The Curation Mechanism for the Czech National Qualifications Framework in Cybersecurity

František Kasl
frantisek.kasl@muni.cz
CERIT – Faculty of Informatics;
Institute of Law and Technology –
Faculty of Law, Masaryk University
Brno, Czechia

Pavel Loutocký
loutocky@muni.cz
CERIT – Faculty of Informatics;
Institute of Law and Technology –
Faculty of Law, Masaryk University
Brno, Czechia

Jakub Vostoupal
jakub.vostoupal@law.muni.cz
CERIT – Faculty of Informatics;
Institute of Law and Technology –
Faculty of Law, Masaryk University
Brno, Czechia

ABSTRACT

The cybersecurity field is a fast-paced, ever-changing, and complex environment. Society's growing dependency on ICT combined with the rising number and seriousness of cyber threats emphasizes the need for a sufficient number of cybersecurity experts, who are, at the moment, still pretty scarce. Furthermore, the lack of common methodology, understanding of individual cybersecurity work roles, and the disparate perspectives of cybersecurity stakeholders from diverse backgrounds (academia, public entities, private sector) further hinder any long-term solutions. In our previous contributions, we presented the National Qualifications Framework in Cybersecurity, which could provide a solution for a sufficiently up-to-date, broad, and granular taxonomy of skills requirements for existing and future cybersecurity work roles that could mitigate this problem. The Platform, including the curation mechanism, was created for this Framework to be easy to navigate, administer, update and flexible. This enabled further utilization (and possibly even development) of the available inputs and synergies from existing qualification frameworks, such as the NICE Framework and the European Cybersecurity Skills Framework. In this article, we introduce and analyze the curation mechanism and the challenges of navigating cybersecurity qualification frameworks and producing a sufficient UI. Primarily we focus on the specific functions of the curation mechanism, e.g., the feedback collection and Framework updates, which could be adapted even for other framework content or languages and thereby implemented in parallel solutions. Therefore, we present the Platform, including the curation mechanism, as a dynamic common reference tool for cybersecurity workforce requirements.

CCS CONCEPTS

• **General and reference** → **General conference proceedings**; • **Security and privacy** → **Human and societal aspects of security and privacy**; • **Social and professional topics** → **Computing education programs**; *Computing education*; • **Software and its engineering** → **Software creation and management**; • **Information systems** → **Database administration**;

KEYWORDS

Cybersecurity; qualifications framework; platform; UI; curation mechanism; API; web application

ACM Reference Format:
František Kasl, Pavel Loutocký, and Jakub Vostoupal. 2023. The Curation Mechanism for the Czech National Qualifications Framework in Cybersecurity. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3600160.3605001

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605001

1 INTRODUCTION

The need for training and education of cybersecurity professionals is a consistent issue in the continued shift towards the digital economy in the EU. There is a persistent gap in adequately skilled personnel [1] [4] [5]. A number of policy and strategy efforts target this area. The overarching strategies, such as the EU strategy Shaping Europe's digital future [3] as well as the EU Digital Education Action Plan (2021-2027) [2], guide specific initiatives as well as national-level efforts.

As we highlighted in detail in our previous contributions [6] [7] [8] [9] [10], the aim of the project "Národní kvalifikační rámec v kyberbezpečnosti" [National Qualifications Framework in Cybersecurity][1] was to provide a solution for sufficiently current, broad, and granular taxonomy of skills requirements for existing and future cybersecurity work roles.

The resulting taxonomy (Framework) is enshrined in an interactive platform (Platform) that contains a curation mechanism allowing for gathering input from interested parties and systematically updating the taxonomy content.

In our previous contribution [10], we introduced in detail the overview of the Framework and the Platform that allow for dynamic and continuous management and utilization of the National Qualifications Framework in Cybersecurity developed under the project.[2]

Furthermore, as the project achieved its objective by the end of 2022, the resulting Platform with the bilingual (Czech and English) Framework is available at https://platform.cyqual.cz/en.

To complement the presentation of the solution provided under the project, as provided in the aforementioned past contributions, this contribution focuses on describing the chosen mechanism for curating the content through the Platform.

[1] Find more at: https://www.cyqual.cz/?lang=en
[2] The Platform represents the Framework; however, it is much more user-friendly, easy to navigate and through the curation mechanism essentially offers the only flexible way to administer the Framework.

The contribution is structured as follows: Section 2 highlights the need and benefits of the curation mechanism. Section 3 contains a detailed description of the chosen solution developed as part of the Platform. In Section 4, we offer an evaluation of the curation mechanism, future potential utilization of the tool and our experience with the user feedback. Finally, we conclude the contribution in Section 5.

2 NEED FOR CURATION MECHANISM

Recognizing the dynamic nature of the cybersecurity landscape and the diverse perspectives of stakeholders from various backgrounds, including the public sector, private entities and academia, our aim while developing the National Qualifications Framework in Cybersecurity was to embed it with a mechanism that will allow for continuous curation and adaptation of the Framework to remain up-to-date and harmonized. For this purpose, a solution using the Platform was devised.

Creating the initial version of the Framework under the project already required a systematic multi-stage curation of a complex dataset. The basic structure and elements were adopted from the NICE Framework; however, the taxonomy's adaptation, optimization and enlargement meant a major endeavor resulting in a taxonomy describing ninety work roles through links to tens or even hundreds of specific Requirements and Tasks. Therefore, the whole dataset representing the current version of the Framework contains over 30.000 links between elements. Pursuant to our mapping of existing solutions and state-of-the-art tools available, which also included discussions with NIST representatives responsible for maintaining and updating the NICE Framework, we established that no similarly complex cybersecurity skills framework is available. The datasets were static in the frameworks that served as inspiration, such as the NICE Framework, with periodic manual content updates.

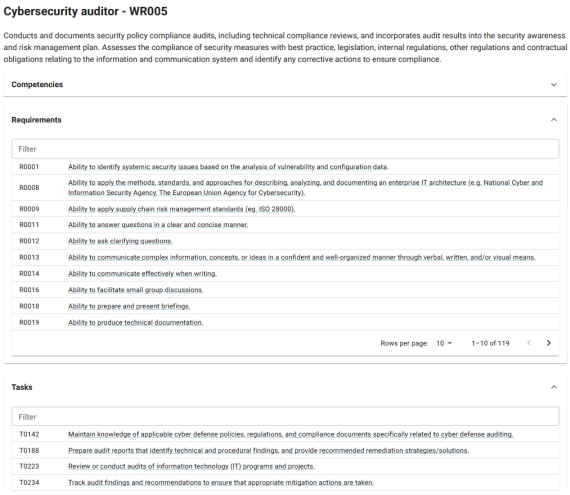

Figure 1: An Example of the Work Role within the Platform

However, our dataset's development and regular updates would be extremely labor-intensive without a suitable curation mechanism that would allow the collection of inputs from multiple stakeholders and user-friendly editing of the dataset. For this reason, the Platform was developed with a content management tool that we describe further in this contribution. This tool allows for regular or irregular rounds of input gathering from interested parties on the obsolete or unsuitable content of the Framework and subsequent update and distribution of up-to-date versions to the public.

The system was tested and employed during the final stage of the project in Q3 and Q4 of 2022, which led to the creation of the currently available version of the Framework on the Platform website.

The presence of a tool for continuous updates as part of the Framework representation in the Platform is a crucial element that we consider a unique contribution to the existing efforts towards developing cybersecurity skills frameworks. Its versatility and flexibility allow for gathering detailed, well-documented and visualized feedback from a broad spectrum of interested parties, ad hoc or continuously. It serves as a crucial enabler for coordinating and unifying varied perspectives on the requirements and definition of work roles that should allow bridging the gap between different perspectives (academic, governmental, sector-specific). Furthermore, combined with the complexity of the taxonomy and the detail presented in the characterizing elements, the taxonomy is a suitable basis for further utilization through analytical tools or other (semi)automated processes.

3 SOLUTION DEVELOPED AS PART OF THE PLATFORM

The curation mechanism was introduced into the Platform through the role of privileged users with a login.

- *Non-logged-in user* uses the Platform to display and access the current version of the Qualifications Framework in a user-friendly way or to download and further utilize the content of the current version in the open data format;
- *Logged-in user* is a role reserved for the representatives of stakeholders, who use the Platform in a similar way to the non-logged-in user, but in addition, use the user-friendly content management tool for providing feedback on the current version of the Framework and suggestions for its modification or addition of further elements;
- *Administrator* is the guarantor of the content of the Framework with access to curation and modifying tool of the content that is made available to all users through the Platform. The recommendations provided by logged-in users are displayed to the administrator comprehensively, providing guidance for modifications of the Framework based on the collected feedback from logged-in users and other channels and inputs.

The registration and activation of the user allowed to log in are fully under the administrator's control. Complete administrator control is chosen due to the purpose for which the registered user function is established on the Platform, i.e., to collect feedback and recommendations for modification of the Framework. The role of the registered user is thus assigned to the representatives of the stakeholders invited by the administrator to collect feedback on the current version of the Framework and suggestions for its completion or modification.

One of the key benefits and added value associated with representing the Framework through the Platform is the possibility to systematically gather feedback from a wide range of stakeholders on the current content of the Framework and thereby achieve and maintain a consistent multi-perspective view on the requirements related to the respective work roles. This then allows for systematic updates of the Framework on a regular basis. The Platform with such a curation mechanism is thus a tool to facilitate the (administrator-coordinated) collection of feedback and steadily develop and adapt the content of the Framework to current needs and uses.

The development of the mechanism was based on the premise that the selection and validation of appropriate stakeholders for feedback is entirely in the administrator's competence, and therefore initiation by the user is not possible through the Platform. It is therefore assumed that the administrator will communicate with stakeholder representatives through other channels regarding account creation and activation.

3.1 Content Management

Creating and activating a new user creates their own editable framework content based on the current version of the Framework for feedback purposes. This can be accessed by logging in. To better navigate through this custom content, the user is automatically redirected to the Content Management sub-page after logging in, through which the logged-in user can access this customizable content. The Content Management sub-page provides an overview structure of the database content and allows direct access to the sub-levels of the corresponding structures.

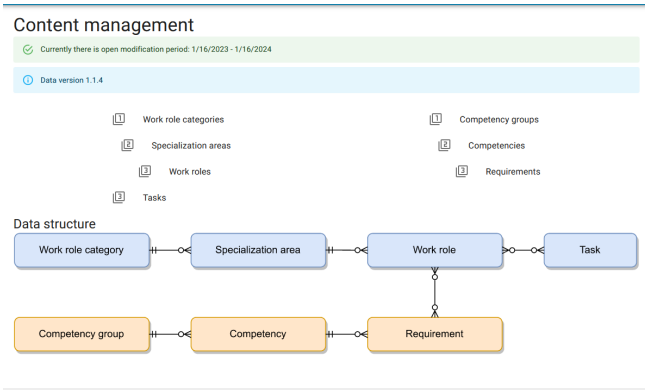

Figure 2: Content Management

Assuming that the administrator sets an editing period and the user logs into his account during this period, he will have permission to suggest content edits via the Content Management sub-page. The current version of the Qualifications Framework, or rather their own copy of the current Qualifications Framework is shown to the logged-in user on this sub-page, which includes suggestions for changes that the logged-in user has already made (e.g. during previous login instances). Changes and additions can be made by this user on all relevant sub-pages under the Content Management tab when browsing the content.

The content under Content Management is structured and navigated in the same way as the current version of the content browsed by a non-logged-in user via the main platform page. The logged-in user thus operates in a very similar environment in Content Management. In addition, by clicking on the name of the Platform in the top left corner of the screen, the user can switch to the platform homepage view and get the same view of the Qualifications Framework that is offered to the non-logged-in user (i.e. view without the logged-in user's own editing suggestions). To suggest the addition of a new element, an icon is available in the top right corner of the content on each overview sub-page. In addition, the added elements are graphically highlighted to the logged-in user with a green background.

Furthermore, the user has the possibility to edit existing elements and their links based on the current version of the Framework. Examples include adding or removing requirements or changing the description of the work role characteristics. These modifications will not only be displayed graphically on the link of the element, but the element will also be highlighted in yellow within the relevant overview.

The logged-in user can also suggest the complete removal of an element from the current version of the Framework via the relevant icon on the element sub-page in the top right corner of the view. An element proposed for removal in this way will be highlighted in red and crossed out in the corresponding overview.

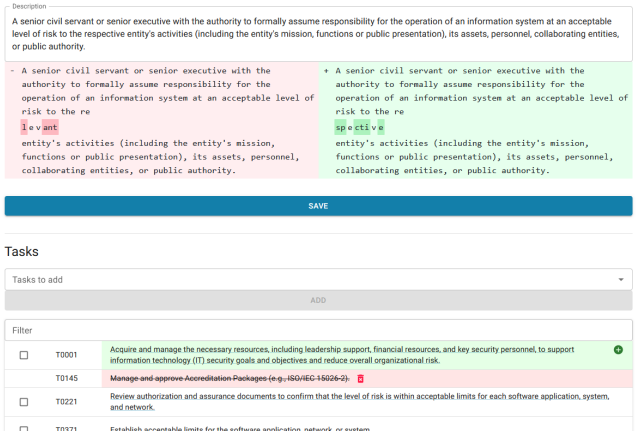

Figure 3: Proposing Changes within the Platform

Given the complexity of the Framework and the number of elements involved in the specification of a particular work role, it is crucial to provide the logged-in user with user-friendly visualization of the previously made changes. The mechanism is intended for periodic as well as irregular updates of the Framework; therefore, the time period for stakeholders to input changes on the current version can be quite extensive. Additionally, a single login can be used by several representatives of the given stakeholder in order to provide more complex insight into the content; therefore, visibility of previous recommendations and modifications is of high relevance. However, it is important to re-emphasize here that the changes visible to the logged-in user regard only their copy of the current version of the Framework. The aggregate view containing

recommendations from all login users is visible only to the administrator. This is the basis of the curation mechanism, whereby the administrator can effectively assess the multitude of suggestions and changes recommended by the stakeholders and transpose them into the new version of the Framework that will then be published and available to all users of the Platform.

3.2 Curation Mechanism

The role of the administrator is central, and we expect that only authorized representatives of the Framework guarantor have access to the administrator account. This role is used to manage the Platform and the content of the current publicly available version of the Framework.

The User Changes sub-page is the central sub-page for collecting feedback from stakeholders (logged-in users). Here, the administrator is continuously provided with all suggestions for changes and additions logged-in users provide through editing their own copies of the current version of the Framework during the editing period. Furthermore, the recommendations are color-coded in the same way as for the logged-in user in their Content Management; thereby, the administrator gets a clear baseline of information when glancing at the User Changes sub-page.

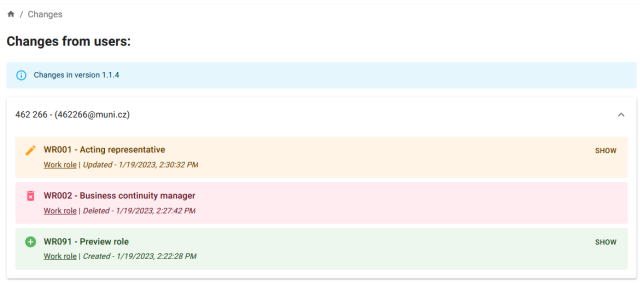

Figure 4: Administrator's View of the Proposed Changes from Users

Since the administrator can work with a large number of versions of the Framework, but logged-in users have their content bound only to the current, i.e., the published version, on the top of the page is highlighted to the administrator, to which version do the users' modifications relate. The changes of each logged-in user are shown together since changes to elements across users may be incompatible with each other, especially with respect to newly proposed elements to add. They are listed with the details of the user who authored the changes and presented in a summary menu that allows for clear browsing of the data when there are a large number of edits from multiple logged-in users.

In case the logged-in user has proposed a change to a specific existing element (e.g. work role), this change is marked with the appropriate icon in the left part and highlighted in yellow, the element to which the change is related is clearly identified in the left part (as seen at Figure no. 4 through its ID within the database = WR001, text designation = Responsible representative and categorization = Work role) and there is a possibility to view the specific modifications that the user proposes to the element in the right part of the corresponding row. It also specifies when the change was made to the logged-in user's copy.

If the user proposes to remove the element entirely from the current version of the Framework, the information is again communicated clearly via the icon on the left of the row and the red-colored background. Although, as this is a removal of an entire element, there is no option to show details in the right-hand section, all details are already provided within the row (as seen in Figure no. 4 for ID within the database = WR002, text designation = Business continuity manager and categorization = Work role). Also, this change is embedded with a time stamp.

If the logged-in user has suggested adding an entirely new element to the database, this suggestion is marked with the appropriate icon on the left-hand side and a green underline. In the right part, there is a View link with the proposal's details. Within the row, there is again the basic information (as seen in Figure no. 4 for ID within the database = WR091; for proposals, an additional ID is always generated after the last element in the current version from which the logged-in user starts, text designation = Preview role and categorization = Work role). A timestamp is also added.

Change suggestions from users are taken as a basis for decision-making by the Framework content guarantor (administrator) when editing or updating the database content, so they are separated from the administrator's Content Management and provided as a summary of possible edits that the administrator can, at their discretion (or based on the frequency of occurrence across logged-in user suggestions), carry forward into the editing of the current version via the Content Management sub-page.

The Platform allows the administrator to work dynamically with the content of the Framework and to offer the current version as a basis for stakeholder feedback via the feedback-gathering function from logged-in users. To better manage the content of the database, the administrator has the Data Version Management sub-page, through which he can determine which version of the database is displayed to users.

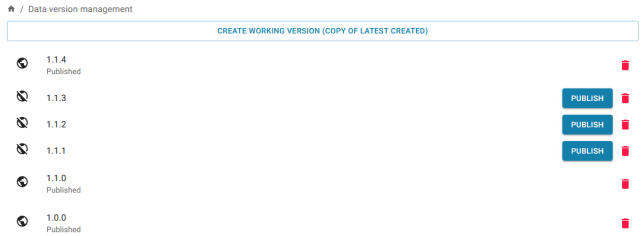

Figure 5: Data Version Management

The current version, which is displayed to all users via the Platform's homepage and on which (assuming an active editing period) logged-in users can make editing suggestions in their copies, is considered the latest version published. On the homepage, the version displayed to non-logged-in users is easily distinguishable by the version label of the open data.

For both the logged-in user and the administrator, the version they are working with within Content Management is also clearly communicated at the top of the relevant sub-page. However, this is always the current version for the logged-in user, i.e., the same version visible to non-logged-in users. On the other hand, the administrator works with the most up-to-date version of the data on the Content Management sub-page, i.e., usually the version that has not yet been published. Therefore, the expected procedure for updating the content is (i) creating a new version of the data, (ii) making administrative modifications according to feedback from logged-in users to update the content version, and (iii) publishing this modified version, which thus becomes the new up-to-date version displayed to all users.

The creation of a new version of the data (which will become a copy of the last version that the administrator had in Content Management, so it can be based on the currently published version, as well as an interim working version that has not been published) is done by the administrator via the appropriate Create Working Version option at the top of the sub-page.

Once a new version of the data has been generated, the administrator will be able to access the new version via Content Management. Although creating a new version does not change anything for users, the content displayed to them or the copies for editing by the logged-in users accessible via Content Management will still be based on the last published version. To make the change visible to users, the administrator must publish the modified version of their choice using the Publish icon on the right side of the corresponding row. This allows for flexibility in the curation process and safeguards from sudden changes to the published content through erroneous content creation steps by the administrator.

Only once the publicly available data has been updated will the version be marked as published and replace the current version and the corresponding .json file of the open data.

In addition, the administrator can also remove versions of the data, both unpublished (e.g., if it was only test or otherwise work-in-progress data) and published (e.g., if a significant deficiency has been identified that cannot be resolved by creating a copy and editing, but a reversion to a previously published version is preferable). If the current version of the data displayed to users is removed, it will be replaced by the previously published version.

4 EVALUATION AND USER FEEDBACK

The inclusion of the curation mechanism into the Platform allowed for the utilization of the available inputs and synergies from existing qualification frameworks, such as the NICE Framework and the European Cybersecurity Skills Framework, and produced a tool that is not only complementary, but shows a way towards further and more dynamic utilization of these frameworks. The curation mechanism can be adapted for other framework content or language and thereby merged or implemented into the parallel solutions. The Platform and Framework represent a tool that retains high complexity and information value typical for NICE Framework, with an EU-centered focus compatible with the ENISA initiative. Combined with the curation mechanism that allows for systematic updates and adaptation of the content, the result is a dynamic common reference tool for cybersecurity workforce requirements with sufficient granularity and availability to be used as a basis for policy approaches as well as extension instruments utilizing the reference database for analytical or guidance purposes.

The curation mechanism is a crucial element that allows for retaining the validity of the content and avoids obsolescence of the tool past project completion. A systematic survey of user feedback has, as of now, not been conducted. Still, the feedback we received during the testing and early deployment phase was positive. The complexity of the orientation in the platform content and editing remains a challenge for some users, which is also given by the sheer volume of the content. However, the tool is not intended to be used by the broad public but only by representatives of selected stakeholders, who were properly instructed beforehand and have a user guide and other materials to the platform at their disposal.

The primary benefit is the significant labor-intensity reduction of maintaining and updating the Framework. This, in effect, makes the updates feasible with annual periodicity or even shorter. The secondary benefit is a user-friendly interface for stakeholder feedback, which increases the volume and detail of this feedback. The stakeholders are also more willing to provide feedback, and their feedback is logged in a form that is specific (not as general comments or vague suggestions) and can be easily incorporated into the update of the Framework.

5 CONCLUSION

In this contribution, we introduced and described the content management tool developed as part of the Platform solution for representing and maintaining the Framework. The Platform is online and freely accessible under the link https://platform.cyqual.cz/en. The current version of the Framework is available for download on the Platform's main page in .json format. The described curation mechanism is visible only to logged-in users for the reasons presented above.

We aim to follow the results of this research with further research aimed at maximal utilization of the Platform, namely potential integration with other frameworks as well as the development of extensions and add-on tools based on the Framework as a reference database, e.g., for cybersecurity curriculum optimization or training and education capacities analysis.

ACKNOWLEDGMENTS

This paper was created on the basis of the project support of the Ministry of the Interior, Czech Republic, within the project "Národní kvalifikační rámec v kyberbezpečnosti" [National Qualifications Framework in Cybersecurity] with the identification code VI20192022161, which was concluded on 31.12.2022.

REFERENCES

[1] 2020. Commission presents European Skills Agenda for sustainable competitiveness, social fairness and resilience. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

[2] 2020. Digital Education Action Plan (2021-2027). https://education.ec.europa.eu/node/1518
[3] 2020. Shaping Europe's digital future. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en
[4] 2021. Digital Economy and Society Index 2021: Overall progress in digital transition but need for new EU-wide efforts. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5481
[5] 2022. The urgency of tackling Europe's cybersecurity skills shortage. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/
[6] Anna Blechová, Jakub Drmola, Jan Hajný, František Kasl, Pavel Loutocký, Miroslav Mareš, Tomáš Pitner, and Jakub Vostoupal. 2022. Mapping Competencies to Cybersecurity Work Roles. *Jusletter-IT* 30-Juni-2022 (2022). https://doi.org/10.38023/2e2f01cf-ae2c-4536-90ad-460613905754
[7] Jakub Drmola, František Kasl, Pavel Loutocký, Miroslav Mareš, Tomáš Pitner, and Jakub Vostoupal. 2021. The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 21)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3465481.3469186
[8] Jan Hajný, František Kasl, Pavel Loutocký, Miroslav Mareš, and Tomáš Pitner. 2021. Progress towards Czech National Cybersecurity Qualifications Framework. *Jusletter-IT* 27-Mai-2021 (2021). https://doi.org/10.38023/f79f430a-ca8b-409f-9a1f-66135b8ff2d8
[9] Jakub Vostoupal. 2021. The Cybersecurity Qualifications as the Prerequisite for the Cybersecurity Certification of Entities. *Jusletter-IT* 27-Mai-2021 (2021). https://doi.org/10.38023/2029e2f5-bd30-4757-aef5-01b27ae61962
[10] Jakub Vostoupal, František Kasl, Pavel Loutocký, Tomáš Pitner, Patrik Valo, Adam Valalský, and Damián Paranič. 2022. The Platform for Czech National Qualifications Framework in Cybersecurity. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3538969.3543800