COURSE DESCRIPTION CARD - SYLLABUS

Course name
Risk management in IT systems [N2Inf1>ZRYZ]

Course

Field of study
Computing

Year/Semester
2/4

Area of study (specialization)
Information Technology in Business Processes

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
part-time

Requirements
elective

Number of hours

Lecture
16

Laboratory classes
0

Other
0

Tutorials
12

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr inż. Tomasz Bilski
tomasz.bilski@put.poznan.pl

Lecturers

Prerequisites

Student should have knowledge on IT system structure and operation. Should have knowledge on computer system architecture, operating systems, computer neworks, data security.

Course objective

Providing knowledge on models, standards, phases of risk management in IT systems. Providing skills on risk management in exemplary IT systems.

Course-related learning outcomes

Knowledge:
Student has detailed knowledge on:
- risk management process,
- risk analysis models,
- risk parameters used in risk analysis,
- risk psychology.

Skills:

Student is able to:
- select risk model,
- perform risk analysis in exempleary IT system,
- select appropriate risk reduction methods,

Social competences:
Student understands:
- causes and results of cognitive errors,
- psychological aspects of risk.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Theoretical knowledge is verified during 45-minute test performed last lecture. Theoretical test consists of 8 questions. To achieve positive result student should get more than 50% of points.
Practical skills are verified during classes and during final practical test. To achieve positive result student should get more than 50% of points.

Programme content

The module consists of the following topics:
1. Introduction.
2. Legal issues
3. Risk management phases.
4. Risk analysis.
5. Risk treatment.
6. Risk psychology.

Course topics

The lecture consists of the following topics:
1. Introduction. Basic terms definitions, including: data security policy, risk, residual risk, risk model (according to NIST 800-30), risk management process. Legal requirements (general and branch), directives, regulations and technical standards related to data security and risk management.
2. Risk management phases: context, evaluation, assessment, monitoring.
3. Risk analysis. Basic phases: initiation, threat identification, vulnerability identification, probability evaluation, impact assessment. Risk analysis methods: (quantitative, qualitative, semiquantitative). Parameters: AV (asset value), EF (exposure factor), SLE (single loss expectancy), ARO (annual rate of occurrence), ALE (annual loss expectancy), ROSI (risk on security investment).
4. Risk reductions. Methods, constraints.
5. Risk psychology. Risk perception factors. Cognitive biases and their impact on decision making, biases in opinions and probability assessment (including: gambler paradox, „hot hand”, conjunction error, certainty effect, risk compensation theory, group polarization).

Classes consist of the following topics:
Students perform risk analysis in exemplary IT systems.

Teaching methods

Interactive lecture (with questions for students) with a use of multimedia presentation. Files with slides provided to students.
Classes in the form of individual and team tasks solution.

Bibliography

Basic
T. Bilski, Problemy społeczne i zawodowe informatyki, Poznań: Wydawnictwo Politechniki Poznańskiej, 2018 (in Polish, PUT Library signature: W 171571).
K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2009 (in Polish, PUT Library signature:W 119656).

J. Łuczak, M. Tyburski, Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Wyd. Uniwersytetu Ekonomicznego, Poznań, 2010 (in Polish, PUT Library signature: A 167841).
J. Krawiec, A. Stefaniak, System Zarządzania Bezpieczeństwem Informacji w praktyce : zasady wyboru zabezpieczeń, Polski Komitet Normalizacyjny, Warszawa, 2011 (in Polish, PUT Library signature: CzO 174604).
Additional
T. Polaczek, Audyt bezpieczeństwa informacji w praktyce : praktyczny przewodnik po zagadnieniach ochrony informacji, Helion, Gliwice, 2006 (in Polish).
D. J. Landoll, The security risk assessment handbook : a complete guide for performing security risk assessments, Boca Raton, FL : CRC Press, cop. 2011.
T. Bilski, Quantitative Risk Analysis for Data Storage Systems, 20th International Conference, CN 2013 Proceedings, [A. Kwiecień, P. Gaj, P. Stera, Editors] Communications in Computer Science and Information Science 370, Springer Verlag, Heidelberg, 2013, s. 124-135.
T. Bilski, Some Remarks Related to Human Behaviour Impact on Data Protection Processes, Information Systems Architecture and Technology [Editors L. Borzemski, A. Grzech, J. Świątek, Z. Wilimowska] Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2014, s. 89–98.

Breakdown of average student's workload

	Hours	ECTS
Total workload	78	3,00
Classes requiring direct contact with the teacher	28	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	50	2,00