

ISBN: 978-1-4239-1222-4

Paperback, 702 pages and various handouts as determined by your instructor

Course Content and Schedule: This schedule is an approximate timeline for the student.

Unit 1: INTRODUCTION TO SYSTEMS DESIGN AND ANALYSIS

Chapter 1 and handouts

1.1 Introduction to systems design and analysis

1.1.1 Introductions

1.1.2 Course Review and Intro

1.1.3 Impact of information Technology

1.1.4 Roll of systems design and analysis

1.1.5 Information systems Components

1.1.5.1 Hardware

1.1.5.2 Software

1.1.5.3 Data

1.1.5.4 Processes

1.1.5.5 People

1.1.6 Future of IT

1.1.6.1 Moore's Law

1.1.6.2 Aspects of security

1.1.6.3 Accreditation

1.1.6.3.1 Certification process leading to successful accreditation

1.1.6.3.2 Importance of accreditation

1.1.6.3.3 Types of accreditation

1.1.6.3.4 Facilitate certification process leading to successful accreditation

1.1.6.3.5 Significance of NSTISSP No.6

1.1.7 Electronic Commerce

1.1.7.1 Disposition of Classified Materials

1.1.8 XML

1.1.9 Enterprise Resource Planning

1.1.9.1 Facilities Planning

1.1.9.2 System disposition/reutilization

1.1.10 Knowledge Management Systems

1.1.11 CASE Tools

1.1.12 Microsoft Solutions Framework

1.1.13 Lifecycle planning

1.1.13.1 Life cycle system security planning

1.1.13.2 System Security Architecture

Unit 2: SYSTEMS PLANNING

Chapter 2

2.1 Strategic Planning

2.2. Mission Statements

2.3 Biometric Devices

2.4 JIT Systems

2.5 CRM Systems

2.6 TCO

2.7 Approvals

2.7.1 Approval to Operate

2.7.1.1 Purpose and contents of ATO

2.7.1.2 Importance of risk assessment to support granting an ATO

2.7.2 Interim Approvals to Operate

2.7.2.1 Describe IATO

2.7.2.2 Purpose and contents of IATO

2.7.2.3 Importance of risk assessment to support granting an IATO

2.7.2.4 Facilitate implementation of risk mitigation strategies necessary to obtain IATO

2.7.3. Systems Security Authorization agreement

2.7.3.1 Importance of the SSAA

2.8 Policy Waivers to continue operations

2.8.1 Risk mitigation strategies necessary to obtain waiver

2.8.2 Ensure risk assessment supports granting waiver

2.9 Recertification

- 2.9.1 Describe recertification
- 2.9.2 Recertification effort
- 2.9.3 Importance of recertification process
- 2.9.4 Identify characteristics of information systems that need re-certification
- 2.9.5 Initiate the recertification effort
- 2.10 Project Management Tools
 - 2.10.1 Fishbone Diagrams

Unit 3: SYSTEMS ANALYSIS

Chapter 3 thru 6

- 3.1 Requirements Modeling
 - 3.1.1 Application Development
 - 3.1.1.1 JAD
 - 3.1.1.2 RAD
 - 3.1.3 The Unified Modeling Language
 - 3.1.4 The Zachman Framework
 - 3.1.5 Sampling
 - 3.1.6 Yourdon Symbols
 - 3.1.7 Data Dictionaries
 - 3.1.8 Structured English
 - 3.1.9 Decision Tables
- 3.2 Object Modeling
 - 3.2.2 Object oriented design
- 3.3 Development Strategies
 - 3.2.1 Outsourcing
 - 3.2.1 Application Service Providers
 - 3.2.2 Value Added Resellers
 - 3.2.3 Contracting for Security and network development services
 - 3.2.3 In-House Software Development
 - 3.2.4 Allocate Resources
 - 3.2.4.1 Resource roles and responsibilities
 - 3.2.4.2 Budget/Resource Allocation
 - 3.2.4.2.1 information assurance budget defense
 - 3.2.4.3 Business Aspects of information Security
 - 3.2.4.3.1 protection of commercial proprietary information
 - 3.2.4.3.2 business aspects of information security
 - 3.2.4.3.3 protecting commercial proprietary information
 - 3.2.5 Benchmark Tests
 - 3.2.6 ANSI
- 3.3 Output and User interface design
 - 3.3.1 Printed Output
 - 3.3.2 Output Control and Security
 - 3.3.3 User Interface Design
 - 3.3.4 Human-Computer Interaction
 - 3.3.5 Input Devices

3.3.6 Data Entry

Unit 4: SYSTEMS DESIGN

Chapter 7 thru 9

4.1 output and User Interface Design

4.1.1 E-Mail

- 4.1.1.1 Printed Output
- 4.1.1.2 Output Control and Security
- 4.1.1.3 User Interface Design
- 4.1.1.4 Human-Computer Interaction
- 4.1.1.5 Input Devices

4.1.2 Data Entry

- 4.1.2.1 HTML
- 4.1.2.2 Referential Integrity
- 4.1.2.3 Entity-Relationship Diagrams
- 4.1.2.4 Cardinality
- 4.1.2.5 Normalization
- 4.1.2.6 Data Warehousing
- 4.1.2.7 Data Mining

4.2 Data Design

- 4.2.1 Total Cost of Ownership
- 4.2.2 Legacy Systems
- 4.2.3 Local and Wide Area Networks
- 4.2.4 Client/Server Architecture
- 4.2.5 Middleware
- 4.2.6 The OSI Reference Model
- 4.2.7 Network Protocols
- 4.2.8 Backup and Disaster Recovery

4.3 Systems Architecture

- 4.3.1 Software Engineering
- 4.3.2 ISO
- 4.3.3 Application Development
- 4.3.4 Pseudo code
- 4.3.5 System Testing
- 4.3.6 Documentation
- 4.3.7 Training
- 4.3.8 Data Conversion
- 4.3.9 System Security Architecture

Unit 5: SYSTEMS IMPLEMENTATION

Chapter 10

5.1 Systems Implementation

- 5.1.1 Help Desks
- 5.1.2 Software Reengineering
- 5.1.3 Configuration Management
- 5.1.4 Version Control

- 5.1.5 Capacity Planning
- 5.1.6 Identity Management
- 5.1.7 Backup and Disaster Recovery
- 5.1.8 IT Credentials

Unit 6: SYSTEMS OPERATION, SUPPORT AND SECURITY

Chapter 11

6.1 Systems Operation, Support and security

- 6.1.1 Objectives
 - 6.1.1.1 Certification and Accreditation
 - 6.1.1.2 Information ownership
 - 6.1.1.3 System Certifiers and Accreditations
 - 6.1.1.4 Risk Analysts
 - 6.1.1.5 Information systems Security manager
- 6.1.2 User support activities
- 6.1.3 Maintenance Activities
- 6.1.4 Managing systems support
 - 6.1.4.1 Information systems Security manager
 - 6.1.4.2 Information system Security Officer
- 6.1.5 Managing system Performance
- 6.1.6 System Security
- 6.1.7 Data Backup and Recovery
- 6.1.8 System Obsolescence

Unit 7: THE SYSTEMS ANALYST'S TOOLKIT

Toolkit 1 through 5

7.1 Communications toolkit

- 7.1.1 Effective Written Communication
- 7.1.2 Grammar Checkers
- 7.1.3 Readability
- 7.1.4 Effective Presentations
- 7.1.5 Presentation Software

7.2 CASE toolkit

- 7.2.1 Fourth-Generation Languages
- 7.2.2 The CASE Tool Marketplace
- 7.2.3 Integrated Development Environments
- 7.2.4 The Visible Analyst CASE Tool
- 7.2.5 The System Architect CASE Tool
- 7.2.6 Certification Test and Evaluation
 - 7.2.6.1 Importance of CT&E as part of the acquisition process.
- 7.2.7 Certification Tools
- 7.2.8 Product Assurance
 - 7.2.8.1 Importance of protection profiles

7.2.8.2 Importance of security targets

7.3 Financial Toolkit

7.3.1 Payback Analysis

7.3.2 Return on Investment Analysis

7.3.3 Present Value Analysis

7.3.4 The Time Value of Money

7.3.5 Contracting for security services

7.3.5.1 When is contracting for security services is appropriate

7.3.5.2 Identifying threats from contracting for security services

7.4 Project Management toolkit

7.4.1 Project Management

7.4.2 Gantt Charts

7.4.3 PERT/CPM

7.4.5 Project Management Software

7.4.6 Software Change Control

7.5 Internet Resource Tools

7.5.1 The World Wide Web

7.5.2 Search Engines

7.5.3 The Invisible Web

7.5.4 Newsgroups

7.5.5 Instant Messaging