

## “Cybersecurity Program (Based on ISACA ITCA and Microsoft SC-900 Materials)”

### Name of the continuing education institution

BCS Koolitus AS (hereinafter BCS Koolitus).

### 1. Name of the curriculum

“Cybersecurity Specialist Training Program (Based on ISACA ITCA and Microsoft SC-900 Materials)”

### 2. Curriculum group and basis for curriculum preparation

**CURRICULUM GROUP:** Database and Network Design and Administration (0612).

**THE BASIS OF CURRICULUM COMPOSITION:** Based on the Lifelong learning standard and industry best practices (ISACA ITCA and Microsoft SC-900 materials).

### 3. Objective and learning outcomes

**OBJECTIVE:** The goal of this retraining program is to provide participants with beginner-level knowledge and practical skills on how to implement cybersecurity controls within an organization. Graduates will gain the vocational foundations needed to start a career as a Cybersecurity Specialist.

#### LEARNING OUTCOMES:

- Understands IT security methodology and management at a basic level
- Knows cybersecurity threats, can associate them with organizational assets, and apply defense measures to mitigate risks
- Performs security monitoring within the IT infrastructure, identifies anomalies, and applies threat intelligence
- Is capable of adequately responding to security incidents
- Knows Microsoft security technologies and can select appropriate security components for their organization or company

### 4. Target group and conditions for starting studies

The course is intended for Individuals who wish to launch a career as a cybersecurity specialist or enhance their existing competence in protecting an organization’s IT infrastructure against cyber threats. It is suitable for those who:

- have basic computer literacy and ability to use common software applications
- have at least B2 level in English
- have time to commit to a 4- month course
- have serious interest in the field of Cybersecurity

### 5. Volume and structure of the study

#### VOLUME AND STRUCTURE OF THE STUDY:

Mentor meetings:	30 academic hours
E-learning <sup>1</sup> and independent study:	134 academic hours
The total amount of study:	164 academic hours (during 4 months or 15 weeks)

<sup>1</sup> e-learning = learning that takes place partially or completely with the help of digital technological means.

**LEARNING ENVIROMENT AND TOOLS:**

The training program is based on [ISACA ITCA: Cybersecurity Fundamentals Online Training](#) and [Course SC-900T00-A: Microsoft Security, Compliance, and Identity Fundamentals - Training | Microsoft Learn](#).

Learners are provided with 30 academic hours of group meetings with mentors. All learning takes place online (including meetings with mentors).

## 6. Description of the learning process, including learning content, learning methods, and materials

**E-COURSE AND CONTENT**

E-course module	
1. module	<p><b>ISACA ITCA: Cybersecurity Fundamentals</b>  <b>(84 academic hours independent study and 19 academic hours mentor meetings)</b></p> <p>This module covers how to perform the basic, professional tasks required of an entry-level IT professional in a cybersecurity capacity.</p> <ul style="list-style-type: none"> <li>• Defining Security and its Roles</li> <li>• Roles, Governance, Continuity, and Recovery</li> <li>• CIA, Least Privilege, and Privacy</li> <li>• Threat Landscape</li> <li>• Motivations, Agents, and the Attack Sequence</li> <li>• Malware and its Symptoms</li> <li>• Common Attack Methods Part 1</li> <li>• Common Attack Methods Part 2</li> <li>• Risk Management</li> <li>• Regulatory Requirements, The Modern Perimeter</li> <li>• Network Security Controls</li> <li>• Understand Firewall Functions</li> <li>• Endpoint Firewalls and Windows Firewall</li> <li>• Mac/Linux Firewalls and IDS/IPS</li> <li>• AAA Controls</li> <li>• Cloud Services</li> <li>• Cloud Security and Models</li> <li>• Data Security</li> <li>• Symmetric Encryption</li> <li>• Asymmetric Encryption, Hashing, Digital Signatures</li> <li>• PKI and Applying Cryptography</li> <li>• Security Operations and Vulnerability Management</li> <li>• Penetration Testing and EDR</li> <li>• Incident Response and Digital Forensics</li> <li>• Network Command-Line Tools</li> <li>• Penetration Testing Tools</li> <li>• Concluding Tools and Techniques</li> </ul>
2. module	<p><b>Microsoft SC-900 Fundamentals</b>  <b>(10 academic hours independent study and 2 academic hours mentor meetings)</b></p> <p>This module provides introductory level knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions</p> <ul style="list-style-type: none"> <li>• Introduction to security, compliance, and identity concepts</li> <li>• Introduction to Microsoft Entra</li> <li>• Introduction to Microsoft security solutions</li> <li>• Introduction to Microsoft Priva and Microsoft Purview</li> </ul>

3. module	<b>Graduation Project</b> <b>(40 academic hours independent study and 9 academic hours mentor meetings)</b>  <b>Developing a Cybersecurity Architecture Plan</b> assessment of the cybersecurity status of an organization with a given IT infrastructure, identification of key risks, and preparation of an annual cybersecurity action plan. Students design an economically feasible security architecture project for a sample or real company, describing the technological components, their functionality, and interoperability
-----------	---

#### LEARNING METHODS:

- E-course lectures
- E-course video lectures
- Workshops with mentor
- Practical exercises
- Independent project work

#### STUDY MATERIALS:

The main learning materials are videos and digital materials.

### 7. Evaluation, i.e. conditions for completing studies

Completing all practical exercises

Participating in at least 75% of mentor meetings

Completing the Graduation Project

### 8. Documents to be issued

For learners who have achieved the learning outcomes and successfully completed the assessment, a certificate will be issued in accordance with the current continuing education standards in Estonia.

If participant fails to meet at least one of the following conditions a certificate of participation will be issued: completing less than 100% of assignments, participating in less than 75% of workshops and not passing the Graduation project.

### 9. Qualification of trainers

The lecturers have

- a minimum of applied higher education or a bachelor's degree or equivalent education level;
- extensive experience in the field of cybersecurity;
- within the past three years have delivered at least three training programmes in this area.

### 10. Language of study

Course is conducted in English.

### 11. Curriculum created:

15.12.2025