

ENC-IKB Implementation of Cybersecurity WS 2026

Cyril Klimeš, Tomáš Pitner

Module Summary

- **Course basics**: exam-based completion (**4 ECTS**), 1 lecture hour per week plus 2 hours of exercises/labs, master level.
- **Learning goal**: a comprehensive orientation in implementing cybersecurity measures into information systems and ICT.
- **Six modules** (Sep 22 – Dec 15): legislation and assets → ISMS and risk → roles, suppliers, HR → operations, changes, incidents, continuity, physical security → technical measures → audit and GAP analysis.
- **Core topics**: ISMS, asset and risk management, organizational and operational security, access control, supplier management.
- **Labs (exercises)**: network protection, user identity verification, access rights, anti-malware, logging and detection, application security, cryptography, availability, industrial systems, digital services.
- **Assessment**: written exam max **60 points** (min 36), seminar project max **40 points** (min 24), scale **A** (90–100) to **E** (60–67).
- **Legislation in force**: Act No. 264/2025 Coll. (since 1 Nov 2025, transposes NIS2) with Decrees Nos. 334/2025 and 408–412/2025; EU acts NIS2, DORA, CER, CRA.
- **Resources**: RevealJS slides, web HTML, and printable PDF; MENDELU e-books; NÚKIB portal and legislation pages in EN.

Basics

- Completion mode: **Exam** (4 ECTS)
- Mode: face-to-face
- Lecture: 1 hr/week = 2 hr/2 weeks, Tomáš Pitner
- Labs/Exercises: 2 hrs/week, Jiří Balej
- Level: **Master Studies**

Learning Goals

- The subject provides a comprehensive orientation in the field of implementing cybersecurity measures into IS and ICT.

Teachers

- Prof. RNDr. Tomáš Pitner, Ph.D. (lectures)
- Ing. Jiří Balej, Ph.D. (exercises/labs)
- Prof. Ing. Cyril Klimeš, CSc. (original lecture notes)
- doc. RNDr. Tomáš Sochor, CSc.(exercises/labs)

Lectures & Schedule

- **Tuesdays, 1 PM** (once-in-2-weeks)
- Alternating weeks:
  - lectures (odd week number)
  - exercises (even week number)
- Summary, examples, and discussions during sessions



Lectures 2 hrs / every odd week (1, 3, 5 ...)

1. Lecture, Tue Sep 22 2026: What We Protect and by What Rule: Legislation, ISMS, Asset Management
2. Lecture, Tue Oct 06 2026: How Much We Risk: ISMS, Risk Management
3. Lecture, Tue Oct 20 2026: Who Manages It: Security Roles, Suppliers, HR Security
4. Lecture, Tue Nov 03 2026: How It Runs and How It Changes: Operations, Changes, Incidents, Continuity, Physical Security
5. (no Lecture on Tue Nov 17 2026 due to state holiday)
6. Lecture, Tue Dec 01 2026: How We Cover It Technically: Access, Network, Malware, Logging, Cryptography, Availability
7. Lecture, Tue Dec 15 2026: How We Verify It Works: Audit, Testing and Forensics, GAP Analysis

Labs (Exercises) 2 hrs/week

1. Implementation of Tools for Network Protection. Implementation of Tools for User Identity Verification.
2. Implementation of Tools for Access Rights Management. Implementation of Tools for Protection

Against Malicious Code.

3. Implementation of Tools for Logging Information and Communication System Events. Implementation of Tools for Detecting Security Events.
4. Implementation of Tools for Collecting and Evaluating Cybersecurity Events. Implementation of Application Security Tools.
5. Implementation of Cryptographic Tools. Implementation of Tools for Ensuring Information Availability Levels.
6. Implementation of Tools for Industrial and Control Systems. Implementation of Tools for Digital Services.
7. Execution of Penetration Testing. Execution of Forensic Analyses.

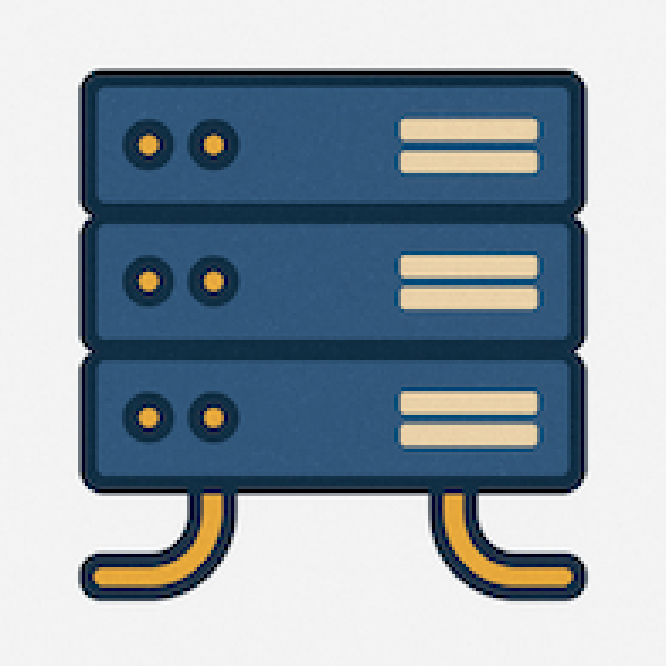
Topics: Security Management

- **Information Security Management System** (ISMS) What is required?
- **Asset** management, **risk** management
- **Organizational** and **operational** security
- **Access control** and **supplier management**



Labs: Practical Topics

- **VLAN attacks**: VTP, DTP, STP
- **Wi-Fi security**, controller, RADIUS
- **OSPF authentication**, uRPF
- **Firewalls**, proxies, **Netflow**, **DNS security**



Assessment and Grading

- Written exam: max **60 points** (min 36)
- Seminar project: max **40 points** (min 24)
- Grading scale: **A (90-100) to E (60-67)**



Resources

Literature

- Klimeš, Pitner: **Cybersecurity Implementation**
- (this material: slides RevealJS/web HTML/printable PDF)
- Security documentation templates
- Act No. 264/2025 Coll. on Cybersecurity (NIS2)
- Bašta et al.: CyberSecurity (CZ.NIC, 2019)

Free MENDELU e-books in Czech:

- Cyril Klimeš: Implementace kybernetické bezpečnosti
- Jiří Balej, Cyril Klimeš, Tomáš Sochor: Implementace kybernetické bezpečnosti – průvodce nasazením vybraných technologií

Standards & Regulative Fundament

The course content is focus both

generally

ISO standards, ruling principles of CS management and

locally

Czech cybersecurity regulative: law on CS, new law on CS, EU NIS2



Most is available in an EN translation!

- NÚKIB – Legislation (EN)

Cybersecurity Legislation in Force

- **Act No. 264/2025 Coll.** on Cybersecurity (**Cybersecurity Act**) — in force since 1 Nov 2025; transposes EU **NIS2** Directive (EU) 2022/2555 into Czech law. The first module explains the act and what it replaced.
- Implementing framework:
  - **Decree No. 408/2025 Coll.** — regulated services
  - **Decree No. 409/2025 Coll.** — security measures (higher obligations regime)
  - **Decree No. 410/2025 Coll.** — security measures (lower obligations regime)
  - **Decree No. 334/2025 Coll.** — NÚKIB Portal (registrations, notifications, incident reporting)
- **Cloud computing for public administration**:
  - **Decree No. 411/2025 Coll.** — security levels of public administration information systems

- **Decree No. 412/2025 Coll.** — security rules for public administration bodies using cloud services
- **Decree No. 505/2025 Coll.** — requirements for entry in the cloud computing catalogue

Portal NÚKIB — authorised EN information NÚKIB – Legislation (EN)

Key EU Cybersecurity Legislation

- Directive (EU) 2022/2555 (NIS2 Directive), on measures for a high common level of cybersecurity across the EU; repeals NIS1 (Directive 2016/1148) and amends other acts. , https://www.twobirds.com/en/insights/2025/understanding-key-eu-cybersecurity-legislative-acts-nis2%2C-cer%2C-and-cra
- Commission Implementing Regulation (EU) 2024/2690, sets technical and methodological requirements for cybersecurity risk-management and defines significant incident thresholds for various service and infrastructure providers.
- Regulation (EU) 2022/2554 (DORA – Digital Operational Resilience Act), establishes an EU-wide framework for ICT risk management, incident reporting, resilience testing, and ICT third-party risk oversight in the financial sector; effective from 17 January 2025.

Key EU Cybersecurity Legislation (cont.)

- Directive (EU) 2022/2557 (CER – Critical Entities Resilience Directive), focusing on the resilience of critical entities; repeals Council Directive 2008/114/EC.
- Regulation (EU) 2019/881 (Cybersecurity Act) established ENISA's mandate and introduced EU-wide cybersecurity certification schemes. https://en.wikipedia.org/wiki/Cybersecurity_Act
- Regulation (EU) 2024/2847 (Cyber Resilience Act – CRA) imposes cybersecurity requirements on "products with digital elements," requiring risk assessments, security updates, vulnerability and incident reporting, with certain fines applicable; manufacturers have until December 2027 to comply.