WORKING PAPER
on
Best Practices for Electronic Collateral Registries

Prepared by

NatLaw

20 JUNE 2021

BEST PRACTICES FOR ELECTRONIC COLLATERAL REGISTRIES

Contents

I. INTRODUCTION

This Working Paper on Best Practices for Electronic Collateral Registries has been produced as part of the **Best Practices in the Field of Electronic Registry Design and Operation project** (BPER project, or the Project). The BPER project is a joint undertaking by the Cape Town Convention Academic Project, in partnership with the UNIDROIT Foundation, Aviareto, and the Aviation Working Group. Aviareto is a Dublin-based joint venture between SITA and the Irish Government which operates the International Registry, as established under the Protocol to The Convention on International Interests in Mobile Equipment on Matters Specific to Aircraft Equipment (Aircraft Protocol).

The Project initially emerged out of the Cape Town Convention on International Interests in Mobile Equipment (the CTC, or the Convention), which provides for the establishment of international registries for interests in different categories of equipment covered by the respective Protocols. Article 28 of the Convention sets out a standard for the responsibility of registrars for losses resulting from a 'malfunction' caused by 'inevitable and irresistible' events but also provides a defense where 'best practices in current use' in the field of electronic registry design and operation have been followed. However, 'best practices in current use' in electronic registries is not defined by the CTC, nor have international parameters been identified.

A. SCOPE: ELECTRONIC COLLATERAL REGISTRIES (ECR)

Electronic registries have emerged as a central element of systems that collect, store, and disseminate data, and, in some cases, establish and transfer property rights. Even though the relevant laws may not require the use of best practices, registrars may be held responsible for various failures that have caused losses to the users. This Working Paper examines best practices in current use in the field of electronic registry design and operation, focusing specifically on electronic collateral registries (ECRs).

ECRs encompass registries for notices of security rights, and similar publicity mechanisms that perform the following three core functions. First, they allow secured creditors and other claimants to make registrations (submit notices for registration) to render their security rights and other interests in assets effective against third parties ('perfection'). Second, the time of registration is the priority point for the security right when competing against other interests and claims to the same asset. Finally, they provide information to searchers who may be the same secured creditors and other parties, including prospective buyers of assets.

The ECRs that are the focus of this Working Paper should be understood broadly. They encompass registries for notices of security rights as envisaged in the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Secured

Transactions, a global standard for secured transactions legal and registration regimes, or the CTC, but also electronic registries established for the registration of notices relating to a specific type of transaction, such as finance leases or assignments of receivables to a factoring company.[1] While these are generally notice-based registries, many ECRs require the submission of an instrument that creates a right in property. The recommendations of this Working Paper apply to those types of ECRs, but, where necessary, additional considerations should be taken into account by the designers and operators. Given the variety of these systems, these considerations are not explored in this Working Paper.

Having in mind a broader focus of the overall project, the recommendations and the analysis below may equally apply to registry systems functionally similar to collateral registries operated by public entities. Those include motor-vehicle registries, intellectual property registries, and companies registries that in many jurisdictions register security rights, in addition to performing other functions. These registries typically include a user interface, such as a webpage or application that allows users to submit registrations and perform searches, and a database that stores information relevant to the perfection of security rights, but also additional data, such as user account information. The lessons drawn from this Working Paper should be adaptable for use in systems that affect the rights of third parties, such as credit referencing systems that complement the functions of collateral registries within the broader credit infrastructure. However, some of these recommendations may need to be adapted to private registries, such as those for the issuance and transfers of electronic equivalents of documents of title, chattel paper and instruments.[2] Further adaptation may be necessary for systems that operate without any centralized authority where records are maintained on a distributed ledger (blockchain).[3]

---

[1] Several countries have established such registries, including Jordan and Palestine. Factoring is an important form of financing — in 2019, global factoring volume reached 2.9 trillion euros. In 2020, UNIDROIT began work to develop a Model Law on Factoring, in careful coordination with UNCITRAL's work in this field. The purpose of the Model Law is to provide an instrument for States that want to introduce a new factoring law or update their existing laws but are not yet in a position to undertake comprehensive secured transactions law reform. *See* https://www.unidroit.org/work-in-progress/factoring-model-law, (last accessed Dec. 28, 2020).

[2] For instance, a different confidentiality standard may apply to such systems since they are not commonly accessible to third-party searchers. *See* further Charles W. Mooney, Jr., FinTech and Secured Transactions Systems of the Future, 81 Law & Contemp. Probs. 1, 8-10 (2018). For electronic registries covering electronic documents of title, *see generally*, Marek Dubovec, *The Problems and Possibilities for Using Electronic Bills of Lading as Collateral*, 23 ARIZ. J. INT'L & COMP. L. 437 (2006).

[3] *See generally*, Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series – Note 1: Collateral Registry, Secured Transactions Law and Practice (World Bank Group, May 2020), https://openknowledge.worldbank.org/bitstream/handle/10986/34007/Collateral-Registry-Secured-Transactions-Law-and-Practice.pdf?sequence=1&isAllowed=y, (last accessed Dec. 28, 2020); *and see generally*, Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series – Note 2: Regulatory Implications of Integrating Digital Assets and

The purpose of this Working Paper extends beyond the mere identification of the best practices required by Article 28 of the CTC to shield the International Registry from liability. It seeks to provide guidance to the designers and operators of ECRs more broadly, such as for establishing a standard for accountability of registrars rather than for liability. Many laws generally refer to liability for certain actions, omissions and failures in connection with various registry functions, but do not detail any measures that may prevent or mitigate the risk of such occurrences. Many domestic policymakers and legislators opt for full immunity of the registry/registrar from any liability, which may also be attributable to the absence of clear guidance on the various aspects of liability. This Working Paper also aims to assist domestic reform initiatives that seek to establish ECRs as well as those that have already led to their establishment.

B. RESEARCH OBJECTIVES: BEST PRACTICES AND CRITICAL PERFORMANCE FACTORS (CPFS) FOR ECRS

This Working Paper aims to identify best practices that exclude or mitigate the risks and liabilities faced by ECRs in performing their core functions. In addition, best practices ensure, among others, that the system is continuously available and accessible to all users, and suitable for their needs, regardless of sophistication.

In the context of systems, the concept of best practice most commonly arises in management of organizations and manufacturing, where a set of actions can be related to resulting outcomes.[4] Determining a best practice, therefore, requires a comparison of actions and outcomes where there is a known causal relationship between the action and the outcome.[5] Moreover, in order to determine the best practice, the comparison must include all comparable cases of the relevant type otherwise the best practice might not have been actually considered.[6] Importantly, to be comparable, whether statistically or on the basis of human judgment, the causal relationships between actions and outcomes must be quantifiable on a scientifically sound basis.[7]

In practice, the above stated necessary conditions to confidently identify the best practice are rarely all attainable simultaneously.[8] Furthermore, each style of research, whether

---

Distributed Ledgers in Credit Ecosystems (World Bank Group, May. 2020), https://openknowledge.worldbank.org/bitstream/handle/10986/34008/Regulatory-Implications-of-Integrating-Digital-Assets-and-Distributed-Ledgers-in-Credit-Ecosystems.pdf?sequence=1&isAllowed=y, (last accessed Dec. 28, 2020).

[4] Stuart Bretschneider et al., "Best Practices" Research: A Methodological Guide for the Perplexed, 15 J. of Public Admin. Research and Theory 307, 307 (2005).

[5] *Id.* at 310.

[6] *Id.*

[7] *Id.* at 311.

[8] *Id.*

economic or technical, tends to produce an incomplete picture with different insights and conclusions.[9] Accordingly, rather than attempt a comparison of existing industry practices, authoritative standards of recommended or mandated practices are often the *de facto* source of best practices. These may be issued by international standards bodies, such as the International Organization for Standardization (ISO), government agencies, such as the National Institute of Standards and Technology (NIST), industrial organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), as well as other organizations with specialized knowledge in the relevant area, including manufacturers and software developers, especially regarding their own products. However, these standards do not cover all relevant aspects of core functions of ECRs.

No studies to identify best practices for ECRs have been produced. However, a survey of database professionals in 40 countries was conducted to determine the sources of best practices and the extent to which they are used.[10] Respondents reported that the most stringently controlled best practices were those related to database security, high availability resilience, and disaster recovery.[11] The survey found that two of the most common sources of best practices were software vendors' websites and industry whitepapers, which predominantly focus on current technology.[12]

Implementation of best practices means that ECRs are:

- Highly available, such that the registry experiences no unscheduled downtime;
- Highly redundant, such that there is no single point of failure (SPOF) and that failure of one or more components and/or datacenters does not make the entire registry inoperable;
- Secure against internal and external threats, so that unauthorized access, tampering, and attacks involving malware and/or denial of service attacks are not possible;
- Protective against the insidious risks posed by human negligence, operational errors, complacency, and false assumptions about technology;
- Capable of addressing natural or human-caused accidents and disasters, such as fires or floods;
- Fully recoverable in the event of a disaster, such that a catastrophic event (e.g. fire, flood, war, terror attack, etc.) impacting one datacenter does not lead to any data loss and a backup can be semi-automatically or automatically provisioned

[9] Michael Cusumano, In Search of Best Practice: Enduring Ideas in Strategy and Innovation, 11, (Oxford Univ. Press, 2010).
[10] Victoria Holt et al, The Usage of Best Practices and Procedures in the Database Community, Information Systems, 49 (2015) 163, 164-68, http://dx.doi.org/10.1016/j.is.2014.12.004, (last accessed Dec. 28, 2020).
[11] *Id.* at 168, 170.
[12] *Id.* at 163-81.

with minimal downtime (e.g. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 0);
- Immutable, such that all entries are tamper proof and that any and all changes can be tracked forensically and verified independently;
- Capable of providing a high level of confidentiality to ensure that information is not disclosed to an unauthorized person, process or device;
- Configured for proper access control policies/procedures;
- Configured to provide adequate monitoring and logging, such that all errors, downtime, and access events are recorded for review and analysis in real-time and/or in the future; and
- Horizontally and dynamically scalable, such that computing and storage resources can be scaled automatically in response to large peaks in system activity and as such, ensure the system does not slow down or cease operation due to overload.

The Project has identified Critical Performance Factors (CPFs) constituting the best practice for ECRs. CPFs are defined as registry system properties and processes without which an ECR is unable to perform its core functions at a level that meets the reasonable expectations of the relevant market participants. From an overarching perspective, CPFs are the characteristics of an ECR that are essential for it to be considered fit for purpose. Following best practices is important, not only to mitigate registry/registrar's liability, but also for ECR performance and reputation instilling confidence in the users.

More broadly, this Working Paper examines the CPFs from the functional perspective by identifying the core elements and functions of registries for which the recommendations would be suitable. For instance, one such function is to ensure that the required information has been provided, but without any verification or validation of that information. An element may be some legal effect that a registration produces, such as with respect to making the right effective against third parties upon registration. This functional perspective enables a broader application of the best practices identified below to the systems that perform functions similar to ECRs, such as a centralized registry to give public notice of transactions involving transferable documents in electronic form (e.g. an electronic warehouse receipt) under the UNCITRAL Model Law on Electronic Transferable Records.[13] Other types of registries, such as one based on blockchain, may not require all of the CPFs identified in this Working Paper (such as Legal Authority of the Registrar). Others may also require additional CPFs beyond this Working Paper's scope, such as land registries that require scrutiny of documentation that purports to transfer property rights.

[13] *See* UNCITRAL Model Law on Electronic Transferable Records (2017), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records, (last accessed Dec. 28, 2020).

C. LEGAL RELEVANCE OF BEST PRACTICES

Collateral registries are established and operate pursuant to various types of legal frameworks. Those include i) international conventions (e.g. the International Registry under the Aircraft Protocol to the CTC); ii) federal laws (e.g. the Australian Personal Property Securities Register); iii) state/provincial laws (e.g. the Canadian Personal Property Security Interests Registries); or iv) laws that contemplate multiple registries (e.g., under the 2011 OHADA Uniform Act Organizing Securities).

While the focus of the Project has been to develop best practices and associated CPFs related to the technical aspects of design and operation of ECRs, a sound legal foundation is essential for any registry system. Registrations in ECRs render property rights in the form of encumbrances and transfers of property rights effective against third parties and establish a priority for those rights, which may not be the case for other electronic registries. Legal frameworks provide ECRs with authority and credibility that foster their use and reliance on their services.

Generally, applicable legislation mandates that the operator of the ECR ensure the provision of prescribed services/core functions. Failure to perform some of those functions may trigger liability of the operator/registrar. However, legislation may or may not provide clear rules detailing the consequences of registry failures. In some States, the registrar may enjoy full immunity from any sort of failure while in others the registrar may be liable for some failures. Many States that have recently implemented collateral registries choose the full immunity approach. This approach may raise concerns in the financial sector that it would preclude any claims against the registrar in case of a loss sustained by inadequate performance of the system. Consequently, deployment of the reformed framework may be disincentivized. In contrast, other regimes subject registries to a variety of liability standards.

Some registries' processes remain manual, but most registries today operate exclusively electronically. Recommendation 56 of the UNCITRAL Legislative Guide on Secured Transactions, adopted in 2007, contemplates a hybrid access and for the liability of such a system, it provides the following:

> "The law should provide for the allocation of responsibility for loss or damage caused by an error in the administration or operation of the registration and searching system. If the system is designed to permit direct registration and searching by registry users without the intervention of registry personnel, the responsibility of the registry for loss or damage should be limited to system malfunction."

Differently, the CTC in Article 28 provides:

> "The Registrar shall be liable for compensatory damages for loss suffered by a person directly resulting from an error or omission of the Registrar and its officers and employees or from a malfunction of the international registration system except where the malfunction is caused by an event of an inevitable and irresistible nature, which could not be prevented by using the best practices in current use in the field of electronic registry design and operation, including those related to back-up and systems security and networking."

Article 28 thus provides for:

1) liability for error or omission by the Registrar or its officers;
2) liability for malfunctioning caused by ordinary events which are not of an inevitable or irresistible nature; and
3) no liability for system malfunctioning caused by an event of an inevitable and irresistible nature if such malfunctioning occurred despite the adoption of best practices in the design and operation of electronic registries.

The CTC establishes that the Registrar owes compensatory damages for losses stemming both from errors or omissions of its employees and malfunction caused by events that are neither inevitable nor irresistible in nature. This liability is strict: it arises regardless of fault, negligence or malice, and cannot be excluded or limited. The Registrar is required to procure adequate insurance as determined pursuant to the respective CTC Protocols. By contrast, for losses stemming from events that are inevitable and irresistible in nature, the Registrar is spared liability if it can show that it had adopted best practices in current use in the field of electronic registry design and operation. The relevant best practices contemplated by the CTC include those related to back-ups, system security, and networking.

The liability matrix articulated by Article 28 of the CTC markedly incentivizes the adoption of best practices. The Registrar will seek to implement such practices to escape liability for losses stemming from events that are inevitable and irresistible in nature. Furthermore, the Registrar will want to implement best practices to avoid human errors or omissions, and to prevent malfunctions due to ordinary events, as liability for losses stemming for such events is strict.

In the context of design and operation of an ECR, the liability can arise from events in three domains:

a) errors or omissions by the Registry officers and contracted third parties (operation only);
b) hardware failure (design and operation); and
c) software failure (design and operation).

Examples of avoidable malfunctions in these domains include: a) human error by an officer manually entering a court order to discharge a registration; b) hardware failure that could have been prevented by implementing a design incorporating redundant hardware; and c) a software programming error that could have been discovered by off-line system testing prior to deployment.

Consider the hypothetical example of a major software vendor that issues a critical update to its widely used software in response to cyberattacks that exploit a previously unknown software vulnerability to gain unauthorized access to data. The registrar receives notification of the update before the registry is affected but fails to install it before a cyberattack accesses, downloads, modifies, and deletes data stored in the registry database. The cyberattack was enabled by a software design fault (domain c) that (for purposes of this example) could not have been prevented even if the registrar followed best practices before the vulnerability was made public. However, failure to respond to announcement of the vulnerability by taking practicable preventive measures may well be an error or omission and not adhering to the software provider's advisory to install the critical software update may constitute a failure to follow best practices. Therefore, in this example, where the registrar could have prevented the cyberattack by promptly installing the software update, the registrar may be subject to the first type of liability for harm caused by the cyberattack.

The worst-case scenario is one in which a system error or inadequacy (e.g. in the implementation of the process for authenticating registrants) is not discovered until identified by an expert witness during legal proceedings.[14] Such an event could raise uncertainty regarding not only any registrations performed by the relevant user, but all registrations by any user.[15]

The objective of this Working Paper is to clarify the meaning of best practices in the context of ECRs, as the liability of this kind may arise in the context of any ECR. In doing so, the Working Paper draws on the earlier work of the Project.[16] Section II describes the 17 CPFs identified as best practice for ECRs. Section III identifies relevant technical standards, and Section IV discusses risks to ECRs. Section V concludes.

---

[14] Rob Cowan & Donal Gallagher, The International Registry For Aircraft Equipment—The First Seven Years, What We Have Learned, 45 UCC L. J. 225, 249 (2014), https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan-Gallagher.pdf, (last accessed Dec. 28, 2020).

[15] *Id.*

[16] *See* Aaron Ceross, *Practices in Electronic Registries*, (Interim Report, Spring 2018), this report was conducted within the framework of the "Best Practices in the Field of Electronic Registry Design and Operation" Project run by the Commercial Law Centre at Harris Manchester College, University of Oxford, *see* https://www.law.ox.ac.uk/research-subject-groups/best-practices-field-electronic-registry-design-and-operation, (last accessed Dec. 28, 2020).

II. CRITICAL PERFORMANCE FACTORS

This Section provides definitions and detailed descriptions of the CPFs and explains their relevance to ECRs. Table 1 lists each CPF accompanied by a definition. Most of the CPFs have both legal and technical aspects, but some are purely technical while others are solely legal in nature. Thus, for many CPFs the descriptions include a technical discussion with references to international standards, and a discussion that references legal standards and provides examples of relevant laws as well as the CPF's application to the International Registry. For other CPFs, the discussion is limited to the technical or legal aspect. For more on international standards, as well as industry standards, see Section IV below.

Table 1: CPF definitions (in alphabetical order)

CPF	**Definition**
1. Access Control	The process of ensuring that access to the registry is authorized and restricted.
2. Accessibility	The property of being able to obtain the use of a resource.
3. Authentication	The process of verifying that a person is who they claim to be.
4. Availability	The property of being accessible and usable upon demand by an authorized person.
5. Confidentiality	The property that information is not made available or disclosed to unauthorized persons.
6. Continuity	The property of delivering registry services at acceptable levels within acceptable timeframes following a disruptive incident.
7. Disposition (Disposal)	The process implementing disposal of records: retention, archiving, destruction and transfer decisions.
8. Integrity	The property that data has not been altered or destroyed in an unauthorized manner.
9. Interoperability	The property of having interfaces to communicate with, or transfer data among systems (e.g. other registries) in an automated manner that does not require the user to be extensively familiar with the operation of the other systems.
10. Legal Authority and Compliance	The property of ensuring that the registry is established pursuant to and operates in compliance with a sound legal framework.
11. Legal Authority of the Registrar	The property that the registrar may exercise certain powers pursuant to a legal authority, including in the process of eliminating a detected failure.

12. Reliability	The property of performing required functions for a specified period of time.
13. Retention	The property of preserving data in a system for a specified period of time.
14. Timeliness	The property of making a registration publicly searchable, and therefore effective, almost instantly after its submission.
15. Trustworthiness	The property of providing confidence to users and third parties that the registry performs its core functions at a level that meets or exceeds their reasonable expectations.
16. User-Centered Design	The property that the approach to the design and development of the registry aims to make the registry more usable by focusing on how the registry is used and applying human factors/ergonomics and usability knowledge and techniques.
17. Validation	The process of confirming, using objective evidence, that the requirements for a specific intended use or application have been fulfilled.

1. Access Control

Definition: The process of ensuring that access to the registry is authorized and restricted.

Access Control encompasses the processes that limit a user's access rights and privileges within the registry after it has been authenticated by the registry (i.e. after determining that the user is in fact who it purports to be – see Authentication *infra*). The user is not only a person that submits information for registration, but also a technician with access to the hardware. Access Control applies to all methods of user access, whether directly, through Interoperability with other registries, through Application Programming Interfaces (APIs), or intermediaries, as well as to physical access, such as by a technician using an ID card.

When a user creates an account or is initially authenticated, its access rights and privileges are granted according to registry rules. Minimal privileges, such as the right to search for registrations, may be granted without authentication or the need to create an account. Upon each attempt to access registry functions, such as submitting a registration, Access Control processes assess whether the user has the right to access those registry functions and data.

This CPF encompasses both electronic access and physical access to the registry hardware. Electronic Access Control (e.g. server-side database permission verification) occurs whenever the user attempts to access a registry function or process such as viewing or entering data. Physical Access Control is ensured through multifarious

security measures. These include personnel identification badges, closed-circuit television, biometric access sensors, locks and any other form of structural solution that prevents unauthorized actors from gaining material access to registry data or its infrastructure.[17]

Various measures can be implemented to counter attempts to gain unauthorized access, including automatically terminating sessions that are inactive for a certain period of time and using technology such as CAPTCHA to identify automated intrusive attempts.[18] An Access Control strategy should also address the threat of harm by a 'trusted insider' whose authorized access is used either maliciously or negligently. Pre-employment, and ongoing screening, and training of trusted insiders (including employees, contractors, and vendors who have access to the registry) is essential. A study of 7,800 publicly reported breaches of information systems between 2012 and 2017 found that 50% of breaches involved insiders.[19] Negligence accounted for 44% of insider breaches.[20] To minimize such risks, access authorization should not exceed what is necessary for an employee's authorized tasks.

Knowledge of employees' background is vital to understanding who is being given access to confidential information. In particular, the super-users that have administrative rights to access data should undergo reasonable levels of scrutiny. Employee screening should be an ongoing requirement, for instance, an employee's financial obligations may change over time and might motivate illicit use of registry data.

Auditing and logging are critical components of Access Control. Audit logs of all user and staff access and operations should be maintained for monitoring activity and diagnosing breaches. Audit controls and audit trails are important tools for addressing issues such as fictitious and fraudulent registrations and collusion between, for example, a database analyst and a bad actor to change information in the registry.

Overarching all of the above measures are governance policies and arrangements, such as for ongoing updating of software, maintenance of physical access, and revoking of access permissions for former employees.

Technical

[17] *See* Knowledge Guide: Secured Transactions, Collateral Registries and Movable Asset-Based Financing, 75, (IFC, Nov. 2019) (*IFC Knowledge Guide*), at 84, http://documents.worldbank.org/curated/pt/193261570112901451/pdf/Secured-Transactions-Collateral-Registries-and-Movable-Asset-Based-Financing.pdf, (last accessed Dec. 28, 2020).

[18] CAPTCHA is the acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart." To continue a session, users must correctly identify numbers or letters contained in randomly generated CAPTCHA images.

[19] *See* https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk, (last accessed Dec. 28, 2020).

[20] *Id.*

ISO 27000:2018 defines Access Control as ensuring that access to assets is authorized and restricted based on business and security requirements.[21] Annex 9 of ISO 27001:2013 sets out requirements for Access Control standards, including, among others, access control policies, management of privileged access rights, and secure logon procedures to prevent unauthorized access to systems and applications.[22]

The National Institute of Standards and Technology (NIST) recommends that all U.S. federal government information systems enforce access control policies that limit access to authorized users.[23]

Legal

Secured transactions laws and regulations implement Access Control requirements in several aspects. For instance, only authorized persons may gain access to the registry to submit registrations, such as under section 46(3) of the Ontario's Personal Property Security Act.[24] Furthermore, some laws require that only authorized secured creditors may submit effective amendments and cancellations, as contemplated in article 5(2) of the Model Registry Provisions of the UNCITRAL Model Law.

International Registry

Regulation 4.1 of the International Registry (IR) provides that, with the exception of access to conduct searches, no registry user entity, or its administrator, may access the IR without the approval of the Registrar. The Registrar shall approve access when it reasonably concludes, without conducting specific legal analysis i) that the prospective registry user entity and its administrator are who they claim to be; and ii) that the prospective administrator is empowered to act as administrator of the entity user. Accordingly, the Registrar is entitled to collect identity information and contact information from each applicant before granting access. With regard to users seeking access to conduct searches only, the Registrar must collect contact information to be able

[21] ISO/IEC 27000:2018 § 3.1.

[22] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, (last accessed Dec. 28, 2020); *and see* https://www.isms.online/iso-27001/annex-a-9-access-control/, (last accessed Dec. 28, 2020).

[23] *See* Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017), App. D., https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf, (last accessed Dec. 28, 2020).

[24] Personal Property Security Act, R.S.O. 1990, c. P.10, 46(3). Similarly, Australia's registry (Personal Property Securities Registry) requires users to first create an account before submitting registrations, *see* Your business guide to the Personal Property Securities Register (PPSR), 17–18, https://www.ppsr.gov.au/sites/default/files/2020-07/PPSR%20Business%20Guide_1.pdf, (last accessed Dec. 22, 2020).

to fulfil the requirements of Regulation 5.17 should they arise.[25] Regulation 4.2.1 requires guest users to provide a valid electronic address at which they can be contacted, and which must be automatically verified, before they are granted access to the IR.[26]

2. Accessibility

Definition: The property of being able to obtain the use of a resource.

The design and operation of a registry system should ensure that all its potential users can fully engage with the system, without the need for special technical instruments, skills or knowledge. For access to international registries, cultural and linguistic heterogeneity of users should be considered, as well as network communication challenges stemming from geographical and temporal (time zones) diversity. Accessibility should also be considered from the economic perspective encompassing the element of cost – any fees, whether for registration or searches, should be set at a level that facilitates Accessibility.[27]

While registry systems may impose some restrictions on Accessibility, they should not require persons who wish to submit a registration or conduct a search to provide justifications for their actions to either the registrar or other authority. This is not inconsistent with the requirements imposed by some ECRs that condition access to the search function to those with some 'authority' to ensure that the search is conducted for an appropriate purpose.[28]

Access to ECRs should be generally provided through the Internet. Where that might be challenging, off-line versions might need to be provided where registrations are uploaded in batches at the end of the day. Further access channels should include the ability to submit registrations through APIs and direct data transfers, without interacting with the registry website. A number of ECRs feature business to government (B2G) APIs that businesses can integrate into their own software to directly access registry web

[25] Following a correction to a registration caused by a malfunction in the IR, Regulation 5.17 requires the Registrar to promptly give notice to, inter alia, 'those who have conducted a priority search on [the affected] aircraft object since the time of the original registration.' *See* Regulations and Procedures for the International Registry, Reg. 5.17, ICAO (2019).

[26] *See* Regulations and Procedures for the International Registry, Reg. 4.2.1, ICAO (2019).

[27] The registry should be granted some flexibility to adjust fees to incentivize accessibility in the face of changing market conditions. *See* U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, U.N. SALES NO. E.09.V.12 (2010) at 158.

[28] For example, where a search is made against an individual grantor, Part 5.5, section 172, of the Australian Personal Property Securities Act requires that the searcher must either have the individual's consent or an 'authorised purpose' defined in the Act. Authorised purposes include, inter alia, needing to decide whether to provide credit or to determine whether personal property is subject to an existing security right. *See* https://www.ppsr.gov.au/searching/do-individual-search, (last accessed Dec. 28, 2020).

services.[29] Expectation and demand for these types of interfaces to ECRs will increase as more users adopt legaltech and fintech technology. Where access is provided through intermediaries, the registrar should ensure that the intermediaries have registry access equivalent to that available to direct users. The registrar does not assume any liability for 'telecommunication risk' where the means of access used fail to deliver the record to the ECR.[30]

Equal access is important and may be legally required in some jurisdictions (e.g. for sightless users and users with limited intellectual ability). The Web Content Accessibility Guidelines (WCAG) provide recommendations for making websites more accessible to a wide range of people with disabilities.[31] Following these guidelines will also often make Web content more usable in general.[32] The guidelines are based on four principles that are the foundation for website Accessibility. They must be i) perceivable, ii) operable, iii) understandable, and iv) robust.[33]

Accessibility can be challenging in areas with prolonged power outages (e.g., unpredictable load shedding) or no internet access or intermittent access. Requirements of equal access for all users, whether in rural areas, or those without access to a computer or the internet, may be met by providing kiosks to accommodate walk-in and infrequent users. One challenge may be financing the significant costs of these facilities, which may be used infrequently.

Excessive registry fees can pose a barrier to Accessibility. ECR fees that may be reasonable for registration of an interest in a high value asset, such as an aircraft, may be excessive for registrations of interests in assets of lesser value such as those likely to be owned by SMEs. An ECR must cover its own costs, including the future replacement of its infrastructure, including hardware and software to ensure its effective continued operation – but no more than what such costs require. Where a public registry is operated by a for-profit private entity, the allowed profit should not exceed the value of the realized increased efficiency.

Technical

Various technical standards apply to different forms of Accessibility. APIs use industry standard protocols such as SOAP (Simple Object Access Protocol) over HTTPS

[29] For example, the Australian Personal Property Security Register (PPSR) and the Texas UCC registry offer SOAP APIs. *See* https://www.ppsr.gov.au/b2g-hub, (last accessed Dec. 28, 2020); *and see* https://direct.sos.state.tx.us/help/help-ucc.asp?pg=ucc_ws, (last accessed Dec. 28, 2020).

[30] CTC Official Commentary 2.199(b) (4th ed. 2019).

[31] *See* Web Content Accessibility Guidelines (WCAG) 2.1, (W3C, 2018), https://www.w3.org/TR/WCAG21/#abstract, (last accessed Dec. 18, 2020).

[32] *Id.*

[33] *See* WCAG 2.1 at a Glance, https://www.w3.org/WAI/standards-guidelines/wcag/glance/, (last accessed Dec. 18, 2020).

(Hypertext Transfer Protocol Secure).[34] The Australian PPSR and the Texas UCC filing office provide SOAP APIs that businesses can integrate into their own software to more efficiently access the system.[35] IACA (the International Association of Commercial Administrators) supports a standard XML (Extensible Markup Language) format recommended for transmitting electronic registrations to UCC filing offices.[36] UCC filing offices that support this filing method use a batch process to register multiple notices contained within each XML file.[37] ISO 40500:2012 [Web Content Accessibility Guidelines (WCAG) 2.0] provides a wide range of guidelines and recommendations to make content accessible to a wider range of people with disabilities.[38]

Legal

The UNCITRAL Legislative Guide contemplates a registry that maintains electronic records that are publicly accessible from any location where internet access is available.[39] Both the UNCITRAL Legislative Guide and the UNCITRAL Guide on the Implementation of a Security Rights Registry (UNCITRAL Registry Guide) recommend that a searcher should not be required to give reasons for the search.[40] The UNCITRAL Legislative Guide recommends that registration and search fees should not be used to raise revenue but rather be set purely on a cost-recovery basis.[41]

Section 190 of the Australian Personal Property Securities Act (2009) authorizes the Attorney-General to determine registry fees, which are calculated to recover 100% of

[34] *See* Interoperability, *infra* II(9).

[35] *See* https://www.ppsr.gov.au/b2g-hub, (last accessed Dec. 28, 2020); and see https://direct.sos.state.tx.us/help/help-ucc.asp?pg=ucc_ws, (last accessed Dec. 28, 2020).

[36] *XML Technical Specifications for Uniform Commercial Code Filings Revised Article 9 - Version 4.00*, IACA (2019), https://www.iaca.org/secured-transactions/xml-technical-specifications/, (last accessed Dec. 28, 2020).

[37] Eg., California and Texas. *See* https://uccconnect.sos.ca.gov/help/faqs.asp#benefits, (last accessed Dec. 28, 2020); and see https://direct.sos.state.tx.us/help/help-ucc.asp?pg=ucc_ws, (last accessed Dec. 28, 2020).

[38] *See* ISO 40500:2012 [Web Content Accessibility Guidelines (WCAG) 2.0], https://www.iso.org/standard/58625.html, (last accessed Dec. 18, 2020).

[39] *See* chap. IV, paras. 23-24, Rec. 54 (f), U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, U.N. SALES NO. E.09.V.12 (2010) at 154, 179; *and see* chap. II, para. 90, U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL GUIDE ON THE IMPLEMENTATION OF A SECURITY RIGHTS REGISTRY, U.N. SALES NO. E.14.V.6 (2014) at 35.

[40] *See* Rec 54 (g), U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, U.N. SALES NO. E.09.V.12 (2010) at 179; *and see* U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL GUIDE ON THE IMPLEMENTATION OF A SECURITY RIGHTS REGISTRY, U.N. SALES NO. E.14.V.6 (2014) at 39.

[41] U.N. COMMISSION ON INT'L TRADE LAW, UNCITRAL GUIDE ON THE IMPLEMENTATION OF A SECURITY RIGHTS REGISTRY, U.N. SALES NO. E.14.V.6 (2014) para. 274.

the operational costs of the PPSR, including personnel costs and the amortization costs of software and infrastructure.[42]

International Registry

While the IR can be accessed via public Internet under the URL: http://www.internationalregistry.aero, all users must provide contact information. International Registry Procedure 7.5 conditions access on the user having a valid digital certificate issued by the Registrar, accepting and abiding by the Registry's terms and conditions of use, complying with its Procedures, and paying in advance any required fees.[43] The Aircraft Protocol requires the IR to recover the reasonable costs of establishing and operating the registry by charging fees for its services, yet leaves discretion to the Supervisory Authority[44] regarding the specifics.[45] By contrast, while the Luxembourg Protocol to the Convention on International Interests in Mobile Equipment on Matters Specific to Railway Rolling Stock (Rail Protocol) similarly provides that registry fees shall be determined so as to recover the reasonable costs of establishing, implementing and operating the registry, it does not preclude the Registrar from operating for a reasonable profit.[46]

3. Authentication

Definition: The process of verifying that a person is who they claim to be.

For a number of reasons, including Access Control, the registry may implement mechanisms to verify the identity of a person who seeks to access a registry function. In

[42] *See Cost Recovery Implementation Statement: Personal Property Securities Register, Australian Financial Security Authority (June 21, 2018)* at 3-6, https://www.ppsr.gov.au/sites/default/files/2020-07/Cost-Recovery-Implementation-Statement-2018.pdf, (last accessed Dec. 28, 2020).

[43] IR Procedures must be complied with by all IR users. They address IR Regulations requirements or otherwise relate to IR technical operation and administrative processes. *See* Regulations and Procedures for the International Registry, Reg. 15.1, ICAO (2019).

[44] The Supervisory Authority of the International Registry is the ICAO (International Civil Aviation Organization) Council and the Registrar is Aviareto, *see* CTC Official Commentary at comment 4.128.

[45] *See* CTC Art 17(2)(h) providing that the Supervisory Authority shall "set and periodically review the structure of fees to be charged for the services and facilities of the International Registry"; *and see* Aircraft Protocol Art. XX(3), "[Fees to be charged for the services and facilities of the International Registry] shall be determined so as to recover the reasonable costs of establishing, operating and regulating the International Registry and the reasonable costs of the Supervisory Authority associated with the performance of the functions, exercise of the powers, and discharge of [its duties]"; *and see* Regulations and Procedures for the International Registry, section 13.4 ('Fees shall be established and adjusted by the Supervisory Authority, as required by the Convention and the Protocol.")

[46] Luxembourg Protocol To The Convention On International Interests In Mobile Equipment On Matters Specific To Railway Rolling Stock, Art XVI(2) provides for fees "to recover, to the extent necessary, the reasonable costs of establishing, implementing and operating the International Registry, as well as the reasonable costs of the Secretariat associated with the performance of its functions. Nothing in this paragraph shall preclude the Registrar from operating for a reasonable profit."

the context of an ECR, one of the functions of Authentication is to collect and verify contact information that enables contacting the secured creditor, such as when the debtor requests the discharge of a registration. In some instances, such verifications require manual efforts by registry staff, such as contacting the institution represented by the user, but, to the extent feasible, the Authentication process should be automated (see Interoperability – CPF 9, *infra*). Different levels of Authentication have been used by registry systems.

Authentication of users that interact with a registry may occur at different stages:

1. First, Authentication occurs upon requesting the establishment of a user account. Examples of Authentication techniques include:
    i. Verifying the existence of a company, as well as the accuracy of its name, against a government business registry.
    ii. Verifying an individual's ID against a national ID database.
    iii. Verifying an individual's identity using facial recognition software (for example, by comparing an image captured during registration with an uploaded copy of a government issued photo ID).[47]
    iv. Verifying a user's identity through the services of a remote identity management (IdM) system that provides authenticated user credentials.[48]
2. Secondly, once a user has been provided with access, Authentication may occur every time the user logs in to interact with the ECR. Examples of Authentication techniques include requiring the use of strong passwords and two-factor Authentication (e.g. requiring confirmation of receipt of a text message or email to authenticate a login attempt).

[47] This technique is used by the Global Aircraft Trading System (GATS), *see* http://awg.aero/wp-content/uploads/2020/04/Airline-Economics-Conference-Dublin-accurate-as-of-21-January-2020-website-2.0-change-in-pic.pdf, (last accessed Dec. 28, 2020).

[48] Although IdM systems are currently generally in the nascent stage, under development by governments and the private sector, they promise an alternative authentication method for registries. Electronic KYC (e-KYC) systems have been implemented in India and South Africa. COVID-19 has accelerated development of an EU (eIDAS) e-KYC system. *See e.g.*, Jack Germain, Linux Foundation Leads Initiative for Better Digital Trust, (LinuxInsider, May 5, 2020), https://linuxinsider.com/story/linux-foundation-leads-initiative-for-better-digital-trust-86647.html, (last accessed Dec. 28, 2020); *and see*, Digital Finance Webinar Series: Open Digital Trust Initiative, (Institute of International Finance, Apr. 28, 2020), https://www.iif.com/Events/RSVP-Event?meetingid=%7B8664CE82-B467-EA11-80E6-000D3A0EE828%7D, (last accessed Dec. 28, 2020); Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; *see also*, OpenID Foundation, https://openid.net/foundation/, (last accessed Dec. 28, 2020); *see also*, Fintech for Financial Inclusion: A Framework for Digital Transformation, (AFI, Sep. 2018), https://www.afi-global.org/publications/2844/FinTech-for-Financial-Inclusion-A-Framework-for-Digital-Financial-Transformation, 11, (last accessed Dec. 28, 2020).

3. Authentication may also occur when searching an ECR. Though the system could also be designed to require both an account and login for conducting searches, it needs to accommodate one-time users. Some Authentication is conducted when the search is subject to a fee requiring the user to enter payment details. For ECRs that provide free access, simpler forms of Authentication could be contemplated, such as capturing contact details in the form of an email address.

ECRs may also implement some mechanisms to ensure that a user acting on behalf of an organization is authorized by that organization to use registry functions (for example, an employee of a financial institution creating an account on behalf of that institution). The ECR does not authenticate whether a person attempting to submit a registration has the proper authority under the agency law to do so. The ECR is not responsible when a registration has not been property authorized, whether by the debtor/grantor for an initial registration or by the creditor with respect to an amendment or cancellation. However, the ECR should implement measures to minimize the occurrence of unauthorized registrations that may affect the Reliability (CPF 12, *infra*) of the registry record.[49] Administrative and criminal laws further deter unauthorized and wholly fraudulent registrations by imposing sanctions.

The level of authentication may depend on measures already established by the entity that hosts/operates the ECR, which may be higher, for example, when the host is the Central Bank. It may also vary depending on the type of user – an ordinary commercial entity as opposed to a court that is given access to register a notice relating to a non-consensual interest.

For international ECRs, Authentication techniques should be designed and operated in a manner that is jurisdiction-neutral; forms of identification and any documents necessary for Authentication originating from all relevant jurisdictions should be recognized and accepted on equal footing. For some ECR users, Accessibility of international ID platforms can be problematic due to blocking of access and lack of required software applications. Issues of data privacy may affect the use of national ID systems, as some States have limitations on cross border dissemination of national IDs The IR verifies the user's identity via a digital certificate issued by a certificate authority using Public Key Infrastructure (PKI) technology.[50]

[49] Under Art. 20 of the CTC, registration of an international interest may be by either party but requires written consent of the other party. Likewise, discharge of a registration may be made by, or with the written consent of, the party in whose favor the registration was initially made.

[50] Cowan & Gallagher, *supra* note 14, at 230; PKI uses industry standard protocol (Secure Sockets Layer (SSL) and Transport Layer Security (TLS)) to establish secure communications that, i) authenticates users and machines with digital certificates issued by trusted third parties; ii) encrypts communications and data transmissions by using a secret private key and a mathematically related public key; and iii) assures non-

Authentication should not hinder Accessibility. Accordingly, the administrative and technical burden of the Authentication processes should be designed and adjusted in light of the user base. Furthermore, the first Authentication process should be completed for a significant majority of users before the ECR is launched so as not to delay access to registry functions.

Technical
ISO 9798-1 describes a variety of Authentication protocols that use security techniques to corroborate that a person's identity is as it claims by collection of the relevant information and, where appropriate, verification with a trusted third party.[51]

Legal
Article 7 of the UNCITRAL Model Registry Provisions requires the registry to maintain information about a registrant's identity, but the registry may not verify the registrant's identity as part of the registration process.

International Registry
Regulation 4.1 of the IR stipulates that, with the exception of access to conduct searches, no registry user entity, or its administrator, may access the IR without the approval of the Registrar. The Registrar shall approve access when it reasonably concludes, without specific legal analysis that i) the registry user entity and its administrator are who they claim to be; and ii) the administrator is entitled to act as administrator of the registered entity user.

4. Availability

Definition: The property of being accessible and usable upon demand.

In general, electronic registry systems should be accessible 24 hours a day, every day of the year, which requires both the relevant technology and the necessary human personnel (e.g. technical support, IT personnel) to be available continuously. Continuous Availability includes access to the help desk. In practice, occasional downtime will be necessary for scheduled maintenance and updates, and the inevitability of technical and security interruptions. Security that ensures Integrity of data should generally take priority over Availability but as with Accessibility and Authentication, an appropriate balance must be struck. Availability is less important in the context of ECRs than

repudiation (i.e. provides proof of the origin and integrity of the transmitted data); *See* https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm (last accessed Dec. 28, 2020).

[51] *See* ISO/IEC 9798-1:2010
Information technology — Security techniques — Entity authentication, (ISO 2010), https://www.iso.org/obp/ui/#iso:std:iso-iec:9798:-1:ed-3:v1:en, (last accessed Dec. 28, 2020).

Accessibility and Authentication. However, it is more important for IRs whose users are located in different time zones.

Availability is a measure of the total amount of downtime that can be expected over a given period. Knowing the amount of time that an ECR has not been available (downtime) during a given time period, Availability can be calculated:

Availability = uptime / (uptime + downtime)[52]

The result can be expressed as the percentage of time that the ECR is available. Alternatively, it can be thought of as the probability that the ECR will be available at any given time.[53] For example, Availability of an ECR that was not available for a total of 24 hours (1 day) during the course of 365 days would be:

Availability = 364 / (364 + 1) = 0.997 (or 99.7%)

Technical
ISO 27000:2018 (3.7) defines Availability as the "property of being accessible and usable on demand by an authorized entity."

Legal
Recommendation 5(b) of the UNCITRAL Registry Guide provides for a continuous operation of a registry.

International Registry
International Registry Regulations provide that, "[t]he International Registry shall be accessible 24 hours a day, 7 days a week, except if precluded by maintenance performed outside peak periods, or technical or security problems, as set out in the Procedures."[54] The Procedures state that "Technical support shall be provided to registering persons, searching persons and administrators by a help desk of the International Registry, which shall be available 24 hours a day, 7 days a week, via telephone and/or email, as set out in the Procedures."[55] The IR Procedures state that "[a]dvance notice of any interruption in access, and expected resumption of service, shall, to the maximum extent practicable, be provided via the website."[56]

5. Confidentiality

[52] Byron Radle & Tom Bradicich, What is Availability?, (National Instruments Mar. 2019), https://www.ni.com/en-us/innovations/white-papers/13/what-is-availability-.html#section--1867287128, (last accessed Dec. 28, 2020).
[53] *Id.*
[54] *See* Regulations and Procedures for the International Registry § 3.4, ICAO (2019).
[55] *Id.* § 3.5.
[56] *Id.* §7.4.

Definition: The property that information is not made available or disclosed to unauthorized persons.

In the design and operation of a registry, both human and technological safeguards should be implemented to prevent disclosure of certain information to unauthorized persons. It should be noted that this Working Paper draws a distinction between Confidentiality, and general data protection (privacy). The former concerns commercially-sensitive information, whereas the latter covers individuals' personal information.

The scope and definition of commercially-sensitive information will depend on the applicable laws. Examples of commercially-sensitive data include i) information contained in user accounts, including payment details; ii) information contained in registrations, such as the nature and specifics of the secured obligations, the maximum amount for which the security right may be enforced, the terms of the secured loan, and the applicable interest rate (when the domestic rules require the entry of such information); or iii) information on serial numbers received in bulk by the IR from the manufacturers of aircraft objects.[57] Notably, commercially-sensitive data falling under ii) may be collected by the registrar for statistical purposes and subsequently disclosed to the public in aggregated and anonymized form.

The legislation that establishes ECRs generally does not specify the level and detail of necessary security measures to preserve Confidentiality. In this respect, the processes and measures adopted by credit registries (a type of credit referencing system) might provide useful reference points, despite the higher level of Confidentiality required for the data generally stored therein. Examples of measures and processes to preserve commercially-sensitive information include IT security, screening, educating personnel and users about Confidentiality policies, restricting database access to authorized personnel, and implementing staff disciplinary measures regarding information misuse and other breaches of security.[58] Other critical methods of ensuring Confidentiality include encryption of data in transport and data at rest to ensure no unauthorized parties can view confidential data, as well as proper permissions and entitlements for access to data.[59]

Technical

[57] The International Registry uploads MSN (Manufacturer Serial Number) Files supplied by manufacturers to assist registry users to complete registrations. These files contain model information and serial numbers issued by the manufacturer and inscribed on the airframe, engine, or helicopter.
[58] *Credit Reporting Knowledge Guide 2018*, World Bank, IFC (forthcoming 2019), at 45.
[59] Widely used methods include Access Control List (ACL) and Role Based Access Control (RBAC) frameworks and policies.

ISO 27000:2018 (3.10) defines Confidentiality as the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes."

With regard to general data protection (privacy), NIST Special Publication 800-122 is a practical, context-based guide to identifying personally identifiable information (PII), determining what level of protection is appropriate and how to provide it.[60] The guide references other NIST publications that cover each element of data privacy protection in more detail, such as SP 800-47, Security Guide for Interconnecting Information Technology Systems, and SP 800-53, Recommended Security Controls for Federal Organizations and Information Systems. The guide outlines topics that should be considered when developing privacy policies, awareness training for personnel, and practices to minimize PII collection, use, and retention. The publication also provides recommendations for developing response plans for incidents involving PII.

Legal
Searches should retrieve only information contained in registrations, rather than that associated with user accounts. Registry regulations adopted in many States provide that certain information must be provided by users but shall not be disclosed to searchers.[61] The UNCITRAL instruments do not take a position one way or another.

International Registry
Article 18(1)(c) of the CTC requires that the Regulations governing the IR ensure the Confidentiality of information other than that related to a registration. Accordingly, the Regulations require that all information in the IR must be kept confidential except when, i) provided in response to a search, in conformance with the Regulations; ii) provided to enable a registry user to file, amend, or discharge a registration; iii) requested by the Supervisory Authority; iv) submitted in court proceedings under Article 44 of the CTC; or v) used for statistics as required by the Regulations.[62]

6. Continuity

Definition: The ability of delivering registry services at acceptable levels within acceptable timeframes following a disruptive incident.

[60] Erika McCallister, Tim Grance & Karen Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - NIST Special Publication 800-122, (NIST Apr. 2010), https://www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii, (last accessed Dec. 28, 2020).
[61] *See e.g.*, registry regulations for Egypt and Jordan that prohibit a search of the registry from returning data entered for statistical purposes — Egypt: Decree of the Minister of Investment no. (108) of 2016, Promulgating the Executive Regulations of Law no. 115 of 2015 on Movable Security, Art. 10(2)(4); *and* Jordan: Regulations on the Registry for Interest over Movable Property no. ( ) for the Year 2018, Issued in accordance with Articles (13), (15/a), and (26/b) of Law on Securing Rights with Movable Property no. (20) for the Year 2018, Art. 21 (c).
[62] *See* Regulations and Procedures for the International Registry § 9, ICAO (2019).

This CPF encompasses the resilience required to recover from minor disruptions such as a system failure or a loss of power, to more disruptive events such as a software or cloud-services provider terminating operations. Continuity is differentiated from Availability by its focus on ensuring the provision of registry services after a disruptive event, whereas Availability relates to the percentage of time that the registry's services are available over a given period.[63]

To address catastrophic events, such as loss of power, that would cause downtime due to malfunction of registry infrastructure, comprehensive disaster recovery (DR) processes that allow the registry to immediately failover to a second (or third) datacenter should be implemented. DR sites should be geographically diverse such that proper distance and non-technical diversity (e.g. of political systems) is achieved such that it is nearly impossible for a total outage across all DR sites. DR processes would ideally achieve a recovery point objective (RPO) of zero (i.e. no loss of data or Integrity[64]) and a recovery time objective (RTO) of zero (i.e. immediate recovery or no reduction of Availability).

In addition to hardware related events, Continuity plans should address other potential sources of disruptions, such as failure of service providers to meet contractual obligations, registry personnel turnover, and even insolvency. If the registry relies on outsourced services, such as cloud-hosted internet-services, the registry must be able to migrate the system to another service provider upon termination of the outsourcing agreement. This includes having the technical capability and legal rights necessary to retrieve registry data and adapt software as necessary for compatibility with another provider's system. In any case, the right to access the data in the ECR is more important than an intellectual property license to operate the system in which the data is stored.

Continuity presupposes portability of data. In the context of cloud computing, portability refers to the ease with which the ECR can be moved from a non-cloud-based environment to a cloud-based one, and between cloud services of different providers.[65] Portability of the ECR data and its application software is essential. Portability is not a binary concept – it may be technically feasible but require considerable effort to transform the ECR data and its application software from its form on the source system to the form required by the target system.[66] In addition to facilitating more rapid and less costly migration, an easily portable system reduces the risk of being locked into a single

[63] *See* Availability – CPF 4, *supra*.
[64] *See* Integrity – CPF 8 *infra.*
[65] *See* CSCC, Interoperability and Portability for Cloud Computing: A Guide Version 2.0, 6, (Cloud Standards Customer Council (CSCC), Dec. 2017), https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf, (last accessed Dec. 16, 2020).
[66] *Id.*

cloud service provider.[67] Portability is a key provision of the contract between the IR regulator and the registry operator (Aviareto).

The registry should prepare transitional plans that identify the elements necessary to ensure Continuity and prepare it for any contingencies. Source code to the system may be held in escrow and the intellectual property rights licensed to the supervisory/regulatory agency and then licensed back to the operator, as in the case of the IR. A contingency fund should also be set aside. When application software is procured from a third-party provider, the registry operator must either acquire all necessary intellectual property rights or perpetual licenses to use, copy, distribute, and modify the software.

ECRs are fully responsible and accountable for complying with all of their regulatory obligations, including outsourced functions.[68] A number of governments have outsourced the hosting of their collateral registries to the company that developed the collateral registry software. These include the Federated States of Micronesia, Jamaica, the Marshall Islands, Palau, Papua New Guinea, the Solomon Islands, Tonga, and Vanuatu. Under a public-private partnership, a private entity developed, maintains and secures the collateral (PPSA) registries of seven Canadian provinces.[69] Outsourcing agreements must provide for ECRs to make and implement decisions related to outsourced functions as well as to continually monitor service provider performance.[70] Outsourcing agreements must also include appropriate confidentiality provisions regarding registry data and other information.[71] The service agreement must provide for ongoing monitoring and management of outsourcing arrangements including evaluation of the CPFs.[72]

Although Continuity relates to uninterrupted provision of services of the registry system itself, rather than the operator or its personnel, Continuity nonetheless requires

[67] *See* ISO 19941 Cloud computing - Interoperability and Portability, Introduction, https://www.iso.org/standard/66639.html, (last accessed Dec. 22, 2020).
[68] Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision, BIS (Jun., 2011), at 16-17; *and See Final Report on EBA Guidelines on Outsourcing Arrangements, European Banking Authority (EBA)*, (2019), at § 35, https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements/38c80601-f5d7-4855-8ba3-702423665479, (last accessed Dec. 28, 2020).
[69] New Brunswick, Newfoundland and Labrador, Nova Scotia, and Prince Edward Island formed the initial partnership with UNISYS in 1996, Northwest Territories and Nunavut signed on in 2001, and Yukon joined in 2016, *see* https://www.acol.ca/en/pprs/about/what-is-acol, (last accessed Dec. 28, 2020).
[70] *See Final Report on EBA Guidelines on Outsourcing Arrangements, supra* note 68, §§ 40.a., 75.h.
[71] *Id.*, § 40.d.
[72] Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021, (Treasury Board of Canada Secretariat, Nov. 28, 2017), https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html#toc8-1-1, (last accessed Dec. 28, 2020); § 100; *see generally*, Guidance for Managing Third-Party Risk, FDIC (2008), https://www.fdic.gov/news/news/financial/2008/fil08044a.pdf, (last accessed Dec. 28, 2020).

sufficiently skilled personnel. Continued operation of a registry system must be ensured, including in a situation where the operator becomes insolvent, a low risk for ECRs, which typically operate under governmental agencies.

Technical

ISO 22301:2019[73] specifies requirements to implement, maintain and improve a business continuity management (BCM) system[74] and can be used to assess an organization's ability to meet its own Continuity needs and obligations. The IR has adopted ISO 22301 and, to provide an independent assessment of its BCM strategy and implementation, the Registrar is audited annually by the British Standards Institute for compliance.[75] Other BCM standards include: ISO/IEC 27001:2013 Information Security Management Systems; the NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs; and BS 25999, the British Standard for Business Continuity Management.[76]

ISO 19941 explains portability between non-cloud and one or more cloud services and between cloud services.[77]

Legal

Regulations and standards often govern implementation of a BCM plan.[78] Some jurisdictions require a plan for handling business-critical operations.[79] Where functions of the registry are outsourced, contracts with service providers should ensure the registrar's right to all data stored in the registry database, or related to its operation, and its return for use or a transfer to an alternate provider upon contract termination. This includes, among others, registrations, search requests and results, entity names and proof of ID required to set up an account, as well as activity and security logs. Geographical diversity may be constrained by statutory data sovereignty mandates.[80]

---

[73] ISO 22301:2019 - Security and Resilience — Business Continuity Management Systems — Requirements, https://www.iso.org/standard/75106.html, (last accessed Dec. 28, 2020).
[74] *See* Section IV *infra.*
[75] Cowan & Gallagher *supra* note 14, at 253.
[76] *Data Protection Best Practices*, Storage Networking Industry Association (SNIA) (Oct. 2017), at 28, https://www.snia.org/sites/default/files/DPCO/Data%20Protection%20BP%20White%20Paper%20Final%20v1_0.pdf (last accessed Dec. 28, 2020).
[77] ISO 19941 Cloud computing - Interoperability and Portability, https://www.iso.org/standard/66639.html, (last accessed Dec. 22, 2020).
[78] *Data Protection Best Practices*, *supra* note 76 at 28.
[79] *Id.*
[80] For example, Government of Canada requires that its departments store all sensitive data under government control in approved facilities within Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic embassy. *See*, Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021, (Treasury Board of Canada Secretariat, Nov. 28, 2017), https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html#toc8-1-2, (last accessed Dec. 28, 2020).

International Registry
Paragraph 4.188 of the CTC Official Commentary includes business continuity among the areas in which the registry should adhere to international standards. Paragraph 4.185 explains that it is the responsibility of the Supervisory Authority to secure any intellectual property rights necessary for IR operation, such as software licenses.[81]

7. Disposition

Definition: The process implementing disposal of records: retention, archiving, destruction or transfer decisions.

Disposition covers processes and policies related to retaining, archiving, deleting, or transferring records. Disposition does not create new records other than in an activity log. ECRs utilize the 'add-only' retention policy whereby any information included in a previous registration is not altered or deleted upon registration of an amendment or cancellation.[82] Designing the registry system so as to ensure that the archived records preserve the original information contained in all registered notices also helps to minimize the potential for registry staff corruption.[83] Although it may be technically possible to store records indefinitely, legal requirements, such as general retention of records law, may limit the length of time that certain records may be maintained within the registry and the conditions under which they may be transferred. Storage costs, such as the maintenance and operation of storage hardware, may also make unlimited storage impracticable. Disposition rules and processes must be designed to comply with such legal and economic limits while also satisfying the minimum time for which the records must be kept available according to the applicable law and registry regulations. Records may be transferred as part of a replication process where records are copied from one database server to another to create a backup copy in another location. The ability to transfer data from the ECR to another platform may facilitate Portability (see Continuity – CPF 6 *supra*).

Technical
ISO 15489-1:2016 Information and documentation — Records management, § 3.8, defines disposition as the "range of processes associated with implementing records retention, destruction or transfer decisions."

[81] *See* Regulations and Procedures for the International Registry ¶ 4.185, ICAO (2019), "It is also the responsibility of the Supervisory Authority to ensure that any rights required for the continued effective operation of the International Registry in the event of a change of Registrar will vest in or be assignable to the new Registrar. These would include any intellectual property rights necessary for the continued operation of the Registry."
[82] Collateral registries should follow an "add-only" policy that "only permit[s] documents to be added to the record, but never removed. *See* IFC Knowledge Guide, *supra* note 17, at 91.
[83] *See* UNCITRAL Registry Guide at para. 138(c).

Legal
Article 30 of the UNCITRAL Model Registry Provisions provides two options with respect to the removal of records from the registry. Option A requires the registry to remove information in a registered notice from the public registry record i) upon expiry of the period of effectiveness of the registration of a notice; or ii) upon the registration of a cancellation notice. Option B provides that information contained in a registered notice must be removed upon expiry of the period of effectiveness of the registration of a notice and may not be removed under any other circumstances. The UNCITRAL Registry Guide recommends that information removed from the public registry record should be archived for a long period of time, such as 20 years.[84]

General retention of records law may require the complete deletion of certain records from the database, including any backup or archived copies. For example, this may apply to certain personal information required for an individual to create a user account in the registry.

International Registry
The IR stores all registrations permanently, unless a court order for removal is issued.[85]

8. Integrity

Definition: The property that data has not been altered or destroyed in an unauthorized manner.

The critical underlying premise of using a registry to store information rests on the Integrity of the stored data. Without Integrity, confidence and trust cannot be placed in the registry as an authoritative source of information submitted to it at a specified time. Integrity relates to the system as well as any decision-making of the registrar and registry staff. Integrity of registry data lends evidentiary weight to registrations – an important factor for efficiently resolving disputes.[86] Parties should not have grounds to either repudiate registration or dispute its status, time, or content.[87] Ensuring Integrity is an ongoing objective that requires regular reviews and updates of security measures in light of emerging threats. Integrity relates not only to the data submitted by registrants, but also any data associated with registrations by the registry. For instance, the registry timestamps all registrations and/or state changes in the ECR, which is critical for establishing the priority of a security right. Such timestamps should be cryptographically secured so as to prevent any tampering with the order in which registrations and state

[84] *See* UNCITRAL Registry Guide at Recommendation 21.
[85] Personal communication with Aviareto, March 9, 2020.
[86] *See* Marek Dubovec, *UCC Article 9 Registration System for Latin America*, 28 ARIZ. J. OF INT'L & COMP. L. 117, 132 (2011), integrity is presumed, but may be questioned if there is some impropriety, especially the ability of the registrar to alter registrations.
[87] *Id.*

changes occur. A forensic audit trail of chronologically ordered events should be maintained. Timestamp assurance and tamper checking systems assure the Integrity of database records.

The ECR must implement certain encryption standards, but also appropriately segregate the duties of registry staff and ensure that access authorization does not exceed what is necessary for an employee's authorized tasks, see Access Control, (CPF 1, *supra*). For example, registry authorization levels should be sufficiently granular that registry staff who must access registry records only have the minimum access level necessary to perform their job duties, such as read-only permissions and limited rights to execute database queries and procedures, to prevent access to confidential data or changes to stored information.[88] In particular, database permissions necessary for the registrar to correct registry errors should be restricted to use by registry staff acting under the Legal Authority of the Registrar (CPF 11, *infra*).

Such measures are even more important during the heightened vulnerabilities created by the COVID-19 pandemic.[89] In March 2020, a ransomware attack on a global financial system used by 90 of the world's largest banks. Ransomware is a type of malware that encrypts computer files. After infecting a computer network, hackers demand a ransom in exchange for the decryption key. In this case, the attack was detected by a monitoring system on a cloud server, alerting the company's IT security team.[90] Despite early detection, the malware had already taken control of network domain controllers, requiring thousands of servers to be taken offline to prevent the attack spreading across the entire system.[91] Restoring affected data from backups and removing the malware from infected servers caused multi-day service outages for many of the company's more than 8,500 customers.[92]

Technical

The ISO 27000 family of standards provides useful reference points both for encryption and algorithms standards. For example, ISO 27040:2015 includes guidelines for the design and implementation of storage security.[93] The ISO standards reference other ISO standards as well as standards developed by other organizations, such as IEEE and NIST. For example, ISO 27040:2015 provides an overview of storage security concepts and

[88] *See* IFC Knowledge Guide, *supra* note 17, at 84.
[89] Attackers appear to be taking advantage of potential security lapses as offices adapt to provide remote access for employees. Malware, such as ransomware that encrypts computer files, is often deployed by "phishing" for responses to fraudulent email sent to unsuspecting recipients. *See* Jordan Robertson, Fintech Company Survived Ransomware Attack Without Paying Ransom, (Bloomberg Businessweek, Apr. 7, 2020), https://www.bloomberg.com/news/articles/2020-04-08/how-finastra-survived-a-ransomware-attack-without-paying-ransom, (last accessed Dec. 28, 2020).
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *See* ISO 27040:2015 § 7

related definitions. It includes guidance on the threat, design, and control aspects associated with storage technology. In addition, it provides references to other international standards that address practices and techniques relevant to storage security, such as IEEE 1619.1-2007 and NIST-FIPS 197, which provide authenticated encryption standards to protect the Integrity of stored data.

Legal
Secured transactions laws and regulations do not expressly provide for standards governing Integrity, which must be ensured through system design and operating procedures and policies, including Access Control and personnel training.

International Registry
Information security techniques employed by the IR provide useful points of reference, including its implementation of custom software that detects any unauthorized interference with the database.[94]

9. Interoperability

Definition: 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.

Interoperability is the registry system's ability to interface with other systems in a manner that is transparent to its users. It may be mandated by a law or enabled by the system provider as a service to the users. Interoperability includes communication and data transfer between the registry and another system; a process that is performed automatically.

Depending on the relevant legal framework, ECRs might need to be interoperable with a number of databases. The operationalization of the ECR may require a transfer of records from other registries that provided registration functions prior to the establishment of the ECR. Interoperability of this nature would be especially critical during the transition from a prior secured transactions regime to a reformed framework.[95]

[94] Cowan & Gallagher *supra* note 14, at 231.
[95] During the transition period, data from traditional registers may be transferred to the new ECR through Interoperability or other, less automated, means. However, even when transfer of registrations is technically possible it may not be practicable. For example, in Australia it was not appropriate to transfer data from 14 of 40 traditional registers, primarily because registration in these registries was not mandatory and did not establish priority of a security right. Transferring such registrations would prejudice the relative priority rights of secured parties who had chosen not to register in those registries. *See* ANTHONY DUGGAN & DAVID BROWN, AUSTRALIAN PERSONAL PROPERTY SECURITIES LAW, 338-39 (2012).

Other interconnections may be contemplated with a companies registry, an intellectual property registry[96], and a motor vehicle registry.[97] Finally, almost all ECRs will have to be interoperable with payment systems that allow users to pay the required fees securely on-line. This, however, is a different mode of Interoperability, since it does not directly relate to information submitted to the ECR and involves minimal transfer of information to, or from, the ECR.

The legal framework may also mandate Interoperability with a national ID management system/database. Interoperability with ID management systems may facilitate and automate detailed Authentication, including using biometric data. Interoperability with Ultimate Beneficial Owner (UBO) and Know Your Customer (KYC) registries can automate verification of debtor names. In practice, when a registrant enters a debtor's/grantor's national ID number into an ECR that is interoperable with a national ID database, the system would perform a search on the national ID database and automatically populate the debtor identification field in the registry with data from the national ID database.[98] If the identification is incorrect, the user would be alerted to a potential error in the ID number entered for the debtor/grantor.[99] The Australian PPSR cross-checks company numbers and organization identifiers entered by users against data held by the Australian Securities and Investments Commission, which is responsible for the registration of companies.[100] The PPSR displays company information, or an alert that the number could not be verified, to assist the user.[101] Similarly, when users enter a vehicle identification number, the PPSR retrieves data periodically updated from national databases of registered vehicles (e.g. National Exchange of Vehicle and Driver Information System – NEVDIS) to provide details such as vehicle color, make, model, year of manufacture, registration expiration date, as well as compulsory product safety recall information and whether the vehicle has been reported as stolen or damaged.[102]

Interoperability, in a form different from the domestic ECRs, is also contemplated by the IR where some registrations may be required to be submitted through a national entry

[96] For the legal challenges presented by the coordination between collateral registries and IP registries *see* Andrea Tosato, Secured Transactions and IP Licenses: Comparative Observations and Reform Suggestions, 81 Law and Contemporary Problems 155-180 (2018), at 175-176.
[97] *See* Marek Dubovec, *supra* note 86, at 127, 139-40.
[98] *Id.*, at 127.
[99] *Id.*
[100] Application for IACA Merit Award 2016, 9, (Australian Financial Security Authority), https://www.iaca.org/wp-content/uploads/Australia-Personal-Propertly-Securities-System.pdf, (last accessed Dec. 28, 2020).
[101] *Id.*
[102] *See* https://www.ppsr.gov.au/enhancements-list, (last accessed Dec. 28, 2020); and *see* https://www.ppsr.gov.au/understanding-motor-vehicle-search-results, (last accessed Dec. 28, 2020); and *see* https://www.ppsr.gov.au/understanding-written-vehicle-codes, (last accessed Dec. 28, 2020).

point.[103] Such interconnections may be established directly or indirectly through a portal.[104] Although not interoperable with aircraft manufacturers' databases, the IR provides users with a database of aircraft object serial numbers and descriptions to assist users and promote accurate data entry.[105] The database is continually updated by uploading files received from manufacturers.[106] Neither the Registrar nor the manufacturers are liable for inaccuracies in the data, which are used subject to acceptance of the manufacturers' disclaimer.[107]

Interoperability facilitates registrations and reduces data entry errors but is not critical to accomplishing the fundamental functions of public notice of ECRs. As such Interoperability should not be considered as a CPF *per se*, but only if the law that governs the ECR in question requires that it is interoperable with other systems.

When Interoperability with other systems (e.g., a companies registry, motor vehicle registry, national ID database, equipment/machinery registry) is a CPF, it is crucial to establish communications and governance protocols for managing Interoperability and data sharing agreements with the other databases. A service-level agreement (SLA) entered into by the provider of the data service and the ECR as consumer of the data service should govern the specific terms and conditions of service, including, among others, service availability, advance notification for any planned downtime, service response time, IT support availability, and problem reporting and escalation procedures.[108]

Technical

ISO 27040:2015 § 7 defines Interoperability.[109] ISO 39794-1:2019 provides Interoperability standards for biometric data interchange, such as fingerprint and face

[103] CTC Official Commentary 4.189. The Registrar does not assume any liability for errors or system malfunction of a national entry point.

[104] *See* also Charles W. Mooney Jr., *Relationship Between the Prospective UNIDROIT International Registry, Revised Uniform Commercial Code Article 9 and National Civil Aviation Registries*, UNIF. L. REV., 1999-2, 335, 343.

[105] Cowan & Gallagher *supra* note 14, at 235.

[106] *Id.* The files are referred to as MSN files, a reference to the manufacturer's serial numbers (MSNs) that they contain.

[107] *Id.*

[108] For a sample SLA, *see* Global Standards Council, Global Reference Architecture (GRA) Information Sharing Enterprise Service-Level Agreement, (US Department of Justice, Global Infrastructure/Standards Working Group, Apr. 2011), https://it.ojp.gov/GIST/60/Global-Reference-Architecture--GRA--Information-Sharing-Enterprise-Service-Level-Agreement, (last accessed Dec. 21, 2020).

[109] *See* ISO/IEC 2382:2015 Information technology — Vocabulary at 2121317, defining interoperability as the "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."

image data.[110] ISO 19941 provides standards for transferring data between non-cloud and one or more cloud services and between cloud services.[111]

The adoption of open technology standards and protocols, such as those developed by the Universal Trade Network Organization (UTNO), facilitates seamless Interoperability between digital trade systems, applications, and networks.[112]

SOAP (Simple Object Access Protocol) is a communication protocol that allows disparate systems to communicate securely using XML (Extensible Markup Language) for SOAP based web-services.[113] SOAP is widely used for secure communications by internet accessible information systems, including ECRs.[114] The Web services Security (WS-Security) standard specification defines how SOAP based web-services should be implemented to protect against external attacks and ensure communication Confidentiality, Integrity, and Authentication.[115] The WS-Security standard uses signatures (defined in the XML Signature standard) to secure parts of SOAP messages.[116]

Legal

The UNCITRAL Registry Guide notes the benefits of Interoperability with other specialized registries, private or governmental.[117] However, the UNCITRAL Registry Guide cautions that the registry should not provide Interoperability unless it is confident that the registry to which it is connected is current, complete, and accurate.[118] Otherwise, it would be providing a disservice and possibly expose itself to liability.[119]

International Registry

Under Article XIX of the Aircraft Protocol, Contracting States may designate "direct entry points" through which information required for registration shall or may be directly transmitted to the IR. Accordingly, Regulations 12.5 and 12.6 of the IR Regulations and Procedures require the IR to establish electronic interfaces with such direct entry points

---

[110] *See* https://www.iso.org/obp/ui#iso:std:iso-iec:39794:-1:ed-1:v1:en, (last accessed Dec. 21, 2020).
[111] *See* https://www.iso.org/standard/66639.html, (last accessed Dec. 21, 2020).
[112] *See* Details of Major Trade Finance Network in Development, (Marco Polo, Dec. 3, 2018), https://www.marcopolo.finance/details-of-major-trade-finance-network-in-development/ (last accessed Dec. 28, 2020).
[113] *See* Simple Object Access Protocol Overview, https://docs.oracle.com/cd/A97335_02/integrate.102/a90297/overview.htm#1007693 (last accessed Dec. 28, 2020).
[114] Communication of NatLaw with Bsystems (Ghana), Feb. 27, 2019.
[115] *See generally* https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, (last accessed Dec. 28, 2020).
[116] *Id.* at 35. The signatures provide assurance that the message has not been manipulated during transmission (Integrity) and authenticate the sender (Authentication).
[117] UNCITRAL Registry Guide at para. 89.
[118] *Id*., at para. 166.
[119] *Id.*

and specify applicable procedures. As of December 2020, no Contracting State had an active direct entry point.[120]

10. Legal Authority and Compliance

Definition: The property of ensuring that the registry is established pursuant to and operates in compliance with a sound legal framework.

A legal framework governing the design and operation of the registry determines the implementation of a number of CPFs.[121] The relevant legal framework includes an international treaty (for international registries), statutes, regulations, procedures, master agreements (for private registries), terms and conditions of use,[122] but also less formal instruments, such as registrar's practice statements and rulebooks.[123] It is critical for the secondary and tertiary sources to be in full compliance with the policies, objectives, and approaches of the primary legislation. The applicable legal framework includes not only commercial laws that provide the legal authority to establish and operate the ECR, but also laws that regulate data security/protection and archiving of records, intellectual property laws, companies and insolvency laws, as well as labor laws.

The legal framework must be assessed to appropriately design the ECR at an early stage, and ideally before a specific registry vendor is procured. This legal framework determines the design methodology, such as the process model narrative (PMN) from which the designer develops and implements the rules and processes of the ECR.[124] The legal framework should not prevent the registrar from updating the ECR design as necessary to fulfil its objectives in the future. The design must be flexible and robust enough to be scalable. Nonetheless, the core functions of the ECR should be regulated by the law to avoid the risk of the administrative agency modifying the regulations to

[120] Communication of NatLaw with Aviareto, Aug. 14, 2020.
[121] *See* also *supra* Section I(C).
[122] The terms and conditions for the use of an ECR may provide "You must comply with all security procedures and take all reasonable actions to protect and maintain the security of your access to and use of the Registry." *See also* UNCITRAL Registry Guide paras. 80-81 explaining that terms and conditions of use may include offering users the opportunity to create user accounts or offering additional services such as statistical reports relating to the operation of the registry, such as the number of searches and registrations over a given period.
[123] For example, the Registrar of the Australian PPSR issues Practice Statements explaining how it performs its functions. PPSR Practice Statements have covered topics such as restricting access to data, maintenance fees, and removal, correction, and restoration of registry data. *See* https://www.ppsr.gov.au/registrars-practice-statements, (last accessed Dec. 28, 2020).
[124] *See* IFC Knowledge Guide, *supra* note 17, 75, describing PMN as "the most essential document" needed by a collateral registry designer or operator. At a holistic-design level, use of enterprise architecture frameworks (EAFs), such as TOGAF (The Open Group Architecture Framework), may be helpful.

implement inconsistent policies. The regulations should address only operational aspects.[125]

ECRs collect and process vast amounts of data in performing their core functions (see Authentication, Confidentiality, Retention). Although this information is largely commercial in nature, a substantial quantity of personal data is also collected in the process. For example, an ECR may be accessible for registrations only upon establishment of user accounts, requiring personal information, such as the user's name and address and possibly payment details. The ECR's legal obligations related to data Retention and Disposition derive from specific legislation and regulation as well as from more general data Retention and Disposition laws. For example, the secured transactions legal framework may dictate the length of time that registrations are retained after the expiry of effectiveness, while general retention of records law may require Confidentiality, and a user's right of access, or right to erasure after a prescribed period. One example of a general retention of records law is the European Union's General Data Protection Regulation (GDPR), which protects natural persons with regard to the processing of personal data and the free movement of such data.[126]

The ECR must be fully compliant with its legal and regulatory mandate and operate in conformity with their requirements and objectives. Compliance includes, but is not limited to, applying appropriate technologies that enable the ECR to make available and secure data in accordance with the rules and regulations related to data Retention, Confidentiality, Integrity, and Availability.

Legal

The laws and regulations that govern registry operation shape the requirements and objectives of each of the CPFs. For example, with respect to Accessibility, the regulation may provide that the registrar is not liable for loss or damage resulting from lack of access precluded by maintenance performed outside peak periods, or technical or security problems.[127] For Availability, the law may provide that anyone may register a notice or that a notice may be registered only through an authorized user account or under a digital signature.[128] For Confidentiality, the law may prescribe that information about users is not to be disclosed.[129]

International Registry

[125] In some cases, the law may delegate some authority to the regulations to supplement an important legal rule. *See* the Aircraft Protocol art. XX(1).
[126] Regulation (EU) 2016/679.
[127] *See* Regulations and Procedures for the International Registry, § 14, ICAO (2019).
[128] *See* Article 5 of the Model Registry Provisions of the UNCITRAL Model Law.
[129] *See* Article 18(1)(c) of the Cape Town Convention.

The IR operates according to the CTC, the Aircraft Protocol, and the IR Regulations and Procedures issued by the Supervisory Authority pursuant to Article 17(2)(d) of the CTC and Article XVIII of the Aircraft Protocol.[130]

11. Legal Authority of the Registrar

Definition: The property that the registrar may exercise certain powers pursuant to a legal authority, including in the process of eliminating a detected failure.

This CPF relates to the authority of the registrar under the applicable legal framework to take certain actions that may affect risks and liability, rather than more broadly any authority, including to enhance its user-friendliness. Its proper application is an important confidence factor for users.

Although in general, only the registrant may submit initial, amendment, and cancellation notices, there are instances when the registrar must intervene to correct errors or register notices of non-consensual interests such as judgment liens or court-ordered cancellations. As for the error corrective types of actions, this CPF is limited to situations where the error is not caused by the user. Errors may affect the system itself or the publicly available data. Errors in the system may not affect parties to transactions, including searchers, and the registrar should have unrestricted authority and ability to correct such errors. Errors in data that have been made publicly available are more difficult to address since they may have already affected those who relied on their accuracy. Any corrective action would need to take into account the interests of affected parties.

This CPF encompasses the responsiveness of the registry to such errors, which comprises four phases: i) detection – a process of continuous or regular checks to detect such errors; ii) response – prompt action to correct errors or otherwise respond as authorized by the legal framework; iii) corrective action to eliminate the cause of an error and to prevent recurrence; and iv) notice – issue prompt notice of such response to affected parties, as required by the legal framework.

The corrective action is not implemented by actually altering any data, but rather, by adding corrective notices. As with Legal Authority and Compliance, the applicable legal framework should set out the duties and the bounds of the Legal Authority of the Registrar.

In addition to correcting errors, this CPF also covers the power of the registrar to enter court-ordered notices, such as when the secured creditor has not cancelled the effectiveness of a registration after the full satisfaction of the secured obligation. The

[130] *See* Regulations and Procedures for the International Registry, § 1, ICAO (2019).

ECR design must contemplate and enable such registrations, which should be clearly identified as submitted by the registrar. Their legal effect, including on the effectiveness of a security right and its priority will be governed by the applicable legal framework.

Legal

Article 31 of the UNCITRAL Model Registry Provisions provides for the correction of registry errors and their legal effect. The correction of an error may also include restoration of an erroneously discharged registration.[131] Article 20 requires a secured creditor to register a cancellation notice, and, if the secured creditor does not comply, the grantor may request the secured creditor to do so. If the secured creditor does not comply with the grantor's request, the grantor may seek a court order. If such a court order is issued, the registry must register the notice without delay.

International Registry

The Registrar is mandated to perform the functions specified in the CTC, the Aircraft Protocol, and its Regulations and Procedures.[132] Regulation 5.17 of the IR Regulations addresses the Registrar's authority and duties regarding an error in a registration or a discharge of a registration, or the chronological order of registrations, caused by a malfunction in the IR.[133] In such an event, Regulation 5.17 authorizes the Registrar to i) correct such an error or discharge a registration; or alternatively, ii) request the named parties to the original registration to amend or discharge that registration, leave it as registered, or seek a court order.[134]

The Registrar's authority to amend or discharge (cancel) an erroneous registration (caused by a malfunction in the registry) comes with specific duties to give notice to affected parties.[135]

12. Reliability

Definition: The property of performing required functions for a specified period of time.

A system's level of Reliability reflects its ability to function consistently over time. The Reliability of a system comprises three primary elements:

---

[131] *See Registrar's Practice Statement No. 8: Restoration of Data to the PPSR*, PPSR (Feb. 2016), https://www.ppsr.gov.au/about-us/laws-rules-and-regulations/ppsr-practice-statements/registrars-practice-statement-no-8, (last accessed Dec. 28, 2020) (describing the process for restoring an erroneously discharged registration in the Australian Personal Property Securities Register (PPSR)).
[132] Regulations and Procedures for the International Registry, Reg. 3.3, ICAO (2019).
[133] *Id.*, Reg. 5.17, ICAO (2019).
[134] *Id.*, the Registrar may do so "provided that such correction or discharge shall be effective only from the time it is made, and shall have no effect on the priority of any other registration."
[135] *Id.*

1. The reliability of the software and hardware that enables data entry, retention, and retrieval.
2. The reliability of the data itself.
3. The reliability of the personnel involved in the operation of the registry.

In relation to software and hardware, Reliability is a measure of the frequency of failures whereas Availability is a measure of their impact. One measure of Reliability is Mean Time Between Failures (MTBF).[136] A longer MTBF indicates less frequent failures and greater Reliability. Mean Time To Repair (MTTR) is a measure of the average impact caused by failures.[137] Total downtime over a given period is the product of the number of failures during that time and the average time required to correct the problem. One failure per annum may suggest good Reliability, but if that single failure resulted in a week of downtime, its impact would be captured as poor Availability. Similarly, frequent failures that required users to reconnect to the system but last only a few seconds would reflect poorly on Reliability but would not greatly impact Availability. These two CPFs are closely related but measure different performance characteristics.

Reliability of the ECR may be affected by various factors and changes. For instance, changes to search logic may negatively impact Reliability in terms of consistent software operation over time that may occur upon the failure to retrieve registrations that previous logic retrieved for identical search criteria. This is a risk associated with ECRs that utilize a close match search logic that may be regularly refined.[138]

Technical

ISO 27040 addresses storage security techniques for information systems. It defines Reliability as the "ability of a system or component to perform its required functions under stated conditions for a specified period of time."[139] ISO 25010:2011 addresses quality of software and computer systems, including Reliability, which it considers more broadly as having sub-characteristics of maturity, Availability, fault-tolerance, and recoverability.[140] The standard defines maturity as the degree to which a system meets

[136] *See* Byron Radle & Tom Bradicich, *supra* note 52.
[137] *Id.*
[138] Section 504 of the UCC Model Administrative Rules (2018) requires that if the filing office changes its standard search logic or the implementation of its standard search logic in a manner that could alter search results, the filing office shall provide public notice of such change.
[139] ISO/IEC 27040:2015 Information technology — Security techniques — Storage security, §3.36. *See also* ISO/IEC 2382:2015 Information technology — Vocabulary, at 2123024, defining reliability as the "ability of a functional unit to perform a required function under given conditions for a given time interval."
[140] ISO/IEC 25010:2011 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, 4.2.5, https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en, (last accessed Dec. 28, 2020); *and see* ISO/IEC 25010, https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&start=3, (last accessed Dec. 28, 2020).

the need for Reliability under normal operation.[141] Fault tolerance is the degree to which a system operates as intended despite hardware or software faults (i.e. without adversely affecting Availability).[142] Recoverability is defined as the degree to which a system can recover from an interruption or failure including restoring any directly affected data (i.e. restore Availability).[143]

13. Retention

Definition: The property of preserving data in a system for a specified period of time.

Retention of registration data is one of the primary purposes of registries. The ECR retains the original record and adds amendment and cancellation notices.[144] The record, as amended, may be retained in the system and publicly available until it is cancelled, or its effectiveness has expired. Retention of records until their expiration, whether or not they have been cancelled, allows a searcher to discover a registration and to assess the prior state of a record that has been amended. This is especially important in those ECRs that operate under laws that determine the effectiveness of a cancellation on whether the secured creditor (of record) provided sufficient authorization.[145]

Records that have been corrected are also retained and made publicly available. If the record is corrected, such as upon discovery of an error made by the registry, a record of the registration prior to its correction may be important to determine liability when a searcher relied on the uncorrected record before the correction was made.[146] Data Retention is essential to data Integrity and Reliability. Disposition policies and processes[147] determine when Retention is no longer required or appropriate for a particular data record, at which point Disposition processes take over from Retention processes. For example, a Disposition process may determine that a record should no longer be retained within the registry database. Alternatively, Disposition policy may dictate that the record be archived (e.g., retained off-site on media suitable for long-term storage) before being deleted from the operational registry database.

Technical
ISO 27001:2013 specifies requirements for assessing security risks affecting information storage and for establishing, implementing, maintaining and continually improving an

[141] ISO/IEC 25010:2011, *supra* note 140 at 4.2.5.1.
[142] *Id.* at 4.2.5.3.
[143] *Id.* at 4.2.5.4.
[144] *See* Disposition, II A(7) *supra*.
[145] *See* UNCITRAL Model Law, Model Registry Provisions, art. 21(Option D), 30(Option B(1)).
[146] *Id.; and see* UNCITRAL Model Law, Model Registry Provisions, art. 31.
[147] *See* Disposition, II A(7) *supra.*

information security management system.[148] ISO 27040:2015 sets out standards for data storage security, focused on protecting data against unauthorized disclosure, modification, or destruction while assuring Availability to authorized users.[149] The standards apply to controls that prevent, detect, or deter harmful events or unauthorized acts as well as to those that correct, or recover affected data.[150] Also relevant to ECRs, ISO 17068:2017 specifies requirements for a trusted third party repository (TTPR) to safeguard provable Integrity and authenticity of digital records and serve as a source of reliable evidence.[151]

Legal
Article 30 of the UNCITRAL Model Registry Provisions contemplates the option of removing from the public registry a registered notice upon expiry of the period of effectiveness of the registration or upon registration of a cancellation (termination) notice. This article also offers the option of archiving registrations removed from the public registry.

14. Timeliness

Definition: The property of making a registration publicly searchable, and therefore effective, almost instantly after its submission.

Timeliness refers to the expectation of Accessibility of information within a reasonable time.[152] Timeliness can be measured as latency, the time delay between when information is expected to be accessible and when it actually becomes accessible.[153] Ideally, information is accessible in real-time as events occur. When accessible information does not reasonably reflect known reality, data-quality is negatively impacted, and the Reliability of the information system suffers.

Under the laws that govern ECRs, a registration (or subsequent amendment) does not generally become effective (and thus does not make the security right effective against

[148] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, 1, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, (last accessed Dec. 28, 2020).
[149] ISO/IEC 27040:2015 Information technology — Security techniques — Storage security, 3.49, https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en, (last accessed Dec. 28, 2020).
[150] *Id.*
[151] ISO 17068:2017 - Information and documentation — Trusted third party repository for digital records, https://www.iso.org/obp/ui/#iso:std:iso:17068:ed-1:v1:en, (last accessed Dec. 28, 2020).
[152] *See* David Loshin, Data Quality and MDM, 5.3.5, (Elsevier, 2008).
[153] *Id.*; *and see generally* Laura Sebastian-Coleman, Measuring Data Quality for Ongoing Improvement, ch. 5, (Elsevier, 2013).

third parties) until it is publicly searchable.[154] Therefore, the ECR should almost immediately accept or reject a notice, as well as any accompanying records,[155] upon its submission (note that this requirement precludes any registry staff intervention).[156] An ECR should be designed to automatically review and process/reject registrations and search requests without any human intervention. Upon accepting a registration, the registry should almost immediately store and index the registration to make it publicly searchable and generate a search result confirming that the registration is effective.[157] This confirmation should include the date and time that the registration became searchable, and thereby effective, as well as the registration number, and all information entered for the notice.[158]

Timeliness is equally important when the registry rejects a registration or search request. This enables the registrant or searcher to take a corrective action for the requested service to be processed.

Timeliness benefits the registrant (creditor), the searcher, and the debtor.[159] Timeliness of a registration in an ECR also has substantial legal implications when secured transactions law intersects with other branches of commercial law.[160] For example, Timeliness of a registration is essential if the commencement of insolvency proceedings is imminent. Timeliness also enhances Reliability of the ECR and overall user experience.

For geographically diverse registries, such as the IR, laws of physics (electronic communications operate at the speed of light) dictate that response times for webpages accessed at great distance from registry servers will be measurably slower than when accessed from locations closer to the registry servers. To improve the speed at which web pages load and update, copies of graphics used by the web pages can be stored on servers at strategic locations around the world while registry databases reside in the jurisdiction whose laws govern the registry.

---

[154] *See* UNCITRAL Guide on the Implementation of a Security Rights Registry, United Nations (Mar. 2014), § 109, recommending, "[i]f the registry is designed to enable users to electronically submit information in an initial or amendment notice to the registry without the intervention of registry staff, the registry software should be designed to ensure that the information becomes publicly searchable immediately or nearly immediately after it is transmitted." *Compare with* UCC 9-516(a) under which a filing is effective upon communication of the record to the filing office.

[155] This may be the case where the ECR permits the registrant to provide an attachment with the notice, such as the UCC filing systems, but also where the law governing the operation of the ECR may require the registrant to submit a copy of a specific document, such as an instrument that creates a charge.

[156] *See* Marek Dubovec, *supra* note 86, at 135; *and see* Charles Mooney, *supra* note 104, at 339.

[157] *Id.*

[158] *See* IFC Knowledge Guide, *supra* note 17, at 89.

[159] *See* Marek Dubovec, *supra* note 86 at 136.

[160] On various forms of commercial law intersections, *see generally* Giuliano Castellano & Andrea Tosato, Commercial Law Intersections, 72 Hastings L. J., (forthcoming 2021), https://ssrn.com/abstract=3558378, (last accessed Dec. 28, 2020).

While a fully automated review and processing of registrations without any human intervention is the best practice for notice-based ECRs, this may not be possible for document-based registries that act as gatekeepers for approval of property rights and perform qualitative evaluation of filed documents. For instance, registries that create a property right based on submitted documentation, such as applications for patents, trademarks, and land titles. Timeliness of these registries can be improved by connectivity and Interoperability with other types of registries to validate key data and improve the Integrity and Reliability of the information in the registry.

Technical
The degree of Timeliness required by a particular system is relative to its intended use, and as such no specific standard for Timeliness exists. However, as a characteristic or measure of data quality, Timeliness is widely included in data quality analyses, for example in the data quality model defined in ISO 25012:2008 for data retained in a structured format within a computer system.

Legal
Under Article 7(3) of the UNCITRAL Model Registry Provisions, a registry may not scrutinize the form or content of a notice or a search request other than to the extent authorized in Articles 5 and 6.[161] Article 5, requires the user to comply with registry access rules, and under Article 6, a registry must reject a registration if no information is entered in one of the mandatory designated fields.[162] Likewise, the registry must reject a search request if no information is entered in one of the fields designated for entering a search criterion.[163] If the registration of a notice or a search request is rejected, the registry must communicate the reason to the registrant or searcher without delay.[164]

International Registry
Regulation 6.2 of the IR Regulations and Procedures requires "prompt electronic confirmation of a registration to the named parties." It provides that such notification is not confirmation of effectiveness of the registration, cautioning that a priority search is necessary to confirm effectiveness.

15. Trustworthiness

Definition: The property of providing confidence to users and third parties that the registry performs its core functions at a level that meets or exceeds their reasonable expectations.

[161] *See* UNCITRAL Model Law, Model Registry Provisions, art. 7(3).
[162] *Id.* arts. 5, 6(1).
[163] *Id.* art. 6(2).
[164] *Id.* art. 6(4).

Trustworthiness is of paramount importance for ECRs. To facilitate commerce, an ECR must perform its core functions at a level that meets or exceeds the reasonable expectations of its users. If it does so, the ECR inspires the necessary trust and confidence that will encourage its use.

Trustworthiness is comprised of two primary components: functionality and assurance.[165] Functionality embodies the features, functions, and services provided by the registry.[166] Assurance is the measure of confidence that registry functionality is implemented correctly, operating as intended, and producing the desired result.[167] Assurance assessments generate relevant and credible evidence about the functionality and behavior of the registry and identify the elements of the registry that produced the evidence. This evidence determines the level of confidence in registry functionality[168] and is also an important element of risk management, as it facilitates the process of continuous improvement by identifying underperforming registry elements that require attention.[169] Regular assessments are essential to achieving the goal of continuous improvement and staying abreast of developing technology and evolving threats.

It is not enough for the registry simply to declare itself trustworthy – an objective process of certification is required.[170] Providing users with the results of objective audits and certification that the registry meets international best practice standards not only provides assurance, it creates transparency and engenders trust among registry users.[171] Independent training and certification of ECR staff in skillsets required to manage and operate the ECR enhances its Integrity, demonstrates competency, and contributes to reputation.

Technical

ISO ISO/DIS 16363:2012 - *Space Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories* defines procedures suitable for objectively auditing and certifying the trustworthiness of registries.[172] A regular cycle of audits and certification is required to maintain trustworthy status.[173] Where the registry can demonstrate that it has implemented practices required by related standards, this may

---

[165] *Recommended Security Controls for Federal Information Systems: Special Publication 800-53,* §2.6, (NIST, 2017), https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf (last accessed Dec. 29, 2020).
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Space Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories (ISO 16363:2012)*, ISO (2012) at § 1.6.
[170] *Id*. at § 1.3.
[171] *Id.* at § 2.1.
[172] ISO 16363:2012 § 1.1, stating that the scope of the document is "the entire range of digital repositories."
[173] *Id.* at § 2.1.

serve to satisfy similar requirements of the audit (e.g., by employing the codes of practice found in the ISO 27000 series of standards).[174]

The scope of ISO 16363 is broad, it encompasses the IT system, including hardware, software, communications equipment and firewalls as well as supporting physical infrastructure, personnel, management and administrative procedures.[175] This includes, among others, fire protection and flood detection systems, as well as management procedures to assess staff skill levels relative to evolving relevant technology, and the registry's intellectual property rights practices.[176] Disaster preparedness and recovery plans are also assessed.[177]

NIST Special Publication 800-53 provides an extensive and diverse list of controls that focus on assurance, such as incident response training, security verification, continuous monitoring, and real-time analysis.[178]

The Information Technology Infrastructure Library (ITIL) defines the organizational structure and skill requirements of an information technology (IT) organization and a set of standard operational management procedures and practices designed to manage an IT operation and associated infrastructure, such as an ECR.[179] In Canada and some US States, many public registries and managed IT services use ITIL as the industry standard for managing those services. ITIL has been used in Canada for more than 15 years, for public registries in particular. Some organizations require ITIL certification for persons implementing or upgrading ECRs.

16. User-Centered Design

Definition: The property that the approach to the design and development of the registry aims to make the registry more usable by focusing on how the registry is used and applying human factors/ergonomics and usability knowledge and techniques.

The terms *ergonomics* and *usability* are key elements of this definition. ISO defines ergonomics as the "scientific discipline concerned with the understanding of interactions among human and other elements of a system, and the profession that applies theory, principles, data and methods to design in order *to optimize* human well-being *and overall system performance*."[180] Usability is defined as the "extent to which a system, product

[174] *Id.* at § 5.2.
[175] *Id.*
[176] *Id.*
[177] *Id.* § 5.2.4.
[178] *See Recommended Security Controls for Federal Information Systems: Special Publication 800-53, supra* note 165 at Appendix E.
[179] *See* www.itlibrary.org, (last accessed Dec. 21, 2020).
[180] ISO 9241-210:2019 §3.5, (emphasis added).

or service can be used by specified users *to achieve specified goals with effectiveness, efficiency and satisfaction* [].”[181] Thus User-Centered Design (UCD) focuses on user-friendly factors to achieve the overarching goal of optimizing overall system performance, effectiveness, and efficiency.

In the context of ECRs, UCD complements Accessibility. The principles set out in the Web Content Accessibility Guidelines (WCAG) are themselves user-centered, stipulating that the user interface be perceivable, operable, understandable, and robust, to meet the needs of all users including those with disabilities.[182] (See Accessibility – CPF 2, *supra*). But UCD goes further, addressing user satisfaction and user experience (UX). UCD features aimed at improving UX may not be statutorily required, but nonetheless may be key to efficient use of the system and may have the added benefit of reducing data entry errors and improving data quality.[183]

An ECR should include a user-interface designed around the needs of its users to encourage its adoption and optimize its benefits and UX.[184] To achieve this, UCD requires engagement with users, to understand not just what they do, but why they do it.[185] UCD is an iterative process of research, design, redesign, and adaption, based on user feedback (initially from system testers) that should be part of every stage of the design and development process and not end with the launch of the ECR, but continue throughout its lifetime.[186]

Involving users to suggest design criteria and validate design changes, and responding to their needs is essential to the process, which should also include feedback from periodic meetings with stakeholders, beta-testing, help-desk call logs, analytics, questionnaires, and surveys.[187] A multi-disciplinary team should be involved in the process, including, among others, members with experience in software development,

---

[181] ISO 9241-210:2019 §3.13, (emphasis added).
[182] *See* WCAG 2.1 at a Glance, https://www.w3.org/WAI/standards-guidelines/wcag/glance/, (last accessed Dec. 17, 2020).
[183] *See* Gavin McCosker and Peter Edwards, Responsibility or Control? Choosing the Right Digital Operating Model for Registry Services, 5, CBLJ 2017, 17 (copy on file at NatLaw).
[184] *Id.* at 15-16.
[185] *See* ISO 9241-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems at 3.7, https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en, (last accessed Dec. 28, 2020); *and see* User Research in Government – Understanding the Problem is Key to Fixing It, https://userresearch.blog.gov.uk/2016/01/12/understanding-the-problem-is-key-to-fixing-it/, (last accessed Dec. 28, 2020).
[186] *See* User Centered Design, Interaction Design Foundation, https://www.interaction-design.org/literature/topics/user-centered-design, (last accessed Dec. 28, 2020); *and see* User-Centered Design: a Beginner’s Guide, (Justin Mind, Jul. 14, 2020), https://www.justinmind.com/blog/user-centered-design/, (last accessed Dec. 28, 2020).
[187] User Research in Government, *supra* note 185.

content design, product delivery, customer service, psychology, ergonomics, and user research.[188]

UCD contributes to UX and ease of use of an ECR, and to overall user friendliness. More broadly, user friendliness includes inviting, and responding to user feedback and the process of consulting with users to foster long-term effectiveness and confidence in the ECR. Soliciting user input to ECR design and enhancement is crucial. Users frequently don't use an electronic system in the manner in which its designers expected. This makes it essential to ask the users how they use the system and what features are lacking or could be improved. For example, the IR discovered that its users printed data entry screens because the system did not provide an alternate means of fully documenting data entry. Some users have highly specialized tasks that they conduct repeatedly, such as creating user accounts for clients. Optimal design features for such users are likely to be different from those envisaged for a user expected to create only a single account.

Beyond the functional aspects of the design (is it effective and efficient to use?), UCD should also address UX, which includes a user's perception of the ECR and their response to using it, including their emotional reaction.[189] At one end of the spectrum are systems that are frustratingly difficult to understand and inefficient to use. At the other end of the spectrum are systems that are user-friendly with intuitive interfaces and helpful features that efficiently accomplish system functions. UX is a product of the ECR's reputation, and its user-interface presentation, functionality, performance, interactive behavior, and assistive capabilities, but also of the user's prior experiences, attitudes, skills, and abilities, which the developer must therefore understand and take into consideration when designing the user interface.[190] A primary goal of UCD is to make the system obvious to use and easy to learn and understand – public registries should, to the extent feasible, enable users to rely on what they see displayed on the screen and to understand it without the assistance of a lawyer.

Technical innovations, concomitant user sophistication, and market developments mean that user needs and expectations are constantly changing. In annual surveys conducted by the IR, its users consistently emphasized improved usability as a primary goal, despite continual improvements. To maintain user satisfaction requires going beyond basic functionality to address users' needs and expectations. Enhancements in response to industry and stakeholder feedback may include UCD features that improve UX and increase user adoption and satisfaction. Some of these may also promote more efficient and reliable data entry. For example, a report listing registrations that are about to expire

[188] *See* Simple, Clear and Fast Public Services – Have a Multidisciplinary Team, Australian Govt. – Digital Transformation Agency, https://www.dta.gov.au/help-and-advice/digital-service-standard/digital-service-standard-criteria/2-have-multidisciplinary-team, (last accessed Dec. 28, 2020).
[189] *See* ISO 9241-210:2019, *supra* note 185, at 3.15.
[190] *Id.*

alerts users to extend registrations to maintain priority.[191] The IR's Closing Room is an example of a registry feature that is not required by the legal framework but is a result of UCD.[192] The Closing Room greatly increases the efficiency of sequential registrations and is one of the IR's most popular features.

A user interface that is difficult to navigate or complex to use is more likely to result in user error than a more intuitive to understand, user-friendly interface. The potential for registrar liability increases with each user error caused by a faulty design. UCD can optimize user interface design to improve usability and data-entry efficiency and accuracy, thereby reducing registrar exposure to liability arising from user errors attributable to poor or inadequate system design. Furthermore, UCD can improve the effectiveness of other CPFs, such as Accessibility and Reliability (of the data entered by a user as well as of a searcher's attempts to search the ECR). Thus, UCD can reduce the risk of improper use arising from these CPFs and demonstrate the registrar's due diligence in addressing them.

Technical
ISO 9241-210:2019 is intended to provide information on human factors/ergonomics and usability to help those responsible for managing hardware and software design and re-design processes. [193] It provides requirements and recommendations for UCD principles and activities throughout the life cycle of computer-based interactive systems. It focuses on the ways in which both hardware and software components of interactive systems can enhance human–system interaction.

17. Validation

Definition: The process of confirming, using objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Validation of data entries improves the quality of data in a registry by rejecting submissions that do not conform to required data specifications. Validation checks that data submitted is both syntactically and semantically valid (in that order) before using it in any way (including displaying it back to the user).[194] Syntax validation checks that the data is in the expected form.[195] For example, verifying that a required field (e.g., to enter a collateral description) has not been left blank or that the required number of digits for an ID number identifying the grantor have been entered. Semantic Validation includes only accepting data that is within an acceptable range according to the rules of

[191] *Id.*
[192] *See* Regulations and Procedures for the International Registry, § 5.21, ICAO (2019).
[193] For the ISO definition of UCD, *see* ISO 9241-210:2019 §3.7.
[194] *See* https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs, (last accessed Dec. 22, 2020).
[195] *Id.*

the ECR.[196] Validation also relates to functions after a record has been created, such as precluding the registration of a cancellation with respect to a registration that has been already cancelled.

Validation improves the Integrity and Reliability of data in the ECR but does not entail verifying whether the data is accurate (especially information entered in free text fields in the registration form) or submitted pursuant to an authorization. These are not the functions that ECRs perform. The registrar is not in a position to determine whether a registration is valid.[197] Some ECR data may lack those two elements (accuracy and authorization), but Integrity of the data, as submitted, is ensured when the data is protected against alteration or destruction. Similarly, the primary concern of the IR is the Integrity of the data rather than its accuracy.[198]

The IR conducts signature Validation to improve data Integrity as well as to prevent malicious behavior. This entails not storing a registration until the submitted data has been emailed to the registrant and returned (unmodified) with an electronic signature that has been verified.

Validation also plays a role in protecting the registry from attempts to gain unauthorized access (e.g., to prevent SQL injection attacks, which imbed a database instruction within submitted data).[199]

Technical

The definition of Validation is based on the ISO/IEC 27000:2018 definition with additional support from ISO 9000 and CNSSI.[200]

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.[201] Among its resources for assisting developers implement web application security are the OWASP Top Ten Proactive Controls 2018 – a list of defensive techniques and controls that should be considered for

[196] *Id*.
[197] Cowan & Gallagher, *supra* note 14 at 231.
[198] *Id.* at 236-37.
[199] *See* https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html, (last accessed Dec. 22, 2020).
[200] *See* ISO 9000:2015 - Quality management systems – Fundamentals and vocabulary, ISO (Sep. 2015); *and see* CNSSI-4009, Committee on National Security Systems (CNSSI) (2015) at 130, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf, (last accessed Dec. 28, 2020); *see also* ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[201] *See* https://owasp.org/, (last accessed Dec. 22, 2020).

every software development project.[202] Ranked in order of importance, Validation is fifth on the list .[203]

Legal
The UNCITRAL Model Registry Provisions require a registry to reject a registration form in which no information is entered for a mandatory designated field but prohibit further scrutiny of its content.[204]

International Registry
The IR does not verify external facts or whether the registration relates to a transaction covered by the CTC.[205] In this vein, CTC Article 18(2) provides that the Registrar has no duty to determine whether a registration is properly authorized.[206]

III. IDENTIFICATION OF RELEVANT TECHNICAL STANDARDS

Without specifically designated best practice standards, information systems administrators have looked to existing industry practices, and authoritative standards of recommended or mandated practices as the *de facto* sources of best practices. These may be issued by national and international standards bodies, specialized industry associations, developers and manufacturers of widely used information technology (IT) software and hardware, as well as by IT service providers. This Part of the Working Paper introduces some of these technical standards, many of which were cited to in the preceding sections. This overview is by no means an exhaustive list, nor is it a comprehensive summary of the standards mentioned, but rather, it assists in explaining why certain standards were chosen to underpin the technical aspects of CPFs.

Standards for technical implementation are divided by subject matter and functionality. Modern ECRs comprise record management, networking, and cloud computing services in order to make the system usable for remote users. Standards related to any of these areas are therefore relevant to the CPFs underpinning ECRs.

The International Standards Organization (ISO) develops widely adopted standards through consultation of a broad range of experts. The process is guided by technical

[202] *See* https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs, (last accessed Dec. 22, 2020).
[203] *See* https://owasp.org/www-project-proactive-controls/v3/en/0x04-introduction, (last accessed Dec. 22, 2020).
[204] *See* UNCITRAL Model Law, Model Registry Provisions, arts. 6(1)(a), 7(3).
[205] *See* CTC Official Commentary 2.197 (4th ed. 2019); CTC art 19(1) provides that 'A registration shall be valid only if made in conformity with Article 20.'
[206] CTC Article 18(2) provides that 'The Registrar shall not be under a duty to enquire whether a consent to registration under Article 20 has in fact been given or is valid.'

committees that oversee the review and update of these standards. Of particular note for information systems are the ISO27001 series of standards.

The National Institute of Standards and Technology (NIST) in the United States has developed a series of standards and publications addressing information systems security. The NIST is responsible for developing information security standards and guidelines for federal information systems.[207] Within NIST, the Information Technology Laboratory (ITL) is responsible for the development of management, administrative, technical, and physical standards and guidelines for cost-effective security of information and protection of individuals' privacy in federal information systems (other than national security-related systems).[208] The 800-series Special Publications (SP) include ITL's guidelines for information systems security.[209] Topics on information systems security covered by ISO/IEC 27001 can generally be found in SP 800-53.[210]

The NIST handbook on information security (SP 800-100) details issues related to staff responsibilities, staff training, service agreements with vendors, risk assessment, incident response.[211] In comparison to ISO27001, the NIST handbook is presented in a less technical that some registry operators and designers may find helpful when adopting the ISO standard.

Cybersecurity addresses similar threats to information security, but focuses on external threats.[212] NIST's Cybersecurity Framework (CSF) is especially helpful as a guide to establishing, or strengthening, cybersecurity procedures around a core framework of five concurrent and continuous functions: "Identify, Protect, Detect, Respond, Recover."[213] The CSF is technology neutral and relies on existing global standards, guidelines, and practices that evolve with technology and business requirements.[214] The five core functions are intended to be carried out concurrently and continuously to adaptively respond to the dynamics of cybersecurity risk.[215] The five functions develop attributes necessary for an organization to address cybersecurity risk:

i) *Identify* develops the necessary understanding to manage cybersecurity risk;

---

[207] *Id.* at i.
[208] *Id.* at ii.
[209] *Id.*
[210] *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NIST (2018), at Table 2: Framework Core, *citing* ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4, https://doi.org/10.6028/NIST.CSWP.04162018, (last accessed Dec. 28, 2020).
[211] Information Security Handbook: A Guide for Managers - NIST Special Publication 800-100, NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, (last accessed Dec. 28, 2020).
[212] *See ISO/IEC TR 27103:2018* at Intro.
[213] *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NIST (2018), at 3, https://doi.org/10.6028/NIST.CSWP.04162018 (last accessed Dec. 28, 2020).
[214] *Id.* at 2.
[215] *Id.* at 7.

ii) *Protect* develops and implements appropriate safeguards to ensure service delivery;
iii) *Detect* develops and implements processes to identify the occurrence of a cybersecurity event;
iv) *Respond* develops and implements responses to detected events; and
v) *Recover* develops and implements plans to maintain resiliency and restore services impaired by cybersecurity incidents.[216]

Each function is divided into categories and subcategories. The CSF provides references to the relevant sections of multiple international and NIST standards for each subcategory.[217] For example *Protect* is divided into six categories which are further divided into subcategories (e.g. "Remote access" is one of seven subcategories under the *Protect* category named "Identity management, authentication and access control").[218] For each subcategory, the CSF provides citations to specific sections of relevant standards which generally include, among others, ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4.[219]

The ISO standard, ISO/IEC TR 27103:2018 is similar to the CSF – it "provides guidance on how to leverage existing standards in a cybersecurity framework."[220] ISO/IEC TR 27103:2018 incorporates a framework of the same five core functions as the CSF: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*.[221] The ISO standard's core functions include many of the same categories as the CSF.[222]

Table 2: List of standards used in assessment of CPFs.

Category	**Standard**	**Scope**
Record management	ISO 15489-1:2016	Records management
	ISO/IEC 9798	Entity authentication
	ISO/TR 13028:2010	Digitization of records

[216] *Id.* at 7-8.
[217] *See Id.* at Table 2: Framework Core. The CSF is available as a free download from the NIST website in English, Spanish, and Arabic. *See* https://www.nist.gov/cyberframework/framework, (last accessed Dec. 28, 2020).
[218] *Id.* at 29.
[219] *Id.*
[220] *See* https://www.iso.org/standard/72437.html, (last accessed Dec. 28, 2020).
[221] ISO/IEC TR 27103:2018, § 6.2, https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27103:ed-1:v1:en, (last accessed Dec. 28, 2020).
[222] *See Id*. at Annex A.

	ISO/TR 17068:2017	Trusted third party repository for digital records
	ISO 13008:2012	Migration of records
Information security	ISO/IEC 27001	Information security management
	ISO/IEC 38500:2015	IT governance
	NIST Cybersecurity Framework (CSF)	Critical infrastructure cybersecurity
	NIST SP 800-53	Security and Privacy Controls
	NIST SP 800-100	Information security and response
	NIST SP 800-160	Systems Security Engineering
	NIST FIPS PUB 199	Standards for Security Categorization
	NIST FIPS PUB 200	Security Requirements
Networking	RFC 2196	Secure development of information systems connected to the Internet
	ISO/IEC 27033-3: 2010	Network security

1. Limitations of Technical Standards

While there is tremendous value in utilizing standards, they are not without their limitations. For example, a caveat of the ISO 27000 family of standards is that the determination of which controls a user should implement is based on the user's own assessment of risk and the user's selection of controls to address the risks it identified.[223] Certification of compliance with the standard is achieved through an audit of the implementation and effectiveness of the selected controls rather than an analysis of the risk assessment and choice of controls.[224] Thus, the standard offers the advantages of a flexible approach but relies on the user's expertise in risk assessment and security to develop an appropriate solution.[225] Applying the standard to a less than optimal solution would only result in a false sense of security. As the British Computer Society (BCS) points out, "it is perfectly possible to be fully compliant with the standard, but be insecure."[226] Reliance on standards as a single, exhaustive measure by which to achieve a state of best practice overlooks the need to follow up their deployment by monitoring and evaluating their effectiveness in order to refine, adapt, and develop the optimal strategy for each registry.

Steps taken to address risks to ECRs should include, among others, employing independent expert information and communications technology (ICT) security consultants to validate the adequacy of security measures through an annual security audit followed, six months later, by a progress review of issues raised by the audit.[227]

2. Information Security Continuous Monitoring (ISCM)

Ongoing monitoring of information security is a critical component of risk management.[228] Information security does not end with the installation of hardware or software, or by announcing a security policy.[229] Instead, continuous monitoring and management is required to protect the confidentiality, integrity, and availability of information.[230] With evolving technology come new threats and vulnerabilities that must

[223] *ISO 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management*, ISO, 2005.
[224] *Id.*
[225] *Why ISO 27001 Is Not Enough* (BCS, 2009), https://www.bcs.org/content-hub/why-iso-27001-is-not-enough/#:~:text=A%20key%20issue%20is%20that,standard%2C%20not%20a%20security%20standard.&text=The%20organisation%20decides%20what%20level,an%20acceptable%20level%20of%20risk, (last accessed Dec. 28, 2020).
[226] *Id.*
[227] For the IR, *see* Cowan & Gallagher, *supra* note 14, at 253.
[228] Kelley Dempsey et al., *NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST (2011), at vi, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf, (last accessed Dec. 28, 2020).
[229] Michael Nieles et al., *NIST Special Publication 800-12 Rev 1: An Introduction to Information Security*, NIST (2017), § 2.7, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, (last accessed Dec. 28, 2020).
[230] *Id.*

be identified and addressed.[231] Information Security Continuous Monitoring (ISCM) is defined as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." [232] NIST Special Publication 800-137 offers guidelines to assist organizations develop an ISCM strategy and implement an ISCM program to monitor threats and vulnerabilities, and the effectiveness of deployed security controls.[233] A registry's ISCM strategy must be based on a clear understanding of security risks that the registry faces and provide meaningful metrics of security effectiveness and compliance with the registry's requirements, including regulations, policies, goals, and standards. [234] By providing actionable information on security status, an effective ISCM program advances the registry from compliance-driven risk management to data-driven risk management.[235]

3. Best Practices Recommended by Industry

Best practices and standards adopted by industry provide input for the creation of international standards, such as the ISO standards, which are developed by experts from industry, governments, academia, and other organizations.[236] This Section presents some common sources of industry standards.

A recent survey of 453 database professionals in 40 countries found that 42% followed published best practices but also developed their own.[237] Another 33% partially followed best practice guidelines.[238] The survey found that two common sources of best practices were software vendors' websites and industry whitepapers. [239] For sources of best practices, 27% always used software vendors' websites while 68% sometimes used them; 21% of respondents always used industry whitepapers and 73% sometimes used them.

Industry organizations often develop and publish best practices for their industry or segment of interest. Examples include the Storage Networking Industry Association (SNIA) and the Data Management Association (DAMA). Some vendors and manufacturers also publish best practices that may be specific to their products or more

---

[231] *Id.*
[232] Kelley Dempsey et al., *supra* note 228, at vi.
[233] *Id.* at 3.
[234] *Id.* at vi.
[235] *Id.* at vii.
[236] *See* ISO, ISO in Brief, 10, (ISO, 2019), https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf, (last accessed Dec. 29, 2020).
[237] Victoria Holt *et al*, *supra* note 10, at 163–181. Most of the respondents had worked for more than ten years in the database field; 40% were based in the U.S. and 33% in the U.K.; more than half worked for organizations with over 500 employees.
[238] *Id.*
[239] *Id.*

general but targeting markets that their products serve. Examples include Microsoft and Amazon Web Services (AWS).

Some of the best practices recommended by these industry publications reference international standards such as those promulgated by ISO and IEC. Other best practices published by manufacturers are specific to configuration and installation of specific products. The value of these publications being that following the manufacturer's recommendations is generally a best practice – keeping in mind that selection of the appropriate product remains the registry designer's responsibility.

Table 3: Examples of industry publications

Publisher	**Title**
Amazon Web Services	Using AWS in the Context of Common Privacy & Data Protection Considerations (2018)[240]
	AWS Well-Architected Framework (2020)[241]
Data Management Association (DAMA)	DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) (2017)[242]
Storage Networking Industry Association (SNIA)	Data Protection Best Practices (2017)[243]

IV. EVALUATION OF RISKS TO CPFS IN ELECTRONIC COLLATERAL REGISTRIES

[240] Using AWS in the Context of Common Privacy & Data Protection Considerations, AWS (May 2018), https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf?secd_dp3, (last accessed Dec. 28, 2020).
[241] AWS Well-Architected Framework, AWS (2020), https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf, (last accessed Dec. 28, 2020).
[242] *See* https://www.dama.org/cpages/body-of-knowledge, (last accessed Dec. 28, 2020).
[243] *Data Protection Best Practices*, Storage Networking Industry Association (SNIA) (Oct. 2017), https://www.snia.org/sites/default/files/DPCO/Data%20Protection%20BP%20White%20Paper%20Final%20v1_0.pdf, (last accessed Dec. 28, 2020).

Section II identified 17 CPFs essential for an ECR to perform its core functions. This Part takes a risk management approach to evaluating the importance of each CPF to the overall security of the ECR. Three CPFs, Confidentiality, Integrity, and Availability are often considered foundational to the overall security of information systems. In the context of ECRs, each of these three CPFs relies on the performance of other CPFs. Accordingly, the risk of negatively impacting the performance of any one of the CPFs should be considered a risk to the overall security of the ECR and its ability to perform its core functions.

A. IDENTIFYING ESSENTIAL ELEMENTS OF A COLLATERAL REGISTRY DATABASE

The CPFs are relevant to two distinct elements of an ECR:

1. A database containing transactional data (registrations); and
2. A database containing information about registry users.

More commonly, these two elements will be held in a single database, but in different parts. The first element does not include a database for information that some ECRs collect solely for statistical purposes. Since this information is not publicly disclosed, with the exception of aggregated statistics, it must be secured similarly to the information about the users. The collection of information for statistical purposes is not a universal model, and not contemplated in the UNCITRAL Model Law, so the application of the CPFs to that database is not examined. While these two elements may share similar risks and CPFs, the emphasis of risk management is different for each element, as is the corresponding hierarchy of related CPFs. For example, confidentiality is more of a concern for personal information and user passwords than for the information in registrations. Some registered information may however be confidential (e.g., an industry in which the debtor operates), and upon its entry into the registry be separated from the other information (e.g., collateral description), in which case Confidentiality (II.5) would apply to it. Similarly, Retention (II.13) and Integrity (II.8) are the primary concerns for transactional data. Both elements of the database require a similar emphasis on Authentication (II.3) and Access Control (II.1) before permitting data entry.

Thus, the importance of each CPF depends to some extent on the context of the specific data and operations they are applied to. For example, registrations must be publicly available at all times and be generally accessible, but the registration function may only be accessible to authenticated and authorized persons. Therefore, in the context of searching, Availability (II.4) and Accessibility (II.2) are far more important factors than Authentication and Validation (II.17). In the context of entering registrations, Availability, Authentication and Validation are important factors that contribute to Integrity. Retention and Integrity are of prime importance to all stakeholders. Nonetheless, best practices for information systems risk management dictate that, at a

holistic level, the system must manage risk commensurate with the highest level of risk in any of three major risk categories: Confidentiality, Integrity, and Availability. Therefore, before the risk management measures required for an ECR may be identified, the risk of non-performance of each CPF in the context of Confidentiality, Integrity, and Availability must be categorized.

B. DEFINING RISK IN ELECTRONIC COLLATERAL REGISTRIES

The risk that the registry won't be able to perform in the manner intended by its designers and expected by its users is inherently difficult to quantify because of its contextual and unpredictable nature – a function of registry implementation, required features, and both the physical and on-line environment that the registry is exposed to over time. As a result, it is generally not possible to reduce risk to zero. Instead, risk management techniques must be adopted to contain risk to an acceptable level. Risk management of an information system has been defined as:

> The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.[244]

This Section focuses mainly on security risks, but registries also face operational risk, reputational risk, and financial risk, among others. Internal auditors should ensure that both preventive and detective controls for these risks have been implemented. The audit should assess cybersecurity risk and response capabilities, with a focus on shortening response time. The Institute of Internal Auditors (IIA)[245] has defined a set of three layers of protection which has worked well for the IR. The IIA's Global Technology Audit Guide (GTAG), Assessing Cybersecurity Risk: The Three Lines Model, was designed to help internal auditors develop competence in providing assurance over cybersecurity risks.[246]

---

[244] U.S. Department of Commerce, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. https://doi.org/10.6028/NIST.FIPS.200, (last accessed Dec. 28, 2020).
[245] *See* https://global.theiia.org/Pages/globaliiaHome.aspx, (last accessed Dec. 23, 2020).
[246] *See* Institute of Internal Auditors, Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk – The Three Lines Model, (Institute of Internal Auditors), https://bookstore.theiia.org/global-technology-audit-guide-gtag-assessing-cybersecurity-risk-2, (last accessed Dec. 23, 2020).

Within information systems literature, security is often described in terms of a triad of three elements: confidentiality, integrity, and availability (CIA).[247] When any element of the CIA triad is compromised, the system is insecure. Thus, risk management focusses on assessing and reducing the risk to these three CPFs.[248]

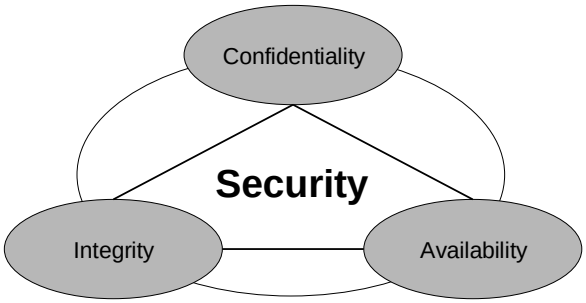

Figure 1: Model of the security triad in information systems.

The three CPFs that form the triad can be considered core CPFs, whose performance is enhanced by, or dependent on 13 other CPFs:

1. Confidentiality requires: Authentication and Access Control to prevent unauthorized access to confidential information (e.g. a user's personal information should only be accessible by that specific user or as specifically authorized for registry purposes – for example, billing information).
2. Integrity requires: Reliability, Retention, Validation, and in some cases: Authentication, Access Control, and Disposition. User-Centered Design may improve data entry accuracy. The Legal Authority of the Registrar to correct errors may be necessary from time to time.

---

[247] *See e.g.*, Michael Nieles et al., *NIST Special Publication 800-12 Rev 1: An Introduction to Information Security*, NIST (2017), § 1.4. *defining* "Security controls" as "The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the *confidentiality, availability, and integrity* of the system and its information." (emphasis added) and *explaining* that "In this document, the terms security controls, safeguards, security protections, and security measures have been used interchangeably." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, (last accessed Dec. 28, 2020); *and see* U.S. Department of Commerce, *supra* note 244, at 1, *explaining*, "[t]he generalized format for expressing the security category (SC) of an information system is:
SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)},
where the acceptable values for potential impact are low, moderate, or high."

[248] For cloud computing, a similar well-established triad consists of security, portability, and interoperability. *See generally*, NIST, NIST Cloud Computing Standards Roadmap: SP 500-291 Version 2, (NIST, Jul. 2013), http://dx.doi.org/10.6028/NIST.SP.500-291r2, (last accessed Dec. 22, 2020); *and see* CSCC, Interoperability and Portability for Cloud Computing: A Guide Version 2.0, (Cloud Standards Customer Council (CSCC), Dec. 2017), https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf, (last accessed Dec. 16, 2020).

3. Availability requires: Accessibility, Reliability, and Continuity; in certain cases, it may require Interoperability.

Legal Authority and Compliance provides the rules that define the requirements for the CIA triad; Trustworthiness is dependent on its effectiveness in securing the registry from potential risks, such as environmental disruptions, human errors, infrastructure failures, and purposeful attacks.[249]

Because risk in information systems is difficult to quantify, risk management focuses on the impact that would result if any of the CIA triad elements were compromised. In this context, for example, the operator may be required to classify impact as either low, moderate, or high for each of the three CIA elements.[250] This categorization must be conducted for each type of information contained in the information system.[251] For example, Confidentiality may be categorized as having a high impact on personal user data as mandated by privacy law. By contrast, the impact of Confidentiality with regard to notice registrations intended for public searches is low. The required security level for the information system is determined by the highest impact level assigned to any of the three CIA elements for any or the information types contained in the system.[252] For example, if the impact of Integrity is considered high for any information type, the system is considered to be a high impact system and must at a minimum employ security controls defined for high impact systems. This is true even if the impact of Availability and Confidentiality is considered to be low (i.e. the highest impact category of any datatype determines the required security level for the system as a whole).[253] For example, all information systems must enforce Access Control policies that limit access to authorized users.[254] However, testing to identify system vulnerabilities to unauthorized access (penetration testing) is only required for high impact information systems.[255]

---

[249] *See Recommended Security Controls for Federal Information Systems: Special Publication 800-53, supra* note 165, at 308, *defining* Trustworthiness as: "The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the **confidentiality, integrity, and availability** of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to can operate within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation." (emphasis added).

[250] Standards for Security Categorization of Federal Information and Information Systems - FIPS Pub. 199, at 4 NIST (2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf, (last accessed Dec. 28, 2020).

[251] *Id.*

[252] *Id.*

[253] Details of the minimum-security requirements that must be implemented for information systems in each of the three impact categories are set out in NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, *supra* note 23.

[254] *Id.* at 327.

[255] *Id.* at 328.

C. IDENTIFYING TYPES OF RISKS TO ELECTRONIC REGISTRIES

The NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems provide definitions and examples for determining the potential impact and corresponding security category of data contained in an information system based on the expected adverse effects of loss of confidentiality, integrity, or availability.[256] These definitions are adapted for ECRs in Table 4 below.

Table 4: Classification of Potential Impact

Potential Impact	**Extent of adverse effect on registry operations and assets**	**Examples of adverse effects that might result**
Low	Limited	i) degradation in registry capability to an extent and duration that the registry is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; ii) minor damage to registry assets; or iii) minor financial loss.
Moderate	Serious	i) significant degradation in registry capability to an extent and duration that the registry is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; ii) significant damage to registry assets; or iii) significant financial loss.
High	Severe or catastrophic	i) severe degradation in or loss of registry capability to an extent and duration that the registry is not able to perform one or more of its primary functions; ii) major damage to registry assets; or iii) major financial loss.

Table 5 identifies the result of non-performance for each of the identified CPFs and suggests the level of impact (low, moderate, or high) this may have on an ECR. Legal Authority and Compliance is not included in Table 5 because it is considered

[256] FIPS Pub. 199, *supra* note 250.

foundational and essential to the performance of the other 16 CPFs. Trustworthiness is not included because it arises from the effectiveness of the other 16 CPFs rather than being a prerequisite for them.

Table 5: Risks and impacts of CPF non-performance

Critical performance factors	**Result of non-performance**	**Impact**
1. Access Control	Inability to restrict privileged access and control. This can negatively impact other CPFs including Confidentiality, Integrity, and Reliability (e.g. unauthorized registrations may be submitted).	High
2. Accessibility	Some resources within the registry or the entire registry are unavailable.	Moderate to high depending on duration
3. Authentication	Inability to verify users and those with privileged access and control. This can negatively impact other CPFs including Confidentiality, Integrity, and Reliability (e.g. unauthorized registrations may be submitted).	High
4. Availability	Users are unable to query or submit information to the registry. (In general, ECRs should be accessible 24 hours a day, every day of the year.	Moderate to high (occasional brief periods of scheduled unavailability may be acceptable)
5. Confidentiality	Information may be acquired by unintended recipients (e.g. personal user information may be acquired by a third party).[257]	High for certain information (e.g. PII); low for notices of security rights
6. Continuity	Resources within the registry or the entire registry are unavailable.	Moderate to high depending on duration of unavailability

[257] For example, *see Id.* § 4.1, ICAO (2019), "Each registry user entity may elect to exclude from the information generated by a search under Section 7.6 its physical address and administrator's telephone number, and in the case of a natural person, his/her date of birth."

7. Disposition	Personal user information is retained in the registry beyond time limits mandated by general retention of records law.	Low to High depending on legal requirements
8. Integrity	The quality of the data is corrupted and not accurate.	High
9. Interoperability	The information is unable to be shared with other registries; information from other registries is unable to be accessed.	Low where not required by law. High if required by law
10. Legal Authority of the Registrar	The quality of the data is corrupted, and a corrective action is not taken promptly.	High
11. Reliability	Search results are incomplete.	High
12. Retention	Effective registrations are not returned in a search.	High
13. Timeliness	Registrations are not immediately searchable or effective.	Moderate to High depending on duration
14. User-Centered Design	The quality of data entry may be compromised.	High
15. Validation	Unable to guarantee that information required to process a registration has been entered.	High

D. CATEGORIZING THE IMPACT RISK OF THREATS TO A REGISTRY

From the above discussion, we can now categorize the CPFs identified for an ECR by their role in the CIA triad and the potential impact of their non-performance to the security. The categorization will depend on the type of registry, including its purpose, as well as the circumstances. Table 6 groups the CPFs by their relevance to the CIA triad and by impact level.

Table 6: CPFs grouped by relevance to the CIA triad and by impact level

CIA Triad Group	CPF	Impact

Confidentiality	Access Control	High
	Authentication	High
Integrity	Access Control	High
	Authentication	High
	Reliability	High
	Retention	High
	Validation	High
	Legal Authority of the Registrar	High
	Disposition	Low to High
	User-Centered Design	Low to High
Availability	Reliability	High
	Continuity	High
	Accessibility	Moderate
	Timeliness	Moderate
	Interoperability	Low to High

A high impact level for any one of the triad groups signals that the registry warrants implementation of high security levels.

V. CONCLUSION

This Working Paper has presented 17 Critical Performance Factors (CPFs) essential for the design, operation, and long-term success of electronic collateral registries (ECRs). These CPFs represent best practices that eliminate or mitigate the risks and liabilities faced by ECRs in performing their core functions. In addition, the CPFs ensure, among other objectives, that the system is continuously available and accessible to all users, and designed to meet their needs, regardless of sophistication.

As part of the BPER project, development of this Working Paper has been the focus of four international workshops and has benefitted from the contributions of a diverse group of experts in ECRs, both domestic and international, as well as other types of public registries.

Although originally conceived to identify the best practices required by Article 28 of the CTC to shield the International Registry from liability, this Working Paper is intended to provide guidance to the designers and operators of ECRs more broadly, such as for establishing a standard for accountability of registrars rather than for liability. Most of the CPFs and cited standards are relevant to electronic registries generally. For each of the CPFs, the Working Paper has provided references. Some of the referenced sources are technical standards, others provide legal guidance, and some are intended for a more general audience.

Registry operators of ECRs require a core competency in IT and in the law. It is hoped that this Working Paper will serve as a useful guide to the intersection of those two competencies. In particular, the body of knowledge contained in this Working Paper provides guidance on the legal aspects, relevant standards, and best practices required to implement the transition from a paper-based registry to an electronic system, or to establish a new ECR.