



**UNIDROIT Foundation**  
**BPER 8<sup>th</sup> Workshop**  
**Project Group Meeting**  
**16 September 2024**

Foundation 2024  
BPER Report  
October 2024

## **Summary Report for the Eighth Meeting of the Best Practices in the Field of Electronic Registry Design and Operation Project**

1. The eighth meeting of the Project on Best Practices in the Field of Electronic Registry Design and Operation (BPER) was held on 16 September 2024 at UNIDROIT and via Zoom. The BPER Project is run under the auspices of the Cape Town Convention Academic Project (CTCAP), a partnership between UNIDROIT and the University of Cambridge, with the Aviation Working Group as its founding sponsor. The BPER Project is supported by the UNIDROIT Foundation and Aviareto.

2. The meeting was chaired by the Directors of the CTCAP, *Mr Ignacio Tirado* (UNIDROIT Secretary-General), *Ms Louise Gullifer* (University of Cambridge) and *Mr Jeffrey Wool* (President of the UNIDROIT Foundation and Secretary-General of the Aviation Working Group). The meeting was opened with a welcome address by *Ms Gullifer*. The agenda for the meeting is provided under [Annexe 1](#) of this Report.

3. As was suggested after the seventh workshop, the eighth meeting sought to further refine the definitions for some Critical Performance Factors (CPFs) for the future Guide on Best Practices for Electronic Business Registries. To streamline the discussion, a detailed working paper was prepared by *Ms Benedetta Mauro* (UNIDROIT Secretariat) and *Ms Ieva Tarailiene*, the external consultant engaged for the project, and circulated to all registered participants before the meeting. 29 participants attended the workshop, including registry experts, academics, and lawyers, from government agencies, leading international organisations, universities, and practitioners involved with electronic companies. A full list of participants is available under [Annexe 2](#) of this Report.

### *Purpose of the workshop, scope, and background of the Project*

4. Following the welcome address, *Mr Wool* highlighted that the Guide should consider matters of policy with a large technical component, but the focus should be on the best practices identified in the broader context of corresponding policies. Once the definitions and other outstanding points were clarified in this workshop, the aim would be to produce a final version of the Draft Guide for the next meeting.

5. *Ms Mauro* thanked the Directors and presented the background of the BPER Project. She elaborated that the project had initially focused on electronic collateral registries (ECRs). The Cape Town Convention referred to the need to follow 'best practices' in registry design and operation. Through an interdisciplinary approach, the BPER Project purported to develop such best practices. In 2021, the Guide on Best Practices for Electronic Collateral Registries was published, which identified 17 CPFs against which properties and processes of ECRs could be assessed.

6. Subsequently, the focus of the BPER Project had switched to developing best practices for electronic business registries (EBRs). To this end, three workshops had previously been held. In 2021, during the fifth BPER workshop, the project group discussed the evolving role of business registries and the scope of a best practices guide. It also identified relevant existing international instruments, focusing on the UNCITRAL Legislative Guide on Key Principles of a Business Registry (UNCITRAL Legislative Guide) and the Financial Action Task Force (FATF) standards. In 2022, the sixth workshop included a presentation on business registry issues and challenges, which highlighted the main differences between business registries and collateral registries and stirred a discussion on the CPFs applicable to business registries specifically.

7. During the seventh workshop, held on 13-14 February 2024 in Rome, the project group discussed a detailed outline for the future Guide on Best Practices for Electronic Business Registries prepared by Ms Tarailiene. It reviewed the existing and proposed additional CPFs and identified further adaptations needed in the context of EBRs. The workshop also included a presentation by the World Bank on data-driven business registries.

8. Following the seventh meeting, in June 2024, a complete draft of the Guide had been circulated to the experts, accompanied by a questionnaire. The feedback received from experts had shaped the discussion points in the working paper for the eighth workshop.

#### Presentation of the working paper

9. Ms Tarailiene introduced the working paper that had been prepared to guide the discussion on several CPFs: Access Control, Accuracy, Correctability, Records Management (which would replace the former CPFs Disposition, Integrity, and Retention), Evidentiary Value, Standardisation/Interoperability, Timeliness, Data Validation and Software Testing (which would replace the former Validation and Verification CPFs), Risk Management, Accessibility, and Continuous Improvement. She explained that, for some CPFs, it was proposed to only reconsider the definition, while for others there was a need to refine the content as well.

10. Ms Gullifer thanked Ms Tarailiene for her introduction. She underlined the need to discuss with experts whether the Guide on Best Practices for Electronic Collateral Registries should be revised if changes related to previously adopted CPFs.

#### Discussion on the Access Control CPF and the proposal to remove the new CPF on Authorisation

11. Ms Tarailiene proposed a new definition for Access Control: '*The process of ensuring that access to the registry is authorised and restricted.*' This CPF would encompass the three access control functions: (i) access request, (ii) access authorisation, and (iii) access administration. It would also emphasise Role-Based Access Control (RBAC), where access was granted based on predefined roles within an organisation. Since the proposed definition would already cover identity and permission verification, Ms Tarailiene recommended integrating the Authorisation CPF into Access Control.

12. Mr Denis Finnegan supported merging the Authorisation CPF into Access Control. He noted that there was no generally accepted international definition of access control. In a widely agreed understanding, it meant regulating access to resources to ensure that only authenticated and authorised users or systems can interact with such resources. Access control includes authorisation also under SOC 2, a North American cybersecurity framework, and Cloud Controls Matrix, a cybersecurity control framework for cloud computing. He noted that, essentially, five key pillars and corresponding principles could be distinguished (Table 1).

<b>Pillars</b>	<b>Principles</b>
Identity management or identity proofing (verifying the legitimacy of an entity)	Need-to-Know
Authentication (confirming identity via credentials)	Defence in Depth
Authorisation (determining what actions can be taken against a resource)	Least Privilege, Segregation of Duties
Access enforcement (applying policies and permissions to identities and resources)	Zero-trust, RBAC
Monitoring and auditing (tracking access to ensure security for accountability and auditability purposes).	Accountability, Auditability

*Table 1. Access Control Pillars and Principles according to Aviareto*

13. Thus, Access Control should be treated as a scale with a broader interpretation that included authentication. Aviareto, therefore, suggested the following definition: *'the process of ensuring that access to the registry is controlled and granted to only validated, authenticated, and authorised identities.'*

14. *Mr Wool* suggested developing a glossary with frequently used terms in the Guide. *All participants* supported this idea. For Access Control, the glossary should explain the meaning of the terms 'validated', 'authenticated', and 'authorised'.

15. *Mr Wool* also pointed out that transparency was a precondition for these processes and should be a foundational CPF for all the other factors.

16. *Ms Kathy Hillman-Weir* noted that the fundamental purpose of most registries was protecting and serving publicly accessible information. One of the biggest challenges public registries encountered was inappropriate access or too much information that was made publicly available. She suggested incorporating RBAC in the revised definition while ensuring that certain information remained publicly accessible.

17. *Ms Teresa Rodríguez de Las Heras Ballell* agreed with Aviareto that there were several stages related to access control. She queried whether the Guide should cover the stage of user identification, validation, and authorisation, or also the stage of verifying whether, according to all the previous stages, a user was entitled to perform a particular action.

18. *Some experts* expressed concern about the word 'restricted' in the proposed new definition as most registries considered that users should be able to access certain information without authorisation. It was suggested to rephrase the last part of the definition as *'authorised and controlled as appropriate'*. There was consensus that 'controlled' was better than 'restricted', but 'as appropriate' might broaden the definition too much. The definition was proposed to be declarative with examples of the different types of users to be provided in the text.

19. The participants discussed whether the proposed definition was compatible with the fact that some information was publicly accessible. *Mr Finnegan* considered that even users who used the system for free and did not go through a vetting process with guest access should be controlled to avoid misuse of the system. Access could already be characterised as *'authorised and controlled'* when a user's IP address was identified. A certain level of authentication happened also when agreeing to the Terms and Conditions when accessing the system. *Mr Finnegan* suggested that the Access Control CPF should also cover the management of identities in the system, including individuals and computer systems.

20. *Mr Wool* remarked that it was essential to identify the best practices related to this CPF. It had previously been discussed that there should be a minimum level of tracking users, for example, via their email addresses or anti-bot verifications. If this was considered to be a best practice, there would be no need to cover all the other practices that might be exercised by the registries.

21. Ms *Rodríguez de Las Heras Ballell* noted that registries had specific resources that were publicly available, while other resources required some level of authorisation. Therefore, it needed to be clarified whether:

- a. access control should be the best practice in any registry for any resources, or
- b. access control should be necessary for some resources, or
- c. the best practice should be to ensure a maximum level of publicly available resources, with access control limited to the cases when it was strictly necessary.

22. Ms *Gullifer* suggested that the best practice should be to establish a *minimum level* of authentication or validation. That would make Access Control an umbrella term, and registries could choose the level of authentication appropriate to their specific operations and information. Another approach should be followed in case it was agreed that some information should be available to anyone without prior authentication, including individuals and computer systems.

23. Ms *Hillman-Weir* made a distinction between access to the registry's database and access to the registry's information. Currently, the level of access control to the registry's database is higher, and to the registry's information is lower. There was also some degree of monitoring of the volume of information extracted through the free search function, and registries had put controls in place to manage that. She suggested defining Access Control as '*the process of ensuring that access to the registry is controlled based on user roles.*'

24. Ms *Laurel Garven* indicated that full access to registry information was the best practice five years ago and expressed concern about identifying it as a current best practice. Ms *Gullifer* noted that the RBAC model could be flexible enough to say that no access control was needed over some types of users.

25. Ms *Rodríguez de Las Heras Ballell* emphasised the importance of incorporating the notions of 'role' and 'access' into this CPF, noting that Access actions could range from searching to changing, modifying, cancelling, or providing input to the registry.

26. Mr *Finnegan* suggested that the definition should allow for anonymous access, even if security concerns remained relevant. He warned that limiting the definition to RBAC might create gaps, as there were other models (e.g., attribute-based access control, mandatory access control, and policy-based access control). Additionally, RBAC may presume that all users were individuals, leaving computer-to-computer communication out of scope.

27. Mr *Finnegan* also shared that a user's identity and its credentials were currently managed separately from the permissions to access the system. The registry authenticated the user's identity through its credentials, determined its authorisation, and then access control enforced the permissions given to the user. Free users had permissions regarding specific actions, and the systems should be able to control those.

28. Mr *Rob Cowan* noted that the definition of Access Control should be concise while the concepts used in the CPF should be broad enough. While public searching remained a contentious issue, controls helped to avoid data harvesting and enforce sanctions. Not all data was meant to be publicly available. The best practice should include verification that the user was a human and, depending on the nature of the risks, provide for some level of identification or not. From a technical point of view, the definition proposed by *Aviareto* did cover public access, but it could be clarified.

29. Several participants agreed that all CPFs should be defined in a concise manner and that best practices should be provided without too many details. Registries needed to ensure themselves that legislative and policy requirements set by governments were fulfilled and identify appropriate tools in their operational context.

30. *Mr Wool* agreed that Access Control should be an umbrella term and it would be coherent with the RBAC concept. He questioned whether a best practice would be that (i) a user should be a human being, and (ii) a purely anonymous search should be allowed.

31. *Mr Justin Hygate* noted that users did not need to be human; API and machine-to-machine interactions and data consumption by governmental agencies and businesses were allowed. He suggested that registries did not need the email address of all its users.

32. *Ms Rodríguez de Las Heras Ballell* agreed that there was a need to prevent data scraping or massive and automated data processing but noted that it was commonly accepted internationally that automated action was functionally equivalent to human action. Therefore, machine-to-machine interaction should not be excluded.

33. *Mr Tirado* highlighted that the Guide's main objective was to provide technical solutions to create a vehicle for the best management of business information. A fundamental question regarded the scope of minimum information that must always be publicly available (e.g., the summary of a business's annual accounts, at least in some countries). While national legislators usually set such requirements, it could also be listed in the Guide.

34. *Mr Wool* pointed out that including such guidance or not depended on whether the Guide was prepared through the prism of *electronic* or *business* registries. Harmonising the minimum public content of the registry would be providing guidance from the perspective of business registries. *Mr Tirado* agreed that the focus of the Guide was more on the *electronic* aspects of business registries but noted that such guidance could still be helpful. *Mr Wool* suggested that a list of publicly available content could be included in an Annexe to the Guide.

35. *It was agreed to (i) create a glossary of terms used in the Guide, and (ii) incorporate the Authorisation CPF into the Access Control CPF. The Access Control CPF should be considered as a scale and should take into account the users' roles. A best practice on Access Control should not restrict users to individual human beings only, and certain information should be accessible without authorisation (publicly available). Guidance on the scope of information that should be publicly available information could be included in the Annexe to the Guide.*

#### Discussion on the Accuracy CPF

36. *Ms Tarailiene* introduced the new CPF on Accuracy and highlighted that the concept of accuracy could be considered in a binary way or as a scale. The UNCITRAL Legislative Guide emphasised that data on the registries should be '*as current and accurate as possible.*' She suggested that registries should assess accuracy instead of ensuring it, as there were limitations in updating outdated information and preventing data entry errors.

37. *Ms Rodríguez de Las Heras Ballell* noted that the Accuracy CPF might set a standard for the duty of care by the registry to ensure data was updated and accurate. It could be interpreted in two ways: (i) substantively – i.e., to which extent does the registry need to verify whether the information corresponded to reality; (ii) technologically – i.e., to which extent is the registry required to implement an error-correcting or updating mechanisms. Finally, limits related to error correction and updating by the registry needed to be distinguished. *Ms Gullifer* agreed that it is challenging to outline correcting and updating activities from a purely technological perspective, as it also requires getting the correct information from the businesses.

38. *Ms Gullifer* and *Ms Mauro* pointed out that the CPF on Accuracy was more substantive, while the CPF on Correctability was procedural.

39. *Mr Wool* agreed that it was necessary to clarify whether interpreting Accuracy substantively would mean setting up processes for maximising Accuracy or ensuring Accuracy in fact, which could raise liability issues.

40. *Ms Gullifer* clarified that the current definition - '*The property of being actual or corresponding to reality*' - seemed to set liability for absolute accuracy. She suggested reformulating it as '*The property of the user being able to assess the accuracy.*'

41. *The participants* expressed support for this proposal and for defining Accuracy in the glossary as a scale. The CPF would describe that accuracy could be assessed in particular by providing users with as much information as possible. Then, the best practice was to make it easy for parties who relied on data to assess its reliability. There was a consensus that this CFP would not impose liability on registries.

42. *Mr Wool* wondered whether the best practice could include both electronic procedural steps to maximise accuracy and user assessment of accuracy through transparency, or only the last one. He proposed an additional part in the CPF, indicating that data collection systems should be designed to enhance accuracy.

43. *Mr Cowan* provided an example of accuracy control, such as the registry verifying VAT numbers against the database. He noted that these controls were helpful but had limitations and should be balanced with the registry's efforts.

44. *Mr Hygate* highlighted the shift towards more rigorous information checking by registries in common law systems. He emphasised transparency as a best practice for EBRs to validate the information electronically in a cost-effective and transparent manner.

45. *Mr Julian Lamb* noted the increased focus on accuracy for certain types of basic and beneficial ownership information due to regulations like FATF. The choice of a particular accuracy check mechanism would depend on the tools and requirements available in the operational context. For example, since November 2022, accuracy checks should also consider data protection according to EU law.<sup>1</sup>

46. *Ms Hillman-Weir* suggested considering Accuracy in the context of business registries' two distinctive functions: confirming incorporation status and acting as information custodians. The legislation that governs the registry provided the standards regarding the confirmation of the incorporation status and its validity. A status renewal process and annual updating of information were essential for maintaining accurate information.

47. *Ms Rodríguez de Las Heras Ballell* agreed that the best practice was using digital tools to enhance accuracy to the maximum extent possible. Expectations about the accuracy of information in the business registry were higher than those set for the online platforms by the EU Regulations, so business registries should make a greater effort to enhance the reliability of information.

48. *Ms Gullifer* agreed and highlighted the points on disclosure, 'as required by law', and cost-effectiveness, which could be taken into account when describing the best practices.

49. *It was agreed that the concept of Accuracy should be considered a scale, and it should not entail liability for business registries. A definition of accuracy should be included in the glossary. The CPF on Accuracy should emphasise transparency and disclosure to allow users to assess Accuracy. Registries should also use electronic means to check and maximise Accuracy.*

#### Discussion on the Correctability CPF

---

<sup>1</sup> Joined Cases C-37/20 and C-601/20 (WM and Sovim SA v Luxembourg Business Registers), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62020CJ0037> , accessed on 04.10.2024

50. *Ms Tarailiene* proposed two possible definitions for the Correctability CPF. She noted that the CPF should set out the scope of Correctability, i.e., whether and in what way it covered different types of errors, such as (i) typographical or manuscript errors, (ii) computed-generated errors, (iii) factual changes, (iv) false registrations. Additionally, it was proposed to discuss the specific rules and responsibilities associated with each type of error, and the tools to manage errors. Possible overlap with the CPF 'Legal Authority of the Registrar' should also be considered.

51. *Mr Hygate* preferred the second proposed definition: '*The process of identifying and rectifying inaccuracies or deviations from accurate information.*' The first definition referred to the correction of errors by both the registrar and the end user, while those were subject to different procedures in many jurisdictions. The registrar's ability to make changes to the record for a broad range of reasons should be taken into account.

52. *Mr Cowan* suggested to refer in the definition to 'detecting' rather than 'identifying' inaccuracies, since the former was broader. He suggested adding to the list of errors an alteration by a non-authorized person through a cyberattack. Regarding the identification of errors, he noted that there were reporting mechanisms for the public to flag errors, as well as technical tools for cyberattacks. Moreover, the specific rules applicable to registries depended on the requirements in the applicable legislation. Additionally, regarding tools to rectify errors, he suggested that the data should be corrected through the registry's application and not on the database itself. *Several participants* endorsed this point.

53. Furthermore, he added several points for discussion: consultation with interested parties, logging of all corrections, and transparency. *Mr Cowan* elaborated that this CPF could include notification and consultation with relevant parties when an error was identified. Further, logging of all corrections was crucial as evidence, and it was performed most easily through the application or, otherwise, with a robust change control process. Finally, transparency would require the registry to be clear about the notifications, consultation practices, procedures, mechanisms, and reporting.

54. *Mr Hygate* raised the issue of public notification of identified errors and their correction, as some changes may need to be visible to the public.

55. *Some experts* underlined that the glossary should distinguish between *errors* and *accuracy*. Errors were defined in the working paper as '*deviations from accurate information*' and categorised into four types: typographical, computer-generated, cyberattack-induced, and factual changes. While the first three were clearly errors, factual changes could be updates or misleading information, which required careful evaluation. A distinction should be made between correcting an error and updating information. Correctability could be phrased as '*The process of identifying and rectifying errors*' to avoid using accuracy as a reference within the definition.

56. To clearly distinguish between the CPFs on Accuracy and Correctability, *Ms Rodríguez de Las Heras Ballell* proposed to make a typology of errors depending on who could detect the error and who could correct it.

57. *Mr Hygate* suggested that a high-level definition should include both the ability to correct an error and to update information. He proposed that the best practice could be that the register should have a process to correct errors in a range of ways, and an error could be defined as something that is '*not accurate at the time and date*'.

58. *Many participants* agreed that the registrar should have the power and technical ability to correct information not only when there was a court order but also when a change was necessary in the absence of an infringement of legislation, including technical malfunctions, cyberattacks, and end-user actions. Correctability was a specific tool the registrar used with urgency to correct information that would materially impact the market.

59. *Ms Gullifer* observed that such actions should usually be performed in accordance with the law and queried whether the Guide should take a more normative approach and recommend a legal power to the registry when none is stipulated by law. She suggested checking whether the UNCITRAL Legislative Guide provided guidance on that matter.

60. *Ms Monica Canafoglia* confirmed that the UNCITRAL Legislative Guide contained recommendations for a law that gives the registrar the authority to correct incidental errors, even without any court order or outside input.

61. *Ms Andrea August* emphasised that corrective actions should not impose a burden on the end-user, as was the case in some civil law countries.

62. *Ms Hillman-Weir* shared that correctability was close to amendment, and registries always had to have an audit trail. When records were altered, particularly under the registrar's authority, registries never obliterated information and had to ensure that the registry reflected the current state.

63. *Mr Wool* and *Ms Gullifer* agreed that the Guide should make reference to the UNCITRAL Legislative Guide and possible implementing legislation. Further, the future Annexe to the Guide, which would set out the minimum amount of information that should be publicly available, should also say that such information should be updated and correctable if needed.

64. *Ms Mauro* referred to an earlier discussion on the CPF 'Legal Authority of the Registrar', during which the group had supported the inclusion of identification authority/technical power to the registrar's legal authority. She stressed that the CPF on Legal Authority of the Registrar partially elaborated on corrective actions by the registrar and asked whether this duplication was acceptable or should be included in the Correctability CPF only. *Mr Gullifer* proposed to outline the technical side of the registrar's ability in this CPF and the legal power in the CPF on Legal Authority of the Registrar.

65. *Ms Rodríguez de Las Heras Ballell* indicated that the correcting process included several stages: (i) identifying/detecting, (ii) correcting, (iii) tracing/logging, and (iv) notifying/publishing processes. Given that detection was presumed in inaccuracy, it could be removed. Then, correctability would mean that there was a process of correcting errors. *Ms Gullifer* noted that error identification or detection was the most problematic aspect as it was closely connected to the types of errors. The presumption of accuracy should also be approached cautiously as it could be seen as a legal point.

66. *Mr Lamb* agreed and noted that registries needed some mechanism for finding discrepancies, inaccuracies, or wrongful information.

67. *Ms Gullifer* queried what standard could be identified for such an error-detecting system and how far the registrar could go in situations with factual changes and false registrations. Identification might be included in the Correctability CPF but would be limited to typographical errors and cyber-attacks.

68. *Mr Cowan* stressed that it should be acknowledged that certain types of errors cannot be detected. Still, appropriate mechanisms should be in place, such as cryptographic measures to do tamper detections and attempts to alter information not through the application, or regular cross-checking with other systems.

69. *Ms Garven* noted that at least three other CPFs were closely related to Correctability: Accuracy, Integrity, and Reliability of data. She suggested keeping the definition short to avoid overlap with these CPFs, and with those on Evidentiary Value, Risk Management, Trustworthiness, Validation and Verification. *Mr Wool* agreed that all these CPFs were connected and invited participants to discuss potential overlaps.



70. *Mr Wool* raised the point that the best practice on Correctability would refer to the registry's ability to do something, while the other CPFs seemed to refer more to the consequences and implications of doing something, without overlap. The question was what would be the best practice in the system's ability to act.

71. *Ms Garven* clarified that she did not mean that the core concept was duplicated but rather that there was overlap in the mechanisms and actions used to detect, assess or continuously review the integrity, validation, and reliability of information. These CPFs were not only consequences but also inputs for determining whether corrective action was necessary. Correctability was the intermediate step that involved measuring, assessing, and detecting the accuracy and integrity of information and taking consequential actions, such as determining whether the corrected information could be relied upon.

72. *Ms Gullifer* came back to whether the Correctability CPF should include error detection or identification processes.

73. Practical examples of error detection were provided. For instance, the registry in Estonia used a blockchain-based system that flagged any changes made outside the app, ensuring that changes to the register were made only through the correct channel. Checking the submitted VAT number with the databases enabled the quick identification of errors. Regarding identifying any attempt at fraud, it was recommended that trends and anomalies relating to financing terrorism and wrongful or misleading information were detected. Registry data could be analysed and cross-checked with third-party databases for this purpose.

74. *Ms Rodríguez de Las Heras Ballell* considered that error detection should not be included in the Correctability CPF, while it should be emphasised that Accuracy was a dynamic process and should include a mistake-detection mechanism. She thus suggested including error detection under the Accuracy CPF or developing a separate CPF. She asked whether the reasonable threshold should be (i) errors should be detected based on a digital mechanism by the registry itself or upon request of the public authorities or end user, or (ii) whether the focus should be only on errors that the registry could detect by itself. *Ms Gullifer* added that a court order could be another reason to correct a mistake that was not detected by the registry, although it would mean that the error had been detected.

75. *Mr Cowan* suggested adding Error Detection as a separate CPF, clarifying its scope and describing technical controls and processes that could be used to flag and minimise errors. Even in less advanced jurisdictions, the best practice would be to try to implement technical error detection controls and notification processes.

76. *Ms Gullifer* agreed with a separate CPF. *Ms Hillman-Weir* suggested it could also be a part of the CPF on Risk Management or Integrity.

77. *It was agreed that the Correctability CPF should instruct registries to put mechanisms in place to rectify information on it, including correction of errors and updating of information. The text of the CPF should refer to the UNCITRAL Legislative Guide concerning the registrar's authority to correct records. Correcting data through the registry application and not through the register itself should be indicated as the best practice in terms of tools to rectify errors. It was suggested to draft a separate CPF on Error Detection for consideration at the next meeting.*

*Discussion on the proposal to replace the CPFs on Validation and Verification with the new CPFs on Data Validation and Software Testing*

78. *Ms Tarailiene* noted that the CPFs on Validation and Verification were unclear and mixed the concepts of software validation, data validation, and verification. The current definition of validation related more to software testing than to data validation and it was therefore suggested to replace it with a new CPF on Software Testing. Furthermore, it was

suggested to replace the Verification CPF by a new CPF on Data Validation keeping the same definition.

79. *Mr Michael Chan* supported the change from Validation to Software Testing, which aligned better with the Software Development Life Cycle (SDLC). Software testing was a crucial phase in showing software quality, in line with the Accuracy CPF. Since the registrars may outsource software development, they should also independently perform software testing.

80. On behalf of *Aviareto*, he proposed defining software testing as '*The process of evaluating the software system or components to verify that it meets specified requirements, assess its quality, and identify any defects.*' Software testing was a broad term, so different levels and types of testing could be distinguished. Test levels focused on specific aspects of software quality during different SDLC stages. Test types referred to the objective of the testing purpose, either functionality, performance, usability, or security. A relevant software testing standard should be adopted in the CPF, and the software testing should be recorded and managed. ISO/IEC/IEEE 29119 provided five internationally recognised standards on software testing, but registries should also have other standards available. By aligning the CPF to those standards, the registries would be able to achieve quality, efficiency, and effectiveness in their testing efforts.

81. *Ms Gullifer* agreed that a footnote could reference the standard and noted that the ECR Guide did not contain this CPF, but it could be considered to add it if necessary.

82. *Ms Garven* raised a concern regarding the term 'software testing,' which did not fully reflect the previous Validation CPF. Additionally, using a specific term from software development could risk introducing more complexity. Software testing primarily focused on application-level aspects, potentially excluding data verification.

83. *Ms Rodríguez de Las Heras Ballell* queried about the specific application of software testing standards relevant to EBRs. She also noted that it was important to clarify who was responsible for the software testing and whether it would be possible to cover exhaustively the other matters coming out of the software testing standard for registry operators. While verification of the data for registry purposes was relevant, she considered that software testing might not be specific enough to be included as a CPF.

84. *Mr Lamb* agreed that the Guide should focus on specificities of different aspects of systems design and operation that would be important for EBR practitioners. The main priority for this CPF should be data usage.

85. *Mr Cowan* explained why software testing was more important for the EBRs, pointing out that registrars could not go back in case of any fault or error. Given that legislation often limited the registrar's power to correct mistakes, the best practice would encourage a higher standard of testing during the SDLC than the one performed in other systems. He suggested that it should be the registrar's legal responsibility to perform detailed testing, as the registrars were liable for the registry system they were running.

86. *Mr Wool* queried whether software testing covered the full range of activities that the Guide needed to cover. He agreed that the definition should be general but relevant to business registries. Several participants had used the terms verification and validation interchangeably, and clarification was required if both terms would continue to be used in the Guide.

87. *Ms Hillman-Weir* agreed on the importance of the software used by the registry and ensuring the requirements were met for the purposes of legal compliance. When registries were operated manually, the registrar and the registrar's office had mechanisms, controls, and practices to ensure that the requirements and the imperatives for legal compliance were fulfilled. In an EBR, these mechanisms, controls, and practices were articulated through the

system. Software testing was just one element of the integrity check, and she, therefore, questioned whether a separate CPF on Software Testing was needed.

88. *Mr Cowan* explained that the definition of the Software Testing CPF in the Guide was broader. He agreed with the need to have a clear understanding of validation and verification and observed that the technology field was full of overlapping and inconsistent definitions, so clarity was essential in the Guide. Data Validation was a concept that ensured that if one was supposed to type in a number, the input was a valid number. The previous definition of Validation focused on software aspects rather than data.

89. *Ms Katarzyna Connell* expressed support for the proposed Software Testing CPF. She agreed that EBRs should prioritise software testing due to the registrar's unique understanding of user interactions.

90. *The participants* supported the idea that Software Testing aimed at ensuring that the system does what it is supposed to do and that Data Validation verified compliance with established criteria, not data accuracy.

91. *Mr Lamb* proposed encouraging the registries to carefully consider the risks in system development and avoid oversimplifying them, as the consequences of registry system malfunctioning were serious. *Ms Gullifer* agreed that this should be reflected in the commentary.

92. *Ms Rodríguez de Las Heras Ballell* pointed out that the reference to 'intended use' in the definition of Software Testing was a crucial threshold. As the registry's operations were of higher societal and market importance, they entailed more risks in their intended use and required higher standards.

93. Both *Ms Gullifer* and *Mr Lamb* emphasised the need for continuous and comprehensive testing to maintain system quality.

94. *Ms Hillman-Weir* suggested defining this CPF as '*the process of confirming, using objective evidence and testing, that the requirements for a specific intended use or application have been fulfilled by the electronic register*'. *Ms Garven* supported the addition of 'testing' in the definition but not narrowing the CPF to 'Software Testing'.

95. *Ms Gullifer* suggested the term 'System Validation', which covered more than a 'system' and more than 'testing,' as long as it was clearly distinguished from Data Validation in the definition with reference to ISO standards. *Mr Hygate* proposed to refer to the 'electronic register' rather than 'the system'. *Ms Gullifer* expressed her concern about this rephrasing.

96. *The participants* agreed on System Validation as the preferred term, accompanied by a clear definition. The term 'verification' should be avoided. Acceptance Testing and System Testing were suggested as potential alternatives, but System Validation was considered the broadest term.

97. *Ms Gullifer* observed that what used to be the Validation CPF was split into a CPF on Data Validation and a CPF on Software Testing. Software testing should address specific challenges faced by EBRs, such as limited correction capabilities. She invited the participants to discuss the proposed new CPF on Data Validation.

98. *Ms Garven* expressed concern about splitting the term Validation into Data Validation and Software Testing. The previous content of Validation did not presuppose Software Testing. At the same time, she supported transforming Validation into Data Validation, as that was the focus of the CPF.

99. *Mr Cowan* shared that the previous definition of Validation seemed not to be limited to data but attempted to cover the software testing aspect as well. *Ms Hillman-Weir* agreed

with Mr Cowan and expressed her preference for the previous definition of Validation as it was more general.

100. *Mr Wool* agreed to avoid using the concept of Verification and replacing it with Data Validation, which means assessing that the data meets the registration criteria. He also agreed with System/Software Validation, which essentially meant confirming that the system and software used were fit for purpose.

101. *Mr Lamb* queried what elements made a difference for the registries in the SDLC. As a best practice, the operational environment and specific risks should be carefully considered during registry design. He opined that the terms 'validation,' 'verification,' and even 'vetting' could be used if needed but in a clear way.

102. *Mr Hygate* agreed with the proposed definition of Data Validation, providing examples of validating that a data input contained numbers when it should, the correct address in a correct jurisdiction, etc. Software testing was crucial for ensuring that registry systems performed in accordance with their established business rules. He opposed to verifying the accuracy of data, as validation did concern accuracy.

103. *Mr Choi* agreed that business rules were key for international registry operations and supported the understanding of software testing as ensuring that the registry system conforms to what it is meant to do and meets the set requirements. Data validation included two aspects: (i) validation that, for example, numeric fields set only numeric data, and (ii) validation that the data matches the specified criteria. It was also important, from a security perspective, that the registry fields do not accept SQL or injection commands aiming to break the system and manipulate the data.

104. *Mr Wool* expressed discomfort with using the term 'registration' in the definition of Data Validation as it was a legal term that carried a lot of meaning and could narrow the definition. He proposed that Data Validation would mean assessing whether the submitted data meets the established criteria. Advanced data validation techniques, leveraging electronic systems, should be implemented whenever possible and should be the best practice.

105. *Ms Hillman-Weir* proposed the terms 'data acceptance' or 'data compliance' to avoid implying endorsement but assessing that the data meets established criteria for its purpose. *Mr Wool* confirmed that the data validation definition would not ensure the correctness of the data entry but only accept that the data meets the established criteria.

106. *Mr Cowan* suggested using 'data input validation' to be more precise with IT terminology. Narrowing down the possible data input in the field would still be appropriately called 'validation', while the 'data acceptance' proposed by Ms Hillman-Weir was another viable approach.

107. *Ms Gullifer* agreed on the Data Input Validation term, as suggested by Mr Cowan. She elaborated that the Guide should list the CPFs not in an alphabetical way but rather in clusters of connected CPFs. She emphasised the possibility that the CPFs on Data Input Validation and System Validation, once agreed, should be translated into the Guide on Collateral Registries.

108. *It was agreed that Data Validation should be rephrased as Data Input Validation, and the definition should mean 'the process of assessing that data meets the established criteria [for its purpose in the registry].'* Software Testing should be rephrased as System Validation, and the definition should indicate 'the process of confirming, using objective evidence and testing, that the requirements for the intended use have been fulfilled by the system/electronic register'. The commentary to the CPF on System Validation should elaborate on the risks of system failure in the specific context of EBRs.

*Discussion on the proposal to merge the Disposition, Integrity and Retention CPFs into a new CPF on Records Management*

109. *Ms Tarailiene* explained that merging Disposition, Integrity, and Retention in a new CPF on Records Management would be in line with a holistic approach to managing the entire lifecycle of records within business registries. This change would acknowledge that data and documents were not static entries but part of a dynamic lifecycle that included retention, archiving, and eventual disposal. Aligning the definition with ISO 15489 would cover the creation, maintenance, use, and final disposition of records as best practice. Proceeding with this change would reduce the overlap between Integrity and Retention CPFs and increase consistency. Inclusive management of all record types, both digital and physical, would be beneficial as well.

110. *Mr Wool* agreed with merging the CPFs on Disposition and Retention into a new Records Management CPF. However, he questioned whether Integrity should be included under this term. The proposed new definition did not mention integrity unless it was implied by the word 'control.'

111. *Ms Caroline O'Brien* noted that Integrity was mentioned throughout the ISO 15489 standard on Records Management in a way that a record that has integrity is one that is complete and unaltered or that a record should be protected against unauthorised alteration. It seemed that the previous definition of Integrity as '*The property that data has not been altered or destroyed in an unauthorised manner,*' was coherent with the ISO standard.

112. *Ms O'Brien* indicated that the latter standard did appear to address the amalgamation of the three CPFs in question. It defined records as '*Information created, received, and maintained as evidence and as an asset by an organisation or person in pursuit of legal obligations or in the transaction of business.*' According to the ISO standard, records, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity, and usability. Such phrasings can be found throughout the entire standard regarding the best practices, policy, creation, and various characteristics of good record management.

113. *Ms Hillman-Weir* shared that her understanding of Integrity was very much tied to the general custodianship and care of the information during its useful and active life, while Disposition and Retention concerned the end of the information's life cycle. She supported the idea of merging Disposition and Retention into a Records Management CPF while maintaining the separate CPF on Integrity.

114. *Ms Gullifer* noted that the ISO standard covered many different concepts, so the fact that the three CPFs seemed to be all included there did not prevent the Guide from keeping them separately. She agreed with combining Disposition and Retention and keeping Integrity separate.

115. *Mr Lamb* noted that a holistic approach to a data lifecycle was important and that it was possible to merge the three CPFs from a practical perspective, capturing all their essential characteristics in the new definition. Registries accepted the need to have a mechanism ensuring that the data provided was not altered and that, ultimately, the user trusts the data, which was linked to Integrity. One of the distinctive features of business registries was that, generally, users must be able to trust the information on the registry.

116. *Mr Wool* deduced from *Mr Lamb's* intervention that Integrity could also be a separate CPF. In that case, he wondered how the definition of Integrity would be different from the term authenticity. *Ms Gullifer* pointed out that the CPF on Authentication referred to a very different process.

117. *Mr Cowan* clarified that the words authentic and authenticity were not used in the Guide in a meaning close to integrity. By 'authentic document,' *Mr Cowan* would understand

the actual, original document that was not made up. In the registrar operations, integrity would allow the registrar to confirm that once something has been submitted to the registrar, it has never been changed, and no records have been lost. Integrity would also not change or delete the invalid or incorrect documents submitted to the registrar.

118. *Mr Wool* cautioned against the understanding provided on page 5 of the working paper that this would include ensuring data integrity, providing accurate and reliable records, and upholding privacy and security standards, as it would go beyond the discussed scope. He also confirmed that Integrity was critical and should be a CPF on its own, keeping the previous definition. In view of this, the authentic document would be the one having integrity. *Ms Gullifer* preferred not to use the word authentic to avoid any misconception with the Authentication CPF.

119. *Ms Garven* pointed out that records management policies and practices differed from one registry to another, while there was a common understanding of the term 'integrity.' While Integrity had a clear meaning in terms of records, it should also be emphasised on a broader systemic level of the registry. *Ms Rodríguez de Las Heras Ballell* supported keeping Integrity separate as it was a well-known concept in the legal sphere.

120. *Ms O'Brien* referred to the definition of an Authentic record from the ISO standard: 'The one that can be proven to be what it purports to be, have been created or sent by the agent purported to have created or sent it, and have been created or sent when purported,' but noted it could create general confusion.

121. *Mr Hygate* raised the point that it was important to make a distinction between records *in* the register and records of transactions *around* the registry. He noted that, in common law jurisdictions, there was a distinction between the data that pertained to the existence of companies, for which a record was generally kept indefinitely, and administrative information, such as receipts, invoices, and other transactional data. The latter served a purpose in the registration process but were covered by a different set of rules in a jurisdiction (typically tax) and could be disposed of. The scope of the concept of 'record' should be refined, potentially to those records that reflect the core data set constituting the register. *Ms Gullifer* explained that the concept originated from the Guide on ECR, which had only one kind of record. However, in the context of EBRs, it seemed that the CPF covered all types of records but in a different way. Retention policies could be tailored to both core data and other records.

122. *Mr Cowan* noted that Records Management was not limited to the end of the life cycle but included the full life cycle of the record being created, looked after, and eventually disposed of. If Integrity was kept as a separate CPF, Disposition and Retention should either also be kept separately or called differently.

123. *Several participants* supported the proposal for the new Records Management CPF while separating it from the Integrity CPF, acknowledging its importance with cross-references to Records Management.

124. *Ms Gullifer* noted that if the Guide aimed to reflect a full life cycle, then it needed to elaborate more on the creation of a record, potentially through the Data Input Validation or other CPFs.

125. *Ms Mauro* observed that the Correctability CPF might be seen as the process and many other CPFs, listed by *Ms Garven*, were the consequences of that process. In a similar way, Integrity may be seen as a consequence of the Records Management process.

126. *Ms Hillman-Weir* noted that Records Management was a self-standing discipline outside the EBR context and was reluctant to narrow it down in the Guide. Many different registry practices contributed to Integrity, not only Records Management, and reducing the registry's function and purpose only to Records Management would not be desirable.

127. *Some participants* observed that Retention was crucial to provide relevant information for court cases lasting longer than mandatory record retention periods set by the legislative requirements. While some EBRs only removed records from public access, and some kept records public infinitely, not taking the record off the registry could be recommended despite legislative requirements. At the same time, the right to be forgotten and other restrictions set out in GDPR should be considered.

128. *Ms Gullifer* noted that, with their current definitions, Disposition and Retention were closely linked and could be included under the same heading. She confirmed that Integrity should be set out separately. *Mr Cowan* suggested simply calling it the 'Disposition and Retention' CPF.

129. *Ms Mauro* queried whether this CPF, called Records Management or not, would still have cross-references to the separate Integrity CPF. *Ms Gullifer* agreed that a CPF on Records Management would deal with the full life cycle of records, not just the end of the cycle. It might, therefore, be preferable to narrow the scope of the CPF and call it Disposition and Retention.

130. *Mr Hygate* highlighted that as the Guide focused on the EBRs, a record could be specified to be an electronic record. *Ms Gullifer* agreed that the term record or electronic record should be defined in the glossary.

131. *Ms Rodríguez de Las Heras Ballell* suggested amending the wording of the CPF as '*deployment and implementation of efficient and systematic control and maintenance of records.*' *Ms Gullifer* proposed it could also be renamed '*electronic records management*' to include record maintenance and raised a question about the creation of a record.

132. *Ms Hillman-Weir* noted that rules related to the creation and maintenance of records and the use of information in the registry were not subject to broad ISO standards but to the legislation specific to the registry. *Mr Lamb* echoed that registries considered many different practices and standards that were specific to EBRs, not only the ISO 15489.

133. *Mr Tirado* referred to the transition from paper-based to electronic registries and wondered whether the CPF should include any guidance on transforming records that are submitted in paper form into electronic records. *Mr Hygate* shared that this transition often happened through the digitisation of paper records, especially for highly searched businesses.

134. *Ms Rodríguez de Las Heras Ballell* pointed out that the transition should eventually ensure that the registry was data-oriented rather than document-oriented, as data allowed for more sophisticated management and analytics. Scanning the paper records would not provide the benefits of the EBR.

135. *Mr Tirado* noted that in many countries, the confirmation of the creation of a company was a paper document, which was then scanned and sent electronically to the registry, i.e., it remained a scanned document, not a data record. Therefore, the question arose whether the Guide should not facilitate the transition to electronic records.

136. *Ms Garven* agreed that it would be in line with the distinction between digital and electronic, which would be relevant for many CPFs, such as those on Data Input Validation. It should be highlighted in the Guide that an electronic record did not mean scanning a paper record but transforming it in a digital record.

137. *Ms Hillman-Weir* added that concepts of data conversion (the discipline of converting from paper to electronic through scanning, data entry, or a combination of the two) and data migration (the transfer of data between systems or their generations) should also be differentiated and addressed.

138. *Ms Gullifer* indicated that during the sixth workshop, participants had suggested addressing these questions in a separate CPF on Electronification that should include digitalisation as well. This Electronification CPF had subsequently been removed from the Guide following rounds of review.

139. *Mr Lamb* noted that even in advanced jurisdictions, registries needed to deal with some paper records. Thus, it should be clear that digitalising processes should allow for analysing and using the information, even received from paper, and the Guide should be more progressive. *Mr Wool* noted that the Guide needed to encourage certain behaviours among the registries on the spectrum of digital transformation.

140. *Ms Mauro* reminded the participants that at the seventh workshop, World Bank representatives had presented their Guidance Note on "Integrated Investment and Business Service Delivery and Data-driven Company Registry." They highlighted the digitalisation of paper-based business registries and a capability maturity model with different levels and factors for this purpose. The Guide could reference the presented work to avoid duplication. *Ms August* would confirm the exact reference.

141. *It was agreed to (i) retain Integrity as a separate CPF, (ii) while uniting the Disposition and Retention CPFs under the title 'Disposition and Retention'. To facilitate the transition from a paper-based to an electronic registry, the Guide could refer to a Guidance Note from the World Bank.*

#### Discussion on the proposal to subsume Standardisation under the Interoperability CPF

142. *Ms Tarailiene* introduced the proposal to merge the elements related to standard data formats and taxonomies into the CPF on Interoperability. She highlighted that EBRs managed extensive data that must be interoperable and accessible nationally and internationally. In light of this, standardising data formats and taxonomies was critical for effective system-to-system communication, and consistent and accurate data sharing.

143. *Ms Gullifer* recalled the latest definition of the Interoperability CPF: '*The property of having interfaces to communicate with or transfer data among systems in an automated manner that does not require the user to be extensively familiar with the operation of the other systems*'. She also stressed that one cannot have Interoperability without Standardisation, but this should be included in the CPF description and not directly in the definition.

144. *Mr Lamb* elaborated that the biggest drivers for interoperability were anti-money laundering and the proliferation of terrorism financing countermeasures. Any jurisdiction needed to demonstrate the ability to share the basic and beneficial ownership information when requested. As EBRs were competent authorities, they needed to be able to communicate with other competent authorities both nationally and internationally. The best practice was the ability to provide data in some standard way and in a generally used form to increase usability, preferably digitalised.

145. *Ms Gullifer* recalled the discussion from the seventh workshop that EBRs generally needed interoperability to provide data to other authorities, while ECRs usually used interoperability to check collateral information against other sources of information. Standardisation was agreed to be normalisation that enabled the data to be shared.

146. *Ms Tarailiene* added that latest CPF on Standardisation mentioned the standardisation of templates for incorporation documents, though, it could be included in the CPF on Accuracy. *Some participants* preferred not to include standardisation of templates in the CPF on Accuracy, as such measures could still facilitate Interoperability.

147. *Ms Garven* agreed that the best practice would be for the registries to be capable of interoperability, not mandating that interoperability should happen *per se*. If needed, it could be at a subnational, national, or possibly regional and international level.



148. *Mr Finnegan* noted that Interoperability needed to be considered at the registry's design stage, for example, even when choosing a character set.

149. It was pointed out that differences caused by company law rules across jurisdictions would not be addressed in the Guide. Still, Interoperability could simplify registration and incorporation processes across jurisdictions by facilitating the exchange of data between registries.

150. *Ms Maureen O'Sullivan* shared that in the EU, the Business Register Interoperability System (BRIS) was set up based on very basic information. Later, with the implementation of the<sup>2</sup>, interoperability started being considered in any registry design. The approach of starting from a limited form of interoperability and expanding it would seem optimal. *Ms Gullifer* noted that interoperability was much more complicated on the international level than on the EU level.

151. *Ms Mauro* shared the outcomes of the discussions on this matter during the seventh workshop. The best practice agreed upon was to require the registry to be as interoperable as the relevant legal framework mandated it to be. The implementation of Interoperability was defined as a policy issue that should not be dealt with by the Guide.

152. *It was agreed to include the Standardisation CPF in the Interoperability CPF, as standardisation enabled and facilitated interoperability.*

#### Discussion on the Evidentiary Value CPF

153. *Ms Tarailiene* elaborated on the current definition of the Evidentiary Value CPF, emphasising the *prima facie* validity of the EBR' data. If agreed upon, this CPF should instead promote procedural and technical best practices without prescribing legal standards. Those could include digital signatures, chain of custody protocols, and detailed logs of processes, ensuring the integrity and reliability of the register's records. At the same time, enhancing the evidentiary value of registry records should not imply legal authority.

154. *Mr Wool* noted that there was no proposal for an alternative definition. He expressed support for the proposed approach regarding the scope and limitations of the CPF, namely to avoid the concept of *prima facie* validity, prescribing legal standards, or engaging in the interpretation of law, and instead focus on procedural and technical best practices.

155. *Participants* agreed that Evidentiary Value should be a separate CPF, avoiding duplication with the closely related CPFs on Correctability, Accuracy, Disposition and Retention.

156. *Mr Hygate* suggested explaining in an annexe to the Guide that the jurisdiction involved needs to be able to use the register in a court case. The best practice then could concern only the register *per se* or suggest that a jurisdiction should make sure that the court could use the register. Alternatively, the proposed threshold could be put as 'meeting one's jurisdiction evidentiary requirements.'

157. *Mr Wool* suggested that the registries should consider their home jurisdiction, international practices, and developments.

158. *Ms Gullifer* highlighted that this CPF was important for dispute resolution, including arbitration, mediation, and others.

---

<sup>2</sup> Directive (EU) 2019/2121 of the European Parliament and of the Council of 27 November 2019 amending Directive (EU) 2017/1132 as regards cross-border conversions, mergers and divisions (Text with EEA relevance), <https://eur-lex.europa.eu/eli/dir/2019/2121>

159. *Mr Cowan* pointed out that from a technical and procedural perspective, this CPF should contain the procedure for data change control and logging of manually changed records. Then, depending on the risk, there may be a need for different levels of integrity controls over logs. The long-term logging storage should be maintained, and with every major system update, the old records should be transferred to stay usable in the new system. Finally, the Evidentiary Value CPF should be considered in the design phase, as was noted by *Mr Lamb*, considering the evidence that must be gathered and the records and logs that should be retained.

160. *It was agreed to keep the Evidentiary Value CPF and delineate its scope as had been suggested in the working paper. It was suggested that this CPF should incorporate procedural and technical processes regarding data change controls and logging of changed records.*

#### Discussion of the Timeliness CPF

161. *Ms Tarailiene* presented the Timeliness CPF, explaining that the definition in the ECR Guide needed to be adjusted to the context of EBRs. In the EBR context, absolute timeliness was emphasised (while relative timeliness was more relevant for ECRs), and registrations had to meet specific legal deadlines. EBR registration decisions were typically staff-led, although automation was increasingly used for faster data registrations. The aim was to have data accessible in real-time data as registrations were completed. Given the above, the proposed definition was *'The property of prompt and efficient processing, updating, and making registration publicly searchable after completion'*.

162. *Mr Hygate* noted that decisions were not always staff led. For example, in terms of name determination, the applications and priorities were treated in the order in which they were received, making the timing relative.

163. *Ms Gullifer* clarified that the definition was tailored to EBRs given that the phrase *'publicly searchable after completion'* indicated that publication occurred once the decision has been made. The CPF did not prescribe how long the completion should take except that it should be prompt and efficient.

164. *Mr Hygate* highlighted another element of timeliness in the EBR: when an action was not performed within a specific time by an end user, there would be a negative effect, e.g., removal of an entity from the register. *Ms Gullifer* observed that this aspect was not captured in the proposed definition as it seemed to be merely one of the registry rules attempting to make it updated. The CPF in question illustrated the idea that the information should be made publicly searchable as soon as possible but not immediately because a decision may have to be made, and it will depend on the way the registry operates in a particular jurisdiction.

165. *Mr Finnegan* suggested rephrasing *'prompt'* as *'without undue delay'*, as the former indicated a sense of urgency and pressure. *Ms Hillman-Weir* agreed with this proposal but highlighted the importance of prompt and efficient registration processing. The understanding should include searchability purposes and other business activities facilitating the movement of the economy. *Ms Gullifer* agreed that while the proposed definition already covered this, it could be explicitly covered in the text.

166. *Mr Cowan* suggested that whoever was designing the system should consider different systems' timeliness and requirements. In the case of ECRs, relative time was more critical than absolute time. For EBRs, sometimes it was the absolute time when there was a statutory requirement to have something filed by a specific deadline. The CPF should not be prescriptive but instruct the system designers to consider the time requirements as key system requirements.

167. *Ms Garven* proposed that 'corresponding' could be added to the listed activities 'processing, updating, and making registration publicly searchable' indicating the provision of information, including reminders and prompts. *Mr Wool* noted that this CPF should be applied to making registrations and updates prompt.

168. *Mr Lamb* observed the general presumption that EBR activities must be quick, information must be up to date, and the competent authorities required information from the registries almost immediately. He suggested phrasing it as 'expeditiously' as it should also be quick to have its full value. *Ms Gullifer* supported this proposal.

169. *It was agreed to expand the definition of this CPF to include 'corresponding' and to substitute 'prompt' with 'expeditious'. The text of the CPF should elaborate that it is not for searchability purposes only.*

#### Discussion on the Risk Management CPF in the context of recent events

170. *Ms Tarailiene* explained that the Risk Management CPF was a new CPF (i.e., not included in the Guide on ECRs) aiming to address external and internal risks impacting the registry operations. Recent events demonstrated that such risks could be connected to technology outages, causing data unavailability, service interruptions, financial losses, and reputational damage. Robust risk management in the IT infrastructure of EBRs could mitigate these risks with contractual safeguards, disaster recovery plans, mandatory redundancy systems, continuous monitoring, vendor management, and staff training. Regarding source code ownership, it should be the best practice to have control over systems and avoid vendor dependency and correlated lock-in risks. This can be implemented through secure source code ownership or perpetual licenses and clear contracts on intellectual property rights. A question was to what extent this should be discussed in the Risk Management CPF, or in the Continuity CPF.

171. *Mr Wool* agreed on the importance of this CPF and asked whether some commercial points made in the text were best practices in design and operation. *Ms Gullifer* pointed out that matters of source code ownership were addressed in the Continuity CPF in the ECR Guide, so this could also be addressing these matters without a new CPF.

172. *Ms Garven* indicated that there were many ways in which EBRs could assess and make commercial and business decisions regarding how they procure, utilise, protect, and ensure the continuity of the system itself. She noted that while source code ownership could vary, ensuring continuity and a clear transition plan were crucial. The CPF should focus on best practices for maintaining access to technology and continuity, regardless of commercial arrangements. *Other participants* agreed that EBRs were highly focused on continuity in having contracts with vendors without interruption rather than obtaining the source code ownership.

173. *Mr Lamb* added that each registry went through a risk assessment in its jurisdiction, particularly regarding data management and system risks, and this CPF could unite all the other areas which link the risks. The text should provide examples of risk areas that the EBR would consider, such as data management and system development, which *Mr Lamb* offered to provide. A high-level CPF on Risk Management would encourage looking at many risks that applied to a registry and provide practical examples.

174. *Ms Gullifer* wondered whether 'threats to the registry operations' should be rephrased as 'risks to the registry operations' in the definition. *Mr Lamb* agreed, as risks could also be interpreted as opportunities.

175. *Ms O'Brien* proposed including 'threats and vulnerabilities' and 'registry design and operations'. Such expansion of the definition would reflect the day-to-day risk management in EBRs more accurately. Vulnerabilities were defined by one of the ISO standards as 'weakness of an asset or control that can be exploited by one or more threats', and

vulnerability management could be seen as a component of the umbrella term of Risk Management. Any Risk Management activities involved vulnerabilities and controls that needed to be used to mitigate and monitor the identified vulnerabilities.

176. Ms O'Brien elaborated on her suggestion to add 'registry design' to the definition. She explained that the risks could be divided into those associated with the registry's design element and the registry's operations. Risk management for the design stage included secure coding, architecture, testing, and audits. Business continuity plans were developed during the design stage to address potential failures. Early identification of risks allowed for proactive mitigation.

177. In addition, Ms O'Brien highlighted the risks associated with registry operations. Controls built in at the software design stage needed to be monitored, and upstream risks, operational changes, and any compliance requirements needed to be continuously assessed. A holistic approach to Risk Management was essential.

178. Ms Gullifer agreed with the proposed revised Risk Management definition, '*The process of identifying, assessing, and controlling threats and vulnerabilities to registry design and operations,*' and proposed adding the term 'vulnerability' to the glossary.

179. *Several participants* were in favour of changing 'controlling' into 'managing' as threats could not be controlled. The commentary would include guidance on ways of managing risks and vulnerabilities.

180. Ms Garven considered that tailoring the Risk Management application to the EBR context was an optimal approach. It should acknowledge the interconnectivity in the risk management system, which was critical for any registry but also extended into technology and the overarching operating concepts. She suggested listing ways to manage the risks and vulnerabilities, such as an Information Security Management System. She stressed that this CPF could provide a hierarchy not only of the types of risks but also of the systems and control mechanisms to manage such risks.

181. Ms Garven proposed expanding on what was already included in the Guide and recommending that the registries undertake robust enterprise risk management and planning to perform their duties, which included specific types of structures.

182. *Several participants* noted that while the Guide should refer to ISO standards, it could also mention that local and regional standards could be used if they are considered better or more relevant, such as SOC 2 for the US market, or if certain countries or regions did not recognise international ones. Updates to the list of relevant standards could be done either by reviewing the Annexe or online by adding a separate page on the CTCAP website.

183. Ms Mauro cited the report of the seventh workshop, recalling that the participants agreed that the technical standards would be retrieved and cited as cross-references. It had also been agreed as a general principle to refer to ISO standards over the local ones whenever available, but not to the exclusion of any other relevant standards. Maintaining the document current in the face of updates to the standards could be done by mentioning ISO and other standards by their name, which should remain the same over time.

184. *It was agreed that the definition of Risk Management should be as follows: 'The process of identifying, assessing, and managing threats and vulnerabilities to registry design and operations'. The CPF should make reference to ISO standards and other relevant standards. The content of the CPF should highlight the perpetuity of Risk Management, list a hierarchy of the risks and vulnerabilities, and suggest systems and control mechanisms that EBRs could implement.*

*Discussion of the proposed amendment to CPF on Accessibility*

185. *Ms Tarailiene* introduced the proposed new definition of Accessibility as '*The property of making resources generally available, regardless of human ability*'. This definition enabled the CPF to focus on inclusivity and equal access for individuals with disabilities in contrast to the previous broad definition of '*The property of being able to obtain the use of a resource*'. Such phrasing did not overlap with general usability aspects covered by the User-Centred Design CPF. Finally, in line with the conclusions of the seventh workshop, economic factors like fees were excluded, as those were policy issues for EBRs.

186. *Mr Wool* agreed that the previous definition might have been too broad but questioned whether Accessibility should be strictly limited to the challenges someone has rather than the ability to use something and the barriers to entry. He wondered what 'human ability' referred to in the suggested definition.

187. *Ms Rodríguez de Las Heras Ballell* agreed that Accessibility usually referred to inclusivity towards all kinds of users and questioned to what extent the information should also be made machine-readable for automated access purposes. *Mr Hygate* reflected that this question may relate rather to the CPF on Access Control.

188. *Mr Hygate* also suggested finding an alternative phrasing to 'human ability'. If this CPF focused on persons with disabilities (e.g., visual impairments), that was a comprehensive category of work in technology, and many governments had specific requirements for these purposes.

189. *The participants* considered a reference to Accessibility in the UNCITRAL Legislative Guide, which stated that '*registries should be designed and operated so as to cater for a broad spectrum of users that may want to register a business without any form of discrimination*'. In that context, Accessibility was considered software-wise, such as having easy access to documents, registration without discrimination against women, minorities, and other users that may not belong to the dominant segment of the population, etc. It was clarified that the registry would not be able to act against legislation that put barriers to accessing the registry.

190. *Ms Garven* mentioned that the concept of accessibility outside of the EBR context was expanding in some jurisdictions to whether it could be discriminatory to use solely electronic means and whether physical locations and agents should be available as ways of accessing and utilising the registry.

191. *Mr Finnegan* noted that people with disabilities were commonly described as 'individuals with limited ability'. He suggested rephrasing 'recourses being generally available' to 'resources being attainable and usable'.

192. *Ms Rodríguez de Las Heras Ballell* noted that considering accessibility from a discriminatory point of view related to the registry system as a whole. The registry system should be accessible because it was affordable and because the technology was available to everybody. However, in the context of EBRs, accessibility could be seen from a technological point of view and focused on the part of information being available even for those who have certain limitations. *Ms Gullifer* agreed with this idea.

193. *Mr Hygate* provided a definition from the W3C Accessibility Guidelines (WCAG) 3.0.<sup>3</sup>, saying that '*Accessibility involves a wide range of disabilities, including visual, auditory, physical speech, cognitive language, learning and neurological disabilities*.' *Ms Connell* highlighted that the WCAG also provided that accessibility '*meets the needs of individuals*', which could be considered for the definition.

---

<sup>3</sup> See W3C Accessibility Guidelines (WCAG) 3.0. <https://www.w3.org/TR/wcag-3.0/>, (last accessed 26.09.2024)

194. *Some participants* added that the scope of the Accessibility CPF should also address the use of mobile phones and other devices to access the registry, slow Internet connection, limitations of access to the website, as well as the age and digital literacy of potential users.

195. *Ms Gullifer* highlighted that, given the proposed expansion of the scope of the Accessibility CPF, it should be clear that it did not overlap with the CPF on User-Centred Design and excluded fees, potentially explicitly, as a policy matter.

196. *Mr Wool* raised a point regarding the phrase 'obtain the use' in the definition from the ECR Guide. Given all the technological considerations, the core point remained that everyone should be able to use the asset.

197. Building on the current and the proposed new definitions, *Mr Finnegan* suggested to define Accessibility as '*The property of resources being attainable/usable by all individuals regardless of their abilities and limitations*'. *Mr Wool* agreed that the definition could be a good suggestion if the machine-readable information point previously raised by *Ms Rodríguez de Las Heras Ballell* would be addressed in another CPF in the Guide.

198. *Several participants* queried whether the definition should mention the registry's 'services' instead of 'resources' or 'data/records/content being attainable and usable', as it was not the registry itself that is supposed to be attainable and usable.

199. *Ms Gullifer* suggested to include 'effectively engage' in the revised definition proposed by *Mr Finnegan*, so that it would read '*The property of being able to effectively engage with the system by all individuals regardless of their abilities and limitations*'.

200. *Participants* agreed that the commentary should clarify that Accessibility did not imply that the registry should be accessible to absolutely everyone.

201. *Some experts* suggested to consult profile organisations on the sensitive terminology used in the Accessibility definition and CPF.

202. *It was agreed that it would be useful to consult experts from profile organisations that were working on promoting accessibility on the potential definition of the Accessibility CPF. The latest draft definition that was proposed was 'The property of being able to effectively engage with the system by all individuals regardless of their abilities and limitations'. The commentary should clarify that Accessibility did not imply that the registry should be accessible to absolutely everyone.*

#### Discussion on Continuous Improvement CPF

203. *Ms Tarailiene* proposed that the CPF should be titled 'Continual Improvement' instead of 'Continuous Improvement' to align with the standard ISO terminology and indicate cyclical, regularly repeated access rather than a constant, uninterrupted process of changes. It would presuppose systematically identifying areas for enhancement and monitoring results to ensure effectiveness.

204. Participants supported this proposed change.

205. *It was agreed to change the CPF on Continuous Improvement into Continual Improvement.*

#### Discussion on the publicly available information on the registries

206. *Ms Mauro* recalled discussions during the sixth and seventh workshops on this matter. Those discussions had centred around the content, purpose, and challenges associated with business registries. Participants had discussed that registries should contain information related to a business's lifecycle, including establishment, operations,

termination, and changes. The goal was to provide legal certainty and reduce transaction costs by offering a one-stop shop for relevant information. It was reiterated that the standards should be framed exclusively as best practices for ERBs regardless of the legal requirements they were subject to.

207. Another key challenge highlighted in the previous workshops on publicly available information was the tension between transparency requirements and confidentiality. A recent EU ruling on beneficial ownership registries had underscored this conflict, as some information could not be publicly accessible. This has led to varying responses across European countries, complicating efforts to establish a uniform definition of legitimate interest.

208. The discussions had also touched on the interplay between EBRs and other regulatory frameworks, such as anti-money laundering and sanctions regimes. Participants had noted that while the EU ruling primarily affected beneficial ownership information, broader transparency requirements remained in place for other types of data.

209. *Mr Tirado* welcomed the discussion on the comparative perspective regarding the best practices related to the information that business registries make publicly available and invited the participants to express their views on the feasibility of a single point of entry, potentially through interoperability.

210. *Ms Gullifer* identified two main aspects: (i) what was registered in an EBR and (ii) what was publicly available for searching, taking into account transparency, privacy, and confidentiality concerns.

211. *Mr Tirado* added that a perfect EBR would have all the information in one place, but there were many instances where several registries existed, and adequate interoperability could be a good way of addressing this.

212. *Mr Hygate* noted that the list of core elements that had been drawn up in previous workshops - which contained the business type, name and address, the constitutive document(s), the powers of attorney, the shareholders and beneficial owners, the financial accounts and annual returns - should also include officers of the company as important information unless this is what was meant by 'the powers of attorney'.

213. *Mr Wool* suggested having an annexe covering paragraph 76 of the sixth workshop report to outline the list of contents of EBRs, adding more utility to the discussion. Regarding 'the powers of attorney', this indeed seemed to relate to the officers and directors. *Mr Tirado* expressed his support for keeping 'the powers of attorney' on the list as a way of reflecting the ability to represent the business in a certain area or with regard to certain assets. *Mr Wool* agreed.

214. *Ms Gullifer* asked whether a legal comparison was expected on the matter, given that the requirements might vary significantly from one jurisdiction to another. *Mr Wool* noted that a list of minimal information to be made public could be drawn up even if it was not required by the legislation.

215. *Mr Lamb* agreed with the impact of the transparency agenda on the information contained in EBRs. Most business registries contained basic information on their registers and now needed to include beneficial ownership information as well. Anti-money laundering standards prescribed full transparency and regularly updated the standards to address any loopholes against it. Thus, the best practice for EBRs should reflect the transparency agenda and list the basic information to be made public, whether they are required to do that by their jurisdiction or not.

216. *Mr Lamb* elaborated on FATF requirements and risk measurements and encouraged taking an aspirational and progressive approach in this case, even if, in some jurisdictions,

it might not be feasible for registers to comply with the full list of information to be included in the Annexe to the Guide.

217. *Mr Wool* agreed that there was a trend toward more disclosure, broadening the use of information on the EBRs. He noted that in a strict understanding of the EBR functions, the beneficial owners were not that important, while those larger uses mentioned before became essential. He queried whether the annexe should list an absolute minimum of items or be aspirational. While it needed to be clear that registrars were not prevented from designing a system that met more than the minimal requirements in their jurisdiction, some best practices with the broader aspirational approach could be suggested.

218. *Mr Lamb* clarified that FATF required beneficial ownership information to be put on the registry, but it did not prescribe whether that should be made private or public as long as it was accessible to the competent authorities.

219. *Ms Gullifer* suggested that a recommendation could be made to the jurisdictions to develop these disclosure requirements. It would also be important to clarify in the Annexe to the Guide whether all CPFs from the Guide applied to the publicly available information, particularly those on Availability and Accessibility.

220. *Mr Wool* asked whether the publishing of financial accounts was sensitive for public or private companies. *Mr Hygate* referred to the International Business Registry survey and noted that 13-15% of registries did not capture the accounts. *Mr Lamb* pointed out that while some registries were not required to capture and publish financial accounts, it could be done as a form of national risk assessment. *Ms Hillman-Weir* stated that these requirements differed across jurisdictions.

221. *Mr Wool* suggested arranging a virtual intercessional workshop on this topic to discuss the potential content of the Annexe further.

222. *It was agreed to organise a virtual intersessional workshop to discuss this topic further and agree on the content of the envisaged Annexe to the Guide.*

#### General remarks

223. If some of the agreed changes and updates were also applicable to the Guide on ECRs, they would need to be reflected in the latter.

224. The Directors would decide on the detailed timeline, but the participants were informed of the following:

- a. A final version of the draft Guide would be prepared and presented at the next workshop (it could then be reviewed line by line and finalised).
- b. An intersessional meeting would be organised to further discuss the matter of what information should be made publicly accessible in EBRs.

\*\*\*

225. *The CTCAP Directors thanked all the participants for their valuable input and closed the meeting.*



**ANNEXE 1****Agenda**

An initiative under the auspices of the Town Convention Academic Project

Project Leads:



Founding Sponsor:



Supported by:



**8<sup>th</sup> Workshop on  
Best Practices in the Field of Electronic Registry Design and Operation  
Draft Agenda  
16 September 2024**

*UNIDROIT, Via Panisperna 28, 00184, Rome,  
and online via Zoom*

\*\* all times are in Central European Summer Time (CEST), UTC +2 \*\*

Chairs: Professor Louise Gullifer, Professor Jeffrey Wool, Professor Ignacio Tirado (CTCAP Directors)

09:00 - 09:10	Opening of the Session <i>CTCAP Directors</i>
09:10 - 09:20	Project background, summary of intersessional work and presentation of the working paper <i>UNIDROIT Secretariat and Ieva Tarailiene</i>
09:20 - 10:00	<i>Agenda item No. 1:</i> Discussion on the Access Control CPF and the proposal to remove the new CPF on Authorisation
10:00 - 10:45	<i>Agenda item No. 2:</i> Discussion on the Accuracy CPF
10:45 - 11:00	<i>Coffee break</i>
11:00 - 11:45	<i>Agenda item No. 3:</i> Discussion on the Correctability CPF
11:45 - 12:30	<i>Agenda item No. 4:</i> Discussion on the proposal to merge the Disposition, Integrity and Retention CPFs into a new CPF on Records Management
12:30 - 13:00	<i>Agenda item No. 5:</i> Discussion on the Evidentiary Value CPF
13:00 - 13:45	<i>Lunch break</i>
13:45 - 14:30	<i>Agenda item No. 6:</i> Discussion on the proposal to subsume Standardisation under the Interoperability CPF
14:30 - 15:15	<i>Agenda item No. 7:</i> Discussion on the Timeliness CPF
15:15 - 15:30	<i>Coffee break</i>
15:30 - 16:15	<i>Agenda item No. 8:</i> Discussion on the proposal to replace the CPFs on Validation and Verification with the new CPFs on Data Validation and Software Testing
16:15 - 17:00	<i>Agenda item No. 9:</i> Discussion on the Risk Management CPF in the context of recent events
17:00 - 17:20	Open discussion, summary and next steps
17:20 - 17:30	Closing Remarks <i>CTCAP Directors</i>

**ANNEXE 2****List of registered participants**

1. Louise Gullifer (University of Cambridge)
2. Ignacio Tirado (UNIDROIT)
3. Jeffrey Wool (Aviation Working Group, UNIDROIT, Trinity College Dublin, Hebrew University)
4. William Brydie-Watson (UNIDROIT)
5. Myrte Thijssen (UNIDROIT)
6. Theodora Kostoula (UNIDROIT)
7. Benedetta Mauro (UNIDROIT)
8. Kateryna Bovsunovska (UNIDROIT)
9. Ieva Tarailiene (NRD Companies)
10. Rob Cowan (Aviareto)
11. Denis Finnegan (Aviareto)
12. Caroline O'Brien (Aviareto)
13. Michael Choi (Aviareto)
14. Angela Sazdova Doneva (Central Register of The Republic of North Macedonia)
15. Maureen O'Sullivan (Companies Registration Office)
16. Katarzyna Connell (ERS)
17. Stephanie Quaile (ERS)
18. Justin Hygate (Foster Moore)
19. Julian Lamb (Foster Moore)
20. Marco Vianello (Infocamere)
21. Kathy Hillman-Weir (ISC)
22. Laurel Garven (ISC)
23. Teresa Rodriguez De Las Heras Ballell (Universidad Carlos III de Madrid)
24. Andrea August (World Bank)
25. Siret Neeve (Civil law and registers division, Legal Policy Department, Ministry of Justice of Estonia)
26. Alexis Lupo (IACA)
27. Silverio Espinola (ICAO)
28. Pier-Olivier Turcot (ICAO)
29. Monica Canafoglia (UNCITRAL)