Quality Criteria for Cyber Security MOOCs

Simone Fischer-Hübner, Matthias Beckerle, Alberto Lluch Lafuente, Antonio Ruiz Martínez, Karo Saharinen, Antonio Skarmeta, Pierantonia Sterlini

Quality Criteria for Cyber Security MOOCs

Simone Fischer-Hübner[1], Matthias Beckerle[1], Alberto Lluch Lafuente[2], Antonio Ruiz Martínez[3], Karo Saharinen[4], Antonio Skarmeta[3], and Pierantonia Sterlini[5]

[1] Karlstad University
[2] Technical University of Denmark
[3] University of Murcia
[4] Jyväskylä University of Applied Science
[5] Trento University

Abstract. Cyber security MOOCs (Massive Open Online Courses) can enable lifelong learning and increase the cyber security competence of experts and citizens. This paper contributes with a review of existing cyber security MOOCs and MOOC quality assurance frameworks. It then presents quality criteria, which we elicited for evaluating whether cyber security MOOCs are worthy to be awarded with a quality seal. Finally, an exemplary evaluation of six selected European MOOCs is presented to exercise the quality seal awarding process. Additionally, the evaluation revealed that criteria for assuring privacy, ethics, meeting professional expectations and openness were on average not clearly met.

Keywords: Cyber Security · Security Education · MOOCs · Quality Assurance and Evaluation.

1 Introduction

The CyberSec4Europe project will, as one of the EU H2020 pilot projects for a future European Cyber Security Competence Network, test and demonstrate potential governance structures for such a network of future competence centres. One area, for which the project will define and evaluate governance structures, is the area of quality assurance for cyber security education provided by MOOCs (Massive Open Online Courses), which have emerged over the last years as an alternative to formal education and as an enabler for life-long learning to a broad group of students.Cyber security MOOCs can thus increase the cyber security competence of experts but also a larger group of the population in Europe. For defining a quality assurance process, a list of quality criteria is needed for evaluating MOOCs if they are worthy to be awarded with a quality seal by a European Cyber Security Competence Network. For eliciting such quality criteria, we have first conducted an initial review of existing cyber security MOOC offerings and of existing rules and practices of operating them at EU level for assuring quality. While MOOC quality assurance frameworks were already proposed by different organisations, we have been particularly interested in eliciting

those quality assurance criteria that should be met specifically by cyber security MOOCs, including cyber range MOOCs, in addition to generic MOOC quality assurance criteria. The objectives of this paper is to present and motivate quality criteria for cyber security MOOCs, and to present and discuss the exemplary evaluations of selected cyber security MOOCs according to those criteria and conclusions drawn from it.

The remainder of this paper is structured as follows: Section 2 provides a short review of existing offerings of cyber security MOOCs in Europe and the existing rules and practices of operating them for providing quality, and concludes with requirements for quality criteria and open issues. Section 3 is briefly summarising the related work of existing Quality Assurance frameworks for MOOCs. In Section 4, we are presenting quality criteria for cyber security MOOCs, which are extending the existing MOOC quality criteria and are addressing the identified open issues. These criteria are then used for an exemplary evaluation of selected cyber security MOOCs for testing a process for awarding a quality seal to cyber security MOOCs based on these criteria, as presented in Section 5. Finally, Section 6 is presenting overall conclusions and next steps to be taken.

2 Review to Existing European Cyber Security MOOCs

This section summarises the review of the landscape of European cyber security MOOCs and the rules for operating them that we conducted for CyberSec4Europe. Our survey of the current landscape showed that cyber security specific topic channels or platforms do not exist yet - existent cyber security MOOCs are rather offered on the dominant learning platforms, such as Coursera, EdX, FutureLearn, Udacity, Edemy, or Canvas. Cyber security MOOCs can be grouped into academic level MOOCs, continuous learning MOOCs and MOOCs utilising cyber ranges, or can be combinations of those categories, and will be reviewed in the following sections.

Among the different MOOC offering, the EIT Digital (a division of the EIT, European Institute of Innovation and Technology) stands out with its focus on the area of Innovation and Entrepreneurship (I&E) education in ICT and the implementation of blended I&E courses. We will review them in the Academic level section albeit they may also fit the Continuous Education section.

2.1 Academic Level MOOCs

Academic level courses or programmes are those offered primarily to students enrolled at a University and award credit points or academic degrees to those enrolled students. Online academic courses can be divided into classical MOOCs that are open to all kinds of participants in addition to enrolled students, and other online courses or programmes, which can only be accessed by students that are formally enrolled at the offering academic institution.

While classical MOOCs for cyber security topics are mostly offered by academic institutions, most of them are MOOCs for continuous learning, whereas

classical academic MOOCs are still rare and only a handful of them could be identified via a search on Class Central and via the Web [1].

Academic courses are typically already governed by existing regulations and university's own rules and quality plans for guaranteeing high quality education. For instance, national higher education acts and ordinances usually regulate student admission criteria, qualification requirements for course instructors and for the publication of course evaluations. For issuing ECTS credits, the university must have an accreditation approved by the Education Accreditation Commission (EQAC) and must provide transparency on course workload and learning outcome, as required by the EU Commission.

The EIT Digital approved courses are slightly different than classical academic MOOCs from the perspective of the governance and approval process.[6] The qualification of the proposing institutions is guaranteed by the involvement of the EIT Digital Network of European universities. The approval of the MOOCs follows a submission-based model similar to the traditional calls for research funding, that typically involves a consortium. More specifically, the development of the courses is based on a cross-university collaboration in accordance with the current EIT Digital I&E education guidelines. The partners submit a proposal to the EIT Digital for co-financing the implementation of a specific MOOC and, if approved by the EIT Digital, the MOOC is realised and ported in the learning platform for the actual execution.

2.2 MOOCs as Continuous Education Courses

Continuing education courses are meant to provide all citizens with specialised education through all phases of their lives and are characterised by a huge variety of formats and characteristics. The dominant classes of providers of Cyber Security MOOCs are higher education institutions and private companies, but some are also offered by non-profit organisations or individuals. Most MOOC platforms have headquarters in the US, hence not necessarily adhering to EU regulations such as the EU General Data Protection Regulation 2016/679 (GDPR).

Access to the courses is often unrestricted, but there are cases in which enrolment is limited by several criteria that may include nationality constraints, for example due to sanctions to specific countries, typically dictated by the platform's legal headquarters: the US in most cases. Academic qualifications are rarely a mandatory criteria to access a course. Most courses, indeed, are offered with no specific criteria on the students' qualifications and previous knowledge, although informal recommendations are usually given. Platforms tend to provide information about content, learning objectives, and professional expectations in an informal way. Certificates are sometimes issued automatically upon completion of the course but without a formal verification.

[6] An example of technical specialisation 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`

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, but qualification criteria for those instructors are usually not provided by the platforms.

2.3 MOOCs utilising Cyber Ranges

The definition of a cyber range currently varies greatly between organisations giving cyber security education. The size of the cyber range currently varies from one virtual machine to thousands. Thus declaring a MOOC to a "Cyber Range MOOC" is troublesome and needs clear criteria.

MOOCs in particular have the problem of being tied to the platform providing registration and distribution of material for the MOOC. Larger platforms might not support technical laboratories (other than basic quizzes or multiple-choice answers) leaving out the technical aspect of cyber security. This leaves universities with the problem of hosting the cyber range by themselves. Generating accounts and instructions on how to use the cyber range next to the MOOC platform requires automatisation and integration of the environments. This also provides challenges to the student, with multiple accounts or environments, who thus may require online support, which in turn increases costs and may hinder the scalability of the cyber range course.

These reasons might be the troublesome parts of the cyber range MOOCs, which without answers leaves the industry without competent, technically oriented workforce. For this reason cyber range MOOCs are currently basically non-existent yet, while rather traditional cyber range courses are offered by several European Universities, such as Tallinn University of Technology (in collaboration with NATO), NTNU and JAMK University of Applied Sciences. Apart from that, also the openness (which is one of the inherent MOOC characteristics) of course attendance and of course material is often, due to the security sensitivity of the course content, an issue for courses on cyber ranges, which therefore typically have restrictions in place.

2.4 Conclusions and Gaps

From our review, we want to highlight especially the following conclusions in terms of quality assurance criteria needed for the different types of cyber security MOOCs: In general, criteria for assuring fairness and transparency in regard to course admission, access to course content and evaluations will need attention. This is especially important for cyber security MOOCs teaching sensitive information about hacking and vulnerabilities. So far, cyber range MOOCs are non-existent, but if developed in future, they will require ethical rules on the openness of course content, student admission and course material.

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

issues of compliance with the GDPR (EU General Data Protection Regulation), especially in regard to the transfers of personal data to third countries regulated in Chapter V of the GDPR.

3 MOOC Quality Assurance and Validation Frameworks

In CyberSec4Europe, we are particularly interested in eliciting quality assurance criteria for cyber security MOOCs including future cyber ranges MOOCs. The definition of such criteria is fundamental for course recognition, certification, and accreditation, and for awarding quality seals to MOOCs. As pointed out by Gaebel (2014) [2] for MOOCs making a change in higher education, they have to award credits, and thus quality assurance criteria for credentialisation play an important role too.

The OpenCred report by JRC [3] addressed the recognition practices of open learning achievements by European non-formal open learners. This study identifies elements of MOOC recognition by another Higher Education Institution (HEI) or employer, including the identity verification of learners, suitable supervised assessment, informative credential that acknowledge learning, and the award of credit points.

For the definition of the quality assurance criteria for cyber security MOOCs, we have considered the review of the main existing MOOC quality assurance and validation frameworks: the OpenupEd label [4], the Quality Reference Framework (QRF) for the Quality of Massive Open Online Courses (MOOCs) [5], and the Instructional and Assessment Design Framework (IADF)[7]. Such specific frameworks for MOOCs were developed, since, as indicated by Hood and Littlejohn (2016) [6], the quality measures and indicators used so far for other type of courses are not always suitable for MOOCs, and quality is not objective because it is a purpose-specific measure. These measures could be even dependent on pedagogy [7], which means that they could differ between MOOCs and courses taught in another form.

The OpenupEd Quality Label [4] is a framework designed to improve the quality of OpenupEd's MOOCs. OpenupEd is an alliance of institutional MOOC providers, which is coordinated by the European Association of Distance Teaching Universities (EADTU). Their MOOCs have eight distinctive features: openness to learners, digital openness, learner-centred approach, independent learning, media-supported interaction, recognition options, quality focus, and spectrum of diversity.

The OpenupEd Quality Label has been derived from the E-xcellence label [8], which provides a methodology to assess the quality of e-learning in higher education and it is based on several benchmark statements. These statements are arranged into six dimensions: Strategic Management, Curriculum Design, Course Design, Course Delivery, Staff Support, and Student Support. As e-learning in HEIs is evolving and changing, the E-xcellence label has undergone several updates from the feedback of its reviewers to reflect this evolution. Through a

[7] https://www.eitdigital.eu/eit-digital-academy/

mapping between the benchmarks and the OpenupEd distinctive features, it is possible for a MOOC to provide evidence confirming that it supports OpenupEd features. These evidences can be gathered by different stakeholders such as management, academics, course designers, tutors, and students.

The Quality Reference Framework (QRF) for the Quality of MOOCs [5] is a development of the European Alliance for the Quality of Massive Open Online Courses (MOOCs), called MOOQ. For the definition of this framework, MOOQ has been based on ISO/IEC 40180. The research they have made by means of Global MOOC Quality Surveys, semi-structured interviews, and the feedback from several MOOQ workshops. In the QRF, they have defined three dimensions: Phases, Perspectives, and Roles. The phases, in turn, are divided into processes. Furthermore, for the design and development of MOOCs, the framework provides the QRF Key Quality Criteria and the QRF Quality Checklist. The former are action items for those actions that could be performed in different processes. The latter consists of leading questions for the defined dimensions to remind the key issues to be considered in the MOOC design and development.

The Instructional and Assessment Design Framework (IADF) has been developed by EIT Digital with the other Knowledge and Innovation Communities (KIC) to assess the quality assessment of courses. This framework consists of four components: Instructional Design, Assessment, Functional Requirements, and Learning Analytics. These components have to be considered by teachers for the design of their courses and by evaluators to evaluate the product developed. However, this is an *evaluation framework that is not tailored to security.*

To the best of our knowledge, no cyber security specific quality assurance or validation framework is existing yet.

4 Proposed Quality Criteria for Cyber Security MOOCs

Our quality assurance criteria for Cyber Security MOOCs presented in this section were (1) derived the conclusions from our review of existing European MOOCs in section 2 in terms of gaps to be addressed and are (2) also based on criteria taken from existing quality assurance frameworks that were presented in section 3. Moreover, some of the criteria are (3) based on existing best practices and our experiences, as well as (4) derived from regulations and ethical standards.

Some of the criteria require the involvement of relevant stakeholders for cyber security MOOCs, which may include cyber security experts from industry or government, data protection officers, privacy activists, representatives from (ethical) hacker organisations and/or from national cyber security agencies.

The categories of quality criteria that we present in the following subsections are corresponding to categories used in the other quality assurance frameworks referred to in the previous section. In addition, we added categories for ethical rules, privacy and for cyber range specific quality assurance criteria, which as our review and gap analysis in section 2 showed, need special attention when it comes to cyber security MOOCs. Cyber security-specific criteria including criteria for

future cyber range MOOCs in each category are especially highlighted, except for three categories that have no cyber-security-specific criteria . The detailed list of all criteria for each category and the sources from which they were derived are available in the CyberSec4Europe project deliverable [1].

4.1 Criteria for the Qualification of the Proposer

In order to create and offer a MOOC of high quality, the proposing institution (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.

Cyber Security Specific Criteria: The proposer should especially be recognised by relevant stakeholders in cyber security, either through academic recognition or through their long experiences in the cyber security domain. Proposers of cyber range MOOCs should have expertise in applied technology & private-public partnership. The proposer's cyber range should be technical, work-life oriented which can mimic realistic phenomena (attack campaigns, threat actors, techniques & tools) from the cyber security field.

4.2 Admission Criteria and Qualification of Participants

It is important that participants (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 participants, as 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. Therefore, the acceptance process should be legit and transparent.

Cyber Security Specific Criteria: For cyber range MOOCs, 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.

4.3 Criteria for the Qualification of Instructors

The qualification of the instructors (teachers) is fundamental to ensure a high quality MOOC. Instructors should usually have an academic degree and should have undergone pedagogical training - for academic MOOCs, national higher education acts often require that the academic degree of the examiner should be higher then the degree that is awarded by the course. For continuous learning MOOCS, relevant working life or industrial experiences should be required.

Cyber Security Specific Criteria: Since the cyber range requires technical operation, the instructor of a cyber range MOOC 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).

4.4 Criteria for Examination, Credentialisation and Recognition

For awarding credits or certificates, course examination has to verify that the participant 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. The examination must be fair and the goals must be transparent, so that the participants know what is expected from them in the exam and that the risk of fraud is minimised. For promoting life long learning, course certificates should be issued enabling recognition of the educational achievements in the professional or life-long/blended learning context. For ensuring recognition in the academic context, academic European MOOCs should be recognised as a valid credit-awarding course within the European credit transfer system.

Cyber Security Specific Criteria: The cyber range activities, laboratory work, and assignments that need to be completed for obtaining a course credential should be clearly stated.

4.5 Course Evaluation Criteria

MOOC evaluations allow student to give 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 [5] provides key quality criteria for the evaluation planning, realisation, review and resulting improvements, which we propose as quality criteria together with criteria from rules and established practices from the academic sector.

Cyber Security Specific Criteria: An evaluation review and follow-up process should be in place that should involve relevant stakeholders, such as the MOOC design team, instructors, director of studies, but also relevant cyber security stakeholders, as the ones named above.

4.6 Criteria for Meeting Professional Expectations

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

Cyber Security Specific Criteria: When providing a cyber range course to a company or an organisation, 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. When participants from an organisation attend a course given for that organisation which utilises a cyber range, the participants should, if there is agreement with the instructor, 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.

4.7 Course Structure and Course Content Criteria

Criteria for the course structure guaranteeing the quality of the course content were partly taken from the OpenupEd suggested distinctive features [9], and some others were motivated by the Checklist for MOOC Accreditation in [10]. These criteria are requiring to clearly specify learning outcomes that can be achieved by the course content. We also require that continuous learning MOOCs offered by companies should not with an inappropriate bias promote commercial products or systems of that company, unless the entire focus of the MOOC is on the teaching or training of the usage of these products or systems.

4.8 Course Platform and Channels Criteria

Quality criteria for platforms and channels are derived from legal requirements. In particular, GDPR compliant platforms and channels must be selected. Moreover, the functionality of the platform should comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies for ensuring inclusiveness.

4.9 Openness Criteria

Openness is a key element of a MOOC and important both in terms of the MOOC content and material (by using an open licensing, e.g. CC-BY-SA, allowing to freely reuse, mix and redistribute material), and in terms of being open to the learner's needs, enabling them to study at any time, place and pace of choice.

Cyber Security Specific Criteria: There should be clear, transparent and justifiable policies for defining any restrictions to digital openness (e.g. for the use of malicious or attack code for teaching purposes) and/or openness of course elements (e.g. those that are hacking-related or for other reason security-sensitive) to learners for ethical or security reasons.

4.10 Ethics and Privacy Criteria

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 define, teach and enforce ethical principles for cyber security courses in regard to ethical hacking, handling security-sensitive information and personal data.

Moreover, many teaching platforms today store personal information about the participants for different purposes. In some cases, this information is used to profile participants 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, the information is used for targeted advertisement and in some cases sold 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 disclose more personal data than it 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 (i.e. the data controller) has an appropriate data processor agreement with the sites that distribute the course material stating how personal data may be processed in compliance with Art. 28 GDPR. There must be GDPR compliant privacy policy statement, both from the platform provider and the course owner that process personal data. 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).

Cyber Security Specific Criteria: While ethics and privacy criteria should be enforced for all types of MOOCs, they are especially relevant to Cyber Security MOOCs teaching security and privacy, for demonstrating that privacy and ethics taught in the course are also enforced in practice, i.e. the course should live up to the standards taught.

4.11 Cyber Ranges Criteria

For cyber ranges to be utilised for future cyber range MOOCs certain quality criteria, in particular in regard to the technical and operational capabilities and capacities should be fulfilled. For instance, 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.

5 Exemplary Evaluation of MOOCs

The project partners conducted an exemplary evaluation of selected cyber security MOOCs by applying a subset of the defined quality criteria, with a focus on those criteria that are cyber security specific. Therefore, Table 1 does not include all criteria categories from Section 4. In addition, since no Cyber Range MOOCs were available, those criteria could not be tested.

The objective of the exemplary evaluation was twofold: First, we wanted to test a process for awarding quality seals to cyber security MOOCs based on our quality criteria in order to propose governance rules for awarding MOOC quality seals by a future European Cyber Security Competence Center and to test the applicability of our criteria. Second, we wanted to test how far information for evaluating the quality of exemplary cyber security MOOCs is openly available

online, so that the MOOCs can be easily assessed by interested students and to what extent the criteria are fulfilled.

5.1 Selection of Exemplary MOOCs

For the evaluation exercise, we selected the following six MOOCs from different European countries in the form of academic and/or continuous learning MOOCs offered by academic institutions and/or industry for having a broad range of different types of MOOCs:

- Continuous learning MOOC: "Information Security: Context and Introduction" by Royal Holloway, UK [11]
- Continuous learning MOOC: "Managing Security in Google Cloud Platform" by Google [12]
- Academic MOOC: "Netzwerksicherheit" by Technische Hochschule Lübeck, Germany [13]
- Academic MOOC: "Privacy by Design" by Karlstad University, Sweden [14, 15]
- Academic MOOC: "Development of Secure Embedded Systems Specialization", EIT Digital Cyber Security course [16]
- Academic and continous learning MOOC: "Cyber Security Base with F-Secure, Academic", by the University of Helsinki and F-Secure, Finland [17]

5.2 Evaluation Procedure

Our evaluation procedure had three phases and basically implemented a peer-review process, which was especially needed for evaluating those criteria that were rather subjective and open for interpretations. In the first phase, each MOOC was independently evaluated by five or six project partners. For each quality criterion, each partner decided to which degree the criterion was fulfilled and assessed it as "yes", "partly", or "no". If information was not retrievable from the openly published course information and material, the assessment was marked as "unclear". In addition, the source of information used for the assessment and a short explanation of the decision process were noted. In the second phase, these five to six evaluation lists were collected and combined into a single document. Afterwards, one partner, assigned for taking the lead, consolidated any unanimous ratings into a combined evaluation list. In the third phase, in case of deviating ratings for criteria, a consensus discussion among involved partners took place. Afterwards, the evaluation was finalised and graphical representations were generated.

5.3 Results and Discussion

Ratings and Openness of Information: Our evaluation exercise showed that not all information for evaluating the quality of MOOCs is openly available. This is illustrated in Table 1, which shows the average percentages of unclear ratings due to a lack of available information for different criteria categories.

Information about the proposing institute were rather visibly published. Also, information needed to evaluate the course examination, credentialisation, and recognition criteria as well as the course structure and content criteria were mostly available online. Considering that students that are interested to enrol, need that information to decide if a MOOC is suitable for them, this comes at no surprise. Nevertheless, it is astonishing that for several of these criteria information could not be found on the related websites.

Ethical considerations for teaching cyber security, including ethical rules for students for handling security-sensitive information, were only clearly addressed for a quarter of the analysed courses. One may argue that some of the selected MOOCs are not including ethical hacking exercises, and thus do not require such ethical instructions for students. Nonetheless, ethical standards are in general of relevance for cyber security experts and should thus be preferably addressed by any cyber security MOOC.

On average only a third of the privacy criteria were clearly fulfilled. In particular, most of the evaluated MOOCs did not have clear policy statements specifying how student-performance related data collected by the course platforms are used by the course owners. Hence, those MOOCs provide no good example of how to implement privacy requirements in practice. Finally it is also notable that criteria about meeting professional expectation were on average only clearly fulfilled in less than 15%. In particular, many of the courses missed to involve cyber security stakeholders in the course in the course design, implementation, realisation, and/or periodic review. This is a further shortcoming, as practical working-life cyber security experiences and perspectives may thus not be well reflected.

Table 1. Average distribution of criteria assessment ratings per criteria category for the evaluated MOOCs in percent.

Category of Criteria	yes	partly	no	unclear
Qualification of the proposing institution	80.5	2.4	12.2	4.9
Course structure and content criteria	55.2	12.8	3.2	28.8
Qualification of instructors	52.8	8.3	2.8	36.1
Course examination, credentialisation, and recognition	40.6	4.2	32.3	22.9
Privacy requirements	37.1	8.6	14.3	40.0
Openness	33.3	0.0	0.0	66.7
Ethical considerations for teaching cyber security	25.0	4.2	20.8	50.0
Meeting professional expectation	14.3	0.0	21.4	64.3
Average	45.2	7.0	14.7	33.1

Quality Seal Awarding Process. The three phase evaluation process consisting of independent evaluation by several experts, consolidation, and moderated consensus discussions and decisions, worked very well and is thus recommended as part of a governance structure for awarding the quality seal to MOOCs by a European Cyber Security Competence Network. We recommend to only award

a quality seal for MOOCs that clearly fulfil all quality criteria that are not formulated as optional. For any 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 seal. An evaluation process based on openly published information only, does not seem to work, even though this is not inline 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 seal. Ultimately, active participation in a MOOC might be needed to reliably retrieve all information needed for the evaluation.

6 Conclusions

In this paper, quality criteria for cyber security MOOCs were elicited and tested with an evaluation exercise for selected European cyber security MOOCs. The results provide a basis for defining a quality assurance process for MOOCs to be awarded with a quality seal by a European Cyber Security Competence Network. As a next step, governance models for a quality seal awarding process will be further developed and refined by the CyberSec4Europe project. Our exemplary evaluations revealed issues in regard to the openness of course meta information that restrain evaluators and interested students to assess the quality of MOOCs. Moreover, criteria for assuring privacy, ethical rules for course participants, as well as for ensuring that professional expectations of cyber security stakeholders are met, were to a large extent not fulfilled by the selected MOOCs. We therefore hope that our quality criteria will also enable cyber security MOOC designers, developers, and owners to generate better courses that will fulfil our criteria. Our criteria are especially important for enabling the development of high quality cyber range MOOCs in future, which will be further investigated by CyberSec4Europe.

Acknowledgements

This work was funded by the European Commission's H2020 Programme under the Grant Agreement Number 830929. We thank all contributors to the CyberSec4Europe Deliverable 6.1, especially Hans Hedbom, Fabio Massacci, Yani Päijänen, Petri Muka, Marko Vatanen, Lejla Islami and Mahdi Akil, for their valuable input.

References

[1] Simone Fischer-Hübner et. al. CyberSec4Europe Deliverable 6.1 – Case Pilot for WP2 Governance. `https://cybersec4europe.eu/publications/deliverables/`, 2019.

[2] Michael Gaebel. *MOOCs Massive Open Online Courses.* European University Association, 2014.

[3] Gabi R Witthaus, Andreia Inamorato dos Santos, Mark Childs, Anne-Christin Tannhauser, Grainne Conole, Bernard Nkuyubwatsi, and Yves Punie. Validation of non-formal MOOC-based learning: An analysis of assessment and recognition practices in Europe (OpenCred). *Joint Research Council, European Union*, 2016.

[4] Jon Rosewell and Darco Jansen. The OpenupEd quality label: Benchmarks for MOOCs. *The International Journal for Innovation and Quality in Learning*, 2(3):88–100, 2014.

[5] Christian M. Stracke, Esther Tan, António Texeira, B. Vassiliadis, A. Kameas, C. Sgouropoulou, and G. Vidal. Quality Reference Framework (QRF) for the Quality of MOOCs. `http://www.mooc-quality.eu/QRF`, 2018.

[6] Nina Hood and Allison Littlejohn. MOOC Quality: The need for new measures. *Journal of Learning for Development – JL4D*, 3(3), 2016.

[7] Valeria Aloizou, Sara Lorena Villagrá Sobrino, Alejandra Martínez Monés, Juan Ignacio Asensio Pérez, and Sara García Sastre. Quality Assurance Methods Assessing Instructional Design in MOOCs that implement Active Learning Pedagogies: An evaluative case study. In *Proceedings of Work in Progress Papers of the Research, Experience and Business Tracks at EMOOCs 2019*, pages 14–19. CEUR Workshop Proceedings, 2019.

[8] Keith Williams, Karen Kear, and Jon Rosewell. *Quality Assessment for E-learning: a Benchmarking Approach*. European Association of Distance Teaching Universities (EADTU), 2nd edition, 2012.

[9] Darco Jansen, Jon Rosewell, and Karen Kear. Quality frameworks for MOOCs. In *Open Education: from OERs to MOOCs*, pages 261–281. Springer, 2017.

[10] Commonwealth of Learning. Guidelines for Quality Assurance and Accreditation of MOOCs. *Commonwealth of Learning*, 2016.

[11] Royal Holloway. Information Security: Context and Introduction. `https://www.coursera.org/learn/information-security-data`, accessed 21 Jan 2020, 2020.

[12] Google. Managing security in google cloud platform. `https://www.coursera.org/learn/managing-security-in-google-cloud-platform`, accessed 21 Jan 2020, 2020.

[13] Technische Hochschule Luebeck. Netzwerksicherheit. `https://www.oncampus.de/weiterbildung/moocs/netzwerksicherheit`, accessed 21 Jan 2020, 2020.

[14] Karlstad University. Privacy by Design. `https://www.kau.se/cs/pbd`, accessed 21 Jan 2020, 2020.

[15] Simone Fischer-Hübner, Leonardo A Martucci, Lothar Fritsch, Tobias Pulls, Sebastian Herold, Leonardo H Iwaya, Stefan Alfredsson, and Albin Zuccato. A MOOC on Privacy by Design and the GDPR. In *IFIP World Conference on Information Security Education*, pages 95–107. Springer, 2018.

[16] EIT Digital. Development of Secure Embedded Systems Specialization. `https://www.coursera.org/specializations/embedded-systems-security`, accessed 21 Jan 2020, 2020.

[17] University of Helsinki and F-Secure. Cyber Security Base with F-Secure, Academic. `https://cybersecuritybase.mooc.fi/`, accessed 21 Jan 2020, 2020.