ITSVET

ICT Security in Vocational Education and Training

Interreg Central Baltic

project No. CB36, ITSVET (ICT Security in VET)

HANDBOOK
for Teacher Training
WP 7

ITSVET

European Union
European Regional Development Fund

Interreg
Central Baltic

Table of contents

Introduction (eng and local)

The project ITSVET (itsvet-project.eu) aim was to create a model for providing ICT security skills on the vocational education level. Reports show that demand for ICT security professionals has grown faster over the past five years than demand for other ICT jobs. Thus, the objective of the project is to meet the needs of the region's employers through developing a VET model for the ICT security specialists to reduce the skill gap of the labour market in the Central Baltic region.

In practice, the project performed a research to identify the needed competences for ICT specialists in the Central Baltic labour market. One of extremely needed competences for IT specialists is knowledge and skills of ICT security. Based on the research results the project partners developed a new curriculum of ICT Security Specialist for vocational education schools in Estonia, Latvia and Finland. To make this a ready-to-go model also were developed learning materials and a teacher's handbook.

The learning materials consists of 4 modules and 26 lab manuals:

- Information Security Management (3 labs)
- Business Continuity Management (5 labs)
- Customer Service / Service Delivery (4 labs)
- Securing IT Solutions (14 labs)

ITSVET project is a good example of collaboration of different partners - VET schools, companies and stakeholders. One important result of this project was the preparation and approval of occupational qualification standard of ICT Security Specialist (Estonia - IT-turvaspetsialist, tase 5 (kehtib kuni 12.11.2023).

Vocational Pedagogy (eng and local)

Vocational education (VET) is one important element of lifelong learning equipping people with knowledge, know-how, skills and/or competences required in particular occupations or more broadly on the labour market. The education should respond to the needs of the labour market, but also provide learner with skills for personal development.

The key actions to improve the quality and efficiency of initial and continuing VET should aim at:

- providing the workforce with high quality labour market relevant vocational skills by increased use of different forms of work-based learning;

- strengthening the development of key competences to ensure the adaptability and flexibility of learners;

Now and in the future the VET providers should understand the changes in learning:

- the learners need personalised learning experiences,
- need to deal with supporting the development of soft skills such as problem solving, collaboration and creativity,
- making learning fun.

Evolving roles of teachers

The future dominated by change as outlined here presents new challenges for teachers, involving new pedagogies, curriculum design, quality assurance, management and administrative tasks. The learning must be related with real life and cases, but especially in IT and IT security rapid development needs constant improvement of "hard" professional/vocational skills. The challenge is to achieve the best possible combination of vocational skills and key competences both to a high standard. The teachers should use different forms of work-based, problem-based and practical learning.

Work-based learning also facilitates the development of the learning outcomes approach in VET with the shift towards competence-based learning, competence-based qualifications and assessments (skills demonstrations).

Active students

Education and training plays a major role in promoting equity, social inclusion and active citizenship.

VET providers should use experience-based learning and expose learners to non-routine work and non-typical situations. There appears to be a need to promote active learning in both work and school-based VET and give individuals the opportunity to control and develop their own learning, also through the use of innovative, creative and tailored made ICT tools.

Scrum in Educations (eng and local)

Scrum is a framework that helps teams work together. Much like a rugby team (where it gets its name) training for the big game, Scrum encourages teams to learn through experiences, self-organize while working on a problem, and reflect on their wins and losses to continuously improve.

Scrum is:

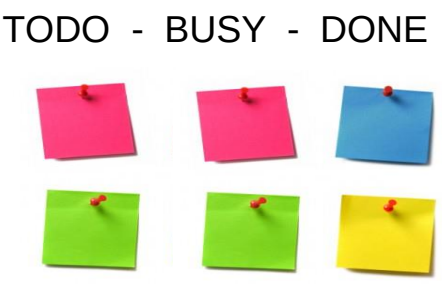
- most used agile software development model;
- can be used for complicated development projects, where the uncertainty is very high;
- flexible framework, suitable for small and big projects;
- a methodology to support teams to organize work and gain the results.

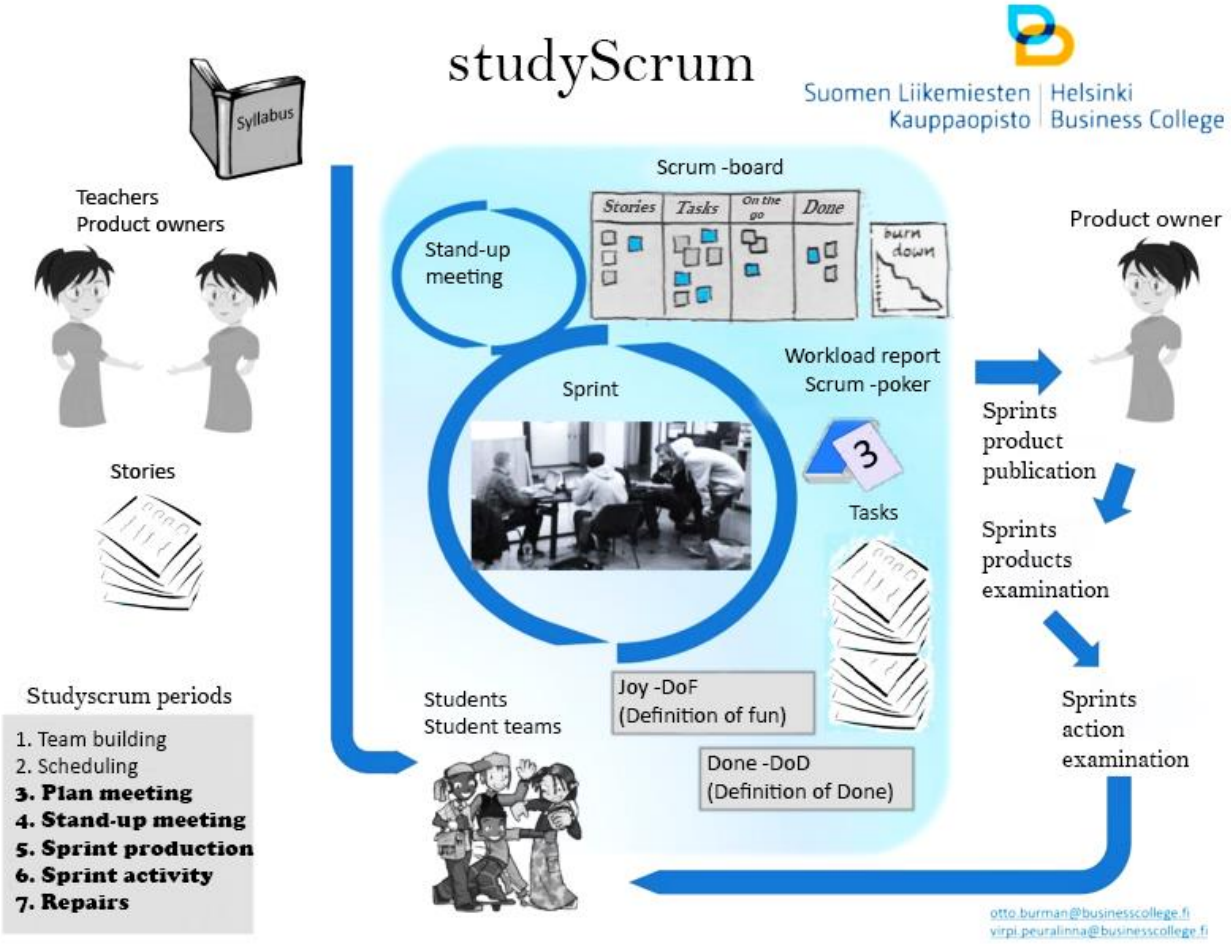
Scrum in Education

- Active method, where learners learn in self-organising teams and are responsible of their own work and learning.
- Learn to manage projects, social skills, creativity and collaboration.
- Suits for learners with different age and skills.

Process

1. Customers' requirements, product/service description, learning outcomes
2. Product backlog, user stories and tasks
3. Every task:
    a. Plan (To Do)
    b. Implement (Busy)
    c. Evaluate (according to requirements, learning outcomes, definition of done) and document (Done)



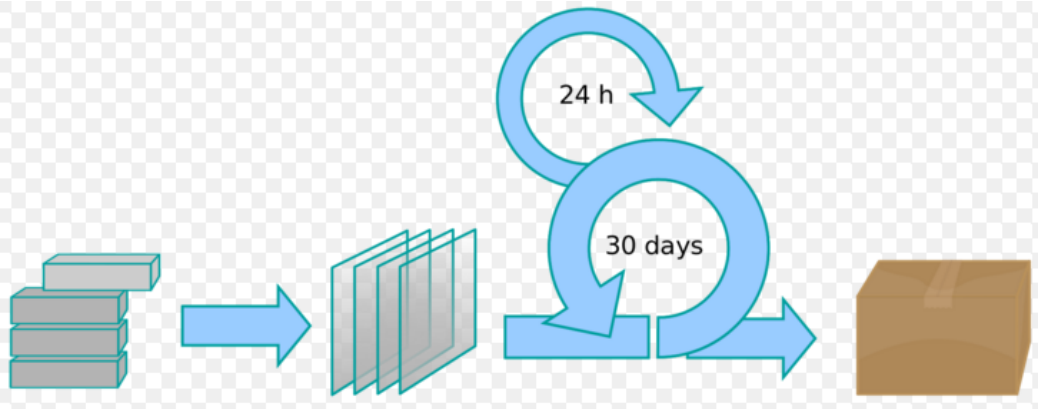

studyScrum
Suomen Liikemiesten Kauppaopisto | Helsinki Business College
Syllabus
Teachers
Product owners
Stories
Scrum -board
Stories
Tasks
On the go
Done
burn down
Stand-up meeting
Sprint
Workload report
Scrum -poker
3
Tasks
Product owner
Sprints product publication
Sprints products examination
Sprints action examination
Joy -DoF
(Definition of fun)
Done -DoD
(Definition of Done)
Students
Student teams
Studyscrum periods
1. Team building
2. Scheduling
3. Plan meeting
4. Stand-up meeting
5. Sprint production
6. Sprint activity
7. Repairs
otto.burman@businesscollege.fi
virpi.peuralinna@businesscollege.fi

Most important elements of Scrum:

- Team
- Product Backlog
- Sprint plan
- Stand-Up meetings
- Sprint results presentation and review
- Retrospective

Teams should also use:

- Product owner
- Scrum Master
- Scrum board
- DoD (Definition of Done)
- DoF (Definition of Fun)
- Burn Down Chart

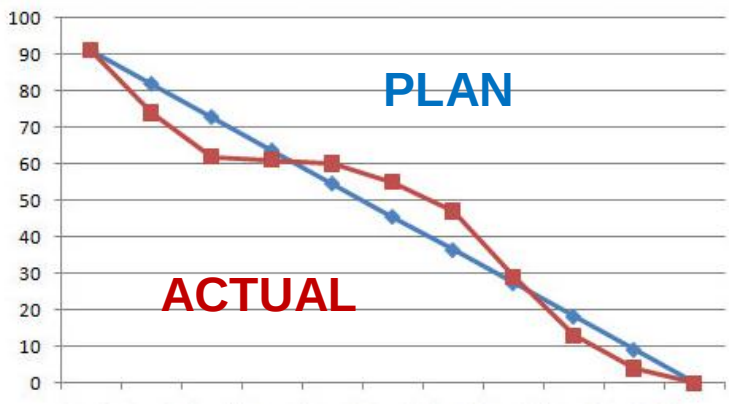


Scrum process

- From customer's requirements to user stories
- User stories and tasks
- Sprint
- Time-table to plan next sprint

Sprint planning

- Tasks
- Burn Down Chart
- Roles and responsibilities
- Time table
- Scrum Board
- Definition of Done (DoD)
- Definition of Fun (DoF)



Stand Up

1. What did you do yesterday?
2. What will you do today?
3. Are there any impediments in your way?

Results presentation, review and evaluation:

- Release
- Review

Retrospective

- What we were doing in last sprint and how?
- What went good?
- What we should improve?

Discussion about teamwork and collaboration.

Learning materials

Learning materials designed to support and train IT specialist in IT security. Most of the practical works are determined to use problem and Project based learning, working in teams and most preferred methodology is Scrum. Practical Works are not meant to be just theoretical lectures, but mostly it should be find the best IT security solutions working in team. Most of the practical works consist of user stories or tasks, what should be solved. The process and results should be documented. Curriculum consist of theoretical topics, learning outcomes, recommended methods and recourses.

As the IT security is discrete topic, then sometimes it is necessary to start with theoretical and legislation topics. If the topics are not so confidential and not so dangerous, then the teacher can use more independent and discoverable learning. Most of the cases it is recommended to use virtual machines or environments. When you are using real cases or systems, then you need to obey safety and security requirements.

Notes: In some cases it is strongly recommended to conduct the practical procedures of labs in discrete test environment. Students must be informed about legislative factors and consequences of “breaking the rules”.

If you are using real organisation or cases some assessments and testing cannot be done without written permission of owner due to legislative factors. If the practical part is to be done on real system it should be ensured that tests performed are controlled by company/organization (using log files etc.). Written commitment not to perform tests for malicious purposes could be asked from student.

If the system contains personal data, describe how Privacy Act concerns will be addressed.

WARNING! Any kind of testing or scanning of a known and not known vulnerabilities can be also classified as attack against of IT system and may cause a claim for damages by owner of the system. This also may have classified as a crime.

Environment

To complete the some labs, specific hardware is not needed. To expand the lab – testing environment may be needed. Test lab must provide a controlled environment for the range of testing throughout the project life cycle — from experimenting with the technology, to comparing design solutions, to fine-tuning the rollout process.

In some cases it would be good to start with a business case of a small company with quite simple and understandable business processes and IT infrastructure. A case company ICT can be simulated with real hardware to make it easier for students to comprehend what it means

when they simulate eg. network cut-off, re-installation of a configured switch, replacing hard drive and bringing back information from backups.

To apply scrum-learning method keep the theory lessons short, but sometimes you need to do more theory beforehand. Most of the labs are designed so that the teacher gives the materials or resources, but also encourages the students to find more themselves. Pick parts of the subject as ‘learning stories’ for the whole project and ask the students to split the learning story to task lists.

If the practical part is to be conducted, physical or virtual environment is required.

List and description of learning materials (eng and local)

Moodul 1. Information Security Management

1. Improvement project of ICT Security policies

The aim oh practical work is to form a managerial level of understanding of information security and to align information security with business strategy and ICT strategy.
Excpexted results:

- Explains the role of information from the strategic viewpoint.
- Explains strategic alignment between business and ICT strategic convergence
- Describes ecosystem cyber security

2. Strategic alignment of cyber security, ICT and business

The lab is designed to give student overview, skills and experiences about how to better align cybersecurity (CS), information- and communication technology (ICT) and business in effective way.

Alignment should start with clear understanding of business and it's strategy. It must be understood that after all, the ICT- and cybersecurity risks are still business risks. Case study.

3. Implementation and testing of vulnerability

The lab is designed to introduce and train student for testing systems in order to find vulnerabilities, which is part of analysis tasks that are required to implement protection measures in the organisation's IT infrastructure against intrusions, security breaches, leaks etc. Physical or virtual environment.

Moodul 2. Business Continuity Management

1. Planning hardware and software changes

The lab is designed to give student overview about change management, configuration management and business continuity management. The Student understands why configurations and changes need to be managed to ensure secure IT operations. Group work with 2-5 members.

2. Implementing hardware and software changes

Student must implement changes in organisation's infrastructure software and/or hardware. Process must be done with minimal or no downtime (depends on whether it's possible to avoid any downtime without any significant impact on cost of implementation – any of these measures should be included only if cost of such solutions won't make it more expensive than useful for the organisation). Integrity of changes and of whole system must be ensured. Any

changes made to the system should improve security of it or, at least, keep it at the same level. Group work, 3 members

3. Implementing hardware and software changes

The expected result of this lab is an experience how to do map vulnerabilities, apply counter measures to know vulnerabilities and how to automate scanning of know vulnerabilities.

In this lab students will learn to:

- find information about vulnerabilities
- make vulnerability assessment based on documentation and publicly available databases
- use vulnerability scanners
- apply patches and workarounds to affected systems

This is important to make sure that the students group are choosing a system where they can find some vulnerabilities and this is also important to choose right scope. Group work

4. Risk management

It is important that departments and their IT users understand what risks exist in their IT environment and how those risks can be reduced or even eliminated. The aim of risk management is “to aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks.”

Student knows and able to identify risks, threats and vulnerabilities from the typical IT infrastructure. How to ensure that security risks are analysed and managed with respect to enterprise data and information. Group work

5. Business continuity plan and disaster recovery plan

Manages business continuity and disaster recovery plans.

Expected results:

- participates in creating and management processes of disaster recovery business continuity plans
- validates disaster recovery plan to ensure that this is up to date and reflects reality

A simplified learning story to the subject would be:

1. Identify risks and make a risk matrix
2. assess the vulnerabilities to those risks
3. determine impact of the business (practical terms)
4. identify the most critical functions and it services within those functions /processes
5. estimate maximum tolerable downtime
6. design proactive and reactive actions

Moodul 3. Customer Service / Service Delivery

1. Incident management

This lab is designed to give the student necessary skills for tracing systematically root causes of technical failures. Student knows how to deploy support tools and can analyse symptoms and if needed can escalate complex or unresolved incidents. Group work.

The Security Incident Response process:

- preparation
- detection
- analysis
- recovery
- after- action / post incident reporting

2. Finding root causes

Aim of this lab is to identify root causes of incidents or any other causes that may disrupt service(-es) and resolve these incidents in a correct manner.

To identify incidents student must know how to utilise system logs and management tools and/or techniques that are used to analyse system logs as well as to react to complaints from personnel or clients which may point to important issues. After identification, the incident(-s) needs to be classified in order to apply correct method(-s) for issue resolution or mitigation and analyse the cause factors to determine what changes may be required in organisation documentation, infrastructure, software or hardware configuration, personnel qualification/competence (e.g. additional training) etc.

3. Building a knowledge base for an organisation

In this lab students work in teams and learn to:

- Choose appropriate software for an organisation depending on the needs and required features
- Keep in line with standards while documenting IT systems, activities and solutions for knowledge base entries
- Update documentation as needed to keep up with changes in IT systems
- Take into account knowledge base target group when building and using the knowledge base

4. Securing remote access of server

The module is designed to teach and practically train students in IT solution security. This involves secure computer network solutions; server, workstation and mobile device security; disaster recovery and cloud computing solutions security. Virtualizing.

Practical work

Moodul 4. Securing IT Solutions

1. Security solutions of the OSI model layers

In this, lab students work in teams and will learn to:

- Understand and map network related vulnerabilities
- plan counter measures to mitigate network related threats
- plan technical solution to protect specific OSI layer in some network solution

2. Advantages and vulnerabilities in the given computer network diagram

The aim of lab is to train students to orient in an unknown network (students have only information and diagrams on that network). In addition to "investigation" of network students need to highlight what are the advantages of given network and, of course, any vulnerabilities or disadvantages that are found during the process. All advantages, disadvantages and vulnerabilities should be explained and justified. As additional task (optional) students propose brief plan of changes to all the found

3. Securing network devices

The module is designed to teach and practically train students in IT solution security. This module is practical work with securing network devices.

Network devices are the core of modern local area and wide area networks. Therefore they are also targets for security attacks. Student will acquire the knowledge of device vulnerabilities and the skills to secure common network devices such as switch, router, wireless router. Student implements hardware and software solutions to mitigate vulnerabilities. Student also ensures protection of wireless networks.

4. Hardening workstations

This lab should give students a practical approach to IT solution security. Hardening workstations is essential skill set to make sure the infrastructure is designed and built for safety. After passing this practical work the student should know how to manage workstations in a secure manner. Student should know how to manage workstations using domain controller solutions and to lock down workstations to ensure their security. Student can implement domain security policies and divide workstation into security groups and implement centralised log management for client devices. Group work

5. Mobile device security

In larger companies where BYOC (Bring Your Own Computer) management comes into daily basis, the IT security staff must implement some security baselines.

The expected result of this lab is a know-how of security measurements which would be basic but still very effective.

In this lab students work in teams and will learn to:

- understand why security policies are required
- planning and topology of mobile device management services
- which policies should be applied to mobile devices
- using best practices to secure mobile devices

6. Group policy

The lab is designed for students to strengthen the skills in development of efficient and secure group policies in the domain controller. Student will have to create and edit existing group policies in order to meet certain requirements. Student must understand that group policy settings may have significant impact on the IT security of organisation (mostly user accounts and computers) if those are not set up or managed in a proper manner. Beside the creation and change of policy settings student must know how to link, unlink, backup, restore, import or sometimes delete group policy objects and the use of organisational units. It is recommended that students had not only theoretically introduced with, but also practiced basic tasks with domain controller group policy, OU's etc. before this lab. Virtualization.

7. DHCP and DNS

In larger companies where IP address management comes a massive overhead very quickly, IT staff should implement DHCP, which usually sides with DNS.

Although DHCP and DNS servers are critical to the operation of most enterprise networks, DHCP and DNS server security is often one of the most overlooked areas of network security.

While DHCP and DNS are usually very easy to initially install, it's still highly recommended to follow certain security policies.

The expected end result of this lab is a know-how of security measurements which would be basic but still very effective.

In this lab students will learn to:

- understand why security policies are required
- planning and topology of DNS and DHCP servers
- which policies should be applied to DHCP servers
- which policies should be applied to DNS server
- using best practices to secure both DNS and DHCP server

Virtualization, group work

8. Securing e-mail server

Mail messaging has and possibly will be the most used neutral e-exchange environment . Students must understand the possibilities of this media channel before they start implementing security measurements.

As the information which is exchanged between recipients is very large, different security policies must be in place before you go live with your mail servers.

The expected end result of this lab is a know-how of security measurements which would be basic but still very effective.

In this lab students will learn to:

- understand why security policies are required
- planning and topology of mail servers
- which policies should be applied to mail server
- using best practices to secure mail servers

Virtualization, group work

9. Securing web server

Websites are most commonly used as public and with rich and ever evolving content – their data must be secured. Web servers are also the most attacked vector which makes them vulnerable when not configured in secure way.

The expected end result of this lab is a know-how of security measurements which would be basic but still very effective.

In this lab students will learn to:

- understand why security policies are required
- planning and topology of web servers
- which policies should be applied to web servers
- using best practices to secure web server

Virtualization, group work

10. AAA implementation and security in directory service

Authentication is the process of verifying that "you are who you say you are", authorization is the process of verifying that "you are permitted to do what you are trying to do" and accounting means that “we keeping track of the things you did”.

Generally directory service is a service which allows the sharing of information about users, systems, networks, services, and applications throughout the network. Some implementations of directory services also implement authorization capabilities and allows to audit and log different activity events.

The expected result of this lab is a implementation of directory services which implement AAA model.

In this lab students will learn to:

- Install and configure directory services
- Configure directory services
- Configure and collect logs needed for auditing and accounting
- Implement RADIUS server which is integrated with a directory service

Local on-premises virtualisation technology is recommended

11. Protection of connection of cloud computing service providers

The lab is designed for students to train in implementation of secure connection (-s) between the enterprise and cloud service provider (where the enterprises' cloud infrastructure / software / platform resides).

Security of such connections mostly is achieved by implementing VPN solutions, specific firewall rules and authentication mechanisms for VPN and/or the cloud solution itself. Additionally, a CDN can be added for availability, additional security (Against DDoS for example).

Student will need to simulate a connection between sites (starting configuration can be given already) and harden its security. CDN part (if necessary) should be described in form of plan of implementation, as for training purposes actual agreement with CDN service providers would be financially inefficient.

Work in pairs

12. Backup management

Backup, or the process of backing up, refers to the copying and archiving of data so it may be used to restore the original after a data loss event. In order to start backing up data, the backup must be first configured. Creating backups protects data, but to ensure that data can be also recovered the backup files must be kept safe. In case of a data loss event or data corruption it is necessary to restore original data from backup. Sometimes the need for restoration might not occur for many years. To ensure that backups are working and information can be recovered from the backup they need to be tested in regular intervals.

In this lab the student will learn how to:

- Configure, schedule and make different versions (rotation) of backup in local and offsite network
- Protect backup files from hardware failure, ensure that data is not intercept during backup and limit access to backup server and files
- Restore data from backup

Verify backup integrity and perform restoration testing

Virtual servers

13. Ensuring backup of network equipment configuration

The lab is designed to train students in creating and maintaining automated backup solutions for network devices (e.g. switches, routers) with centralised and/or decentralised storage.

(Which means that backup can stored on one server and the most recent copy (-ies) are still held at the device itself for additional redundancy and ease of access)

Student will be provided with a network diagram that shows how devices are interconnected and their premade configurations. Basing on given devices student must choose appropriate solution that supports backup of configuration for particular network device manufacturer.

As the lab involves work with network devices and server, it is strongly recommended to do this lab using real devices or their virtualised equivalents. Individual tasks.

Guidelines for schools curriculum development (local)

How to use ITSVET curriculum?

Starting with implementing the curriculum, you have to start from the local legislation. For example in Estonia you have to start from the professional standard, what is the base of vocational curriculum - IT-turvaspetsialisti kutsestandard (tase 5) https://www.kutsekoda.ee/et/kutseregister/kutsestandardid/10696711

How to use practical works?

If you want to use practical works then you have to think about the next topics:

- Who are the target groups, they should persons who have passed IT specialist training
- What kind of skills and knowledge your students want to have?
- Create needed environment, usually it is virtual.
- Most reasonable is to use the result of one practical Works as a input for the next practical work.
- Try to feel the goal and situation of the practical work to create suitable learning environment.
- Try to use practical and real cases.
- Try to use active learning methods.
- As the goal is to learn new skills, so you have to use practical methods.
- Most of all try to use Scrum as a learning method.

Resources

Project ITSVET publications http://itsvet-project.eu/materials/

What is Scrum?

https://www.scrum.org/resources/what-is-scrum

https://www.tutorialspoint.com/scrum/scrum_framework.htm

Scrum Guide https://www.scrumguides.org/scrum-guide.html

Daily Scrum https://www.mountaingoatsoftware.com/agile/scrum/meetings/daily-scrum