Cyber Security for Europe

D6.1

Case Pilot for WP2 Governance

Document Identification	
Due date	31 July 2019
Submission date	31 July 2019
Revision	4.0 (30 April 2020)

Related WP	WP6	Dissemination Level	CO
Lead Participant	KAU	Lead Author	Simone Fischer-Hübner (KAU)
Contributing Beneficiaries	KAU, UNITN, DTU, JAMK, UMU	Related Deliverables	D2.1, D2.2, D2.3, D6.6

Abstract:

This deliverable on a "Case Pilot for WP2 Governance" reviews the offerings of Cyber Security Massive Open Online Courses (MOOCs) in Europe, which have the form of academic courses, continuous learning courses and cyber range courses.
Moreover, it defines a quality assurance process for MOOCs to be branded CyberSec4Europe MOOCs based on a list of quality assurance criteria for MOOCs, which are both generic and cyber-security specific. Based on this quality assurance process and criteria proposed, CyberSec4Europe's task 2.3 on "Governance Structure Design" will design a decision process of governance structures for cyber security MOOCs in Europe.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The deliverable on a "Case Pilot for WP2 Governance" has the objective to provide an initial review of existing offerings of European cyber security MOOCs in the form of academic, continuous learning and cyber range courses. Moreover, the goal is to present a quality assurance process based on quality assurance criteria to be proposed.

The review of MOOC offerings provided in chapter 2 showed that cyber security MOOCs in Europe are mainly offered by academic institutions, but academic MOOCs in cyber security awarding credit points for participants are rare and cyber range MOOCs are basically non-existent in Europe. Moreover, cyber security topic platforms or channels do not exist yet either – existent cyber security MOOCs are rather offered on dominant learning platforms, such as Coursera, EdX, FutureLearn, Udacity, Udemy, or Canvas or Cisco Networking Academy.

Aspects identified by our review that need to be addressed by quality criteria include a well-balanced and unbiased course content as well as fairness and transparency of admission for continuous education MOOCs that are offered by commercial organisations. In addition, there is a need for ethical rules for course participants as well as policy rules for a restricted openness to the course content, student admission or course material for cyber range MOOCs. Moreover, today's most prominent MOOC platforms are hosted in the US, which requires attention for achieving compliance with the GDPR's rules allowing data transfers to third countries outside of Europe.

This deliverable also reviews existing MOOC Quality Assurance and Validation Criteria as related work in chapter 3, which are however not generic in nature, as no cyber security course specific MOOC Quality Assurance Criteria frameworks have been proposed previously yet.

In addition, certification models for MOOCs as well as models for the accreditation of certification bodies are briefly discussed in chapter 4, where we also propose the involvement of cyber security expert stakeholders, such as ENISA, governmental cyber security agencies, contingency or cyber security industry representatives as certifiers or as contributors to certification schemes.

The set of Quality Assurance Criteria that we are then proposing in chapter 5 as the core of the quality assurance process are comprising criteria for the qualification of the proposing institutions, qualification of participants, qualification of instructors, for course examination, credentialisation and recognition, for course evaluation, meeting professional expectations, course structure and content criteria, requirements for platforms and channels, as well as criteria for cyber ranges.

Chapter 6 is then showing how the quality criteria can be assessed as part of a proposed quality branding process.

Finally, this deliverable concludes in chapter **Error! Reference source not found.** with a proposed prioritisation of the quality assurance criteria for the pilot of governance structures for cyber security MOOCs in Europe to be designed by work package 2. Quality assurance criteria for the qualification of the proposing institution, for meeting professional expectations as well as course content and course structure criteria are considered to be of high relevance for the pilot. Moreover, cyber security specific quality assurance criteria, should be given high priority, including quality criteria for cyber ranges, ethical hacking rules and policies for restricting the openness of courses or course material for cyber range courses.

Document information

Contributors

Name	Partner
Simone Fischer-Hübner, Hans Hedbom, Lejla Islami, Mahdi Akil, Matthias Beckerle	KAU
Fabio Massacci, Pierantonia Sterlini	UNITN
Alberto Lluch Lafuente	DTU
Jani Päijänen, Karo Saharinen, Petri Mutka, Marko Vatanen	JAMK
Antonio Skarmeta, Antonio Ruiz Martínez	UMU

Reviewers

Name	Partner
Vashek Matyas	BRN
Borislav Sestrimski	ICITA
Robin Henrich	GUF

History

0.01	2019-03-28	Simone Fischer-Hübner	1st Draft document structure
0.02	2019-04-17	Hans Hedbom	Added initial text to 2.1
0.02	2019-04-17	Simone Fischer-Hübner	Several changes to section 2.1
0.3	2019-05-02	Hans Hedbom	Integrated contributions from DTU and UNITN in the document and restructured Annex A and B
0.4	2019-05-23	Simone Fischer-Hübner, Hans Hedbom	Integrated input for chapter 2 (JAMK), chapter 3 (UMU), chapter 4 (KAU, DTU)
0.5	2019-05-30	Simone Fischer-Hübner, Hans Hedbom	Changes to chapter 2, 4 and adding input by Hans for chapter 5.
0.6	2019-06-10	UMU	Revisions to chapter 2 and 3
0.7	2019-06-18	Simone Fischer-Hübner	Integrated input for UNITN, DTU and JAMK on chapter 2, 3, 4.
0.8	2019-06-23	Simone Fischer-Hübner	Completed chapter 6

0.9	2019-06-28	Simone Fischer-Hübner	Integrating input from UMU and JAMK for chapters 3 and 4
0.10	2019-06-29	Simone Fischer-Hübner	Adding chapter 1 and 6
0.11	2019-06-30	Simone Fischer-Hübner	Adding executive summary and abstract, finalising review version
Final V.01	2019-07-25	Simone Fischer-Hübner	Addressing review comments with the help of all partners
Final V.02	2019-07-28	Simone Fischer-Hübner	Minor changes by KAU
Final V1	2019-07-30	Simone Fischer-Hübner	Final version completed
Final Version V2	2019-11-21	Simone Fischer-Hübner	Title of chapter 2 corrected
Final Version V2.1	2020-03-24	Simone Fischer-Hübner	Changes by KAU and DTU for addressing EU reviewer comments
Final Version V2.2	2020-03-25	Simone Fischer-Hübner	Changes by UMI and JAMK for addressing EU reviewer comments
Final Version V3	2020-04-06	Simone Fischer-Hübner, Matthias Beckerle	New chapter 6 updated and introduction and executive summary updated. Changes for section 3.2.4 by UNITN added.
Final Version V4	2020-04-17	Simone Fischer-Hübner	Final editorial changes based on comments by internal reviewers.
4.0	2020-04-30	Ahad Niknia	Final check and preparation for submit

List of Contents

List of Figures

List of Tables

List of Acronyms

BRN	Masaryk University
CISSP	Certified Information Systems Security Professional
CTF	Capture the Flag
DFIR	Digital Forensic and Incident Response
DNS	Domain Name Service
DTU	Technical University of Denmark
DO	Digital openness
EADTU	European Association for Distance Teaching Universities
ECTS	European Credit Transfer System
EIT	European Institute of Innovation and Technology
ENISA	European Network and Information Security Agency
EQAC	Education Quality Accreditation Commission
EU	European Union
GDPR	General Data Protection Regulation
GUF	Goethe University Frankfurt
HEI	Higher Education Institution
IADF	Instructional and Assessment Design Framework
ICITA	International Cyber Investigation Training Academy
I&E	Innovation and Entrepreneurship
IPR	Intellectual Property Right
ISACA	Information Systems Audit and Control Association
ISP	Internet Service Provider
IL	Independent learning
ISO	International Organisation for Standardization
JAMK	Jyväskylän ammattikorkeakoulu (University of Applied Science)
JRC	Joint Research Center
KAU	Karlstad University
KIC	Knowledge und Innovation Communities
KTH	Kungliga Tekniska Högskola
LC	Learner-centered approach
LO	Learning Outcomes
MI	Medi-supported interaction
MOOC	Massive Open Online Course
MOOQ	Massive Online Open Education Quality
MSc	Master of Science
NATO	North Atlantic Treaty Organization
NTP	Network Time Protocol
UNITN	Trento University
OL	Openness for Learners
PKI	Public Key Infrastructure
QC	Quality Criteria
QCA	Quality Criteria – Academic
QCC	Quality Criteria – Continuous
QCR	Quality Criteria – Cyber Range
QF	Quality Focus
RO	Recognition options
SD	Spectrum of Diversity
UMU	University of Murcia

1 Introduction

1.1 Aims & Scope

CyberSec4Europe, as one of the EU H2020 pilot projects for a Cyber Security Competence Network, tests and demonstrates potential governance structures for such a network of competence centres. One area, in which governance structures will be implemented and evaluated, is the area of cyber security education based on MOOCs (Massive Open Online Courses), which have emerged over the last years as an alternative to formal education and enabler for life-long learning to a broad group of students.

The objective of this deliverable on a "Case Pilot for WP2 Governance" by the project's task 6.3 on "Virtual Education" is the initial review of existing cyber security MOOC offerings and of existing rules or practices of operating them at EU level for assuring quality. Moreover, this deliverable defines a quality assurance process based on a list quality assurance criteria that we elicit for MOOCs to be branded as "CyberSec4Europe MOOCs". While MOOC quality assurance frameworks were already proposed by different organisations, we have been particularly interested in eliciting also those quality assurance criteria that should be met specifically for cyber security MOOCS including cyber ranges MOOCs in addition to generic MOOC quality assurance criteria.

Based on the quality assurance process and criteria proposed in this deliverable, CyberSec4Europe's task 2.3 on "Governance Structure Design" will design a decision process of governance structures for cyber security MOOCs in Europe.

1.2 Approach

We first reviewed existing MOOCs and online course offerings for four types of courses: Academic courses that award credit points, continuous learning courses, cyber range courses and courses offered by the European Institute of Innovation & Technology (EIT) Digital. For the review of academic, continuous learning and cyber range courses, we first reviewed ENISA's database on available cyber security educations in Europe, which however includes only a short list of online courses and no MOOCs that do not require a student enrolment. We reviewed also web resources for MOOC offerings, lists of distance educations offered in Nordic countries, as well as the MOOC offerings at the dominant international online learning platforms. Moreover, we conducted a search on the web with search terms including "MOOC" or "online courses", "Cyber Security", "IT Security", "Information Security", "Privacy" or "Data Protection" and with the translation of these terms in German, Swedish and Italian. Our objective was not to find an exhaustive list of all MOOC offerings but rather to find a representative set of course offerings as a basis for reviewing the current landscape and the existing rules or practices for the operation of these types of MOOCs.

The review of existing MOOCs, online courses and the existing rules and practices for operating them allowed us to analyse open questions and issues for cyber security MOOCs, for which we then defined quality assurance criteria in this deliverable for addressing these issues. For the list of quality assurance criteria provided in the deliverable, we also reviewed related work on quality assurance criteria and frameworks for MOOCs, which allowed us to derive mostly generic quality assurance criteria that should also be met by cyber security MOOCs. Furthermore, the list of quality assurance requirements is also based on existing rules and regulations, best practices and our experiences.

Also the certification and accreditation process models discussed in the deliverable are based on common rules and practices.

A quality branding process is proposed as another component of the quality assurance process, which we have exercised in a pilot evaluation exercise and which also includes a peer review process of quality criteria that are not objectively measureable.

Finally, a relevance rating of quality assurance criteria for the pilot implementation by WP2 is proposed based on a first round of independent ratings by the main contributors to this deliverable followed by joint discussions for reaching to a consensus for any deviating individual ratings.

The relation of the different chapters is depicted in the Figure 1 below.

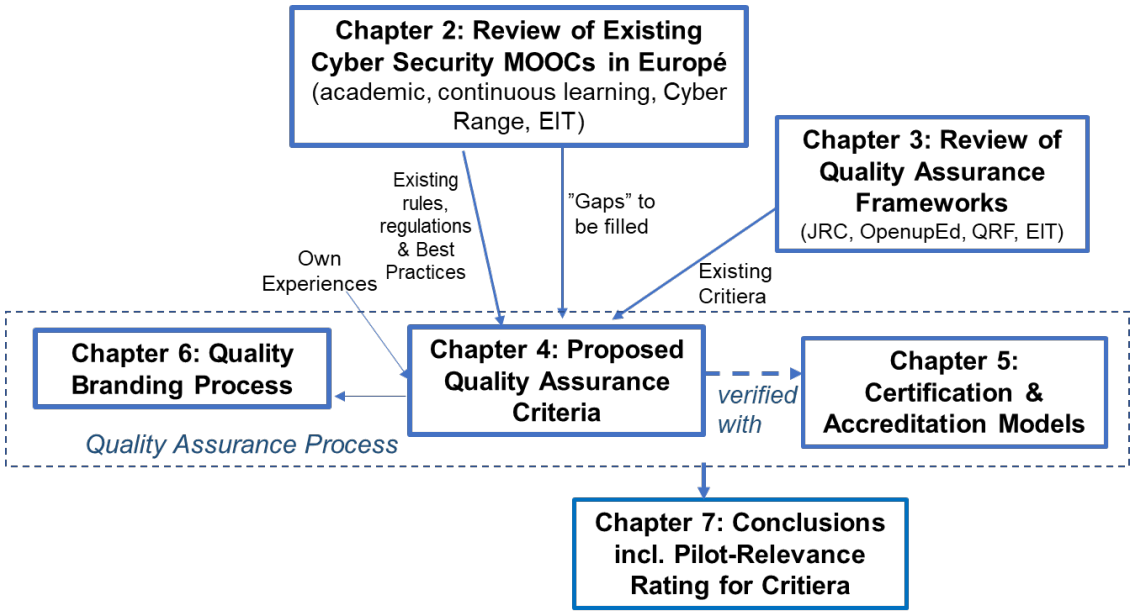


Figure 1. Relation of the chapters for proposing the Quality Assurance Criteria and Process.

1.3 Document Structure

The remainder of this deliverable is structured as follows:

- Chapter 2 provides the review of existing offerings cyber security MOOCs in Europe, as well of the rules and practices of operating them for providing quality, as well as open issues concerning quality assurance.
- Chapter 3 summarises relevant existing MOOC quality assurance and validation models as important related work.
- Chapter 4 is briefly outlining certification and accreditation models to be applied for the accreditation of a future Cyber Security Competence Network certifying cyber security MOOCs.
- Based on the finding of chapters 2 and 3, chapter 5 is then defining our proposed set of quality assurance criteria for MOOCs in Europe as the core of a quality assurance process, which present one of the main contributions of this deliverable.
- Chapter 6 is then outlining a proposed quality branding process based on the defined criteria.

- Finally, chapter 7 is concluding by discussing gaps and open issues as well as the cyber security relevance of the proposed quality assurance criteria and proposing a pilot relevance rating for the criteria.
- Appendix A.1 provides a list of selected cyber security MOOCs and online courses offered by European organisations.
- Appendix A.2 lists the top channels and platforms that we identified that offer cyber security MOOCs.
- Appendix B provides more detailed description of three selected exemplary MOOCs and their rules and practices of operation.

2 Review of Existing Cyber Security MOOCs in Europe

This chapter provides a short review of the existing European MOOCs and online courses in cyber security as well as rules and practices for operating them. Based on this review, we can then draw conclusions in terms of established and well-working rules and practices, gaps and challenges to be addressed by quality assurance criteria to be proposed in chapter 5.

In section 2.1, we will first review academic level courses and programmes which are offered to students enrolled at academic institutions and award credit points or academic degrees. Continuous learning courses, which are then reviewed in section 2.2, are offered for the broader public and do not require their students to be enrolled if the course is offered by an academic institution. Cyber range courses, reviewed in section 2.3, involve cyber ranges for practical training purposes and could be either academic level or continuous education courses. As special examples, MOOCs offered by the European Institute of Innovation & Technology (EIT) Digital and its governance structure for operating the EIT MOOCs are reviewed in section 2.4.

For these four types of courses, we will in the respective subsections first briefly describe the existing landscape of courses in Europe and will then focus our attention on describing those course characteristics that are important for the quality validation and will thus also be addressed by the quality assurance criteria in chapter 5.

Finally, conclusions are drawn in section 2.5.

2.1 Academic level courses

By offering online education on academic level, universities can broaden their student base and reach out to new student groups. From the student point of view, there are benefits in terms of enabling them to a larger degree to make educational choices based on their interest, rather than for mobility reasons.

Existing landscape of courses. The current landscape of academic online education can be divided into three types of offerings: Traditional MOOCs, fully online courses and fully online programs. In some cases, it is hard to draw the line between what is an academic MOOC and what is an online course. In this report, we define those courses for which the course material is publicly availability as MOOCs. Online courses, in contrast, will only make the course material available for students accepted and enrolled at the offering university. Reviewing each of these categories led us to the following observations.

While MOOCs for cyber security topics are more commonly offered by universities, there are 26 related course offerings from European universities on (Class Central, 2019), a web source that covers MOOCs from 901 universities. We found that none of the offered MOOCs for cyber security on (Class Central, 2019) can be classified as MOOCs at academic level, i.e. MOOCs that award credits or academic degrees. When searching (non-exhaustive) outside of the platforms that are covered by (Class Central, 2019),, we found only one in Finland [A.09], one in Sweden [A.27], one in Germany [A.26], two in Italy [A.16], [A.18] and one in France [A.28] (please refer to Table 3 in Appendix A.1). The channels used are usually one of the well-known learning platforms available (e.g. Coursera, EdX, Canvas), either run by the universities themselves or by third parties. In addition, also university-owned MOOC platforms are in use (e.g. mooc.fi, oncampus.de). The material is mostly freely available, but students wanting credits or an attendance certificate usually must either enrol as a student or pay a fee for the examination or both. The degree to which online courses in cyber security are offered by academic

institutions is country-dependent as well. In densely populated countries, such as Germany, most universities do not offer online courses, except for Virtual Universities. In rarely populated countries, like Sweden, with areas that are remotely located from universities, there are however several offerings from different universities for online courses related to cyber security (see

Table 4 in Appendix A.1 for an overview of selected online courses). 50% of these courses do not have any mandatory physical meetings or attendance requirements, 12% state that a few meetings might take place, and in the rest of the cases no information can be found even though they state that they are place independent. The level of the courses ranges from introductory or basic level courses up to advanced level courses. The course material is, in our examples, not available until students are admitted to the course with admission criteria similar to the ordinary campus courses. Fees and the possibility to attend the course as a stand-alone course (i.e. without being a program student) varies with the rules and practices of education in the different countries, where the hosting institution is situated. However, all the academic examples in Table 3 can be stand-alone. As the channel, the ordinary learning platform of the university is usually used.

In addition, there are also a number of European academic institutions and virtual Universities offering online Bachelor or MSc programs for the cyber security area (see

Table 5 in Appendix A.1 for an overview of selected programs). Applying for and attending these programs are in many cases similar to campus programs with the major difference that no physical lecture attendance is needed and that the study time is more flexible.

Qualification of proposing institutions. For any education offering credit points (ECTS) or academic degrees, the qualification criteria and accreditation rules must be the same as for regular university education in the specific country. One of the MOOCs and one of the educational programs were offered by Universities in cooperation with industry [A.09]) or by industry in cooperation with a university ([A.46]). However, in these cases, the examination is done by the cooperating university.

Qualification of participants and admission criteria. Student admission criteria are in general regulated by National Higher Education Acts. For courses at Bachelor level, typically an upper secondary education is at least required, and for courses at Master Level, the student must have been awarded a Bachelor's degree from an internationally recognised. In addition, university program-specific entry requirements and requirements for language proficiency may have to be fulfilled as well.

Qualification of instructors. Not all of the academic courses that we surveyed present the instructors/teachers of the course or the course responsible. In general, qualification requirements for teachers of academic courses are, in most cases, regulated by national law or by university regulation. For example, in Sweden, the requirements for employing senior teachers at Universities, such as professor or senior lecturers, are regulated by the National Higher Education Ordinances (Utbildningsdepartementet, 1992). Also, for the MOOCs at academic level that we surveyed, teachers that were specified usually hold an academic degree, and typically at least a PhD. University or national rules will usually also govern minimum requirements for examiners. However, the examiner does not necessarily have to be the teacher taking part in the course.

Examination, credits and/or course certificates. Academic MOOCs usually either offer credit points /ECTS for enrolled students, and/or course /participation certificates for either enrolled or participating students. For issuing credit points (ECTS), the university needs to have an accreditation approved by the Education Quality Accreditation Commission (EQAC) (Education Quality Accreditation Commision, 2019).

Description of course content, learning objectives, and professional expectation. A vast majority of the courses describe content and topics, learning objectives and skills to be acquired, and professional expectation. In many cases this is done in a structured way. This might be because the universities in many places have legal requirements on course documentation. If ECTS credits are awarded, the institution must also define and provide transparency on the course workload and learning outcomes (European Commission, 2019). However, in a small minority of the cases it is hard to find any information on the webpage besides an overview of the course and the titles of the lectures given in the syllabus.

Course evaluation. Course evaluations are typically done according to the university rules and procedures for promoting education of high quality and to improve the follow-up work. Course evaluation summaries may be published for transparency purposes, which may also be required by university rules. Course and programme evaluations and the Universities quality management work may also be required and/or regulated by National Higher Education Acts (Utbildningsdepartementet, 1992) and Ordinances (Utbildningsdepartementet , 2019) (see for instance Section 14 of the Swedish Higher Education Ordinance) (Utbildningsdepartementet , 2019).

Openness. As pointed out above, the major difference between the classical MOOCs and the online courses is the way that participants enroll and who is eligible for enrolment. For classical MOOCs anybody can enrol to follow the course, however participants wanting credits for the course need to enrol at the university as a student. The academic MOOCS from Finland, Germany and Sweden mentioned above use (CC, BY, NC, SL) Creative Commons 4.0 (International Attribution - NonCommercial - ShareAlike License), For the Italian academic MOOCs, one has to enrol to get the content and the information. However, they claim to follow OpenupEd (see 3.2.1), so it is highly likely that they will have Creative Commons or similar license.

2.2 MOOCs as continuous education courses

Continuing education courses are a fundamental instrument to ensure that European citizens have access to specialised education through all phases of their lives. By enabling lifelong learning, continuing education courses contribute to increase and develop competitiveness, growth and welfare in Europe.

Existing landscape of courses. In addition to traditional presence-based continuing education courses, European citizens have access to a vast amount of continuing education courses accessible through online learning platforms. A dominant representative class of such platforms are worldwide online learning platforms such as Coursera, EdX, FutureLearn, Udacity, Udemy, Canvas, and Cisco Networking Academy, to mention a few (see list in Appendix A.2)[1]. We focus our review on this class of platforms for continuing education courses since they have the potential to provide equal access to quality education to all European citizens, which is one of the European Union's central goals. Continuing education courses in the above mentioned platforms are characterized by a huge variety of formats and characteristics.

Qualification of proposing institutions. The dominant classes of providers of online continuing education courses in the reviewed platforms are higher education institutions and private companies. Other less frequent classes include non-profit organizations (e.g. [A.14]) and individuals (e.g. [A.33]). Some platforms have partnerships with specific course providers. As an example, Coursera, EdX and FutureLearn have partnerships with European higher education institutions in Belgium (e.g. KU Leuven), Denmark (e.g. DTU), France (e.g. ENS), Germany (e.g. TUM), Italy (e.g. Sapienza), Netherlands (e.g. TU Delft), Norway (e.g. University of Oslo) Spain (e.g. IE Business School), Sweden (e.g. Lund University), and UK (e.g. Imperial College). Note, however, that all reviewed platforms have US headquarters (Coursera, EdX, Udacity, Udemy, Canvas. Cisco Networking Academy) with the exception of FutureLearn, which is UK based.

Qualifications of participants and admission criteria. Some platforms provide unrestricted access to selected courses that are hence open and free to all citizens with no specific criteria on the students' qualifications and previous knowledge. Recommendations and indications on the difficulty level, assumed background and expected pre-requisites are usually given. In other cases, enrolment is limited by several criteria that may include schedule constraints, payment of fees, enrolment to education programmes (e.g. nanodegrees, certification programmes), having passed pre-requisite courses, and

[1] In this section, we focus on the worldwide learning platforms offering courses in English, but the list in Appendix A.2 also lists 2 further examples of country/language-specific ones.

nationality constraints, for example due to sanctions to specific non-European countries (for example, Coursera applies US regulations that affect citizens from several countries).

Qualification of instructors. Information about instructors in all reviewed platforms is typically publicly available in the description of the courses. Some exceptions are courses where the instructors are described as a team (e.g. [A.24]) or as an entity (e.g. [A.14]) with no individual information. Information about individual teachers often includes pictures, names, affiliations, and short biographies. In some cases the information provided is very rich, while in others it is limited to names and pictures [A.04]. The typical qualification for courses provided by higher education institutions is that of a teacher at the corresponding institutions (lecturer/professor). In the rest of the cases, teachers are often experienced professionals with a variety of profiles (developers, analysts, trainers, consultants) that tends to be less detailed. In some cases teachers do not have a higher education degree in the area of expertise of the course.

Examination, credits and course certificates. Some platforms offer verified certificates of completion, but since courses often do not have a formal status, these certificates are typically issued automatically by the platform, based on learner progress data. Typically, platforms offer two options: to pay for a certificate or to take the course without receiving a certificate at the end. Certificates are provided by the platform, in some cases jointly with the partner providing the course.

Description of course content, learning objectives, and professional expectation. Most courses describe content and topics, learning objectives and skills to be acquired, and professional expectation. However, most platforms do not provide such information explicitly in structured way. Very often, such information is included in the general overview or in the syllabus of the course. An exception is FutureLearn that explicitly includes sections on “What topics will you cover?” (content), “What will you achieve?” (learning objectives) and “Who is the course for?” (professional expectation).

Course evaluation. Some platforms (Coursera, Udemy) provide public ratings and reviews by previous students, while other platforms (EdX, Udacity, etc.) do not disclose any information about course evaluations.

Openness (for participation, free and open access to material for students and teachers). All reviewed courses require some sort of registration/sign-in in order to access the course materials and/or to join the course. Some courses are free while others require a registration fee. As for the material, most platforms reviewed do not provide teaching material openly and require enrolment to be able to access and/or download it. In some cases, previews of the materials (e.g. videos in [A.33]) is openly provided.

2.3 MOOCs as Cyber Range courses

The definition of a cyber range has not matured, but varies (Yamin, et al., 2019). ECSO defines cyber ranges as

> *A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation’s ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional*

components which are, in turn, desirable or required for achieving specific cyber range use cases.

(European Cyber Security Organization (ECSO), 2020)

It is notable that the ECSO report does not speak out requirements related to OSI layer 1, e.g. CPU, RAM, hard disk, network, but it states that a cyber range should meet the requirements for the indented use cases. This reliefs the requirements so that a cyber range can scale from learning a single technology or skill to having full blown structured cyber exercises.

Existing landscape of MOOCs concentrating on cyber ranges or the usage of them is non-existential within EU. During our research, we found no evidence that MOOCs concentrating on cyber ranges exists. However, there are online courses utilizing cyber ranges, but there is only limited public information available of cyber range usage during the course. Thus, the content of this chapter is described on a generic level.

Typically, a range is owned by an organization that the higher education university has a collaboration agreement with, e.g. NATO CCDCOE & Tallinn University of Technology (Tallinn University of Technology, 2019). Still the Bachelor's Degree at Tallinn University does not have any implication of cyber range usage within the courses (Tallinn University of Technology, 2019; Tallinn University of Technology, 2019). Multiple other cyber range courses without implication of usage of the cyber range have been observed, e.g. in South-Eastern Finland University of Applied Sciences degree structure (South-Eastern Finland University of Applied Sciences Xamk, 2019) vs their Cyber Lab environment (South-Eastern Finland University of Applied Sciences Xamk, 2019). Norwegian University of Science and Technology (Norwegian University of Science and Technology, 2019) and their Norwegian Cyber Range (NTNU - the Norwegian University of Science and Technology, 2019). Same goes for JAMK University of Applied Sciences Cyber Range (JAMK University of Applied Sciences, 2019) and the Bachelor's Degree- (JAMK University of Applied Sciences, 2019) (JAMK University of Applied Sciences, 2019) & Master's Degree - programme (JAMK University of Applied Sciences, 2019). The unofficial course plan at JAMK has more specific details on the usage of a cyber range (ENISA European Union Agency, 2019).

EdX, Coursera, EIT Digital and Udemy had no courses on cyber ranges. The verification is still invalid as it depends on the definition of a cyber range. Singular courses might have elements within them, but cannot be verified through open descriptions. One good example of this is the course from the Royal Institute of Technology in Sweden (KTH) on Ethical Hacking (KTH Royal Institute of Technology, 2019). The course describes the technical environment as "Infrastructure" that is ran in Google Cloud. The organizer is not running the range, but paying for the infrastructure. The environment, exercises and data is subject to Google's Terms and Conditions.

Thus, no good governance models can be collected from them. Further investigation should be done in WP6 D6.2 as higher education is reviewed by country. ENISA gives a good reference list for this work (ENISA European Union Agency, 2019). As European MOOCs for cyber range courses are not existent yet in Europe, the following criteria description is based on cyber range courses in general and particularly cyber range courses providing online access.

Qualification of proposing institutions. There is a wide variety of cyber ranges at different scales that can be utilized for several different educational and research purposes. Overall requirements for a cyber exercise depend on targeted audience, and focus and scale of the exercise, which defines properties of

technical cyber range environment and required level of exercise planning. The scale of the exercise can vary from a single computing system to the whole internet infrastructure, and the audience from critical national infrastructure service provider organizations to individual cyber experts. The required expertise for exercise planning and hosting capabilities for different types of exercises can vary a lot. Therefore qualifications for exercise hosts and educators must reflect this situation. In order to formulate compatible EU-wide qualification system for cyber range educators, classification system for different course types is needed.

Offering institutions have separated the course descriptions from the actual cyber range used, thus they keep the right to use what platform necessary or available for the institution. **Topics, course & presentation format** cannot be concluded from our study. Reference (JAMK University of Applied Sciences, 2019) gives insight, but is a singular case. **Channels** to provide the educational material follow the organizations guidelines giving instructions.

Qualification of participants, admission criteria and qualification of instructors. Existing students appear to be Master's Degree oriented, as cyber ranges are big concepts to grasp and exercise in. Typically, Bachelor's Degree students appear to have smaller laboratory exercises or Capture The Flag -style scenarios. Thus, the qualification of target students/admission criteria follows the guidelines of the higher education organization and same goes for the qualification of teachers also.

Examination, Credits and/or Course certificates. Awarded credits seems to follow European Credit Transfer System and possible recognition of prior learning -processes can be gone through to verify the students' knowledge. Typically, this means the student has participated in an event utilizing a cyber range and has a certificate of it e.g. KYHA in Finland (JAMK University Of Applied Sciences, 2019) or Locked Shields in CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence, 2019).

Description of course content, learning objectives, and professional expectation. If the target audience of cyber range-based course are individuals, most courses describe content and topics, learning objectives and skills to be acquired, and professional expectation. Also, credits acquired by students passing the course are usually stated, and they can be used to estimate required student work effort to pass the course. Technical details of a course based on cyber range are not described.

When an the target audience is some other entity than an individual, such as a single team from an organization or a company or representatives from several functions of an organization attending to a large scale realistic cyber range based exercise, then addition to the individual perspective mentioned above, there are the organizations learning objectives and targets. At organisational scale they may differ between organizations at detailed level. In general, organizations attend to large scale cyber exercises in order to improve organization's readiness and resilience against modern cyber threats and to discover development areas in processes, procedures, or personnel's expertise.

Course evaluation. Since the MOOC courses on cyber ranges are non-existent in Europe, type and size of ranges vary, and they can be utilised for several different educational (and research) purposes, course evaluation is difficult. For example, cyber exercises where organizations learn about their operational processes should not be evaluated on same basis as exercises targeted for individual cyber professionals. The same goes with the focus of the exercise; if it is on crisis management and chain of command, evaluation should be different from courses focused more on technical capabilities and operational processes. In order to sketch compatible EU-wide evaluation system, classification for different course types is needed first.

Openness. Openness of courses and course material is basically the issue with courses on cyber ranges. The lack of visibility hinders the ability to have good governance models. Singular cases give perspectives, but cannot be generalised as best practices without good cyber range flagship events (such as WP6 D6.4).

2.4 MOOCs as EIT Digital courses

Among the different MOOC offerings, the one by EIT Digital is particularly relevant for the Network of Competence Centres. EIT Digital is a division of the European Institute of Innovation & Technology (EIT). EIT activities are organized through KICs (Knowledge and Innovation Communities), which are essentially large partnership consortia).

Existing landscape of courses. Among the various KICs courses, the EIT Digital KIC is the most relevant for cyber security - Its mission consists of promotion and spread of digital innovations and entrepreneurship in education across Europe. EIT Digital different strategic domains (Digital Industry, Digital Cities, Digital Wellbeing, Digital Infrastructure and Digital Finance) have a close correspondence with CyberSec4Europe project verticals.

As part of its innovation projects, EIT Digital has developed, in collaboration with multiple universities and educational institutions across Europe, a series of educational programs focusing on Innovation and Entrepreneurship (I&E). Starting in 2011 EIT Digital have developed "traditional" classroom based Master Degrees with an innovation component (around 30 ECTS are on I&E over 120 ECTS) which are managed by consortia. For example, the Master Programme is coordinated by ELTE University in Budapest and includes the University of Trento, the University of Rennes 1, the University of Turku and other universities. Students spend one year in a university and a second year in another university and thus obtain a double degree. In the most recent years, EIT Digital has extended its education activity towards the production of MOOCS focusing on the area of I&E and on piloting some blended Masters.

Qualification of proposing institutions. All the participating Universities are part of the partner network of EIT Digital. Up to now, EIT Digital has mostly focused on a submission-based model analogous to traditional call for research projects

1) The partners, typically European Universities[2], gather together to form a consortium with a minimum of three countries (albeit in some occasion only two countries have been allowed). In their proposals, partner universities commit to develop and deliver courses and pedagogical assets in accordance with the current EIT Digital I&E education specifications and implementation guidelines.
2) The partners submit a proposal to EIT Digital for co-financing the development of a specific MOOC specialization after some consultation with business developers and action line leaders from EIT Digital.
3) The review of the project focused mostly on the adherence of the specialization on EIT Digital Business Plan for the next year and its coherence with the action lines. As we mentioned action lines essentially coincide with CyberSec4Europe verticals.
4) If approved the partners develop the MOOCs and submit deliverables for their realization.

[2] European universities were actively involved in developing the courses. Participating in the development of these courses means an opportunity to demonstrate excellence in education and increase academic reputation.

5) The MOOC specialisations are then ported into Coursera for operational execution.

In this set-up there is only a limited part for accreditation and quality verification of the curriculum. Most of the activity is indeed done during step (3).

Qualification of Delivery Platforms. MOOC courses are hosted in a variety of platforms and, in the framework of this activity, EIT Digital -in cooperation with the other KICs- has performed an analysis of the different modalities in which the MOOCs can be delivered (Segers & al., 2018) The first difference is Internal LMS vs. external MOOC platforms (e.g. Coursera). Among the Internal platforms one can still differentiate between among KIC-owned platforms vs. platforms through partner organizations (e.g. Universities) Out of the various possibilities EIT Digital has opted for 1) use an external platform (Coursera and EIT DigitalX learning analytic tools) and 2) retain ownership of content. For example, the majority of the course available on https://www.eitdigital.eu/eit-digital-academy/online-education/ are in Coursera while EIT Digital retain the ownership of the contents. The choice of Coursera is due to its global reach, its collaboration with universities, and its business model, which allows also for a revenue sharing (which is particularly relevant for EIT Digital's own sustainability). The detailed analysis of the pros and the cons of each choices is described in [X-KIC-D1-2018].

Qualifications of the participants and admission criteria. A peculiarity of Coursera's MOOCs is the concept of cohorts. Cohorts are used to define sets of students that have enrolled for a specific session of a course. Essentially, the courses can either be accessible at any time, or through the cohorts. Cohorts are useful mostly for organizational purposes and for mapping students back into classical academic degrees. Similarly to what happens in a University, cohorts allow Coursera's content providers (e.g. EIT Digital through its partner universities) to organize the staff member needed for taking care of that session of the course (grading assignments, answering questions, among other tasks). In some cases, cohorts may overlap but typically new enrolled learners are always given the chance of registering on the newest cohort.

Qualification of instructors. EIT Digital gives information about individual teachers (called "instructors"), including names, pictures, affiliations and short bios in the courses descriptions. All the instructors have a demonstrated significant expertise and as a team, they have a variety of profiles.

Examination, Credits and/or Course certificates. Both EIT Digital and EIT InnoEnergy KICs have identified a way in which Coursera modules can be assembled to achieve the equivalent of at least a semester of normal Master Course albeit the actual operational recognition into a normal academic programme is still under discussion in the current EIT Digital Master School Framework Agreement. Within Coursera, courses can be either independent modules (spanning typically less than 1 ECTS in term of learning effort and hours) or can be clustered in "specializations" (e.g. [A56], [A57]) if they designed to master a specific topic. EIT Digital has focused on the approach toward delivery of specializations in the range of 4-6 ECTS: this is implemented by 3-4 modules followed by a capstone project.[3]

[3] An example of technical specialization is available at https://www.coursera.org/specializations/embedded-systems-security whereas a I&E specialization is available at https://www.coursera.org/specializations/value-creation-innovation.

Course evaluations. Since EIT Digital use Coursera it borrows the public ratings and reviews by previous students provided by Coursera. EIT Digital have further created an evidence-based Instructional and Assessment Design Framework (IADF) to both guide teachers in developing online learning materials, and to collect data for learning analytics. The IADF framework serves as i) a teacher support when developing MOOCs, ii) an evaluation guide and checklist for teachers about pedagogical strategies, iii) an evaluation guide for educational support staff. It can also be used to evaluate iv) the actual final product (i.e. the MOOC specialization) developed within each project proposal if applied by project reviewers. It is further described in Section 3.

Description of course content, learning objectives, and professional expectation. The courses descriptions report information about contents and topics, learning objectives and skills and knowledge to be acquired through the training. They are published both in the abstracts that outline a general overview of each course and in the syllabus that contains detailed descriptions for all the modules offered, included their duration (expressed in number of hours). Professional expectations are not defined explicitly. After completing a course, the students have the possibility to indicate in their review of the course if they started a new career after it and/or if they got a tangible career benefit from the participation to it, as the Coursera platform has this option.

Openness. The online contents are used by all the Universities in the network. All the materials are offered on the shared platform where the students are given access and follow the related online materials for the course at hand. EIT Digital gradually shares parts of its programmes in order to make it accessible to a wider audience.

2.5 Conclusions from the review

Our review shows that a majority of courses including continuous learning and cyber range courses, are offered by academic institutions.

Classical academic MOOCs were rare and in general academic courses are typically already governed by existing regulations and university's own rules and quality plans for guaranteeing high quality education. Quality assurance criteria defined in such rules and regulations should thus to be considered in chapter 5.

Quality assurance criteria and processes for non-academic courses are less well defined. Especially for commercial MOOCs quality criteria for assuring a well-balanced course content, which is not un-proportionally biased towards promoting commercial systems or products (unless the course is focusing entirely on teaching these systems or products), need discussion. Moreover, criteria for assuring fairness and transparency in regard to course admission and evaluations will need attention.

So far, cyber range MOOCs are non-existent, but if developed in future they will require the discussion of ethical rules on the openness of course content, student admission and course material.

Our survey of the current landscape also showed that cyber security related topic channels or platforms do not exist yet. In Appendix A.2 we list the most common MOOC platforms and channels that are offering cyber security related courses at the moment.

Furthermore, MOOC platforms and channels are typically hosted by US American providers, which means that personal data including student attendance and performance tracking may be transferred to

the USA, which raises privacy and GDPR compliance issues (in regard to the transfers of personal data to third countries regulated in Chapter V GDPR) that need to be addressed.

Finally, it is important to consider: to foster open learning recognition in Member States, regulatory enablers need to be defined; research into the Member States' regulations and practices would enable the setting up of specific strategies for advancing the recognition of open education in Europe. Moreover, it will be important to disseminate good practice on the integration of open learning into regular HEI programs; and ensure that Member States policies on validation and recognition of non-formal learning embrace open education and MOOCs, removing discrimination between 'how' and 'where' the learning takes place. Member states can also promote policies that encourage and facilitate both learners and employers to explore open learning recognition further.

3 MOOC Quality Assurance and Validation Frameworks

When we talk about MOOC validation and quality assurance framework, we can find two kinds of studies. One of them more focused on the validation and recognition principles around the MOOC contents (see section 3.1) and other more focused on the pedagogical and quality of the MOOCs (see section 3.2).

3.1 Recognition Practices

The OpenCred study (JRC report, 2016) investigated how European non-formal open learners are assessed and what credentials they can obtain for their open learning achievements. It focuses particularly on emerging recognition practices in formal higher education and continuing professional development.

In the study, they point out that for recognition we can distinguish between two main distinct processes: firstly, credentialisation and, secondly, the actual recognition of learning outcomes (see Figure 2). That is, for the recognition, as a first step, we perform the credentialisation of a learner's learning outcomes or achievements. Next, as a second process, the actual recognition of Learning Outcomes takes places. Although this second process is sometimes made by the same institution that performed credentialisation, in general, it is made by a different institution or an employer. Figure 2 aims to clarify the difference between the two processes.

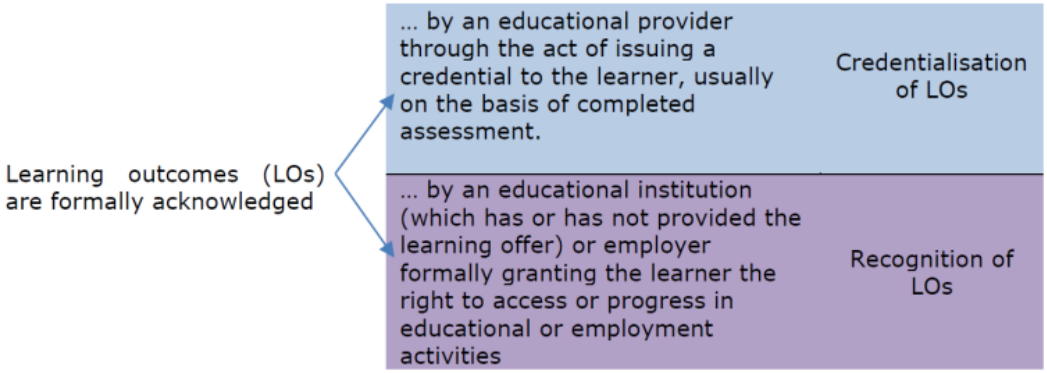


Figure 2. Learning Outcomes Acknowledgements (JRC report, 2016).

In higher education, the recognition of non-formal learning – whether open or not – can be considered for the following purposes (JRC report, 2016):

- Access: this recognition can be a way so that individuals can gain access to educational institutions programmes;
- Progression: the recognition can also allow to registered students be fast-tracked through their studies by exempted them from part of the programme;
- The award of a full degree.

It is also important to mention that in the world of employment, the recognition of open, non-formal learning is also valuable for entry and progression purposes. It can play a role in recruiting new employees for jobs, and it can also aid the career progression of working professionals.

At the same time, taking into account that knowledge society is fast changing the skills and competences required, the recognition of the learning outcomes achieved through open learning could be a help so that higher education institutions and employers can keep pace with these changes. This should imply different aspects (more details in (JRC report, 2016)):

- Pockets of experimental practice in workplace organisations/ employer bodies;
- Academic recognition for own or partners' MOOC provision;
- Integration of externally-provided open learning to complement mainstream higher education courses;
- Building entire degree programmes based on open learning.

JCR report considers that there are six central elements of MOOC provision to facilitate future recognition by other HEIs or employers:

- Identity verification of the learner;
- Suitable supervised assessment;
- Informative credentials such as (digital) certificates or online badges that acknowledge learning;
- Quality assurance;
- Award of credit points;
- Partnerships and collaboration with potentially "recognizing" institutions or bodies.

Figure 3 shows the OpenCred's open learning recognition traffic light model represents these elements:

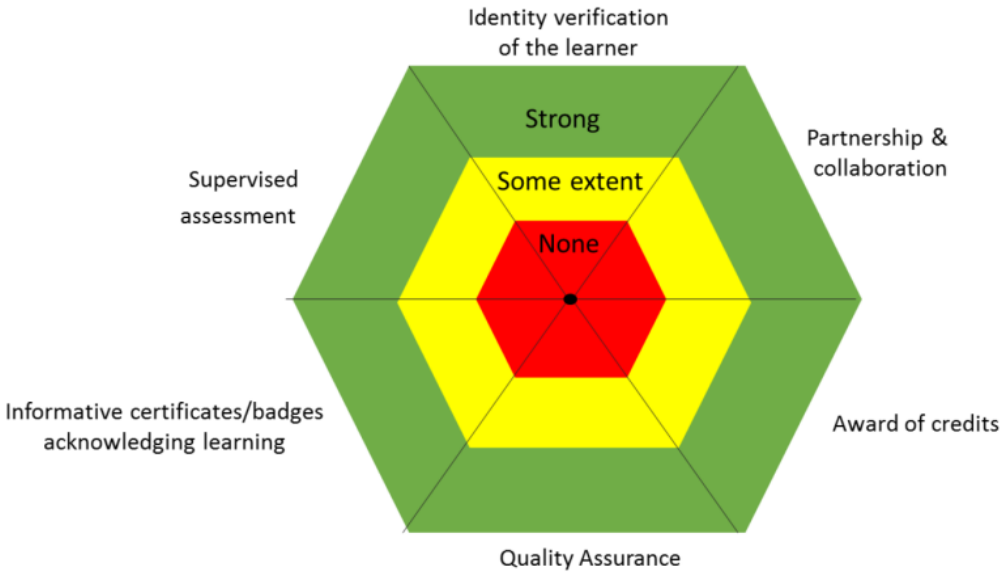


Figure 3. Open learning recognition traffic light model (JRC report, 2016).

3.2 Quality Frameworks

Three different frameworks, presented in the following three subsections, are being considered in this review.

3.2.1 OpenupEd label, quality benchmarks for MOOCs

The OpenupEd partnership for the provision of MOOCs is an alliance of institutional MOOC providers and coordinated by the European Association of Distance Teaching Universities (EADTU). The

partnership decided the development of quality level for MOOCs, the OpenupEd Quality Label, and follow the quality principles and practices defined in it. The OpenupEd's commitment aimed at helping with the opening up of education through MOOCs so that both learners and wider society can be benefited that European values such as equity, quality and diversity are reflected. To achieve this goal, partners integrated in their MOOCs the eight distinctive features that are shown in Table 1 (Jansen, et al., 2017).

Table 1. OpenupEd distinctive features description (Jansen, et al., 2017).

OpenupEd distinctive features	**Explanation**
Openness to learners [OL]	This captures aspects such as: open entry (no formal admission requirements), freedom to study at time, place and pace of choice, and flexible pathways. A broader perspective stresses the importance of being open to learners' needs and providing for a wide variety of lifelong learners.
Digital openness [DO]	Courses should be freely available online but in addition apply open licensing so that material and data can be reused, remixed, reworked and redistributed (e.g. using CC-BY-SA or similar).
Learner-centred approach [LC]	Courses should aid students to construct their own learning from a rich environment, and to share and communicate it with others; they should not simply focus on the transmission of content knowledge to the student.
Independent learning [IL]	Courses should provide high quality materials to enable an independent learner to progress through self-study.
Media-supported interaction [MI].	Course materials should make best use of online affordances (interactivity, communication, collaboration) as well as rich media (video and audio) to engage students with their learning.
Recognition options [RO]	Successful course completion should be recognised as indicating worthwhile educational achievement.
Quality focus [QF]	There should be a consistent focus on quality in the production and presentation of a course.
Spectrum of diversity [SD]	Courses should be inclusive and accessible to the wide diversity of citizens; they should allow a spectrum of approaches and contexts, accounting for a variety of language, culture, setting, pedagogics and technologies.

The OpenupEd Quality Label provides framework for improving the quality of their MOOCs. This label was derived from the E-xcellence label (Williams & Kear, 2012) and it provides a methodology which is aimed at assessing the quality of e-learning in higher education. The review process defined in E-xcellence is based around a number of benchmark statements. These statements are grouped according to the six dimensions of Strategic Management, Curriculum Design, Course Design, Course Delivery, Staff Support and Student Support. The E-xcellence label has been periodically updated from the feedback of its reviewers in order to reflect the changing nature of e-learning in Higher Education Institutions (HEI).

The benchmarks defined at (Williams & Kear, 2012) have been mapped to the OpenupEd distinctive features. This means that the benchmarks can also be used to gather evidence that a MOOC (or more broadly a program of MOOCs) support the OpenupEd features. In turn, supporting these features helps to ensure that OpenupEd MOOCs reflect the values of equity, quality and diversity.

Evidence should then be gathered, ideally by a small team that includes different stakeholders such as management, academics, course designers, tutors and students. The output from this self-evaluation should be an agreed document that provides, for each benchmark, a judgment of achievement supported by brief evidence. A roadmap of improvement actions should then be prepared.

3.2.2 Quality Reference Framework (QRF) for the Quality of MOOCs

The Massive Online Open Education Quality (MOOQ) Project proposed a Quality Reference Framework (QRF) developed by the European Alliance for the Quality of Massive Open Online Courses (MOOCs), called MOOQ (Stracke, et al., 2018).

The Quality Reference Framework provides the QRF Key Quality Criteria and the QRF Quality Checklist for designing and developing MOOCs. Main target groups of the Quality Reference Framework are the designers, facilitators and providers of MOOCs as well as the MOOC learners.

The Quality Reference Framework can be used to analyse the needs and demands for MOOCs, to design, develop and implement new MOOCs and to evaluate and improve existing MOOCs. The main benefits of the Quality Reference Framework are:

- It provides a generic framework that can be adapted to each specific context.
- It identifies key quality criteria for better orientation on the MOOC design.
- It presents a checklist for the quality development and evaluation of MOOCs.
- It enables a continuous improvement cycle for MOOC design and provision.

The Quality Reference Framework is based on the International ISO standard ISO/IEC 40180 (former ISO/IEC 19796-1) and the results from the mixed methods research by MOOQ.

The QRF consists of three dimensions including quality criteria and instruments:

- Dimension 1: Phase taking into account aspects like Analysis, Design, Implementation, Realization, and Evaluation.
- Dimension 2: Perspectives taking into account aspects like Pedagogical, Technological, and Strategic.
- Dimension 3: Roles taking into account aspects like Designer, Facilitator, and Provider.

Within these dimensions, they have defined criteria that are related to:

- The initiation of the analysis of the MOOC considering an incubation team and the re-use of existing MOOC (if applicable).
- The identification of internal and external stakeholders and those core ones are represented in the design and development team as well as the identification of target learners and their profiles.
- The definition of objectives regarding learning, learning content, pedagogical model, instructional design, learning activities, and institutional objectives.
- The identification of external and organization context.
- The estimation of costs and the development of a financial plan.
- The definition of team content experts, roles and facilitators.
- The definition of didactical approaches, structure for the content and possible levels of certification.

- The consideration of different technical issues, media design, the communication of the concept and the interaction with stakeholders is made and how the feedback is provided.
- The design of tests and assessments.
- The implementation of a draft MOOC and its finalization through testing considering content, design, media, technical issues, organization of use, and testing and evaluation.
- The development of the MOOC addressing administration, learning activities and learning support, and review of the competence levels.
- The evaluation and improvement of the MOOC considering evaluation planning, evaluation realization, evaluation review, and improvements and optimization.

The complete list of the criteria that they defined by indicating the different dimensions they belong to can be found in (Stracke, et al., 2018).

3.2.3 Quality Assessment by EIT KICSs

As we mentioned in chapter 2, EIT Digital in cooperation with the other KICs have developed an evidence-based Instructional and Assessment Design Framework (IADF) to assess the quality assessment of the courses.

The IADF consists of four components to be filled in by teachers and developers of MOOCs:

(1) Instructional Design; (2) Assessment; (3) Functional Requirements; and (4) Learning Analytics. Instructional Design and Assessment are the most important in providing teachers and developers with insight into the needed pedagogies to teach and develop a high-quality MOOC.

The Instructional Design component consists of 9 categories of characteristics to describe the instructional design of the MOOC and/or individual videos, including: organization, learning goals, problem-centred subject matter, activation/prior knowledge, scaffolding/guidance, differentiation, demonstration, application, integration and collaboration. Each category is made up of several criteria that describe what should be taken into account when designing and developing a MOOC. The criteria are scored on a scale from 1 to 3, where 1 means insufficient, 2 sufficient, and 3 excellent. In case the criterion is not applicable or relevant for the course and/or video, 0 is scored. A MOOC scoring 3 on each criterion can be considered pedagogically sound. The Assessment Design component focuses on the different assessments offered to students in the MOOC. Both in-video quizzes, and assessments to be completed after videos/lectures/the course can be designed and evaluated using this component of the IADF. Also, the Assessment Design component can be used to develop summative, formative and peer assessments. Similar to the Instructional Design component, teachers and educational consultants can fill it in on course level and on individual assessment level. Here the individual assessment, instead of videos is adhered to, since not every video necessarily has an assessment. Also, the scoring is similar to the Instructional Design component (1-3). The Assessment Design component consists of 6 overarching categories essential for the design of assessments, including general design of questions/assessment, stem of the question, options, feedback, distracters, evaluation, each with several criteria.

The Functional Requirements component consists of 2 categories with different criteria used to assess especially the slides used in a MOOC and its individual videos. The first category is ‘Slide style and layout’ and focuses on the looks of the slides. The second category is ‘Information check’ and aims to get an overview of the accuracy of displayed information, its language and grammar. This component can only be filled in on individual video level. Each video should contain properly designed slides and

accurate information. A course level evaluation could overlook mistakes made in specific videos regarding criteria in this component. The scoring of 1 to 3 applies, as well as the choice of filling in 0 if the criterion is not applicable to a certain video.

The Learning Analytics component serves the purpose of showing students their learning behaviour and progress, giving teachers an overview of student performance and appreciation of the MOOC, and giving educational consultants and teachers insight in possible improvements for the MOOC during the run of the course or for a subsequent run. The component consists of only 7 criteria that can be scored on course level. The component can only be scored y (yes) or n (no). In the case of a score 1, the framework gives space to explain how data are given back to teachers and students.

The IADF and its separate components can be used by teachers to design their own courses, by evaluators (e.g. educational support stuff or EIT itself) to evaluate the actual final product to decide whether additional changes are needed to improve it. Teachers can consult the IADF as a guide to design and develop their MOOC. After having developed (part of) the MOOC, the IADF can be filled in. Most criteria can be scored both on course level and on video level. This means that teachers can score for each video how much it complies with the different criteria in the framework. This framework can be further used for quality assessment.

This helps teachers (as well as evaluators) to get a detailed view of how they designed and developed their lectures, and in what lectures improvements could be made. The overall course score helps to get the broader picture of the instructional design of the course as a whole. Scoring the criteria themselves (at least for the whole course) helps when educational support staff also evaluates the course using the IADF. Teachers and support staff can then check for similarities and differences in scoring. This offers both stakeholders an idea of where added support in developing the MOOC might be needed. If a criterion is too low, it is advised that teachers try to make changes to the video/course in order to achieve a minimum quality level. This is important for sustainability: there seems to be mounting evidence that the cause of learners drop-out after 4-5 minutes of lectures is not that videos are too long but that lectures/videos are too poor.

An interesting extension of the IADF might be to provide quality assessment criteria for the appropriateness of the video to different action line specializations as they are the key vehicles used by EIT Digital to provide I&E offering that are not casted into degrees.

4 A Note on Certification and Accreditation Models

Before defining quality assurance criteria in the next chapter as part of the quality assurance process for MOOCs that could be branded CyberSec4Europe MOOCs in future, we will in this chapter provide a brief description of the mechanisms behind certification and accreditation models, since the adherence to the quality assurance criteria needs to be verified with the help such models.

First, we would like to clarify what we mean by certificate and accreditation in this context, since the words are ambiguously used. In this chapter, when we are mentioning certificates, we do not refer to a course certificate but rather a certificate in the sense of a certified product, a certified professional or a certified organisation. When we are using the term accreditation, we refer to the process of verifying that the certification body to be accredited has the creditability and the skills, personnel and processes in place to be able to conduct a certification. Thus, this chapter is not about the accreditation of education and the handing out of course certificates that an higher educational institution is doing as part of its normal operation, but rather about the verification that the institution (e.g. future Cyber Security Competence Network certifying MOOCs) follows the requirements and practices set up by a standard or an organisation (e.g. the principles of the framework described in chapter 3 or the quality assurance criteria defined in chapter 5).

4.1 Potential quality assurance processes for different types of courses

In order to make the right choices for the model for approval, one needs to understand the formal concepts and ideas behind accreditation and certification. The central point is how you acquire trust for the certificate or seal. However, the choice between accreditation and certification is also dependent on the purpose of the certificate.

Generally speaking, anybody can construct and award a certificate and construct their own certification schemes, but there might be doubts on the trustworthiness of this certificate by third parties unless it is awarded or backed up by a widely trusted and recognised entity within the specific area. This is usually solved by having an independent trustworthy third party validating and approving that the body or person awarding the certificate has the right knowledge, procedures and practices in place in order to perform the certification process in a good manner. This third-party verification is usually done by an accreditation organisation. This organisation is in many cases one that has especially been appointed by law and European agreement. This goes for most internationally recognised organisations, product and person certification schemes. There are also cases where a well-known and respected company or industrial organisation or a similar body performs the accreditation.

The accreditation will add a level of trust that the certificate has been rewarded in a correct manner according to its requirements and that the body doing the certification is following the stated procedures.

There are a number of international standards used in this area that put general requirements on certification bodies that are always used by the national accreditation authority and sometimes by other accreditation bodies as well in order to award an accreditation to a certification body for a specific certification scheme. Examples are ISO/IEC 17065 for bodies performing product certificates, ISO/IEC 17025 for accreditation of laboratories and ISO/IEC 17024 for accreditation of bodies operating certification of persons. As an example, the different actors in the Common Criteria scheme are accredited under different accreditation standards. The certification body that grants the certificate to the product is accredited under ISO/IEC 17065. However, the certification body reviews test results

from accredited laboratories in this process and these laboratories needs to be independent from both the certification body and the customer. These laboratories needs to be accredited under ISO/IEC 17025 and approved by the certification body.

These types of standards may or may not be suitable for the approval process depending on the purpose of the certificate. If the purpose is to certify the product or the organisation, then the organisation performing this certification should preferably be accredited. This means that for the certification of Cyber Security MOOCS (e.g. those to be branded CyberSec4Europe MOOCS), we suggest that the Cyber Security Competence Network conducting this certification should be accredited. If it is about a professional certificate given to the student, then the organisation providing the course should be accredited. In any case, there needs to be a scheme put in place stating the requirements and process for getting the certificate and the requirements put on the certification body.

4.2 Potential stakeholders as certifiers and accreditation bodies

There are a number of stakeholders that can be involved in the process of certification and accreditation. However, the stakeholders directly impacted by the certificate, such as students, educational platforms and course developers, are all potentially biased and should not be part of the certification or accreditation body. There are also a number of potential stakeholders that could or should be part of the development of the certification scheme. For instance, for the certification of cyber security MOOCs, important stakeholders can be (and should) include governmental bodies (e.g. cyber security agencies, ENISA, contingency agencies), cyber security industry organisations or representatives and academic or professional societies (e.g. computer societies, bar associations or other charter giving organisations). These could also be certification organisations if they are independent of the entity or of the object that is certified. However, the body performing the accreditation should not have a vested interest in the certification scheme or any other dependencies tied to the certificate. This should ideally be a third party that is not a stakeholder in the certificate as such or dependent of the reputation and trustworthiness of the certificate.

5 Proposal for Quality Assurance Criteria

This chapter presents our proposed quality assurance criteria for MOOCs and online courses. The criteria are based on (1) existing best practices and our experiences, (2) rules, regulations and ethical standards, (3) conclusions drawn from our review of existing European MOOCs and online courses in cyber security in chapter 2 in terms of gaps to be addressed or criteria that need special attention and (4) criteria taken from existing quality assurance frameworks that were presented in Chapter 3.

In the following subsection, quality criteria that mainly apply for academic MOOCs are marked with the code QCA. These include also criteria mandated by Higher Education laws and rules that exclusively apply to academic MOOCs as defined in chapter 2. Criteria that apply for MOOCs as continuous courses have the code QCC, whereas criteria that are specific for cyber ranges are marked with QCR. The criteria that we suggest as general criteria applying to all types of MOOCs are marked with QC.

The criteria are listed under different categories in the following subsections, which correspond to categories for quality criteria used in other quality assurance frameworks referred to in chapter 3. In addition, we added categories for ethical rules, privacy and for cyber range specific quality assurance criteria, which, as also our review and gap analysis in chapter 2 showed, need special attention when it comes to cyber security MOOCs.

Relevant stakeholders for cyber security MOOCs, to which we refer in this chapter, comprise cyber security experts from industry or government representing potential employers, data protection officers of the educational institutions that can advise on relevant GDPR aspects to be covered in courses related to privacy, privacy activists, representatives from (ethical) hacker organisations, and/or representatives from (national) cyber security agencies.

The quality criteria are relevant for the different phases of a MOOC lifecycle, including Analysis, Design, Implementation, Realisation and Evaluation as defined by (Stracke, et al., 2018). In Table 7 in Appendix C, we show which criteria are relevant for life-cycle phases. The table also classifies the criteria into the type of procedure needed for assessing the fulfilment of the criteria. These types, which will be further discussed in chapter 6 that outlines the quality branding process, are: “Peer reviewed” (for rather subjective criteria that should be evaluated by a group of experts in a peer-review process), “Objective finding” (for criteria which are measurable by a third party), and “Official legal document” and “Internal policy document” (for criteria that are fulfilled if such documents exist).

5.1 Qualification of the proposing institution

In order to create and offer a MOOC of high quality, the proposer should have the proper qualification and experiences to be able to develop, run and evaluate the MOOC in a professional manner. The quality of the proposer is also essential for the recognition of the MOOC by the community and for the recognition of credentials. In the light of this, we propose the following criteria:

(QC 1) The proposer should be recognised by the relevant stakeholders in the cyber security community as having expertise in the area. This could be either by academic recognition or long experience within the area or related areas or other criteria that the stakeholders may find relevant.

(QCA 1) The proposer should be recognised as a valid higher education institution in the country or region where it has its main site.

(QCA 2) The MOOC should be approved by a recognised higher education institution, i.e. it should have passed the same approval and quality process as any other university courses have at that institution.

(QCA 3) The MOOC should be recognised as an eligible course that can be counted towards a degree in at least one awarded degree program at the higher educational body that is responsible for the course.

(QCC 1) The proposer should have partnerships and collaborations with other recognising academic institutions (as also suggested by the OpenCred study (JRC report, 2016)).

(QCC 2) The proposer should either be an academic institution fulfilling the criterion (QCA 1) or another type of institution that has built a reputation with certified courses or certification courses.

(QCR 1) The proposer should have a well-founded background in applied technology & private-public partnership.

(QCR 2) The institution's cyber range should be technical, work-life oriented which mimics realistic phenomena (attack campaigns, threat actors, techniques & tools) from the cyber security field.

Criteria (QC1), (QCC2), (QCR 1) and (QCR2) are based on existing best practices and our own experiences, (QCA 1) and (QCA 2) reflect Higher Education rules and regulations, and (QCA 3) and (QCC 1) are enabling formal credentialisation and recognition as required by the OpenCred study and OpenupED distinctive feature [RO].

5.2 Qualifications of participants and admission criteria

For properly benefitting from a MOOC, it is important that students know what is expected from them in terms of prerequisites and that the teachers know what to expect from the participants. However, prerequisites that are not essential for the MOOC should not be used for excluding students. In principle the aim should be to be as inclusive as possible for enhancing cyber security competence in Europe. Participants must also be able to find out whether they are qualified for a MOOC and/or why they are not accepted for enrolment. For this reason, it is important that the acceptance process should be legit and transparent. We therefore propose the following criteria:

(QC 2) The MOOC should only have the requirements that are needed to follow and understand the course content by the participants.

(QC 3) The MOOC requirements should be motivated when they are stated. It must be indicated how to acquire the requirements (e.g. pointing to specific courses or teaching material) by the participants.

(QC 4) The MOOC must accept participants in a fair and transparent manner and should state the acceptance process and, if the number of participants is limited, the criteria and process for selection of participants.

(QCA 4) The participants should have academic merits that show that they fulfil the qualifications for the MOOC. Alternatively, the participants must proof other types of qualifications that are recognised by the higher education institution that is approving the course.

(QCC 3) The participant should meet the requirements of the MOOC in form of relevant industrial experience, academic degrees, or specific skills needed to engage in the specific MOOC.

(QCR 3) The participant should have the skills necessary to operate a technical cyber range platform or the learning objective of the course should be that the participant learns how to operate such platform.

(QC 2), (QC 3) and (QC 4) should enable the openness to learners, i.e. [OL] OpenupEd distinctive feature, (QCA 4) is needed for complying by higher education rules and (QCC 3) and (QCR 3) are drawn from best practices and our own experiences.

5.3 Qualification of instructors

The qualification of the instructors (teachers) is fundamental to ensure a high quality of a MOOC.

(QC 5) The responsible instructor must have an academic degree or other relevant qualifications and experiences within the area.

(QC 6) The instructors should have pedagogical training either by prior teaching experiences and/or having taken and past courses on pedagogics for higher education or by other means.

(QCA 5) The MOOC must be taught, examined or supervised by a person that fulfils the (legal and local) requirements to be recognised as an instructor at the appropriate level of the MOOC by the higher educational institute that has approved the course. Typically, the instructor should have at least the degree that is awarded and the supervisor and examiner of a course/educational programme should have at least one academic degree higher than the degree that is awarded.

(QCC 4) At least one of the instructors in the course should have applied research experiences, relevant industrial or work life experience in the area of the course or experiences with collaborating with industry or government.

(QCR 4) Since the cyber range requires technical operation, the instructor should have such technical skills for conducting and supervising such operations or the course should have dedicated personnel for this task (e.g. cyber range specialists).

All criteria listed in this action should guarantee the OpenupED distinctive feature of a Quality focus [QF]. (QC 6) and (QCA 5) also reflect to higher education rules. (QCC 4) and (QCR 4) are also derived from best practices and our own experiences.

5.4 Course examination, credentialisation and recognition

For awarding credits or certificates, course examinations have to verify that the student has achieved the goals of the education and assure that the awarded credits or the certificate correctly reflects the quality with that the goals were achieved. Also for this reason, it is important that the examination is fair and transparent so that the participants know what is expected from him/her in the exam and that the risk of fraud is minimised. Moreover, for credentialisation and recognition criteria should be met, as also suggested in the OpenCred study and OpenupEd framework presented in chapter 3. We therefore suggest the following criteria:

(QC 8) Examination content, especially in terms of course learning outcomes to be demonstrated in the exam, and the assessment form and assessment criteria should be clear and transparent.

(QC 9) Assessment methods must be aligned with the learning objectives and be measured by valid means (see (JRC report, 2016)).

(QC 10) The examination process must be fair, follow legal procedures, take appropriate measure to correctly identify the participants to be examined and thus minimize the possibility of cheating – independently of whether the course examination takes place online or at a physical location.

(QC 11) The time frame, in which the course needs to be finished in order to receive the credits or credentials, must be clearly stated. Also, the expected course workload including efforts for course assignments or laboratory work, etc. and deadlines for completion, need to be made clear and transparent.

(QCA 6) Course examinations must be aligned with the rules for the higher education institution that approves the course.

(QCA 7) The MOOC should be recognised as a valid credit-awarding course within the European credit transfer system (ECTS).

(QCA 8) The higher education institution that awards credits as well as the requirements that need to be fulfilled in order to achieve credits should be clearly stated.

(QCA 9) An academic MOOC must offer participants course credits if they are formally eligible for credits and successfully pass the course examination.

(QCA 10) The course should offer participants, who do not fulfil the formal prerequisites for obtaining credits, a course certificate instead, if they successfully participated and passed the course.

(QC 12) Obtaining a course certificate should not just be based on payment of fees, but on an actual verification that the participant fulfilled the learning objectives.

(QC 13) Course certificates should be designed to enable recognition of the educational achievements in the professional or life-long/blended learning context.

(QCR 5) The cyber range activities, laboratory work, and assignments that need to be completed for obtaining a course credential should be clearly stated.

(QC8), (QC 10), (QC 11), (QCA 8) are motivated by the requirements for ECTS credits by the EU Commission (European Commission, 2019), national regulations for higher education, and/or by other MOOC quality criteria by (Learning_of_Commonwealth, 2016) by QRF (Stracke, et al., 2018). (QC 9), (QCA 7), (QCA 10), (13) are derived from (JRC report, 2016) and are reflecting the recognition option [RO] of OpenupEd. (QCA 6) ensures legal compliance, (QC12) enhances the recognition [RO] of OpenupEd. (QCR 5) is based on our own experiences.

5.5 Course evaluations

MOOC evaluations allow student feedback and ratings for continuously improving the course quality, and by this, reduce the number of course dropouts. Published course evaluations provide information allowing to judge a MOOC and its usefulness from a participant's perspective. Course evaluations are commonly regulated in the academic sector. In particular, the Massive Online Open Education Quality (MOOQ) QRF Framework (Stracke, et al., 2018) provides key quality criteria for the evaluation

planning, realization, review and resulting improvements, which we partly take up in the criteria that we propose below along with criteria from rules and established practices from the academic sector:

(QC 14) The instructors and/or proposers should review the MOOC and its content periodically, so that the content is current and that it continues to fulfil its learning goal. The period of this review should be appropriate to the speed of development and changes in the area of the course scope.

(QC 15) There should be means in place for the participants to continuously, or at least periodically, evaluate the MOOC and to provide feedback. Suitable course-specific feedback channels or discussion fora should be used for receiving continuous participant's feedback. If the evaluation is done periodically, it should be conducted at least twice: once when the participants are halfway through the course and once when a participant finishes the course.

(QC 16) Means for conducting anonymous online course evaluations by the participants should be offered.

(Please note however that anonymity cannot necessarily be guaranteed, as this depends for instance also on the number of course participants, i.e. the anonymity set size, and other factors).

(QC 17) An evaluation review process should be in place that should involve relevant stakeholders (such as MOOC design team, instructors, director of studies). The relevant stakeholders should utilise available learning analytics, document the findings, and provides recommendations to improve the MOOC.

(QC 18) Summaries of evaluations and measures taken in response to the evaluation to remedy shortcomings or improve the MOOC should be easily accessible and published on the same channel/ platform as the MOOC.

(QC 19) The implementation, effect, and changes of proposed improvements should achieve their expected impact. Relevant stakeholders should evaluate this.

(QC 15), (QC17), (QC 18) and (QC 19) are motivated by the Quality Reference Framework (QRF). (QC 14) and (QC 16) reflect best practices.

5.6 Meeting professional expectation

For meeting professional expectations, suitable stakeholders, especially from working life and the employment side, should be involved in different MOOC phases:

(QC 20) In the early development phases of the course, an analysis should be done identifying stakeholders and their expectations.

(QC 21) Different relevant stakeholder representatives should be involved in the design, implementation, realization, and in periodic reviews of the MOOC. This means that their involvements can be in the form of advisors, guest teachers or external evaluators.

(QCR 6) Stakeholders' statements should be addressed when designing a course, its learning objectives and the scenarios run in the course.

(QCR 7) When providing a cyber range course to a company or an organization, it should be "realistic enough", i.e. simulate operational and supporting services and systems available for the participants. The extent of realism should be discussed and agreed upon during designing the course.

(QCR 8) When participants from a company or an organisation attend a course which utilises a cyber range, the participants should follow their own organisations' processes and guidelines when detecting abnormal or malicious activity and when starting or even performing incident management. This approach should bring to awareness the need to update the organisation's guidelines and process documentation and guidelines, and eventually train staff for the updated documentation, thus advancing the organisation cyber resilience (European Cyber Security Organization (ECSO), 2020)..

If participants from a company or organisation are not utilising their organisations guidelines or manuals, then the original goals set by their own organisation for the cyber range course may not be fully or even partially met. This could be due a limitation of the range capabilities, attending individuals' knowledge, skills, competencies, poorly planned organisational objectives for the training or lack of expertise of the cyber range offering party, or some other reason.

(QC 20) and (QC 21) are motivated by the Quality Reference Framework QRF. (QCR 6), (QCR 7) and (QCR 8) are based on our own experience and best practices.

5.7 Course structure and content criteria

In this section, we suggest quality criteria in terms of the MOOC content and structure. Some of the proposed criteria were taken from the OpenupEd suggested distinctive features (Jansen, et al., 2017), and some others were motivated by the Checklist for MOOC Accreditation in (Learning_of_Commonwealth, 2016) or by QRF (Stracke, et al., 2018).

(QC 22) There have to be specific learning outcomes defined for each MOOC and course examination and quizzes should be aligned with the learning outcomes. The evaluation of participants should test the alignment.

(QC 23) The MOOC should provide an overview, which prominently and in sufficient detail publishes the purpose and structure of the MOOC, the main content, format (the teaching methods used and learning activities required of students, assessment methods and criteria), reference literature, language, the learning outcomes including knowledge and skills (memorize, understand, apply, analyse, evaluate, or create) as prerequisites and knowledge (theoretical), skills to be acquired (practical, methodological, or applied), and instructor's profiles.

(QC 24) The content of the MOOC should be such the learning outcomes can be fulfilled. There must be alignment between the teaching methods, learning activities, assessment methods and the learning outcomes.

(QC 25) The MOOC should cater for different learning styles and strategies to reach the leaning outcomes.

(QC 26) MOOCs should follow a Learner-centred approach, as defined by OpenupEd: They should "aid students to construct their own learning styles from a rich environment, and to share and communicate it with others; they should not simply focus on the transmission of content knowledge to the student" (Jansen, et al., 2017).

(QC 27) MOOCs should enable independent learning and should, as suggested by OpenupEd, provide high quality materials to enable an independent learner to progress through self-study (Jansen, et al., 2017).

(QC 28) MOOCs should provide "media-supported interactions", as proposed by OpenupEd: "Course materials should make best use of online affordances (interactivity, communication, and collaboration) as well as rich media (video and audio) to engage participants with their learning" (Jansen, et al., 2017).

(QC 29) As suggested by OpenupEd, there should be a consistent focus in terms of the production and presentation of the MOOC (Jansen, et al., 2017).

This also means that all course material is appropriately cited and copyright clearance has been obtained if necessary. Web links used are relevant and functional.

(QC 30) The course material's design should be made accessible to different audience and should meet the requirements of EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies. In particular, videos should include subtitles or scribes of the voice recording in English.

(QC 31) The MOOC should include instructions that clarify how participants can obtain technical support.

(**QCC 5)** The MOOC should not in an inappropriate biased manner promote commercial products or systems of offering institutions, unless the entire focus of the MOOC is on the teaching or training of the usage of these products or systems.

(QC 22), (QC 23) and (QC 24) are motivated by QRF. (QC 25) and (QC 27) reflect the independent learning feature [IL], (QC 26) the learner-centred approach feature [LC], (QC 28) media-supported interaction feature [MI], and (QC 29) the quality focus distinctive feature [QF] of OpenupEd. (QC 30) is a legal requirements and also meeting the spectrum of diversity feature [SD] of OpenupEd. (QCC 5) addresses one of the gaps that we identified in our review of existing Cybersecurity MOOCs section 2.5.

5.8 Criteria for platforms and channels

Important quality criteria for platforms and channels include visibility and criteria are derived from legal requirements:

(QC 32) Privacy and security concerns should be addressed when selecting channels and platforms for learning content. Particularly, GDPR compliant platforms, preferably located in Europe, must be used, and platform should be hosted by trustworthy third parties or hosted directly by the MOOC provider.

(Further legal privacy requirements are listed in section 5.11below).

(QC 33) It should be easily possible for a broad audience to find and use the platforms used for the MOOC.

(QC 34) The platform should provide the functionality to comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies.

(QC 32) and (QC 34) are legal requirements. (QC 33) and (QC 34) are also motivated by the spectrum of diversity feature [SD] of OpenupEd.

5.9 Criteria for cyber ranges

For cyber ranges to be utilised for future cyber range MOOCs certain quality criteria should be fulfilled (see also Figure 4. Challenges defining Quality Criteria for Cyber Range courses.):

(QCR 9) The institution's cyber range should have automated realistic legitimate end user behaviour simulation, e.g. www-browsing, communication via email or other channels and business systems usage, allowing course attendees to practice their knowledge, skills and competence in order to distinct and detect the malicious network activity from normal network usage.

(QCR 10) The institution's cyber range should be either a federation ready to be used as an entity in a network of cyber ranges, or it should be customizable to be used as standalone. Federation capability enables cross-usage of cyber range resources, potentially enabling lowered costs for the joining parties and higher operational efficiency for the cyber range operator, and richer educational content for attendees (European Cyber Security Organization (ECSO), 2020). The cyber range should have scalability in terms of capacity and capability, so that it can be used in exercises and educational events, e.g. Capture the Flag (CTF), Digital Forensic and Incident Response (DFIR), or live exercise for structured full-scale cyber security exercise that is based on real events to increase the realism on selected exercise scenarios.

(QCR 11) Live exercises in a cyber range should scale in a way that is realistic enough to accommodate multiple simultaneous organizations (i.e. service providers, subcontractors, internal and external partners) that are depend on each other for providing business services.

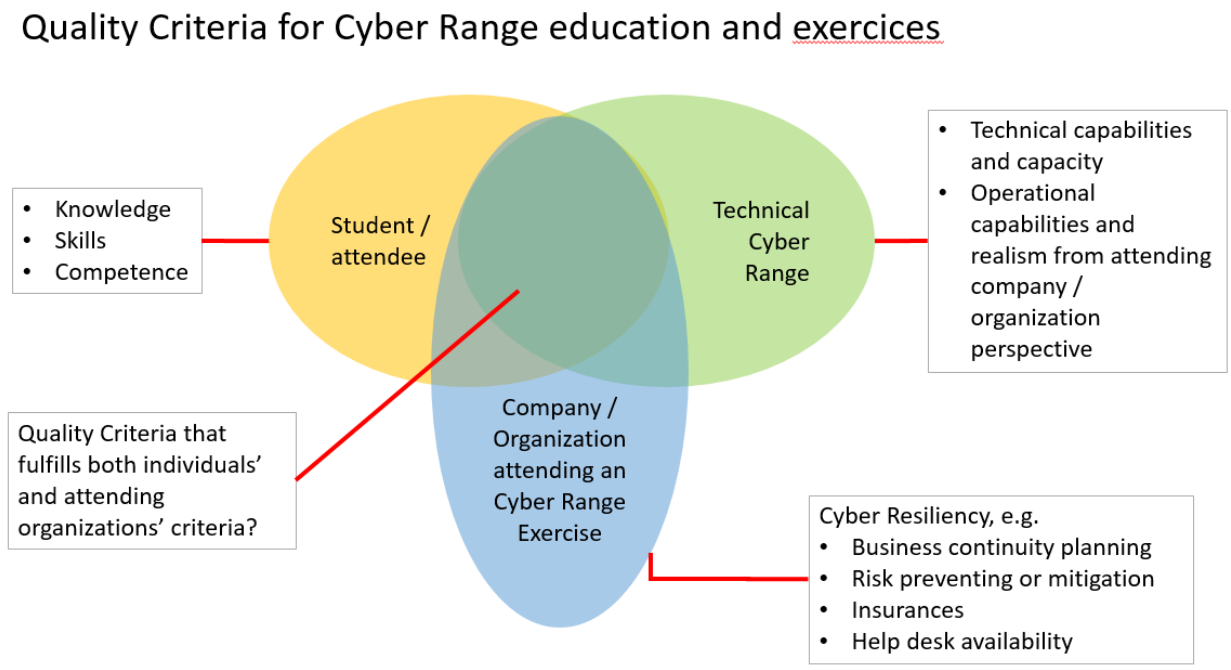


Figure 4. Challenges defining Quality Criteria for Cyber Range courses.

(QCR 12) The institution's cyber range should contain business specific environments (e.g. electricity distribution, banking, e-commerce) for the exercising companies, including network topology, network services and, business systems processes and data flows between the systems and services for end users.

(QCR 13) The institution's cyber range should have realistically modelled internet structure, architecture and services, such as global ISP infrastructure, DNS and NTP infrastructure, and global certificate and/or PKI infrastructure, cloud services as part of the "global internet", update repositories for updating applications and operating systems, news and social media sites and functionalities, and attendees should be able to build their own systems and services and connect them to the cyber range. Software required by the attendees should be available pre-installed or from the update repositories. The global ISP infrastructure should have sufficient amount of Border Gateway Protocol (BGP) autonomous systems (AS) compared to the learning goals and targeted level of realism.

(QCR 14) The institution's infrastructure should contain infrastructure for the Threat Actor to enable implementing or utilizing real world attack vectors, multiphase attacks with real malware and gathered threat intelligence information.

(QCR 15) The institution's cyber range should provide systems and services for planning, running and doing post-exercise analysis and also provide systems and services for the defending team to prevent, detect, mitigate and recover from cyber incidents.

All quality criteria defined in this section are based on our own experiences and common practices.

5.10 Openness

Openness is a key element of a MOOC. Openness is important both in terms of the MOOC content and material and in terms of being open to the learner's needs, which is captured by the following suggested criteria.

(QC 35) The MOOC should enforce openness to learners by adapting to their needs, as suggested by OpenupEd (Jansen, et al., 2017). It should as far as possible try to enable the freedom to study any time, place and pace of choice.

(QC 36) MOOCs should enforce digital openness: They should "be freely available online but in addition apply open licensing so that material and data can be reused, remixed, reworked and redistributed (e.g. using CC-BY-SA or similar)" (Jansen, et al., 2017).

In some cases, it may not be possible to make content freely available due to legal or other reasons e.g. restricted openness of cyber range technical details to course participants (for ethical / security reasons). However, the aim should be to make the course as freely available as possible, and therefore we suggest:

(QC 37) There should be suitable policies for defining any restrictions to digital openness and/or openness to learners for ethical or security reasons.

(QC 38) The MOOC should use open educational literature and resources.

(QC 35) and (QC 36) were taken from the OpenupEd distinctive features as referenced above. (QC 37) addresses a gap that we have identified by our review of existing European MOOCs and online courses in cyber security in chapter 2. (QC 38) was taken from (Learning_of_Commonwealth, 2016).

5.11 Ethics & Privacy

5.11.1 Ethical Considerations for Teaching Cyber Security

Education in cyber security by its nature must also cover attack methodologies and how vulnerabilities arise and/or could be misused. This knowledge is needed for teaching how to secure systems against threats and weaknesses in computer-based systems, e.g. administrative systems, industrial control systems and computer networks. A deeper understanding of threats and risks is also needed when performing risk assessment, risk analysis and risk management. However, this knowledge could also be exploited for malicious purposes. Because of this dual nature of this knowledge, it is important to teach and enforce certain ethical principles for cyber security courses. Below are some suggested criteria that should be considered.

(QC 39) There should be a code of conduct for course participants stating expected and unacceptable use of knowledge, tools and facilities, both during and after the course.

(QC 40) The MOOC should avoid going into detailed aspects of attack methodology and techniques for finding vulnerabilities, if it is not necessary for achieving the learning outcomes of the MOOC. This should especially be considered in totally open courses.

(QC 41) MOOC participants should be made aware of the ethical and privacy aspects of security monitoring and surveillance technologies, and countermeasures

(QC 42) MOOC participants should be made aware of the proper way of handling and reporting vulnerabilities that they might find.

(QC 42) reflects the IEEE code of ethics principles 6.08 and 1.04. (QC 39) and (QC 41) reflect ACM guidelines for cyber security curricula (ACM, 2017) and national requirements for teaching ethics as part of computer science curricula. (QC 40) addresses ethical best practices that need to be addressed if course are opened up without restrictions (which we also discuss as an issue to be addressed in chapter 2).

5.11.2 Privacy Requirements

Many platforms today store personal information about the visitors for different purposes. In some cases, this information is used to profile visitors for either platform improvement or for market purposes. This profiling can reveal sensitive personal data like political opinions, religious believes or ethical origin e.g. when tracking and storing course preferences and browsing patterns. On platforms like YouTube or other types of “free” channels, it is obvious that the information is used for targeted advertisement and in some cases soled on for market purposes. With this in mind, it is important to give the participants choices for where to access the learning material and not force the student to give more personal data than is necessary for fulfilment of the course and the examination. For example, if video course material is made available through YouTube, there should be an alternative more privacy friendly channel made available for accessing the material. It is also important that the “owner” of the course have an appropriate processor agreement with the sites that distribute the course material stating how personal data may be processed in compliance with the GDPR.

Users may be also profiled or tracked on course level for monitoring the progress of learning and/or analysing usage behaviour for the purpose of course improvements. Also for the purpose continuous learner identification, the options of using video monitoring or biometric authentication via key stroke dynamics are for instance discussed in (JRC report, 2016). Nevertheless, privacy enhancing solutions

should be implemented (following the Data Protection by Design principle) so that the privacy of the students is protected at the same time.

As a basic requirement, the platform and the MOOC provider have to follow the legal requirements of the GDPR. Especially, the following privacy requirements for teaching platforms, channels and courses need to be emphasized:

(QC 43) Privacy Policy (Art. 29 GDPR): There must be a clear policy statement, both from the platform and the MOOC owner, which includes information about the data controller of the different types of personal data, what personal data is processed by whom and for what purposes. Particularly the extent, purpose and consequences of participants profiling needs to be made transparent and should require the participant's explicit consent.

(QC 44) The platform and MOOC provider must assure that the participants can exercise their data subject rights pursuant to the GDPR, preferably also by electronic means.

(QC 45) If personal data is used for marketing purposes there should be an opt in mechanism rather than an opt out mechanism for that purpose.

(QC 46) There must be a valid and clear data processor agreement between the "owner" of the MOOC (in the role of the data controller) and the platform (in the role of the data processor) (Art. 28 GDPR).

(QC 47) If a privacy "unfriendly" channel is used, the participants of the MOOC should be given a more privacy friendly alternative.

(QC 48) The platform and course instances storing personal data about the participants must be secured by appropriate security controls and should be designed by the Data Protection by Design and Default principle (Art. 25 GDPR).

All criteria in this section are derived from the GDPR and were identified as important practical issues to be addressed in chapter 2 (ACM, 2017).

6 Quality Branding Process

In this chapter, we describe our initial proposal for a quality branding process for MOOCs to be conducted by a European Cyber Security Competence Network. It is based on an internal exemplary evaluation that we conducted and that will be described in more detail in an upcoming deliverable. The proposed process consists of the following eight steps:

1) Application

In the first step, the institution seeking a quality branding submits its application. Our evaluation exercise showed that not all information for evaluating the quality of MOOCs is openly available. Therefore, an evaluation process based on openly published information only does not seem to work, even though this is not in line with the inherent openness characteristic of MOOCs. Nonetheless, we conclude that the MOOC proposers will have to add documentation demonstrating how quality criteria have been met by them, when they submit their application for a quality branding.

2) Evaluation of factual assessable criteria

As mentioned in chapter 2, there are different types of quality criteria. In step 2, all criteria that can be objectively assessed are evaluated. These are all the criteria of the category "Objective finding", which are measurable by a third party, and the categories "Official legal document" and "Internal policy document" that are fulfilled if such documents exist (please refer to Table 7 in Appendix C for the quality criteria categorisation).

3) Peer-review of criteria

In step 3, all remaining quality criteria, i.e. those of the category "Peer reviewed" that are rather subjective, are evaluated by a group of at least 3 experts in a peer-review process. In this peer-review process, the experts first assess the fulfilment of the criteria independently based on their expertise and experiences. Then a discussion of all reviews takes place among the experts followed by a moderated consensus meeting for agreeing on an assessment and decision. If all criteria are fulfilled, step 6 follows next.

4) Rebuttal and resubmission phase

We recommend to only award a quality seal for MOOCs that clearly fulfil all quality criteria that are not formulated as optional. For any non-optional criteria that are not met, partly met or that are unclear, the proposer should be requested to address these open issues first and then resubmit the application for a quality branding.

5) Repeat step 2-4

Upon resubmission, steps 2 to 4 are repeated.

6) Preliminary Quality branding for first-time MOOCs

Ultimately, active participation in a MOOC might be needed to reliably retrieve all information needed for the evaluation. Even creating an account and subscribing to a course often does not provide all information needed, since some MOOCs are not active at the moment of review and the related information is not (yet) retrievable. If a MOOC runs for the first time, a preliminary assessment and quality branding should be given that is revaluated after the first iteration of the MOOC is completed.

7) MOOC evaluation by course participants for verification

Any preliminary quality branding evaluation is complemented by gathering feedback from students that participated in the MOOC. If the course evaluations reveal issues in regard to the practical fulfilment of the quality criteria, these issues need to be addressed and re-evaluated through step 2-4 before the period for the quality branding can be extended.

8) Quality branding for an extended time period

If all quality criteria are met for a MOOC that has been successfully given at least once, a quality branding is awarded for a longer time period, it is important to decide how often a provided quality branding should be revaluated since MOOCS naturally are subject to changes and may get outdated. While ideally, a revaluation should happen after each iteration of a MOOC for considering any changes, the costs and time for re-evaluations need to be considered as well. Hence, longer periods for 1-3 years for the validity of quality brands may be appropriate.

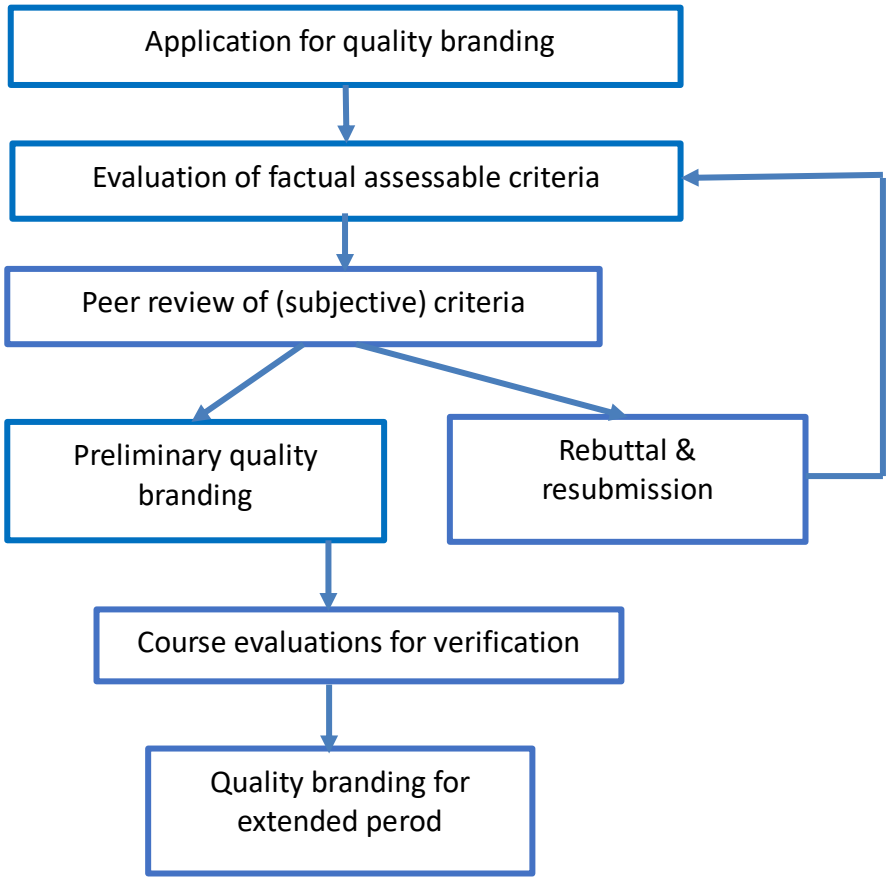


Figure 5. Sequence of Steps of Quality Branding Process

7 Conclusions

In this final conclusion chapter, we point out some of further limitations of existing MOOCs in cyber security provided in Europe and quality assurance frameworks, and discuss the relevance of our proposed MOOC quality criteria for the governance pilot to be implemented in WP2.

Our survey of existing European MOOCs in cyber security in chapter 2 showed that even though most of today's existing MOOCs are offered by academic institutions, only a few formally award (ECTS) credit points to course participants. Also for that reason, governance structures for the recognition of credentials including credit points need to be further developed.

Moreover, our survey also showed that MOOCs for cyber ranges are globally non-existent at the moment. This might be due the fact that cyber range infrastructure development, maintenance and operations requires resources, e.g. to pay salaries for the laboratory engineers and cyber security experts, electricity, networking and devices, software licenses, etc. Yet the requirements for capabilities and capacity of a cyber range varies from a rather simple implementation Capture The Flag (CTF) to full scale structured multi-organization or company cyber exercise. The former has relaxed technical, capability and capacity requirements (e.g. a few dozen networked virtual machines) compared to latter which requires several thousands of virtual machines and vast amount of software automation behind the scenes in order to enable the infrastructure and Live Exercise to meet the participating parties' requirements and learning objectives. Yet, even if the technology is available given enough resources are available, competencies are needed to develop a cyber range MOOC. Even a cyber range MOOC would consist from several federated (inter-connected) cyber ranges, each providing distinct capabilities and capacities, meeting distinct technical requirements and run by two or more institutions, the funding should be secured to the parties. When a cyber range MOOC is established, there should be arrangements (e.g. contractual, patents) in place to secure IPRs for the relevant parties.

Existing quality assurance frameworks for MOOCs that we reviewed in chapter 3 are mostly generic and not cyber security specific. Also, the quality assurance criteria that we propose in chapter 4 are to a large extent generic, meaning that they also apply for MOOCs or for MOOC platforms or channels in general.

Still, we also propose cyber security specific quality assurance criteria in chapter 4, which existing quality frameworks do not include or address. These include criteria for:

- The qualification of the proposing institutions, participants and instructors of cyber ranges courses.
- Involvement of suitable stakeholders from the cyber security community for meeting professional expectations.
- Providing suitable and realistic services for cyber range MOOCs for meeting professional expectations.
- Ethical hacking rules for participants to be communicated, taught and enforced.
- Clear and transparent policies for restricted openness of hacking-related course elements.
- The educational institution's cyber ranges to be utilised for cyber range MOOCs.

Moreover, criteria for addressing privacy issues in terms of profiling learners, achieving data protection by design and GDPR compliance were suggested by us in chapter 4, and are novel as they are mostly not addressed yet by existing quality assurance frameworks for MOOCs. While privacy and technical

privacy by design requirements are generic requirements for MOOC platforms and channels, they are also specifically important for MOOCs teaching privacy and the GDPR to give a good example and show practically how legal privacy requirements pursuant to the GDPR are correctly addressed in practice.

For the governance model for MOOCs that will be piloted in WP2, the authors of this deliverable deem especially those quality criteria to have a high relevance that are cyber security specific, while we think that all generic criteria are less relevant and should have a lower priority for the pilot implementation. However, other reasons need to be taken into consideration as well when deciding on how to prioritise criteria for the WP2 governance model pilot implementation, e.g. whether respective governance rules for implementing the criteria are lacking at the moment and should for that reason be addressed with more emphasis.

In Table 2 below, we finally provide our proposed rating for the relevance and priority for the WP2 pilot implementation together with our justifications:

Table 2. Pilot Relevance of the proposed Quality Criteria

Quality Assurance Criteria	**Relevance**	**Justifications**
Qualification of the proposing institution	Medium-High	Reputation is important. However, for academic courses, there are already well-established governance structures. Still, cyber range specific criteria (QCR 1) and (QCR 2) will need attention.
Qualification of participants & admission criteria	Low-Medium	It is important to have a fair admission process, and to be clear with the requirements to avoid frustration on the participant. However, selection criteria of who attends may change over time and from centre to centre of different Member States in the eventual Network, as they might have different policies of educating people not relevant for the actual delivery. Moreover, the proposed criteria are mostly generic.
Qualification of instructors	Medium	It should be ensured that courses are taught by qualified instructors. However, while qualification of instructors is important, a top professional or researcher might give a very bad presentation, so courses should be assessed primarily by content, if the presenter is “reasonably” qualified. Moreover, the proposed criteria are mostly generic.
Course examination, credentialisation and recognition	Medium	Currently, there is a lack of academic courses issuing ECTS, and also other courses that do not offer credentials. The type of credits resulting from evaluation may vary from member state to member states. The way in which we actually evaluate the skills resulting in certificate should fit into the content. There might be also the issue of recognition of credits with professional organization (e.g. ISACA requires continuous education to maintain a CISSP certificate) and not necessarily with universities. However, most of the proposed criteria are generic.
Course evaluations	Low-Medium	This is an instrument for improving quality, but is not always effective. Different parties might be interested in different types of evaluation. For example, they might offer sideways their educational curricula (e EIT Digital I&E courses for the master school) or as a prerequisite for actual enrolment (e.g. Politecnico of Milano School of Design). Our proposed criteria are all generic.
Meeting professional expectations	High	This is a key part of the mandate of the eventual Network, to provide improved professional skills to the vertical domains.

		It is therefore critical for the pilot. Moreover, most of the proposed criteria are cyber security or cyber range specific.
Course content and structure criteria	High	As we are delivering a "bill of knowledge" to people, understanding what the courses actually delivers in terms of skills is important. It is fundamental that a course has appropriate learning outcomes.
Criteria for platforms and channels	Low	These are generic criteria (even though generally important criteria).
Criteria for cyber ranges	High	All criteria are cyber security specific.
Openness	Low in general, (QC 37) is High	In general, these criteria address general issues. However, (QC 37) is cyber security/range specific and is important to address.
Ethics	High	These criteria are all cyber security specific and so far not regulated by MOOC quality assurance frameworks. Ethical hacking rules are however fundamental both for the respective course and later for the work life.
Privacy & GDPR	Medium	While most of the privacy criteria are general legal requirements, they are still important for giving a good example, especially for courses teaching privacy, for reasons discussed above. Mostly of the popular MOOC platforms and channels raise privacy issues. However, existing Quality Frameworks for MOOCs are not addressing privacy & GDPR compliance yet.

8 References

Utbildningsdepartementet , 2019. *Högskoleförordning (1993:100).* [Online] Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/hogskoleforordning-1993100_sfs-1993-100

ACM, 2017. *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* [Online] Available at: https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
[Accessed 20 03 2020].

Class Central, 2019. *Universities.* [Online] Available at: https://www.classcentral.com/universities

Education Quality Accreditation Commision, 2019. *ECTS COURSE CREDIT CERTIFICATE.* [Online] Available at: http://www.accreditation.info/ects-certificate.html

ENISA European Union Agency, 2019. *Education map.* [Online] Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities
[Accessed 31 05 2019].

European Commission, 2019. *Resources and tools.* [Online] Available at: https://ec.europa.eu/education/resources-and-tools/european-credit-transfer-and-accumulation-system-ects_en

European Cyber Security Organization (ECSO), 2020. Understanding Cyber Ranges: From Hype to Reality.

JAMK University of Applied Sciences, 2019. *Course information: Cyber Security Exercise (Master's).* [Online]
Available at: Course information
[Accessed 31 05 2019].

JAMK University of Applied Sciences, 2019. *Course information: Designing and Preparing a Cyber Exercise (Bachelor).* [Online]
Available at: https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=TTKW0310&knro=&noclose=+&lan=e&ark=
[Accessed 31 05 2019].

JAMK University of Applied Sciences, 2019. *Course information: Implementation of a Cyber Exercise (Bachelor).* [Online]
Available at: https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=TTKW0320&knro=&noclose=+&lan=e&ark=
[Accessed 31 05 2019].

JAMK University of Applied Sciences, 2019. *Cyber Range.* [Online] Available at: https://jyvsectec.fi/cyber-range/overview/
[Accessed 31 05 2019].

JAMK University of Applied Sciences, 2019. *Cyber Security Exercise - Course Details.* [Online] Available at: https://gitlab.labranet.jamk.fi/YTCP0400/cyber-security-exercise [Accessed 31 05 2019].

JAMK University Of Applied Sciences, 2019. *Valtionhallinto harjoittelee kansallisessa kyberturvallisuusharjoituksessa Jyväskylässä.* [Online] Available at: https://www.epressi.com/tiedotteet/tietotekniikka/valtionhallinto-harjoittelee-kansallisessa-kyberturvallisuusharjoituksessa-jyvaskylassa.html [Haettu 31 05 2019].

Jansen, D., Rosewell, J. & Kear, K., 2017. Quality frameworks for MOOCs. In: M. J. e. al., ed. *Open Education: from OERs to MOOCs.* s.l.:Springer, pp. 261-281.

JRC report, 2016. *Validation of Non-formal MOOC-based Learning: An Analysis of Assessment and Recognition Practices in Europe (OpenCred),* s.l.: s.n.

KTH Royal Institute of Technology, 2019. *Course information: Online Course in Ethical Hacking.* [Online] Available at: https://www.kth.se/nse/studies/online-course-in-ethical-hacking-7-5-hp/course-information-1.819016 [Accessed 31 05 2019].

Learning_of_Commonwealth, 2016. *Guidelines for Quality Assurance and Accreditation of MOOCs,* s.l.: ISBN 978-1-894975-82-7.

Norwegian University of Science and Technology, 2019. *Study Cyber and Information Security: Design a Secure Digital Society.* [Online] Available at: https://www.ntnu.edu/iik/cyber [Accessed 31 05 2019].

NTNU - the Norwegian University of Science and Technology, 2019. *Norwegian Cyber Range.* [Online] Available at: https://www.ntnu.no/ncr [Accessed 31 05 2019].

Segers, H. & al., e., 2018. *D1. Report on taxonomy of the KICs approaches, experience and competence, in Learning Analytics Overview of Online Learning Repositories and Corresponding Learning Analytics Capabilities of the KICs.,* s.l.: InnoEnergy.

South-Eastern Finland University of Applied Sciences Xamk, 2019. *CyberLab Learning Environment.* [Online] Available at: https://www.ictlab.fi/index.php/en/ [Accessed 31 05 2019].

South-Eastern Finland University of Applied Sciences Xamk, 2019. *Cybersecurity, master studies structure.* [Online] Available at: https://opinto-opas.xamk.fi/index.php/en/2676/en/123587/CSKT19SY/year/2019 [Accessed 31 05 2019].

Stracke, C. M., Tan, E., Texeira, A. M. & Carmo, M. d., 2018. *Quality Reference Framework (QRF) for the Quality of Massive Open Online Courses,* s.l.: www.mooc-quality.eu/QRF.

Tallinn University of Technology, 2019. [Online]
Available at: https://www.ttu.ee/nato-ccdcoe-and-tallinn-university-of-technology-will-strengthen-cooperation
[Accessed 31 5 2019].

Tallinn University of Technology, 2019. *Cyber Security Engineering, structure of curriculum version.* [Online]
Available at: https://ois.ttu.ee/portal/page?_pageid=37,674560&_dad=portal&_schema=PORTAL&p_action=view&p_fk_str_yksus_id=50001&p_kava_versioon_id=50405&p_net=internet&p_lang=EN&p_rezhiim=0&p_mode=1&p_from=
[Accessed 31 05 2019].

The NATO Cooperative Cyber Defence Centre of Excellence, 2019. *France Wins Cyber Defence Exercise Locked Shields 2019.* [Online]
Available at: https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/
[Accessed 31 05 2019].

Utbildningsdepartementet, 1992. *Högskolelag (1992:1434).* [Online]
Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/hogskolelag-19921434_sfs-1992-1434

Williams, K. & Kear, K. a. R. J., 2012. *Quality Assessment for E-learning: a Benchmarking Approach (2nd ed.). :.* Heerlen,: European Association of Distance Teaching Universities (EADTU). [available online: http://excellencelabel.eadtu.eu.

Yamin, M. M., Katt, B. & Gkioulos, V., 2019. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security,* Volume 88.

Appendix A. Overview of existing MOOCs and Platforms in Europe

A.1 Existing MOOCs, online courses and programs

In this appendix, we provide a non-exhaustive list of MOOCs, online courses and online programmes offered in Europe. ENISA also provides a database of available cyber security educations and courses in Europe[4], which however is not exhaustive/complete either. Moreover, it only includes so far a short list of online courses but no MOOCs. In the table below, we also list the online courses provided by ENISA's list and complement it with other sources for European online education including MOOCs.

In our table, courses are marked as academic only if they award credit points. Courses that only award certificates are classified as continuous, even if they are given by academic institutions.

Table 3. Selected Traditional MOOCs in Europe

Traditional MOOCs		
Course Title & URL	**Organisation**	**Type**
[A.01] *"An Introduction to Cryptography"* (https://www.futurelearn.com/courses/cryptography)	Coventry University	Continuous
[A.02] *"Area of Security, Freedom and European Justice, between Terrorism and Technological Challenges"* (https://learn.eduopen.org/eduopenv2/course_details.php?courseid=335)	University of Foggia	Continuous
[A.03] *"Arithmetic: On the way for cryptography (Arithmétique : en route pour la cryptographie)"* (https://www.fun-mooc.fr/courses/lille1/54001/Trimestre_1_2015/about)	University of Lille	Continuous
[A.04] *"Authentication & Authorization: OAuth"* (https://eu.udacity.com/course/authentication-authorization-oauth--ud330)	independent teachers	Continuous
[A.05] *"Azure Security and Compliance"* (https://www.edx.org/course/azure-security-and-compliance-3)	Microsoft	Continuous
[A.06] *"Basics of Network Security"* (https://www.futurelearn.com/courses/network-security-basics)	Coventry University	Continuous
[A.07] *"Challenges & issues in cybersecurity"* (https://www.fun-mooc.fr/courses/course-v1:ubs+160001+session01/about)	Universite Bretagne Sud	Continuous
[A.08] *"Code-Based Cryptography"* (https://www.fun-mooc.fr/courses/inria/41006S02/session02/about)	Inria	Continuous
[A.09] *"Cyber Security Base with F-Secure"* (https://cybersecuritybase.mooc.fi/)	University of Helsinki and MOOC.fi in collaboration with	Academic & Continuous

[4] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

	F-Secure Cyber Security Academy	
[A.10] *"Cyber Security Economics"* (https://www.edx.org/course/cyber-security-economics-delftx-secon101x-0)	TU Delft (DelftX)	Continuous
[A.11] *"Cyber Security in the Software Development Life Cycle"* (https://www.futurelearn.com/courses/cyber-security-in-the-software-development-life-cycle)	Coventry University	Continuous
[A.12] *"Cyber Security: Safety at Home, Online, in Life"* (https://www.futurelearn.com/courses/cyber-security)	Newcastle University	Continuous
[A.13] *"Datensicherheit im Netz – Einführung in die Informationssicherheit"* (https://open.hpi.de/courses/informationssicherheit2019)	Universität Potsdam - Hasso Plattner Institut	Continuous
[A.14] *"Digital Security and Human Rights"* (https://www.edx.org/course/online-and-digital-security)	Amnesty International	Continuous
[A.15] *"Ethical Hacking: An Introduction"* (https://www.futurelearn.com/courses/ethical-hacking-an-introduction)	Coventry University	Continuous
[A.16] *"European Area of Freedom, Security and Justice"* (https://www.uninettunouniversity.net/en/mooc-program.aspx?lf=it&courseid=4078&degree=209&planid=252&faculty=0)	Universita Telematica Internazionale UNINETTUNO	Academic
[A.17] *"Firebase in a Weekend: iOS"* (https://eu.udacity.com/course/firebase-in-a-weekend-by-google-ios--ud0351)	Google	Continuous
[A.18] *"Information and Communication Technologies"* (https://www.uninettunouniversity.net/en/mooc-program.aspx?lf=it&courseid=3803&degree=149&planid=255&faculty=7)	Universita Telematica Internazionale UNINETTUNO	Academic
[A.19] *"Information Security: Context and Introduction"* (https://www.coursera.org/learn/information-security-data)	Royal Holloway	Continuous
[A.20] *"Introduction to Cyber Security"* (https://www.futurelearn.com/courses/introduction-to-cyber-security)	The Open University (OU)	Continuous
[A.21] *"Introduction to GDPR: General Data Protection Regulation"* (https://www.futurelearn.com/courses/gdpr)	University College London and PA Consulting	Continuous
[A.22] *"IT and Freedoms on the internet (Informatique et libertés sur internet)"* (https://www.fun-mooc.fr/courses/CNAM/01013/session01/about)	The CNAM (Le CNAM)	Continuous
[A.23] *"IT Fundamentals for Business Professionals: Cybersecurity and social implications"* (https://www.edx.org/course/it-fundamentals-for-business-professionals-social-implications)	Universitat Politècnica de València	Continuous
[A.24] *"Managing Security in Google Cloud Platform"* (https://www.coursera.org/learn/managing-security-in-google-cloud-platform)	Google	Continuous
[A.25] *"Network Security"* (https://eu.udacity.com/course/network-security--ud199)	Georgia Tech	Continuous

[A.26] *"Netzwerksicherheit (#nwsMOOC)"* (https://www.oncampus.de/weiterbildung/moocs/netzwerksicherheit)	Technische Hochschule Lübeck	Academic & Continuous
[A.27] *"Privacy by Design"* (https://www.kau.se/cs/pbd)	Karlstad University	Academic
[A.28] *"Privacy Protection in the digital world (Protection de la vie privée dans le monde numérique)"* (https://www.fun-mooc.fr/courses/course-v1:inria+41015+session03/about)	Inria	Academic
[A.29] *"Protection of Personal data: The new Right (Protection des données personnelles : le nouveau droit)"* (https://www.fun-mooc.fr/courses/course-v1:CNAM+01032+session02/about)	National Conservatory of Arts and Crafts (Conservatoire National des Arts et Metiers)	Continuous
[A.30] *"Public Privacy: Cyber Security and Human Rights (iversity)"* (https://www.mooc-list.com/course/public-privacy-cyber-security-and-human-rights-iversity)	Utrecht University	Continuous
[A.31] *"System Validation"* (https://www.canvas.net/browse/halmstad/courses/system-validation)	Halmstad University	Continuous
[A.32] *"The connected consumer & his / her personal data (Le consommateur connecté & ses données personnelles)"* (https://www.fun-mooc.fr/courses/course-v1:INC+150001+session01/about)	National Institute of Consumption (Institut National De La Consommation)	Continuous
[A.33] *"Web Application Security for Absolute Beginners (no coding!)"* (https://www.udemy.com/web-application-security-for-absolute-beginners-no-coding/)	independent teachers	Continuous
[A.33b] "Introduction to Cybersecurity" (https://www.netacad.com/courses/security/introduction-cybersecurity	Cisco	Continuous

Table 4. Selected Online Courses in Europe

Online Courses		
Course Title & URL	**Organisation**	**Type**
[A.34] *"Cyberhygene online course"* (https://www.ttu.ee/news/news-2/internal-2/ttu-cyberhygene-online-course/)	TTÜ-Tallinn University of Technology	Academic
[A.35] *"Dataskyddsjuridik"* (https://www.du.se/sv/Utbildning/kurser/kurs/?code=GRV22R&applicationcode=V2Z5V)	Högskolan i Dalarna	Academic
[A.36] *"Enterprise Security Architecture"* (https://www.ltu.se/edu/course/A00/A0001E/A0001E-Sakerhetsarkitektur-1.87211?termin=H19)	Luleå Tekniska Universitet	Academic
[A.37] *"Information Security"* (https://www.ltu.se/edu/course/A00/A0004N/A0004N-Informationssakerhet-1.67489?termin=H19)	Luleå Tekniska Universitet	Academic
[A.38] *"Internetsäkerhet"* (https://lnu.se/kurs/internetsakerhet/distans-internationell-deltid-engelska-ht/)	Linné Universitetet	Academic
[A.39] *"Introduktion till datasäkerhet"* (https://www.hkr.se/kurs/DA563A)	Högskolan Kristianstad	Academic
[A.40] *"Introduktion till IT-rätt och datasäkerhet"* (https://www.miun.se/utbildning/kurser/data-och-it/datavetenskap/datavetenskap-gr-a-introduktion-till-it-ratt-och-datasakerhet-75-hp/om-kursen/?term=ht2019-vt2020)	Mittuniversitetet	Academic
[A.41] *"IT-Sicherheit - Konzepte, Standards, Verfahren und Anwendungen"* (https://isdb.fernuni-hagen.de/weiterbildung/index.php/informatik-kurse/it-sicherheit)	FernUniversität Hagen	Continuous
[A.42] *"Online Course in Cybersecurity"* (https://www.diplomacy.edu/courses/cybersecurity)	DiploFoundation	Continuous
[A.43] *"Online Course on Cybersecurity and Blockchain: tackling irrastreability in the network"* (https://www.onlinestudies.com/Online-Course-on-Cybersecurity-and-Blockchain-tackling-irrastreability-in-the-network/Spain/IUIOG-(centro-adscrito-a-la-Universidad-Complutense-de-Madrid)/)	Instituto Universitario de Investigación Ortega y Gasset	Continuous
[A.44] *"Praktisk cybersäkerhet"* (https://www.mdh.se/utbildning/kurser?kod=DVA446&l=sv_SE)	Mälardalens Högskola	Academic
[A.45] *"Säkerhet i datornätverk"* (https://www.mdh.se/utbildning/kurser?kod=DVA240&l=sv_SE)	Mälardalens Högskola	Academic

Table 5. Selected Online Programmes

Online Programs		
Course Title & URL	**Organisation**	**Type**
[A.46] *"Applied IT Security"* (https://www.is-its.org/fernstudiengang-it-sicherheit-master-of-science-in-applied-it-security)	isits – International School of IT Security AG, in cooperation with Ruhr -University Bochum	Academic (Master) & Continuous (Certificate)
[A.47] *"Bachelor i cyber security"* (https://www.noroff.no/studier/hoyskole/cyber-security)	Noroff School of technology and digital media	Academic (Bachelor)
[A.48] *"Bachelor i digital etterforskning (digital forensics)"* https://www.noroff.no/studier/hoyskole/digital-etterforskning	Noroff School of technology and digital media	Academic (Bachelor)
[A.49] *"Forensic Computing and Cybercrime Investigation (FCCI)"*	University College Dublin	Academic
[A.50] *"Informationssäkerhet"* (https://www.ltu.se/edu/program/FMISA/FMISA-Informationssakerhet-master-1.76734?termin=H19)	Luleå Tekniska Universitet	Academic (Master)
[A.51] *"Integritet, informationssäkerhet och cybersäkerhet"* (http://www.his.se/integritet-informationssakerhet-och-cybersakerhet-masterprogram/)	Högskolan i Skövde	Academic (Master)
[A.52] *"Law of the Digital Society"* (https://www.uninettunouniversity.net/en/giurisprudenza-indirizzo-diritto-della-societa-digitale.aspx?faculty=1&degree=240&idindirizzo=56&mode=cs)	Universita Telematica Internazionale UNINETTUNO	Academic (Master)
[A.53] *"Masters in Cybersecurity"* (https://www.onlinestudies.com/Masters-In-Cybersecurity-(online)/Spain/IMF/)	IMF Business School, Deloitte and the University Camilo Jose Cela	Academic (Master)
[A.54] *"MSc Cybersecurity"* (http://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity/)	University of Central Lancashire, Cyprus	Academic (Master)
[A.55] *"MSc Cybersecurity"* (http://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity/)	University of Central Lancashire, Cyprus	Academic (Master)

Table 6. EIT Digital Cyber Security Courses

EIT Digital		
Course Title & URL	**Organisation**	**Type**
[A.56] *"Development of Secure Embedded Systems Specialization"* (https://www.coursera.org/specializations/embedded-systems-security)	EIT Digital	Academic (Master)
[A.57] *"Bachelor i cyber security"* (https://www.coursera.org/specializations/value-creation-innovation)	EIT Digital	Academic (Master)

A.2 Selected MOOC platforms offering courses in cyber security.

The most commonly used platforms for Cyber Security MOOCs are the following:

- Coursera (www.coursera.org)
- EdX (www.edx.org)
- FutureLearn (www.futurelearn.com)
- Udacity (www.udacity.com)
- Udemy (www.udemy.com/)
- Canvas (www.canvas.net)
- Cisco Networking Academy (www.netacad.com/courses/security)

In addition to these platforms, academic Cyber Security courses are also offered at University-owned platforms, such as mooc.fi or www.oncampus.de.

There are also other country- or language-specific platforms that are offering a few cyber security courses in languages other than English. Examples are Iversity (www.iversity.org/)) operated by Springer offering courses in German including one course on the GDPR. Another example is MiriadaX (miriadax.net, used by Spanish and South America universities), where course are mainly offered in Spanish with two courses related to security/cyber security.

Appendix B: Examples of structures for selected courses

B.1 Examples for Academic Courses

Detailed example of course [A.9].

This is an illustrative example of a course provided by a Higher Education Institution and a company on an online platform.

Qualification of proposing institutions. The course is provided by a reputed Higher Education Institution (University of Helsinki) and a company (F-Secure Cyber Security Academy) on an online platform (MOOC.fi). The institution has a partnership with the platform.

Qualifications of target students/admission criteria. The course describes that there are no formal prerequisites for registering, however, a basic understanding of coding, networks, and cyber security are needed to follow some of the course material. Some programming background and ICT experience is required as well.

Qualification of teachers. The names of the teachers are not provided, neither is provided any specification on the qualification of the teachers.

Examination, Credits and/or Course certificates. The grading is pass or fail. Readings, essays, quizzes, and puzzles are used in different modules. Some modules include projects and programming assignments for students to work on. There is also a capture-the-flag competition at the end of the course. The Open University of University of Helsinki provides a total of 10 ECTS credits for the course. An online certificate is issued as well.

Course evaluation, Course accreditation by institution, students, government. Course reviews are not publicly available.

Course content, learning objectives, and professional expectation. The course series consists of multiple smaller courses, each with a specific theme. Themes include a brief introduction to cyber security, operational security, web software development, types of vulnerabilities typical of web software, discovery and mitigation of such vulnerabilities, and advanced topics such as secure software architectures and cryptography. There will be several case studies as well as projects for participants. At the end of the course series, a friendly capture-the-flag competition where participants will try to solve some security puzzles.

Openness (for participation, free and open access to material for students and teachers). The course is open for enrolment and is free. Teaching material is available even before enrolment however in order to answer the quizzes question you need to be enrolled and signed in.

B.2 Examples for Continuous Education Courses

Detailed example of course [A.9].

This is an illustrative example of a course provided by a Higher Education Institution and a company on an online platform.

Qualification of proposing institutions. The course is provided by a reputed Higher Education Institution (University of Helsinki) and a company (F-Secure Cyber Security Academy) on an online platform (MOOC.fi). The institution has a partnership with the platform.

Qualifications of participants and admission criteria. The course describes that there are no formal prerequisites for registering however, a basic understanding of coding, networks, and cyber security are needed to follow some of the course material. Some programming background and ICT experience is required as well.

Qualification of instructors. The names of the instructors are not provided, neither is provided any specification on the qualification of the teachers.

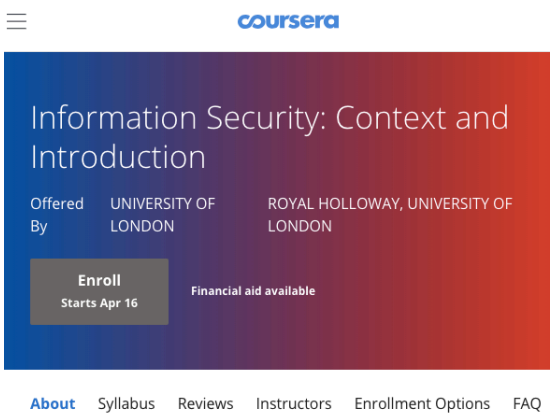
Examination, Credits and/or Course certificates. The grading is pass or fail. Readings, essays, quizzes, and puzzles are used in different modules. Some modules include projects and programming assignments for students to work on. There is also a capture-the-flag competition at the end of the course. The Open University of University of Helsinki provides a total of 10 ECTS credits for the course. An online certificate is issued as well.

Course evaluation. Course reviews is not publicly available.

Course content, learning objectives, and professional expectation. The course series consists of multiple smaller courses, each with a specific theme. Themes include a brief introduction to cyber security, operational security, web software development, types of vulnerabilities typical of web software, discovery and mitigation of such vulnerabilities, and advanced topics such as secure software architectures and cryptography. There will be several case studies as well as projects for participants. At the end of the course series, a friendly capture-the-flag competition where participants will try to solve some security puzzles.

Openness. The course is open for enrolment and is free. Teaching material is available even before enrolment however in order to answer the quizzes question you need to be enrolled and signed in.

Detailed example of course [A.19].



This is an illustrative example of a course provided by a Higher Education Institution on an online platform.

Qualification of proposing institutions. The course is provided by a reputed Higher Education Institution (Royal Holloway) on an online platform (Coursera). The institution has a partnership with the platform.

Qualifications of target students/admission criteria. The course is described as being of "intermediate level". No further qualification/admission criteria are explicitly specified.

Qualification of teachers. The teachers are two university professors and a university lecturer. They all hold a PhD and are experts in the field of knowledge of the course.

Examination, Credits and/or Course certificates. A certificate can be issued if purchased (49 USD). It includes graded assignments. No ECTS credits are provided.

Course evaluation, Course accreditation by institution, students, government. The course description has 497 ratings and 130 reviews. Only the average rating is public (4.6/5.0).

Course content, learning objectives, and professional expectation. The course description includes an overview of the course and a detailed syllabus where, for each lecture, topics and materials (videos, reading quizzes) are listed. A list of high-level acquired skills is included (cyber security, cryptography, information security, security management) together with an extended explanation in the overview.

Openness (for participation, free and open access to material for students and teachers). The course is open for enrolment in two options: free and with certificate (49 USD). Teaching material is only available upon enrolment (even without certificate). Financial aid is available.

Detailed example of course [A.24].

This is an illustrative example of a course provided by a company on an online platform.

Qualification of proposing institutions. The course is provided by a reputed company (Google Cloud) on an online platform (Coursera). The company has a partnership with the platform.

Qualifications of target students/admission criteria. The course is described as being of "beginner level". No further qualification/admission criteria are explicitly specified in a dedicated part of the description, but the overview provides a very detailed list of prior knowledge to get the most out of the course. The course is part of a specialization (on Google Cloud Platform) but can be taken independently.

Qualification of teachers. The names of the teachers are not provided. The teachers are said to be part of the Google Cloud Training team. The description of the team does not specify qualifications of the members of the team.

Examination, Credits and/or Course certificates. A certificate can be issued if purchased. It includes graded assignments. No ECTS credits are provided.

Course evaluation, Course accreditation by institution, students, government. The course description has 96 ratings and 14 reviews. Only the average rating is public (4.7/5.0).

Course content, learning objectives, and professional expectation. The course description includes an overview of the course and a detailed syllabus where, for each lecture, topics and materials (videos, reading quizzes) are listed. A list of high-level acquired skills is included (cyber security, cryptography, information security, security management).

Openness (for participation, free and open access to material for students and teachers). The course is open for enrolment with 7-day trial fee. After that access to the course costs 39 USD per month. Teaching material is only available upon enrolment. Financial aid is available.

Detailed example of course [A.33b].

This is another illustrative example of a course provided by a company on an online platform.

Qualification of proposing institutions. The course is provided by a reputed company (CISCO) on their own online platform (Cisco Network Academy).

Qualifications of target students/admission criteria. The course is described as being of "beginning level and having "No prerequisites required". No further qualification/admission criteria are explicitly. The course is part of a "cybersecurity courses" and can be taken as a standalone course.

Qualification of teachers. No details about the teachers are provided. The course can also be taken without instructors ("self-paced").

Examination, Credits and/or Course certificates. A certificate of completion can be obtained. No ECTS credits are provided.

Course evaluation, Course accreditation by institution, students, government. No information is provided about course evaluation.

Course content, learning objectives, and professional expectation. The course description includes a very brief list of 4 skills that students will learn. There is description of course content and professional expectations.

Openness (for participation, free and open access to material for students and teachers). The course is free without instructor support. Teaching material is only available upon enrolment.

Appendix C: Evaluation and Lifecycle of Criteria

Table 7. Evaluation and Lifecycle of Criteria

QC	Evaluation criterion	Lifecycle
QC 1	Official legal document or Peer reviewed (meta/expert knowledge based)	Analysis (Planning)
QCA 1	Official legal document	Analysis (Planning)
QCA 2	Internal policy document	Implementation, Evaluation
QCA 3	Internal policy document	Implementation
QCC 1	Objective finding - measurable by third party	Analysis (Planning)
QCC 2	Peer reviewed (meta/expert knowledge based) Objective finding - measurable by third party Official legal document Internal policy document	Analysis (Planning)
QCR 1	Peer reviewed (meta/expert knowledge based)	Analysis (Planning)
QCR 2	Peer reviewed (meta/expert knowledge based)	Analysis (Planning)
QC 2	Objective finding - measurable by third party (for academic courses) or Peer reviewed	Design
QC 3	Objective finding - measurable by third party	Implementation
QC 4	Objective finding - measurable by third party	Implementation, Realization
QCA 4	Official legal document Internal policy document	Realization
QCC 3	Peer reviewed (meta/expert knowledge based)	Realization
QCR 3	Peer reviewed (meta/expert knowledge based)	Realization
QC 5	Official legal document (academic degree) or otherwise Peer reviewed (meta/expert knowledge based)	Implementation
QC 6	Official legal document Peer reviewed (meta/expert knowledge based)	Implementation
QCA 5	Official legal document	Realization
QCC 4	Peer reviewed (meta/expert knowledge based)	Implementation
QCR 4	Peer reviewed (meta/expert knowledge based)	Implementation
QC 8	Peer reviewed (meta/expert knowledge based)	Implementation Realization
QC 9	Peer reviewed (meta/expert knowledge based)	Design, Evaluation during Realization
QC 10	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Realization
QC 11	Objective finding - measurable by third party	Implementation
QCA 6	Internal policy document	Design Realization
QCA 7	Official legal document	Implementation
QCA 8	Objective finding - measurable by third party	Implementation
QCA 9	Objective finding - measurable by third party	Realization
QCA 10	Objective finding - measurable by third party	Realization
QC 12	Peer reviewed (meta/expert knowledge based)	Realization
QC 13	Peer reviewed (meta/expert knowledge based)	Design

QCR 5	Peer reviewed (meta/expert knowledge based)	Implementation
QC 14	Peer reviewed (meta/expert knowledge based)	Evaluation (in different phases), Analysis
QC 15	Objective finding - measurable by third party	Realization Evaluation
QC 16	Objective finding - measurable by third party	Implementation
QC 17	Peer reviewed	Evaluation, Analysis
QC 18	Objective finding - measurable by third party	Evaluation
QC 19	Peer reviewed (meta/expert knowledge based)	Evaluation
QC 20	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Analysis (Planning)
QC 21	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Analysis (Planning)
QCR 6	Peer reviewed (meta/expert knowledge based)	Design
QCR 7	Peer reviewed (meta/expert knowledge based)	Design, Implementation, Realization
QCR 8	Objective finding - measurable by third party	Realization
QC 22	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Design, Implementation, Realization, Evaluation
QC 23	Objective finding - measurable by third party	Implementation
QC 24	Peer reviewed (meta/expert knowledge based)	Design, Realization
QC 25	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Design, Realization
QC 26	Peer reviewed (meta/expert knowledge based)	Design, Realization
QC 27	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Implementation
QC 28	Objective finding - measurable by third party	Implementation Realization
QC 29	Objective finding - measurable by third party	Implementation Realization
QC 30	Objective finding - measurable by third party	Implementation
QC 31	Objective finding - measurable by third party	Implementation
QCC 5	Objective finding - measurable by third party, Peer reviewed (meta/expert knowledge based)	Design
QC 32	Objective finding - measurable by third party	Implementation
QC 33	Objective finding - measurable by third party	Implementation
QC 34	Objective finding - measurable by third party	Implementation
QCR 9	Peer reviewed (meta/expert knowledge based)	Design Implementation Realization
QCR 10	Objective finding - measurable by third party	Design Implementation
QCR 11	Peer reviewed (meta/expert knowledge based)	Realization
QCR 12	Objective finding - measurable by third party	Design
QCR 13	Objective finding - measurable by third party & Peer reviewed (meta/expert knowledge based)	Design Implementation
QCR 14	Peer reviewed (meta/expert knowledge based)	Implementation
QCR 15	Peer reviewed (meta/expert knowledge based)	Implementation Realization

QC 35	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Implementation Realization
QC 36	Objective finding - measurable by third party	Design Implementation
QC 37	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Design Implementation
QC 38	Objective finding - measurable by third party	Design
QC 39	Objective finding - measurable by third party	Design Implementation
QC 40	Peer reviewed (meta/expert knowledge based)	Design Implementation Realization
QC 41	Peer reviewed (meta/expert knowledge based)	Realization
QC 42	Peer reviewed (meta/expert knowledge based)	Realization
QC 43	Objective finding - measurable by third party	Implementation
QC 44	Objective finding - measurable by third party	Implementation Realization
QC 45	Objective finding - measurable by third party	Implementation
QC 46	Objective finding - measurable by third party Official legal document	Implementation
QC 47	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Implementation Realization
QC 48	Objective finding - measurable by third party Peer reviewed (meta/expert knowledge based)	Implementation