UiO : Department of Informatics
IN2120 Information Security
Reading syllabus 2018
Lectures 1 - 12

Text book: Harris & Maymí, CISSP All-in-One Exam Guide, 7th Edition, 2016

Reading syllabus according to the 8th Edition 2018 comes in October 2018.

L01: Course Info + Basic IS Concepts   Date: 21.08.2018

- CISSP 7th Ed.: Ch.1. Security and Risk Management
    - Fundamental Principles of Security (p.1–6)
    - Security Definitions (p.6–8)
    - Control Types (p.8–13)

Total pages: 13

L02: Cryptography   Date:28.08.2018

- CISSP 7th Ed.: Ch.3. Security Engineering
    - Cryptography in Context (p.335-340)
    - Cryptography Definitions and Concepts (p.340–350)
    - Types of Ciphers (p.350–353)
    - Methods of Encryption (p.353–369)
    - Types of Symmetric Systems (p.369–380)
    - Types of Asymmetric Systems (p.380–388)
    - Message Integrity (p.388–388)

Total pages: 73

L03: Key Management and PKI   Date: 04.09.2018

- CISSP 7th Ed.: Ch.3. Security Engineering
    - Public-Key Infrastructure (p.399–404)
    - Key Management (p.404–407)

Total pages: 19

L04: Communications Security   **Date: 11.09.2018**

- CISSP 7th Ed.: Ch.4. Communication and Network Security
  - o Open Systems Interconnection Reference Model (p.479–497)
  - o TCP/IP Model (p.497–512)
  - o Remote Connectivity
    - ▪ VPN (p.649–657)

Total pages: 45

L05: IS Management, and Human Factors in IS   **Date: 18.09.2018**

- CISSP 7th Ed.: Ch.1. Security and Risk Management
  - o Security Frameworks (p.13–32)
    - ▪ ISO 27000 Series
    - ▪ Enterprise Architecture Development
  - o Privacy (p.70-72)
    - ▪ The increasing Need for Privacy Laws (p.72-73)
    - ▪ Employee Privacy Issues (p.81-83)
  - o Policies, Standards, Baselines, Guidelines and Procedurest (p.86–94)
  - o Personnel Security (p.154–159)
    - ▪ Hiring Practices
    - ▪ Termination
    - ▪ Security-Awareness Training
- CISSP 7th Ed.: Ch.7. Security Operations
  - o Liability and Its Ramifications (p.1053–1060)

Total pages: 46

L06: Incident Response and Digital Forensics   **Date: 25.09.2018**

- CISSP 7th Ed.: Ch.7. Security Operations
  - o The Incident Managwment Process (p.993-1002)
  - o Investigations (p.1038–1053)

Total pages: 30

L07: Computer Security   **Date: 02.09.2018**

- CISSP 7th Ed.: Ch.3. Security Engineering
    - System Architecture (p.248–252)
    - Computer Architecture (p.252-270)
    - Operating Systems
        - CPU Architecture Integration (p.287–290)
        - CPU Operation Modes (p.290-291)
        - Virtual Machines (p.298–300)
        - System Security Architecture (p.301–307)
    - TPM - Trusted Platform Module (p.407–409)

Total pages: 38

L08: Risk Management, and Business Continuity Planning   **Date:09.10.2018**

- CISSP 7th Ed.: Ch.1. Security and Risk Management
    - Risk Assessment (p.94–98)
    - Threat Modelling (p.98-102)
    - Risk Assessment and Analysis (p.102–126)
    - Business Continuity and Disaster Recovery (p.130–153)
- CISSP 7th Ed.: Ch.7. Security Operations
    - Disaster Recovery (p.1002-1030)
    - Insurance (p.1030-1031)
    - Reovery and Restoration (p.1031-138)

Total pages: 90

L09: User Authentication   **Date: 16.10.2018**

- CISSP 7th Ed.: Ch.5. Identity and Access Management
    - Identification, Authentication, Authorization and Accountability
        - Identification and authentication (p.727–728)
        - Authentication (p.739–762)
    - Threats to Access Control (p.834–840)

Total pages: 30

L10: Identity and Access Management   **Date:23.10.2018**

- CISSP 7th Ed.: Ch.5. Identity and Access Management
  - o Identification, Authentication, Authorization and Accountability
    - ▪ Authorization (p.762–776)
    - ▪ Federation (p.776-785)
    - ▪ Identity as a Service (p.785-786)
  - o Access Control Models (p.787–795)
  - o Access Control Techniques and Technologies (p.796–799)
- CISSP 7th Ed.: Ch.3. Security Engineering
  - o Security Models
    - ▪ Bell-LaPadula Model (p.307–308)

Total pages: 37

L11: Network Perimeter Security   **Date: 30.10.2018**

- CISSP 7th Ed.: Ch.4. Communication and Network Security
  - o Networking Devices
    - ▪ Firewalls (p.581–605)
    - ▪ Proxy Servers (p.605–606)
    - ▪ Honeypot (p.607)
    - ▪ Unified Threat Management (p.607–608)
  - o Wireless Networks
    - ▪ WLAN Components (p.664–665)
    - ▪ Evolution of WLAN Security (p.665–672)
    - ▪ Best Practice fpr Securing WLANs (p.677)
- CISSP 7th Ed.: Identity and Access Management
  - o Access Control Monitoring (p.822–832)   Total pages: 48

L12: Application Security and Secure Software Design   **Date: 06.11.2018**

- CISSP 7th Ed.: Ch.8. Software Development Security
    - o Building Good Code (p.1077–1078)
    - o Where do we place security? (p.1078–1083)
    - o Software Development Lifecycle (p.1084–1097)
    - o Secure Software Development Best Practice (p.1097–1098)
    - o Web Security (p.1146–1154)
    - o Malicious Software (p.1178–1193)
- CISSP 7th Ed.: Ch.4. Communication and Network Security
    - o Networ Attacks (p.696-700)
- CISSP 7th Ed.: Ch.6. Security Assessment and Testing
    - o Auditing Technical Controls
        - ▪ Vulnerability Testing (p.866–869)
        - ▪ Penetration Testing (p.869-873)

Total pages: 60