Project Title	**Boosting Smart Specialization and Encouraging Spin-offs in IT across Danube Region**
Call	**Danube Region Programme**
Project number	**DRP0200277**
Coordinator	**ZEDA**
Project duration	**30 months 0 days**
Project website	https://interreg-danube.eu/projects/spinit
Specific objective	**Creating a framework outlining the obligatory elements of each curriculum/methodology to be developed. This framework should align with the project goals and the developed LAP.**
Activity	**Activity 2.2 Next-gen Pilot Projects for Smart Specialization and IT**

SpinIT

Reporting Template for Deliverable D.2.2.3 Development / Selection of appropriate methodology / curriculum for pilot project implementation			
Due date:	30.06.2025.	Actual submission date:	10.05.2025.
Organization:	Zenica Development Agency - ZEDA	Authors:	Jasmin Azemović and Mirza Sikirić
Status: Final (F) Draft (D) Revised draft (RV)	F	Dissemination level: Public (PU) Confidential, only for members of the consortium (CO)	CO

Table of Contents

1. Introduction

During D2.2.3 each Territorial Partner (TP) will design and utilize a tailored methodology and curriculum for the implementation of their chosen pilot project focusing on areas such as ICT, Edtech, AR/VR, AI, Industry 4.0, visibility, transparency, predictive capacity, adaptability, and ICT cross-sectoral collaboration. These methodologies and curricula will be specifically designed to enable the effective execution of the Local Action Plan (LAP).

The purpose and aim of this document is to ensure the alignment of methodologies with project goals and local requirements by providing common template for each TP to fill. The following information is to be provided below: basic information about the TP and their pilot project; detailed description of the pilot project; skills to be developed, learning methodologies to be used during the pilot project; curriculum and schedule of the pilot project; and finally, every resource (books, articles etc.) used during the pilot project implementation.

2. TP and pilot project identification

Please provide information about yourself and your selected pilot project.

Use the following table as a template.

Territorial Partner (TP)	
Name of the organization in original language	Zenička razvojna agencija ZEDA
Name of the organization in English	Zenica Development Agency ZEDA
Organization abbreviation	ZEDA
Pilot project	
Name of the pilot project	**SpinIT CyberSafe (BASIC & PRO Modules)**
Name of the lead organization in original language	**Zenička razvojna agencija ZEDA**
Name of the lead organization in English	**Zenica Development Agency ZEDA**

3. Introduction of the selected pilot project

The SpinIT CyberSafe pilot project is an educational initiative developed by the Zenica Development Agency (ZEDA) aimed at improving cybersecurity awareness and practical skills among SMEs, public institutions, NGOs, and academia in the Zenica-Doboj Canton and the wider region. The project was selected based on a structured process of stakeholder engagement through Local Discovery Group (LDG) workshops and reflects the expressed needs of the local ecosystem.

Cybersecurity emerged as a top priority during the LDG process due to a lack of awareness and preparedness among organizations facing rising digital threats. The pilot consists of two training modules:

- CyberSafe BASIC, conducted on 16 May 2025, targeted non-technical staff and general employees. It focused on fundamental cybersecurity knowledge, hygiene practices, threat recognition, and digital risk awareness.
- CyberSafe PRO, scheduled for 13 June 2025, is intended for IT professionals and advanced users. It will cover advanced topics such as threat modeling, incident response, encryption, and vulnerability assessments.

Both sessions are led by Prof. Dr. Jasmin Azemović, a prominent cybersecurity expert with extensive academic and practical experience, including over 30 years in information security and leadership roles in corporate cybersecurity operations.

The CyberSafe BASIC training successfully trained more than 60 participants, who showed measurable improvement in familiarity with key cybersecurity topics, including phishing, password security, and data protection. Entry and exit questionnaires demonstrated knowledge growth, while participant feedback confirmed high relevance and impact.

The entire training was recorded and will be made publicly available on the SpinIT YouTube channel, ensuring long-term accessibility and enabling replication in other regions.

The project is fully aligned with local and regional development strategies, particularly the Development Strategy of the City of Zenica 2021–2027 and the Strategy for SME Development, both of which emphasize digital transformation and cybersecurity capacity-building. It also supports the Federation of Bosnia and Herzegovina's RIS3-relevant goals in digitalization and innovation.

By combining live training, recorded content, expert-led sessions, and participant engagement, SpinIT CyberSafe contributes to building a digitally resilient and security-aware community and serves as a replicable model for cybersecurity upskilling across the Danube Region.

4. Learning objectives

Please explain what the expected results of the pilot project are.
Use the following table as a template.

Field to be developed Select one or more.	☒ Smart Specialization ☒ Industrial Transformation ☒ Industry 4.0 Transition
Skills and key competences to be developed	SpinIT CyberSafe BASIC • Cybersecurity awareness and hygiene practices • Ability to recognize phishing, ransomware, and social engineering attacks • Understanding of secure password management and multi-factor authentication • Knowledge of cryptographic principles and basic encryption tools • Safe use of mobile devices and cloud storage • Awareness of AI-related risks, data privacy, and regulatory compliance (e.g. GDPR, EU AI Act) • Familiarity with real-world security breaches and cyber incident response practices • Critical thinking for identifying suspicious digital behavior SpinIT CyberSafe PRO • Understanding of security strategy and cost modeling • Knowledge of SOC operations, offensive/defensive security • Hands-on incident response and containment planning • Familiarity with compliance standards (ISO 27001, SOC2, GDPR) • Application of SQL Server encryption models
Specific learning outcomes and results	• 30 participants successfully trained through the SpinIT Cybersafe BASIC event • Entry and exit questionnaires confirmed significant improvement in cybersecurity knowledge and self-confidence:

	o e.g. phishing recognition scores improved from 2.61 to 3.22, encryption awareness from 3.09 to 3.56 • Participants gained practical knowledge in recognizing cyber threats and applying daily protective measures • Improved digital safety habits among participants (e.g. safer passwords, use of MFA, use of password managers) • Participants committed to applying newly acquired practices in their workplaces, boosting institutional resilience • The training helped reduce the knowledge gap in cybersecurity between technical and non-technical staff • Established a foundational training model for future regional replication and further development (PRO level)

5. Teaching and Learning Methods

Please explain the methodology for conducting the pilot project.
Use the following table as a template.

Pilot project implementation and knowledge transfer	
Form Select one or more.	☒ In person ☐ Hybrid ☒ Online (e.g. digital platform, e-learning) ☐ Other (such as):
Description	The pilot project consists of two main live training events: • CyberSafe BASIC (May 16, 2025) – In-person session targeting non-technical staff and employees from SMEs, public institutions, NGOs, and academia. Focused on fundamental cybersecurity principles, digital hygiene, and awareness. • CyberSafe PRO (June 13, 2025) – In-person training for IT professionals and advanced users, focusing on technical cybersecurity competencies, including threat modeling, incident response, and vulnerability assessment. Supplementary online materials such as slides, checklists, and recorded video lectures are provided to participants after each session via the SpinIT YouTube channel. This ensures continuous learning and broader accessibility of the training content.
Instructional approaches	
Instructional approach Select one or more.	☒ Lectures ☒ Workshops ☐ Other (such as):
Description	Lectures delivered by Prof. Dr. Jasmin Azemović introduced core concepts of information security, cryptography, cyber threat landscape, cyber hygiene, and AI-related risks. Workshops included:

	- Simulated phishing exercises and analysis of major real-world breaches (e.g. Uber, SolarWinds, Log4j). - Interactive demonstrations using tools like haveibeenpwned.com, password strength testers, and security.org. - Discussion-based learning with participants contributing personal practices and challenges. Training was highly practical, with examples relevant to SMEs and public institutions, and structured around real case scenarios.
Methodologies	
Assessments Select one or more.	☒ Preliminary-pilot knowledge test ☒ Post-pilot knowledge test ☐ Mid-term exam ☐ Final exam ☒ Other (such as): Simulation exercises, informal testing, live discussion-based validation
Description	Participants completed structured entry and exit questionnaires. Entry results revealed moderate awareness levels, with ratings between 2 and 4 (on a 1–5 scale) across topics such as phishing, password creation, and use of MFA. Exit surveys showed increased familiarity, with 80% of participants rating themselves at 4 or 5, and 100% stating they plan to improve personal or organizational cybersecurity practices. Simulation exercises, password audits, and real-time scenario problem solving were included to reinforce understanding and encourage self-evaluation.
Feedback Select one or more.	☐ Preliminary-pilot knowledge test ☒ Post-pilot knowledge test ☐ Mid-term exam ☐ Final exam ☒ Other (such as):Instructor-led debrief, written evaluations, participant reflections
Description	Feedback was collected via Google Forms and open discussions. Participants valued: - Practicality of examples

	• Instructor’s industry insights • Hands-on demonstrations • Case studies and AI-related challenges

6. Structure and content

Please draft the planned curriculum and schedule of the chosen pilot project. This must include:

- theoretical and practical parts
- training framework (units/timeframes): full list of modules with name and duration

Use the following table as a template.

Duration	4 h
Teaching topics Please provide a list of topic titles.	SpinIT CyberSafe BASIC • Cybersecurity Fundamentals – 45 min • Cryptography Basics – 30 min • Threats and Data Breaches – 60 min • Cyber Hygiene Practices – 45 min • AI and Cybersecurity – 30 min • Self-assessment and Security Tools – 30 min SpinIT CyberSafe PRO
Learning aims	• Understand cybersecurity as an ongoing process; distinguish security, safety, and privacy • Understand basic cryptographic principles; recognize applications in daily tools • Recognize how breaches happen; understand their consequences and prevention strategies • Adopt safe digital behavior; evaluate and improve personal and institutional security habits • Learn about the intersection of AI and security; understand regulatory expectations • Identify personal and organizational risk exposure; evaluate baseline security readiness
Methodologies e.g. learning video of 5 minutes, quiz, word cloud via Mentimeter	• Lecture, real-time Q&A, interactive discussion • Presentation with visual aids, practical examples • Case analysis, video excerpts, group reflection • Kahoot quizzes, online tool demos (haveibeenpwned.com) • Lecture, real-world AI misuse examples • Hands-on demonstrations, simulation tools

SpinIT CyberSafe BASIC

Cybersecurity Fundamentals	
Duration	45 min (01:30 – 47:41)
Content	This session introduced participants to the foundational principles of cybersecurity. The instructor emphasized that security is a continuous process, not a final destination, and that no system can ever be 100% secure. Participants learned to differentiate between “security,” “safety,” and “privacy,” and explored the many environments where information security is crucial — from business operations and healthcare to smart cities and personal devices. The goal was to build a mindset of vigilance and ongoing learning as the baseline for any cybersecurity culture.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Live lecture with real-world examples • Q&A with participants • Interactive conversation based on instructor’s experience
Cryptography Basics	
Duration	30 min (47:42 – 1:04:58)
Content	In this segment, participants were introduced to the essential concepts of cryptography, cryptanalysis, and cryptology. The training covered the use of ciphers and encryption keys, highlighting the differences between symmetric and public-key systems. Real-life applications were explained, such as HTTPS in web browsing, email encryption, and secure messaging platforms. The topic helped participants understand how cryptography protects sensitive data in everyday digital interactions.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Visual presentation with examples • Verbal walkthrough of cryptographic flow (plaintext → ciphertext → decryption) • Live explanation using diagrams
Threats and Data Breaches	

Duration	60 min (1:05:07 – 2:18:15, 2:21:22 – 2:23:38, 2:23:48 - 2:34:03)
Content	This part of the training focused on real-world cyber incidents that demonstrated the impact of security failures. Participants reviewed notable case studies such as the Uber breach, SolarWinds attack, and the exploitation of the Log4j vulnerability. The session included insights into how these breaches occurred, the scale of data loss, and their consequences on businesses and end-users. A special focus was placed on how health data breaches (e.g., the Johnson & Johnson incident) can lead to high-value data being sold on darknet markets and used in phishing or fraud attempts.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Case study presentation (slides) • Open discussion about breach consequences • Quiz questions via Kahoot to test comprehension
Cyber Hygiene Practices	
Duration	45 min (2:34:04 – 3:35:15)
Content	This highly practical section helped participants evaluate their digital habits and recognize everyday vulnerabilities. Topics included how to create strong, unique passwords, enable multi-factor authentication (MFA), install and update antivirus software, and protect smartphones and USB devices. The instructor demonstrated tools such as haveibeenpwned.com and password strength checkers. Participants reflected on unsafe practices like opening suspicious attachments or reusing passwords, and discussed how to avoid common cyber traps such as social engineering and phishing emails.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Live tool demos (e.g. haveibeenpwned.com) • Answering quiz questions via Kahoot • Step-by-step hygiene checklist • Group reflection on habits and institutional weaknesses
AI and Cybersecurity	
Duration	30 min (3:40:25 -4:02:30)

Content	This module explored the intersection between artificial intelligence and cybersecurity. Participants learned how AI models can embed social biases, how attackers can manipulate AI outputs through prompt injection, and how unregulated use of AI may violate data privacy laws like GDPR. Case examples included biased hiring algorithms and data leakage in healthcare settings. The segment concluded with a brief overview of the regulatory landscape, especially the upcoming requirements of the EU AI Act, which mandates fairness, transparency, and accountability in AI use.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Lecture with practical examples • Instructor-led explanation of regulatory context • Real-world stories (e.g. AI denying loans, violating HIPAA)
Self-assessment and Security Tools	
Duration	30 min
Content	In the final session, participants were introduced to practical tools they can use to assess their personal or organizational cybersecurity readiness. The instructor demonstrated VPN tools, endpoint protection software, and phishing test platforms. Attendees engaged in self-evaluation exercises to measure their risk exposure, assess password strength, and identify weak spots in their cyber hygiene. This concluding activity empowered participants to take immediate and concrete steps toward improving their security posture.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Guided exploration of free online tools • Instructor demo of how to audit personal accounts • Reflection activity on what to change after the training

Strategic Cybersecurity and Security Departments	
Duration	45 min (00:00 – 37:59)
Content	This session introduced participants to the strategic importance of dedicated cybersecurity departments in organizations. It debunked the misconception that “IT equals security” and clarified that roles like CEO, COO, or even CTO do not inherently include cybersecurity oversight. Through the lens of real-world risks and breach consequences, the instructor presented a decision-making model for assessing whether and when a company needs a security department. The “Ground Zero” model outlined how to start from an internal security baseline, identify missing elements, and establish governance from scratch. Participants reflected on their organizational environments, assessing whether they had appropriate ownership of security responsibilities.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Live lecture using business risk examples • Interactive discussion with participants on organizational structure • Strategic models illustrated through visual slides and hypothetical cases
Building and Leading Security Teams	
Duration	45 minutes (38:30 – 57:28)
Content	In this segment, participants explored how to structure and manage security teams using the defensive (blue team) and offensive (red team) models. The instructor explained how a Security Operations Center (SOC) supports detection, monitoring, and response efforts. The defensive role was presented as safeguarding internal processes and systems, while offensive roles were aligned with ethical hacking, vulnerability testing, and red-teaming. Real organizational practices were discussed, including the importance of not using SOC

	team members on delivery projects, how to ensure reporting loops between compliance and security, and how to manage security across hybrid IT environments.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Diagram-driven presentation (SOC structure, team roles) • Instructor-led explanation of real-world team setups • Role-based learning through use cases
Incident Response and Containment Strategies	
Duration	45 minutes (59:32 – 2:09:33)
Content	This critical session offered a step-by-step walkthrough of how security teams respond to cyberattacks. Using a simulated phishing attack scenario, the instructor showed how attackers bypass basic controls, capture credentials, and attempt to infiltrate systems. The session emphasized early detection signals, SOC responsibilities during mitigation, and containment actions such as user isolation, forced password resets, and MFA reinitialization. Post-incident steps like log analysis, reviewing accessed files, and root cause documentation were also covered. Participants gained insight into how well-coordinated response efforts minimize disruption and protect organizational assets.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Case study presentation (slides) • Open discussion about breach consequences • Quiz questions via Kahoot to test comprehension
Compliance and Security Standards	
Duration	30 minutes (2:26:29 – 3:13:50)
Content	This module focused on the legal and procedural side of cybersecurity. Participants learned the differences and overlaps between various international standards such as ISO/IEC 27001, HIPAA, GDPR, SOC2, and TISAX. The role of compliance teams was contextualized as the bridge between security policies and legal mandates. Emphasis was placed on aligning security practices with documentation, auditing procedures, and evidence-based controls. The instructor explained how a well-

	integrated compliance function supports continuous improvement and stakeholder trust.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Overview of security governance frameworks • Comparison tables of regulatory requirements • Case-based discussion of non-compliance examples
SQL Server Encryption – Case Study	
Duration	60 minutes (3:15:39-4:04:25)
Content	The final and most technical session demonstrated best practices in database-level encryption using Microsoft SQL Server. Participants learned about data-at-rest protection through Transparent Data Encryption, column-level Symmetric Key Encryption, and client-side Always Encrypted implementations. The instructor illustrated how these mechanisms are applied in production environments, including their cryptographic hierarchies and performance considerations. The importance of separating encryption keys from application layers and securing backups was emphasized. The session concluded with SQL code examples and resources for further reading, including links to Microsoft Docs, GitHub repositories, and white papers.
Methodology e.g. watching a video, answering quiz questions via Kahoot	• Technical walkthrough with SQL Server diagrams • Instructor-led demo of encryption hierarchies • Discussion of common misconfigurations and performance impacts

7. Resources

7.1. Materials Developed and Used

PowerPoint Presentations:
Customized slide decks for both BASIC and PRO levels, covering theory, tools, case studies, and technical procedures. These materials were delivered live and distributed in PDF format post-training.

Recorded Sessions:
Both workshops (BASIC and PRO) were professionally recorded. The videos will be uploaded to the SpinIT YouTube channel, ensuring long-term access and enabling reuse by other partners and regions.

Entry and Exit Questionnaires:
Digital self-assessment forms designed to gauge participant familiarity with cybersecurity topics before and after the training. The results informed content focus and measured impact.

Interactive Quizzes:
Used during the BASIC session (via Kahoot) to reinforce learning, particularly in cyber hygiene and threat recognition modules.

Practical Exercises and Simulations:

- Phishing scenario breakdown
- SQL injection demonstration (PRO)
- Account compromise and incident response sequence

7.2. Tools Introduced to Participants

Participants were encouraged to explore the following free or open-source cybersecurity tools:

- https://haveibeenpwned.com – Credential breach checker
- https://www.security.org/how-secure-is-my-password/ – Password strength tester
- SIEM, SOAR, XDR platforms (introduced conceptually in PRO session)
- VPN applications (discussion of safe selection and usage)
- Password managers (Bitwarden, KeePass, 1Password – mentioned as examples)

7.3. Compliance and Reference Frameworks

The following international frameworks and regulations were discussed and referenced:

- ISO/IEC 27001 – Information security management systems
- GDPR – General Data Protection Regulation (EU)
- HIPAA – Health Insurance Portability and Accountability Act (US)
- SOC2 – Service Organization Control for data protection
- TISAX – Trusted Information Security Assessment Exchange

Participants were advised on how to align organizational practices with these frameworks and the implications for public and private sector compliance.

7.4. Additional Reading and Learning Links

The following resources were recommended for continued learning:

- Microsoft SQL Server Encryption Documentation
- SQLShack – SQL Server Cryptography Tutorials
- GitHub Repository: github.com/jasminazemovic/Book-Securing-Sql-Server

7.5. Transferability

The training modules, tools, and materials developed under the SpinIT CyberSafe pilot are fully transferable. The curriculum can be replicated across partner regions using the provided recordings, training decks, and questionnaires. Due to the modular design, local stakeholders can adapt the content to fit basic or advanced target groups depending on their digital maturity.