GUIDE ON BEST PRACTICES FOR ELECTRONIC BUSINESS REGISTRIES

Preliminary Draft for Consultation

Cape Town Convention Academic Project August 2025 UNIDROIT

ACKNOWLEDGEMENTS

TBA.

MESSAGE FROM THE DIRECTORS

TBA.

FOREWORDS

TBA.

CONTENTS

ACRONYMS AND ABBREVIATIONS

3CL - University of Cambridge Faculty of Law, Centre for Corporate and Commercial Law

3LoD – Three Lines of Defence

ABAC – Attribute-Based Access Control

AI – Artificial Intelligence

AML – Anti Money Laundering

API - Application Programming Interface

AWG - Aviation Working Group

AWS - Amazon Web Services

B2G - Business to Government

BCM - Business Continuity Management

BCS - British Computer Society

BO – Beneficial Owner

BPER - Best Practices in the Field of Electronic Registry Design and Operation

BRIS - Business Register Interconnection System

CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart

CIA - Confidentiality, Integrity, and Availability

CFT - Combating the Financing of Terrorism

CPF - Critical Performance Factor

CSF - National Institute of Standards and Technology's Cybersecurity Framework

CTC - Cape Town Convention on International Interests in Mobile Equipment

CTCAP - Cape Town Convention Academic Project

DAC – Discretionary Access Control

DAMA - Data Management Association

DR - Disaster Recovery

EBR - Electronic Business Registries

EBRA – European Business Registry Association

ECR - Electronic Collateral Registries

ELI – European Law Institute

EU – European Union

FATF - Financial Action Task Force

GATS - Global Aircraft Trading System

GDPR - European Union’s General Data Protection Regulation

IACA - International Association of Commercial Administrators

ICT - Information and Communications Technology

IdM - Identity Management

IEEE - Institute of Electrical and Electronics Engineers

IFC - International Finance Corporation of the World Bank Group

IIA - Institute of Internal Auditors

ISCM - Information Security Continuous Monitoring

ISO - International Organization for Standardization

IT - Information Technology

ITIL - Information Technology Infrastructure Library

KYC - Know Your Customer

MFA – Multi-Factor Authentication

ML – Machine Learning

MTBF – Mean Time Between Failures

MTTR - Mean Time to Repair

NFPA - National Fire Protection Association

NIST - National Institute of Standards and Technology

OWASP - Open Web Application Security Project

PII - Personally Identifiable Information

PKI - Public Key Infrastructure

PoLP – Principle of Least Privilege

RBAC - Role Based Access Control

REST - Representational State Transfer

RPO - Recovery Point Objective

RTO - Recovery Time Objective

SNIA - Storage Networking Industry Association

SOAP - Simple Object Access Protocol

SoD – Segregation of Duties

SP - Special Publication

SPOF - Single Point of Failure

TTPR - Trusted Third Party Repository

UBO - Ultimate Beneficial Owner

UCD - User-Centred Design

UNCITRAL - United Nations Commission on International Trade Law

UNIDROIT – International Institute for the Unification of Private Law

UX - User Experience

WCAG - Web Content Accessibility Guidelines

WS-Security - Web Services Security

XBRL - eXtensible Business Reporting Language

XML - Extensible Markup Language

I. INTRODUCTION

This Guide on Best Practices for Electronic Business 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 an initiative of the Cape Town Convention Academic Project, supported by the UNIDROIT Foundation and Aviareto.[1] The Cape Town Convention Academic Project is a joint undertaking between the International Institute for the Unification of Private Law (UNIDROIT) and the University of Cambridge Faculty of Law, under the auspices of the Centre for Corporate and Commercial Law (3CL), with the Aviation Working Group (AWG) as its founding sponsor.

The BPER Project originated from 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(1) of the Convention sets out a standard for the liability of its Registrars for errors, omissions, or malfunctions of the Registry and its staff, '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.' However, 'best practices in current use' in electronic registries was not defined by the CTC, nor had international parameters been identified.

Acknowledging the lack of comprehensive guidance on 'best practices', the BPER Project responded by developing a Guide on Best Practices for Electronic Collateral Registries, which was published in 2021. The evident need for such guidance inspired the BPER Project Group to continue its efforts. This Guide aims to extend the existing framework, successfully utilised to identify best practices for electronic collateral registries (ECRs), to encompass electronic business registries (EBRs). This expansion addresses pivotal issues and considerations within the business registration and operation landscapes. The adoption of best practices by business registries can limit their liabilities under domestic law as well as increase their effectiveness, enhance accuracy of registry data, and strengthen user trust in line with international standards.

A. SCOPE: ELECTRONIC BUSINESS REGISTRIES

In recent decades, digital transformation processes have impacted both the public and private sectors. Governments have increasingly been adopting electronic service delivery for business registration in response to the growing demands from residents and businesses for faster, more accessible, and convenient services. Electronic registries have emerged as a cornerstone of systems that collect, store, and disseminate data, and, in some cases, establish and transfer property rights. Even though the relevant domestic laws may not specify the use of best practices, registrars may be held liable for various failures in electronic systems that result in losses to their users.

[1] 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).

While not all business registries are fully accessible through electronic channels, most business registries have undergone some degree of digitisation. Even in cases where electronic services are unavailable to the public, business registry data is typically stored digitally in databases, and can be processed and transferred electronically to other information systems.

This Guide examines specific best practices for electronic business registries, encompassing systems that are fully based on electronic data submission and processing, and hybrid systems which also accept paper-based submissions.[2] The scope of this Guide excludes paper-only systems, as well as paper-based systems where documents are merely scanned for digital retrieval, as these do not leverage the full benefits of electronic registry systems.

Accordingly, the purpose of this Guide is to provide guidance to the designers and operators of electronic business registry systems at various stages of the digital transformation of business registry frameworks. In its Legislative Guide on Key Principles of a Business Registry, the United Nations Commission on International Trade Law (UNCITRAL) endorses electronic registries as the ultimate goal,[3] reflecting a strategic vision in harmony with the evolving technological landscape and global trend toward digitisation. This transition enhances not only efficiency and accessibility but also improves transparency, streamlines processes, and strengthens the overall effectiveness of business registry systems. Increased reliance on such electronic systems further emphasises the need to adopt best practices.

B. OVERVIEW OF BUSINESS REGISTRIES

Every jurisdiction maintains a business registry, which is essential for facilitating the formal operations of businesses within its respective economy. This registry forms part of a broader regulatory framework, which may also include taxation, social security authorities, and other relevant regulatory bodies.

Despite sharing similar objectives, business registries across different jurisdictions exhibit distinct characteristics, influenced by legal frameworks, administrative structures, technological maturity, and cultural norms. The following attributes highlight differences among business registries:

- Administrative or Judicial System — Business registration processes may be administered by an administrative authority, like in the United Kingdom, Australia, and Canada, or placed under a judicial system, like in Paraguay and France.

- Funding Model — The funding of business registries can differ, ranging from government funding, such as in Azerbaijan and Peru, to financing from registration fees or annual maintenance fees, like in Tunisia and France. Some jurisdictions also adopt mixed funding models, incorporating both public funds and contributions from users of registry information, such as in Paraguay and the Netherlands.

- Technological Maturity — Business registration services may be offered fully electronically or in a hybrid way with varying maturity levels of digitalisation across jurisdictions. For instance, the Danish Business Authority makes use of emerging machine learning (ML) technologies, while the Greek

[2] The CPFs provided in the present Guide are equally applicable to electronic components of hybrid business registry systems.

[3] UNCITRAL Legislative Guide on Key Principles of a Business Registry (2019), p. 28, https://uncitral.un.org/en/texts/msmes/legislativeguides/business_registry (last accessed 7 July 2025) ('UNCITRAL Legislative Guide').

Commercial Registry has implemented fully automated, real-time business registration but does not employ ML tools.

- Dissemination of Registry Information — The accessibility and availability of registry information differ greatly. Some jurisdictions provide comprehensive public access to registry data, while others may limit access and offer certain data through paid services. For instance, in Finland, basic data is available free of charge, but fees are charged for other data, such as the responsible persons for a business and information on capital. Certain jurisdictions impose restrictions on the reuse of registry data or limit access to commercial service providers.

- Centralised or Decentralised Registry — The choice between centralised and decentralised depends on factors such as the jurisdiction's administrative structure, technological capabilities, and regulatory policies. For example, business registries are centralised in Belgium, Chile, and Bangladesh, while in Spain and Canada, they are decentralised.

1.1. Registry Functions

The traditional role of a business registry is to provide businesses with an identity that is recognised by the State and to serve as an official repository of information related to registered businesses.

The fundamental functions of a business registry, which should be defined by legislation, are outlined as follows in the UNCITRAL Legislative Guide:

(a) registering the business when it fulfils the necessary conditions established by the law;

(b) providing access to publicly available registered information;

(c) assigning a unique identifier to the registered business;

(d) sharing information among the requisite public authorities;

(e) keeping the information in the business registry as current as possible;

(f) protecting the integrity of the information in the registry record;

(g) providing information on the establishment of the business, including the obligations and responsibilities of the business and the legal effects of the information publicly available on the business registry; and

(h) assisting businesses in searching and reserving a business name when required by the law.[4]

When these functions are categorised, the core components of a business registry revolve around three central aspects: data and information collection, storage, and provision to third parties. These elements form the foundation of business registries worldwide, serving as essential tools for promoting transparency, accountability, and legal compliance in the business environment.

[4] UNCITRAL Legislative Guide, Recommendation 10.

Data Collection	Data Storage	Data Provision
(a) Registering the business when it fulfils the necessary conditions established by the law (c) Assigning a unique identifier to the registered business (h) Assisting businesses in searching and reserving a business name when required by the law	(e) Keeping the information in the business registry as current as possible (f) Protecting the integrity of the information in the registry record	(b) Providing access to publicly available registered information (d) Sharing information among the requisite public authorities (g) Providing information on the establishment of the business

1.1.1. Data collection

The business registry is responsible for collecting and verifying data related to registered entities. This includes details on the legal form, establishment, management structure, legal status, financial standing, and any other information necessary for the identification and documentation of businesses.

The registration process legitimises businesses by formalising their existence, granting them legal status, and including them in the register. It involves the submission of required documents, verification of information, and the allocation of a unique identifier to each registered entity.

Different mechanisms are adopted across the world to verify data authenticity and ensure compliance with the legal requirements. The authority to examine and validate business data may be delegated to notaries, courts, or directly to business registries. In some systems, especially civil law jurisdictions, the registration process is subject to *ex-ante* verification by judicial authorities, where intermediaries like notaries and judges play a crucial role in verifying the data before registration. The information recorded in the registry is presumed to be accurate and complete, creating a legal presumption of reliability unless proven otherwise in accordance with established laws and regulations. Some jurisdictions, including common law systems, structure business registration as a ‘declaratory system’, making registration an administrative process without *ex-ante* judicial approval. This way, registries often lack this presumption of accuracy, relying more on *ex-post* judicial scrutiny to determine the credibility and reliability of information recorded in registries.

In jurisdictions where the business registry is solely responsible for the registration process, it is typically endowed with broader authority to verify data accuracy and quality. This expanded mandate often includes the power and responsibility to conduct thorough checks and verifications of submitted information, enforce stringent compliance measures, and impose penalties for inaccuracies or non-compliance.

1.1.2. Data storage

Once data is registered, the business registry employs a secure storage system to house this information. This system is designed to ensure that data is organised in a structured manner and is available whenever needed. Moreover, stringent security measures are implemented to safeguard the stored information against unauthorised access, tampering, or data breaches, preserving its integrity and confidentiality. Given that the trustworthiness and reliability of the business registry depend on the integrity and security of the stored information, maintaining robust data protection mechanisms is a priority. By upholding high standards for data integrity and cybersecurity, the registry maintains the trust of stakeholders and fulfils its crucial role as a dependable repository of business information.

1.1.3. Data provision

The business registry enables access to accurate and up-to-date information for a diverse range of third parties, including the public, government agencies, financial institutions, legal entities, etc. By maintaining and disseminating reliable and searchable business data in a suitable format, the registry facilitates informed decision-making and empowers stakeholders to engage in commercial activities with confidence, contributing to the overall integrity and efficiency of business transactions.

The business registry also provides data for statistical analysis and reporting, supporting the generation of accurate economic indicators and facilitating research and reporting across various sectors. Researchers and policymakers leverage registry data for in-depth studies, trend analyses, and policy assessments.

Importantly, the business registry contributes to regulatory enforcement by providing verified data for anti-money laundering (AML), counter-terrorism financing (CFT), counter-proliferation financing, and sanctions efforts. The availability of verified beneficial ownership (BO) data helps to conduct effective due diligence and risk assessments. The role of business registries is evolving, accelerated by their now electronic nature.

1.2. The evolving role of business registries

In today's dynamic business landscape, the traditional role of business registries has undergone a redefinition, transforming them into efficient service providers with multifaceted responsibilities that extend beyond record-keeping. Contemporary business registries are increasingly significant for economic development and governance. They achieve this, in part, by leveraging their vast datasets to generate valuable insights that benefit policymakers, researchers, financial institutions, and businesses. As described in Section 1.1.3, these insights are instrumental for business statistics and enhance policy design, thereby facilitating economic activities.

Furthermore, business registries act as catalysts for economic growth and investment facilitation by enabling online business registration and providing accessible, reliable, and up-to-date information.[5] Their commitment to efficiency, interconnection with other systems (such as collateral, statistical, and tax registries), and a user-centric approach are vital in supporting entrepreneurship and reducing bureaucratic barriers across borders. Business registries that embrace innovative technologies further streamline business operations and enhance supply chain transparency.

In response to global concerns related to money laundering, terrorism financing, and other illicit financial activities, business registries now function as vigilant gatekeepers in enforcing regulatory compliance. The World Bank's Data-Driven Company Registry Guidance Note[6] highlights this expanded role, underlining the

[5] Digitalisation of business registration services tends to improve not only foreign investment procedures but also general business establishment procedures, thereby reducing administrative hurdles not only for foreign investors but also for domestic businesses, including micro, small and medium-sized enterprises (MSMEs) and women-led businesses. See more: UNCTAD, World Investment Report 2024. Chapter IV "Investment Facilitation and digital government", https://unctad.org/system/files/official-document/wir2024_ch04_en.pdf (last accessed 15 May 2025).

[6] World Bank Group, Data-Driven Company Registry, Guidance note (2022), https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf (last accessed 7 February 2025).

prevention of fraud as a growing imperative for modern business registries. To effectively meet this challenge, registries not only integrate data from various governmental and financial systems but also leverage advanced analytics, pattern recognition, predictive modelling, and risk assessment frameworks. Through the integration of these advanced tools and technologies, business registries substantially contribute to efforts aimed at maintaining financial system integrity.

Moreover, business registries have become essential for ensuring tax compliance. Through collaborative initiatives with tax authorities, digital integration with tax systems, and enhanced data-sharing mechanisms, they facilitate the early detection of non-compliance and actively contribute to fostering a culture of tax responsibility among businesses. This proactive function as a tax compliance promoter further solidifies their position as integral participants in broader regulatory frameworks.

1.3. The evolving role of business registrars

In parallel with the transformation observed in the role of the business registry, a similar evolution is altering the responsibilities and expectations of the registrar. The traditional perception of the registrar as an administrator of records has shifted to encompass managerial oversight and adept navigation of dynamic legal, regulatory, technological, and business frameworks shaped by international and regional practices and national laws. Consequently, transformative leadership is a practical imperative for the registrar to ensure that the business registry remains fit for its purpose in this complex environment.

With the business registry assuming more functions, including compliance and oversight, growing reliance on registry data and customer expectations of speed, reliability and 24/7 access, the registrar should adopt a proactive and legally informed approach, exercising their functions with due diligence and transparency.[7] This role extends beyond internal management of records and cases to encompass the entire system, composed of legal, technical, compliance, and human resources aspects, as well as engagement with external stakeholders, including legislators, financial institutions, tax agencies, and social security authorities. This collaborative approach ensures that the registry aligns with both national and international standards and best practices, fostering an environment conducive to economic growth and regulatory compliance.

In summary, the transformation of the business registrar's role reflects a broader shift towards proactive, strategic, and technologically adept management within business registries, essential for maintaining their efficiency and relevance in today's complex business environment.

C. AUTOMATION AND EMERGING TECHNOLOGIES

This evolution of EBRs is leading to process automation based on both existing and emerging technologies. With the increasing expectation of immediate data at little or no cost, automation is indeed a best practice for EBRs, since it streamlines data collection, storage, and provision, significantly improving the overall efficiency, transparency, and security of EBRs.

[7] This change is underscored by the UNCITRAL Legislative Guide, which emphasises the importance of transparency and accountability in the registrar's role in its Recommendations 6 and 7.

Essentially, automation refers to actions carried out by computer systems without the necessary review or intervention of a natural person.[8] For EBRs, automation involves leveraging technology to execute routine processes without human intervention, such as application processing, fee calculation and payment, monitoring, amendments, annual returns, deregistration, and enforcement.[9] For instance, automated checks and alerts monitoring changes within the registry and relevant external data sources, along with automated notifications of non-filing of accounts by a registered company all enhance the accuracy of EBR records.

Automated processes can significantly reduce administrative costs, the risk of human error, and operational delays. Moreover, automation minimises manipulation and corruption risks by limiting direct interactions between applicants and registry staff, enabling real-time data verification, and facilitating seamless system-to-system integrations. Built-in checks for legal requirements or automated assignment of cases to case officers further reduce opportunities for manipulation, contributing to transparent and predictable EBR operation and increasing businesses' trust in the EBR.

Legislation directly impacts the level of automation of business registries. Clear, detailed rules that limit the discretionary power of registrars or registry staff and avoid exceptions simplify the automation of processes. Defined procedures and obligations reduce ambiguity and ensure that automated processes align consistently with regulatory requirements.[10]

However, automated and interactive machine-to-machine access control is often introduced in an *ad hoc* manner by system administrators, vendors, or integrators, leading to a lack of formal lifecycle management processes.[11] This underlines the need for a robust approach to automating processes and systems, ensuring that automation is implemented with design, testing, maintenance and risk management.

However, despite its advantages, automation may introduce challenges. Systematic maintenance and oversight are essential to ensure that automated processes do not inadvertently introduce new risks, such as vulnerabilities from software bugs or inadequate access controls.[12] Therefore, registries must adopt robust governance policies, conduct regular audits, and continuously monitor automated processes.

Notably, automation processes in EBRs must be tailored to the local ICT infrastructure, which may vary significantly between jurisdictions. In developing countries, challenges such as limited internet bandwidth, unreliable power supply, or outdated regulatory frameworks may hinder full-scale automation.[13] In these cases, phased implementation is advisable, starting with basic electronic services and progressively integrating more advanced functionalities as infrastructure improves.[14]

[8] UNCITRAL, Model Law on Automated Contracting (2025), https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf (last accessed 18 July 2025).

[9] Investment Climate Advisory Services by the World Bank Group, 2012, Innovative Solutions for Business Entry Reforms: A Global Analysis, (last accessed 24 March 2025).

[10] Id.

[11] NIST IR 7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH), 2015, (last accessed 24 March 2025).

[12] Investment Climate Advisory Services by the World Bank Group, 2012, Innovative Solutions for Business Entry Reforms: A Global Analysis (last accessed 24 March 2025).

[13] Willie, J. et al, (2011) World Bank, Investment Climate in Practice, Business Regulation - Leveraging technology to support business registration reform: insights from recent country experience; (last accessed 21 March 2025).

[14] UNCITRAL Legislative Guide.

Significant automation of business registration procedures can be achieved, requiring minimal or no intervention from the registrar to process applications and issue decisions on initial registrations or registration changes. The advanced level of automation allows EBRs to take *decision-making* actions carried out by computer systems without necessary review or oversight by a natural person,[15] for instance, real-time company registration. Attaining such a level of automation requires data validation using high-quality business registry data, complementary data, and data exchanged between stakeholders. The real-time company registration switches the registrar's focus from checking and processing registration applications to continuously improving EBR data management and algorithms. [16]

It should be noted that the broad term 'automated system' encompasses, amongst other things, artificial intelligence (AI) and ML systems. Automated systems can be programmed to operate in a deterministic or non-deterministic manner. Deterministic automated systems consistently generate the same output given the same input. By contrast, non-deterministic AI and ML systems adapt over time and generate outputs that may not be predicted in a particular case but fall within a range of possibilities.[17] Such technologies, including AI and ML, are increasingly used by the EBRs have the potential to further enhance their functionality. These technologies can be used for automated decision-making and optimise various registry functions, from automating document verification, customer support, and predictive analytics for identifying potential fraud or non-compliance, to refining backup management.[18] However, given the emerging nature of these technologies and the wide variety of standards and regulatory frameworks surrounding them, the present Guide does not delve into their technical specifics in detail. Maintaining the principle of technological neutrality, all CPFs outlined in this Guide remain relevant for EBRs regardless of the adoption of AI/ML capabilities.

Cloud computing is also recommended as an infrastructure solution for EBRs, offering cost reduction, scalability, and enhanced reliability through, for instance, elastic storage, automated disaster recovery, centralised hosting, and instantaneous data backup.[19] Cloud security standards, such as those outlined in ISO/IEC 27017, provide guidance on implementing secure cloud services, ensuring that data stored in the cloud is protected against unauthorised access and breaches. While this Guide acknowledges the advantages of cloud computing, it does not address in detail the specific opportunities and risks associated with its use. Instead, all CPFs defined in this Guide remain applicable regardless of the technological infrastructure adopted.

Automation and cloud computing are best practices for modern EBRs, augmenting their operational efficiency, reducing errors, and promoting transparency. Nevertheless, their effectiveness is contingent

[15] Legal rules on the validity and enforceability of automated decision making are still evolving in national law. For international and transnational instruments on automated decision making, see UNCITRAL, Model Law on Automated Contracting (2025), https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf (last accessed 18 July 2025) and European Law Institute (ELI) Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (2025), https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Algorithmic_Contracts/Guiding_Principles_and_Model_Rules_on_Digital_Assistants_for_Consumer_Contracts.pdf (last accessed 18 July 2025).

[16] World Bank Group, Data-Driven Company Registry, Guidance note (2022) (last accessed 27 Mar. 2025).

[17] UNCITRAL, Model Law on Automated Contracting (2025), para 29, **https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf** (last accessed 18 July 2025).

[18] OECD, Governing with Artificial Intelligence: Are governments ready?, 2024, OECD Artificial Intelligence Papers, No. 20, OECD Publishing, Paris, (last accessed 26 March 2025).

[19] P. Amadi-Echendu, J. E. Amadi-Echendu, 2016, Proceedings of PICMET '16: Technology Management for Social Innovation, A Study on Data and Information Integration for Conveyancing, Cadastre and Land Registry Automation (last accessed 24 March 2025).

upon the establishment of a robust legal framework, implementation of ongoing risk assessments, and deployment of reliable ICT infrastructure. Collectively, these elements allow EBRs to remain resilient, secure, and trustworthy over time.

D. RESEARCH OBJECTIVES: BEST PRACTICES AND CRITICAL PERFORMANCE FACTORS (CPFs) FOR EBRs

This Guide aims to apply the best practices identified in the context of ECRs to EBRs, and identify any additional best practices specific to this type of registry. Best practices refer to working methods or sets of working methods that are generally accepted as being the best to use in a particular business or industry.[20] Best practices not only mitigate risks and liabilities faced by EBRs in performing their core functions – they ensure that the systems are continuously available, accessible to all users, transparent and efficient.

Before the 2022 survey on e-services conducted by International Business Registry Insights, few studies had explored best practices for EBRs.[21] With responses received from 88 jurisdictions, the results of the survey on e-services demonstrated that 92% of business registries already accepted electronic applications for incorporation or entity formation for any entity type, while more than one-third of registry jurisdictions indicated that they were planning to adopt digital identity authentication to better perform and secure their services. This emphasises the pressing need to identify best practices relevant for business registries.

In the context of systems, the concept of best practice most commonly arises in organisational and manufacturing management, where a set of actions can be related to resulting outcomes.[22] 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.[23] Moreover, in order to determine the best practice, the comparison must include all relevant cases; otherwise, the best practice might be overlooked.[24]

Importantly, to be comparable – whether statistically or based on human judgment – the causal relationship between actions and outcomes must be quantifiable on a scientifically sound basis.[25] In practice, the above-stated conditions to confidently identify a best practice are rarely all met simultaneously.[26] Different styles of research, whether economic or technical, tend to produce incomplete or divergent insights and conclusions.[27]

Given these challenges, authoritative standards of recommended or mandated practices, rather than a comparison of existing industry practices, are often the *de facto* sources of best practices. These may be issued by international standards bodies, such as the International Organization for Standardization (ISO);

[20] Definition according to the Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/best-practice (last accessed 18 March 2025).

[21] The 2022 survey conducted by International Business Registry Insights explored best practices on E-Services. The survey, covering 88 registry jurisdictions in the Americas, Europe, Africa, Asia and Oceania, recorded responses concerning electronic filing, filer identification methods, the use of e-service solutions for various types of registry services, and emerging technologies. See more at International Business Registry Insights, E-Services, 2022, http://ibrr.net/reports/e-services-2022 (last accessed 26 February 2025).

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

[23] Id. at 310.

[24] Id.

[25] Id. at 311.

[26] Id.

[27] Michael Cusumano, In Search of Best Practice: Enduring Ideas in Strategy and Innovation, 11, (Oxford Univ. Press, 2010).

government agencies, such as the National Institute of Standards and Technology (NIST); industrial organisations, such as the Institute of Electrical and Electronics Engineers (IEEE); and other organisations with specialised knowledge in the relevant area, including manufacturers and software developers, especially regarding their own products. However, these standards do not comprehensively cover all aspects of the core functions of EBRs, highlighting the need for further research and refinement.

A 2013 survey of database professionals in 40 countries was conducted to determine the sources of best practices and the extent to which they are used.[28] Respondents reported that the most stringently controlled best practices were those related to database security, high availability resilience, and disaster recovery.[29] The survey also found that two of the most common sources of best practices were software vendors' websites and industry whitepapers, which predominantly focus on current technology.[30]

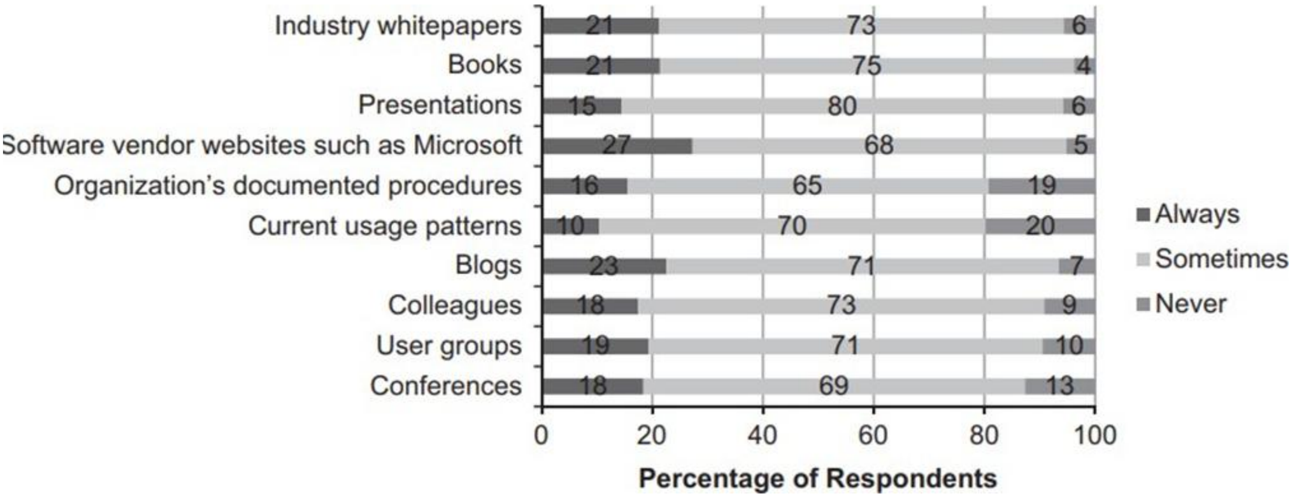


Figure 1. Responses to the question: Where do you personally find database best practice guidelines to follow? [31]

The Guide on Best Practices for Electronic Collateral Registries identified 17 critical performance factors (CPFs), 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 relevant market participants. Alternatively, CPFs can be considered as the characteristics of an ECR that make it fit for purpose. While all of those 17 CPFs remain largely applicable and reusable in the context of EBRs, two of them have been merged into one (CPF 18 on Retention and Disposition), and eight additional CPFs have been specifically identified for EBRs. Importantly, although the EBR Guide is fundamentally informed by the ECR Guide, it has been structured as a self-contained document with some terminology and aspects of best practices from the ECR Guide adjusted for clarity and applicability to EBRs.

Implementing best practices will allow EBRs to ensure that they are:

- accessible to all users, including persons with disabilities, with usable, inclusive, and publicly searchable interfaces and services;

[28] 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 7 February 2025).

[29] Id. at 168, 170.

[30] Id. at 163-81.

[31] Id. at 169

- authenticated, with all access and interactions validated through secure identification methods;
- governed by robust access control, defining clear roles to access, read, modify, or delete data;
- capable of providing a high level of confidentiality and privacy, protecting stored information from unauthorised disclosure;
- accurate and trustworthy, with mechanisms to detect, validate, and correct data throughout its lifecycle;
- interoperable, using open standards and APIs to exchange data efficiently and securely;
- monitored and logged, with tracking of errors, system events, and anomalies in real time;
- highly available and scalable, ensuring continuous service and capacity during peak usage;
- redundant, eliminating single points of failure (SPOFs) to maintain uninterrupted registry operations;
- secure, managing internal and external threats, including unauthorised access, tampering, malware, and denial of service attacks, within an appropriate risk management framework;
- resilient against operational vulnerabilities, including human error and negligence;
- prepared for natural or human-caused accidents and disasters;
- recoverable, with reliable backups and minimal downtime in case of catastrophic failure;
- immutable, ensuring all entries are tamper-proof and auditable;
- trusted by users and authorities alike, based on consistently applied standards, secure operations, and a record of reliability, transparency, and legal soundness; and
- subject to continual improvement, informed by lessons learned, feedback, and performance assessments.

Following best practices is important not only to mitigate the registrar's liability and implement its legal mandate, but also to enhance EBR performance and credibility. Globally, adherence to best practices facilitates compliance with international standards and fosters collaboration, creating an interoperable and accessible network of modern, responsive business registries. Importantly, best practices should not be applied in a rigid or uniform manner; their implementation must always be contextual, thoughtfully tailored to the specific legal, economic, and technological environment of each jurisdiction. When appropriately contextualised, best practices enable EBRs to evolve into resilient, trustworthy, and future-oriented institutions, reinforcing their role as trusted pillars of the business ecosystem.

E. LIMITATIONS OF TECHNICAL STANDARDS AND SELECTIVE ADOPTION

This Guide seeks to bridge the gap between ambitious best practices and their practical application within EBRs. While best practices establish a *de facto* benchmark for optimal performance, security, and trustworthiness, their implementation frequently relies on technical standards developed by recognised national and international bodies. These standards serve as widely accepted references for system design, risk management, service delivery, and information governance.

The technical standards referenced in this Guide are drawn from international, regional, and national standard-setters, among which the already-mentioned ISO and NIST, as well as the International Electrotechnical Commission (IEC) and the European Telecommunications Standards Institute (ETSI). ISO develops widely adopted standards through consultation with a broad range of experts. Together with IEC, it establishes joint technical committees that oversee the review and update of these standards. The NIST is responsible for developing management, administrative, technical, and physical standards and guidelines for cost-effective information security and protection of individuals' privacy in federal information systems in the United States. NIST's Special Publications and Federal Information Processing Standards are influential outside the United States and can be useful for EBRs worldwide. ETSI, among other regional bodies, sets relevant standards by taking into account specific regulatory contexts, for example, the European Interoperability Framework. All these organisations benefit from broad stakeholder engagement and periodic revision, which enhance the legitimacy and applicability of their outputs.

While there is tremendous value in utilising 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 registry should implement is based on the registry's own assessment of risk and its selection of controls to address the risks identified.[32] 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.[33] Thus, the standard offers the advantages of a flexible approach but relies on the registry's expertise in risk assessment and security to develop an appropriate solution.[34] 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'.[35] Reliance on standards as a single, exhaustive measure by which to achieve a state of best practices overlooks the need to follow up on deployment by monitoring and evaluating effectiveness in order to refine, adapt, and develop the optimal strategy for each registry.

In this regard, reliance on standards should not substitute critical analysis, institutional experience, or contextual judgment. Overreliance on formal certification may produce a false sense of security. EBRs are encouraged to supplement standard adoption[36] with independent expert information and insights from communications technology security consultants to validate the adequacy of security measures through annual security audits, followed by progress reviews of issues raised by the audits.

It is also neither practical nor necessary for EBRs to adopt every standard listed below in this Guide. Instead, the registry should (i) map each CPF and its performance in their design and operation, (ii) identify corresponding standards that support the legal, operational, and technological goals of the registry, (iii) document its rationale for selecting, adapting, or omitting specific standards, and (iv) review and revise standards in use as a part of continual improvement. This approach to adoption of the present Guide, proposed best practices and recommended standards supports informed and responsible decision-making.

F. LEGAL RELEVANCE OF BEST PRACTICES

[32] ISO 27002, Information Technology, Security Techniques, Code of Practice for Information Security Management, 2022, https://www.iso.org/standard/75652.html (last accessed 26 February 2025).

[33] Id.

[34] Why ISO 27001 Is Not Enough (BCS, 2009), https://www.bcs.org/articles-opinion-and-research/why-iso-27001-is-not-enough/ (last accessed 7 February 2025).

[35] Id.

[36] The present Guide does not provide recommendations regarding obtaining certification in any of the referenced standards.

EBRs are institutions of domestic law, which establishes their legal existence, defines the powers of the registrar, and determines the legal consequences of registration. The type of legislation governing EBRs varies from jurisdiction to jurisdiction. Some incorporate registry-related provisions within their companies act, delineating procedures for business formation, the registration process, and the operational framework of the registry authority. In such cases, the companies act serves as the primary legal instrument outlining the roles and responsibilities of the registrar and the mechanisms for maintaining accurate records. Alternatively, certain jurisdictions enact separate legislation dedicated to the establishment and registration of legal entities. This could be embedded within a broader legal framework, such as the civil or commercial code, encompassing provisions related to business formation, registration requirements, and the regulatory functions of the registration authority. Regardless of legislative structure, the legal foundation provides the registrar with both the authority and the duty to maintain accurate and up-to-date records, ensure accessibility, and enable legal recognition of registered entities.

Beyond the specific business registry law or company law, business registries are also bound by cross-cutting legislative requirements, including those governing data protection, privacy, and public access to information. In this context, it is worth noting the increasingly important standards and responsibilities imposed on digital platforms. For instance, in the European Union (EU), NIS2 Directive (Network and Information Security Directive) and DORA (Digital Operational Resilience Act) affect security measures implementation in EBRs operating in EU Member States.

This illustrates how EBR operation is increasingly shaped by international and regional standards that impose functional requirements and expectations in different domains. Globally, the Financial Action Task Force (FATF) defines the guidelines that registries have to follow to comply with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) policies, while the EU develops binding legal instruments, such as the Company Law Directive 2017/1132[37] and Directives 2019/1151[38] and 2025/25[39] on the use of digital tools and processes in company law that prioritise transparency, improve data quality, and cross-border interoperability across registries in EU Member States.

While the Project focuses on developing CPFs and associated best practices to strengthen the technical aspects of EBR design and operation, a sound legal foundation is indispensable for any registry system. Registration in EBRs confers legal identity upon business entities, granting them legal rights and recognition. Legal frameworks provide EBRs with authority, credibility, and enforceability that foster their use and reliance on their services. Applicable legislation generally mandates that the registrar ensures the provision of prescribed services and core functions.

A question of registrar liability arises where operational failures, infrastructure faults, or inadequate responses to known risks result in harm: legal systems adopt varying approaches to determining such liability. In some jurisdictions, the registrar’s liability is assessed separately under fault-based or strict

[37] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017L1132 (last accessed 25 February 2025).

[38] Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law, http://data.europa.eu/eli/dir/2019/1151/oj (last accessed 25 February 2025).

[39] Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law, http://data.europa.eu/eli/dir/2025/25/oj (last accessed 3 March 2025).

liability rules. In others, registrars are considered to be exercising public functions on behalf of the State, in which case general principles of public law or administrative liability apply, without a distinct separation of institutional liability from that of the State. Recommendation 47 of the UNCITRAL Legislative Guide affirms that the applicable law should establish whether and to what extent the State is liable for loss or damage caused by error or negligence of the business registry in the registration of businesses or the administration or operation of the registry. Therefore, registrars should carefully consider their liability and how it arises and use this to conduct risk assessments that determine how the registry will be designed, built and operated.

In more general terms and in the context of the design and operation of an EBR, liability can arise from events falling into the following categories:

(a) errors or omissions by the registry officers/employees and contracted third parties (operation only);

(b) infrastructure failure attributable to hardware (design and operation);

(c) infrastructure failure attributable to software (design and operation); and

(d) unexpected outcomes or unexpected actions (design and operation).

Liability of a registrar arising from events in the first three categories is typically based on error or negligence, on the basis of an avoidable failure.[40] Examples of avoidable failures in the first three categories include:

(a) human error by an officer manually entering a court order discharging a registration;

(b) failure of a hardware component of infrastructure that could have been prevented by implementing a redundancy principle in design; and

(c) error in the software component of infrastructure programming that could have been discovered through pre-deployment testing.

Consider the hypothetical scenario where a major software vendor releases a critical security update to address a software vulnerability. Although the registrar receives notification of the update before any breach occurs, it fails to install the update in time. A cyberattack exploits the flaw, resulting in unauthorised access and registry data modification and deletion. While the underlying software design fault (category (c) above), for the purposes of this example, could not have been prevented, the registrar's failure to respond to the notification by taking preventive measures may constitute an error or omission. Not installing the security update may thus constitute a failure to follow best practices, and the registrar may be subject to the above category (a) of liability for harm caused by the cyberattack, which could have been avoided by timely action. The nature and extent of this liability will depend on applicable law.

[40] The rules on liability for such unforeseen consequences are still evolving in national law. For international and transnational instruments recommending liability rules, see UNCITRAL, Model Law on Automated Contracting (2025), **https://uncitral.un.org/sites/uncitral.un.org/files/2424674e-mlautomatedcontracting-ebook.pdf**; ELI, Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (2025), https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Algorithmic_Contracts/Guiding_Principles_and_Model_Rules_on_Digital_Assistants_for_Consumer_Contracts.pdf; Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402853. UNIDROIT has also accepted a proposal for a project on "Regulation of Digital Risk Through Civil Liability Law" into its Work Programme 2026-2028, https://www.unidroit.org/wp-content/uploads/2025/05/C.D.-105-4-rev-Proposals-for-the-New-Work-Programme-for-the-triennial-period-2026-2028-.pdf (last accessed 18 July 2025).

In an even more extreme scenario, a system error or inadequacy (e.g., in the process of authenticating registrants) is not discovered until legal proceedings are underway. Such an event could raise uncertainty regarding not only any registrations performed by the relevant user but all past registrations by any user in the registry system, undermining the evidentiary value of the registry as a whole.[41]

The legal relevance of best practices in the context of EBRs cannot be overstated. While best practices are not binding rules of law, they serve as authoritative reference points for designing, building, and operating registries in a legally defensible manner. Established legal frameworks and international standards, such as those set by the FATF, EU, and the UNCITRAL Legislative Guide, provide guidance as to the scope of the registrar's responsibilities and potential liabilities. In this sense, best practices do not replace legal obligations; rather, they complement them by operationalising general duties of care, diligence, and compliance in the digital environment. When applied consistently, they contribute to mitigating legal risks and liabilities, improving institutional credibility, and maintaining public trust.

This Guide clarifies the meaning of best practices in the context of EBRs. In doing so, the Guide draws on the earlier work of the Project[42] and encourages all stakeholders involved in EBR design and operation to adopt the 24 CPFs identified herein. These performance factors are structured around key legal, technical, and operational principles, offering a comprehensive framework for reliable and trustworthy registry systems. Chapter II describes the 24 CPFs. Chapter III discusses in more detail risk management in EBRs. Chapter IV presents a conclusion for the Guide, while Chapter V provides a Glossary of terms. Annex I provides an overview of the international framework on the scope of publicly disclosed information by EBRs, and Annex II provides a detailed summary of identified relevant technical standards, which may be used as a reference for the CPFs in the present Guide.

[41] 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 25 February 2025).

[42] See Aaron Ceross, Practices in Electronic Registries, (Interim Report, Spring 2018), this report has been 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 21 March 2025).

II. CRITICAL PERFORMANCE FACTORS

This Chapter provides definitions and detailed descriptions of the CPFs and explains their relevance to EBRs. 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. For other CPFs, the discussion is limited to the technical or legal aspect.

Critical Performance Factor	Definition
Access Control	The process of ensuring that access to the registry is controlled and granted to only verified, authenticated, and authorised identities
Accessibility	The property of being able to effectively engage with the system by all individuals regardless of their abilities and limitations
Accuracy	The property of providing information that is adequately accurate considering the specific business and legal context
Authentication	The process of verifying that a person is who they claim to be
Availability	The property of being accessible and usable upon demand
Confidentiality	The property that information is not made available or disclosed to unauthorised persons
Continual Improvement	The process of systematically identifying areas for improvement, making changes, and monitoring the results to ensure that they lead to positive outcomes
Continuity	The property of delivering registry services at acceptable levels within acceptable timeframes during and following a disruptive incident
Correctability	The process of identifying and rectifying errors in a timely, accurate, and legally sound manner
Data Input Validation	The process of assessing that the data meets the established criteria for its purpose in the registry
Disposition	The process of archiving, destroying or transferring data at the end of the retention period
Error Detection	The process of detecting discrepancies, inaccuracies, or wrongful information within the registry data
Evidentiary Value	The property of constituting evidence or having the quality of evidence
Integrity	The property that data has not been altered or destroyed in an unauthorised manner
Interoperability	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
Legal Authority and Compliance	The property of ensuring that the registry is established pursuant to and operates in compliance with the applicable legal framework
Legal Authority of the Registrar	The property that the registrar may exercise certain powers pursuant to a legal authority, including in the process of correcting detected errors

Privacy	The property of protecting personally identifiable information
Reliability	The property of consistently performing required functions for a specified period of time
Retention	The process of preserving data in a system for a specified period of time
Risk Management	The process of identifying, assessing, and managing threats and vulnerabilities to registry design and operations
System Validation	The process of confirming, using objective evidence and testing, that the requirements for the intended use have been fulfilled by the system
Timeliness	The process of considering time in the context of system design and operations
Transparency	The process of disclosing, in an open and understandable manner, how a system or process operates, including how it produces and presents data
Trustworthiness	The property of providing confidence to users and third parties that the registry performs its core functions in accordance with legal and technical expectations
User-Centred Design	The property that the approach to the design and development of the registry aims to make the registry more usable by considering how the registry is used and applying human factors, ergonomic and usability principles

Table 1. CPF definitions (in alphabetical order).[43]

1. Access Control

Definition: The process of ensuring that access to the registry is controlled and granted to only verified, authenticated, and authorised identities

Access Control encompasses the processes that define and limit a user's access rights and privileges within the registry. Access control can range from open access, where data is publicly available without authentication, to arrangements where only specific users can access the resources. Authentication encompasses two elements: first, confirming that the individual or system is indeed who or what they claim to be by verifying their identity, and second, confirming that a user is who or what they claim to be by checking the digital credentials assigned to that identity (for more details, see CPF 4 on Authentication).

Once authenticated, Access Control authorises the specific actions the user is permitted to perform, such as viewing, editing or submitting information, based on their assigned roles or access levels within the system. Authorisation policies should be designed in accordance with the principle of least privilege (PoLP)[44], which ensures that internal users are granted only the minimum level of access necessary to perform their tasks and that others, such as the public, are able to satisfy their legal entitlements, but no more. This reduces the risk of accidental or malicious misuse of registry data or functions. In addition, segregation of duties (SoD)[45] should be implemented for internal staff or those who operate the registry to prevent any individual from having end-to-end control over critical registry processes.

[43] Please note that CPFs containing two definitions, such as CPF on Confidentiality and Privacy and CPF on Retention and Disposition, are indicated separately.

[44] ISO/IEC, Information security, cybersecurity and privacy protection – Information security controls: ISO/IEC 27002:2022; 2022, https://www.iso.org/standard/75652.html, p. 27, §5.15 Access Control (last accessed 26 June 2025); See also NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, 2020; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, (last accessed 3 April 2025).

[45] ISO/IEC, Information security, cybersecurity and privacy protection – Information security controls: ISO/IEC 27002:2022; 2022, https://www.iso.org/standard/75652.html, p. 12, §5.3 Segregation of Duties (last accessed 26 June 2025).

Modern Access Control paradigms include zero-trust architecture,[46] role-based access control (RBAC),[47] attribute-based access control (ABAC),[48] and discretionary access control (DAC),[49] emphasising granular control and continuous verification. This ensures that users, whether individuals or systems, have access only to the specific resources necessary for their tasks.

Entities are authorised and access rights and privileges are managed through the issuance of credentials or tokens to designated individuals or entities. These tokens serve as proof of identity. Upon each attempt to access registry functions, such as submitting a registration, Access Control mechanisms evaluate whether the user has the right to access those registry functions and data by validating the token and matching it against the permissions associated with that identity.

Public access permissions, such as the right to search for registrations, may be granted without authentication or the need to create an account. For instance, the company's basic information registered on the European e-Justice Portal through the Business Register Interconnection System (BRIS) is available without authentication. This demonstrates the application of varying Access Control levels depending on the EBR's policy, based on relevant legislation, which is further elaborated in CPF 6 on Confidentiality and Privacy.

Access Control applies to all methods of access, including direct user access, interoperability with other registries, Application Programming Interfaces (APIs),[50] and intermediaries. It also extends to physical access of registry locations and infrastructure, such as using identification badges, biometric sensors, closed-circuit television, locks, or other security measures. Electronic Access Control (e.g., server-side database permission verification) occurs whenever the user attempts to access a registry function or data. Physical Access Control prevents unauthorised actors from gaining material access to registry data or its infrastructure.[51]

Various controls can be implemented to counter attempts to gain unauthorised access, including automatically terminating sessions that are inactive for a certain period and using technology such as CAPTCHA to detect and deter automated access attempts.[52] Governance policies and arrangements underpin all these controls, including the periodic updating of software, monitoring and maintenance of physical access, and promptly revoking access permissions for users no longer authorised.

An Access Control strategy should also address the risks posed by a 'trusted insider' whose authorised access is used either maliciously or negligently. Organisational measures, such as pre-employment screening and

[46] NIST, Zero Trust Architecture, Special Publication 800-207, 2020, https://www.nist.gov/publications/zero-trust-architecture (last accessed 7 February 2025).

[47] InterNational Committee for Information Technology Standards (INCITS) 359-2012 (R2022), Information technology - Role Based Access Control, 2012, revised in 2022, https://webstore.ansi.org/standards/incits/incits3592012r2022?source=blog&_gl=1*16xxwwu*_gcl_au*NzAyOTA1OTE2LjE3NDA2OTgwNDU (last accessed 7 February 2025).

[48] NIST, Guide to Attribute Based Access Control (ABAC) Definition and Considerations: Special Publication 800-162; 2014, https://csrc.nist.gov/pubs/sp/800/162/upd2/final (last accessed 7 February 2025).

[49] NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, 2020; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 3 April 2025).

[50] See What is an API (Application Programming Interface)?, https://aws.amazon.com/what-is/api/, (last accessed 7 February 2025).

[51] See IFC, Knowledge Guide: Secured Transactions, Collateral Registries and Movable Asset-Based Financing, 75, 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 7 February 2025).

[52] CAPTCHA stands 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.

regular training of trusted insiders (including employees, contractors, and vendors who have access to the registry) are essential. In particular, the 'super-users' who have administrative rights to access data should undergo reasonable levels of scrutiny.

The 2024 Insider Threat Report, based on insights from 413 IT and cybersecurity professionals, found that 83% of organisations had experienced at least one insider attack in the past year, with 21% facing between 11 and 20 incidents – a fivefold increase from the previous year.[53] The PoLP mentioned above serves to minimise such risks, ensuring that access authorisations do not exceed what is strictly necessary for employees' tasks.

Monitoring, auditing and logging are critical components of Access Control. Audit logs of all user and staff access and system operations should be maintained to monitor activity, identify breaches, alert security personnel, and investigate accidents. Audit trails are important tools for addressing issues such as fictitious and fraudulent registrations and collusion between, for example, a database analyst and a malicious actor. Additionally, auditing and logging have a deterrent effect, especially against insider threats, as long as the logs are tamper-resistant and their collection is made known.

Technical

ISO/IEC 27000 defines Access Control as ensuring that access to assets is authorised and restricted based on business and security requirements.[54] Annex A of ISO/IEC 27001 sets out requirements for Access Control standards, including, among other things, Access Control policies, management of privileged access rights, user responsibilities, and secure log-on procedures to prevent unauthorised access to systems and applications. It outlines the requirements for controlling access to information assets based on business requirements for confidentiality, integrity, and availability. ISO/IEC 27001 provides a framework for organisations to establish appropriate authorisation mechanisms as part of their broader information security management practices.[55]

NIST also recommends that all United States (US) federal government information systems enforce Access Control policies that limit access to authorised users.[56]

Legal

National legislation, usually company laws and regulations, provides a framework for implementing Access Control requirements. For example, it is often a legal requirement that data submitted to the business registry must come from a legal entity acting through its management or their authorised representatives. Only individuals with the legal right or authorisation to represent the entity are permitted to act on its behalf, submitting data and documents to the business registry.

[53] See Cybersecurity Insiders Gurucul, 2024 Insider Threat Report (2024); https://gurucul.com/2024-insider-threat-report/ (last accessed 7 February 2025).

[54] ISO/IEC 27000 family; Information security management, 2022, https://www.iso.org/standard/iso-iec-27000-family (last accessed 26 February, 2025).

[55] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements, https://www.iso.org/standard/27001 (last accessed 7 February 2025).

[56] See NIST Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, Revision 5 (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 23 December 2024).

Similarly, according to Recommendation 21 of the UNCITRAL Legislative Guide,[57] when registering a business in the business registry, it is essential to record the identity of the person(s) authorised to sign on behalf of the business, or serving as the business's legal representative(s). This highlights the significance of ensuring that individuals acting on behalf of the entity possess the legal authority to do so. This entails having explicit legal authorisation, such as through appointment by the entity's governing body or under relevant laws and regulations. Robust access controls and security measures within the registry are essential to avoid corporate identity theft or prevent unauthorised individuals from acting on behalf of the entity.

2. Accessibility

Definition: The property of being able to effectively engage with the system by all individuals regardless of their abilities and limitations

Accessibility can be seen from a technological perspective, where information and services should be accessible to people with limitations related to physical disabilities, access to technology, or digital literacy. For example, technologies such as screen readers, mobile-friendly interfaces, offline access, and simplified workflows contribute to inclusive interaction with the registry. Through prioritisation of the usability of information, registry systems can remove barriers and promote equal access to services for individuals with limited resources or abilities.

The design and operation of business registry systems should cater to a broad and diverse spectrum of users without the need for special technical instruments, skills, or knowledge.[58] The overarching goal is to create an inclusive system allowing access to as broad a range of people as possible. To this end, a registry system should be designed considering a range of physical and intellectual abilities, as well as cultural and linguistic diversity, time zones and distance.

Non-discriminatory access to business registry services is a fundamental right in modern society. Eliminating biases based on factors such as race, gender, language, religion, or social origin fosters an inclusive business environment that offers equal opportunities to all users. [59]

However, Accessibility does not equate to unrestricted and universal access to the registry by any person at any time. While business registries should be designed to remove unnecessary barriers for eligible users and ensure inclusiveness, Accessibility does not trump Access Control.

In some jurisdictions, equal access is a legal obligation; for example, accommodations may be required for sight-impaired users and users with intellectual disabilities. The Web Content Accessibility Guidelines (WCAG) provide a widely adopted framework with recommendations for making web pages accessible to a broad range of people with disabilities.[60] Following the WCAG will also often make web content more usable in general (see more in CPF 24 on User-Centred Design). They are based on four foundational principles,

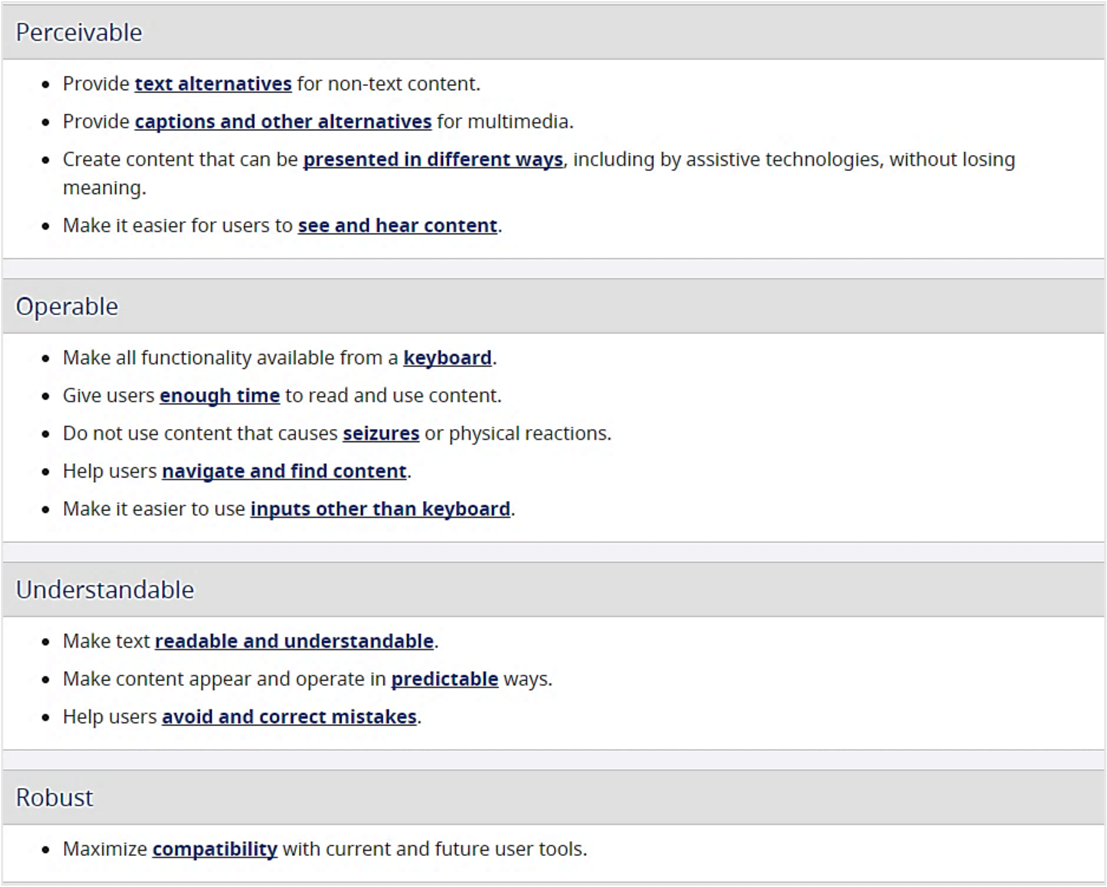
[57] UNCITRAL Legislative Guide, Recommendation 21.

[58] UNCITRAL Legislative Guide, Recommendation 4.

[59] UNCITRAL Legislative Guide, Recommendation 33.

[60] See Web Content Accessibility Guidelines (WCAG) 2.2, (W3C, 2024), https://www.w3.org/TR/WCAG (last accessed 7 February 2025).

that information, user interface, and navigation must be: i) perceivable, ii) operable, iii) understandable, and iv) robust.[61]



Perceivable

- Provide **text alternatives** for non-text content.
- Provide **captions and other alternatives** for multimedia.
- Create content that can be **presented in different ways**, including by assistive technologies, without losing meaning.
- Make it easier for users to **see and hear content**.

Operable

- Make all functionality available from a **keyboard**.
- Give users **enough time** to read and use content.
- Do not use content that causes **seizures** or physical reactions.
- Help users **navigate and find content**.
- Make it easier to use **inputs other than keyboard**.

Understandable

- Make text **readable and understandable**.
- Make content appear and operate in **predictable** ways.
- Help users **avoid and correct mistakes**.

Robust

- Maximize **compatibility** with current and future user tools.

Figure 2. The four WCAG Principles[62]

Access to EBRs is generally provided through the internet. Further access channels should include the ability to submit registrations through APIs and direct data transfers, eliminating the need to interact directly with the registry website. Where access is provided through intermediaries, the registrar should ensure that the intermediaries grant registry access equivalent to that available to direct users.

Accessibility can be challenging in areas with unreliable internet connectivity or frequent power outages (e.g., due to unpredictable load shedding). To uphold equal access for all users, especially those in rural areas or those without access to a device or the internet, business registries may need to offer alternative access points. These may include walk-in self-service desks, mobile registration units, partnerships with local post offices or municipal offices, etc. Such mechanisms ensure that users without internet access or digital literacy are not excluded from essential registry services.[63] While such facilities can be critical for Accessibility, business registries can incur significant costs for their establishment and maintenance, especially if they may be used infrequently.

Technical

[61] See WCAG 2 at a Glance, https://www.w3.org/WAI/standards-guidelines/wcag/glance (last accessed 7 February 2025).

[62] Id.

[63] OECD (2022), "OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age", OECD Public Governance Policy Papers, No. 23, OECD Publishing, Paris, https://doi.org/10.1787/2ade500b-en (last accessed 14 April 2025).

ISO/IES DIS 40500 is being developed on the basis of the WCAG principles, which, as mentioned above, provide comprehensive recommendations to make content accessible to a wider range of persons with disabilities.[64]

Legal

The UNCITRAL Legislative Guide emphasises the importance of universal access to business registry services. It highlights that the law should allow access to the business registry without any form of discrimination, including factors such as race, colour, gender, language, religion, political or other opinion, national or social origin, property, birth, or any other status. Moreover, if access to business registry services is provided electronically, the law should always ensure continuous availability.[65]

Recommendation 39 of the UNCITRAL Legislative Guide further sets out that the law should ensure easy access to public information about registered businesses.[66] This should be achieved by avoiding unnecessary barriers, such as mandating specific software installation, imposing high access fees, requiring mandatory user registration or the provision of personal identity information.

3. Accuracy

Definition: The property of providing information that is adequately accurate considering the specific business and legal context

For the purposes of this Guide, Accuracy is a measure of how accurate information published on the EBR is, considering the specific business and legal context. However, Accuracy is not binary; it is a spectrum. Rather than an absolute guarantee, Accuracy represents a balance between the efforts of registries, registrants, and regulatory authorities, and the practical and legal frameworks within which registries operate. For instance, at the high end of the Accuracy spectrum is the financial statement of a business which has been independently audited to the appropriate accounting standards. It will not be exact, as auditors allow for immaterial errors, which do not need to be corrected.[67] Other registered data may of course be located at a different point on the Accuracy spectrum.

In considering Accuracy, context is crucial. Business accounts published on the registry are accurate enough for their purpose; they are adequate. Other data may be less accurate but still accurate enough for its intended purpose. For instance, for the addresses of directors, even though there may be a legal obligation on the business secretary to update this data when it changes, individual directors may not be fully aware of their responsibility to notify the business secretary. Although the data may be reconfirmed annually when the business is being audited, there may be times between audits when the address of one or more directors is not correct. Whether this is accurate enough depends on the purpose of the data.

[64] See WCAG 2.2, https://www.w3.org/TR/WCAG (last accessed 7 February 2025).

[65] UNCITRAL Legislative Guide on Key Principles of a Business Registry (2019), Recommendations 32, 33, 35 .

[66] UNCITRAL Legislative Guide on Key Principles of a Business Registry (2019), Recommendation 39.

[67] See https://media.frc.org.uk/documents/ISA_UK_320_Updated_May_2022_aJAQtFV.pdf for a discussion of materiality under International Auditing Standards.

Accuracy requires the registrar to consider three interrelated questions in designing and operating an EBR. First, what is the purpose of the data? Second, how accurate does the data need to be, given its purpose? Third, how can a user of the data assess its Accuracy?

In addressing the first question, the registrar will consider the underlying legislation, regulatory policy concerns, and who is entitled to access the information and for what legal purpose. The second question should be addressed through the lens of CPF 19 on 19. Risk Management. What is the potential impact, including financial losses, for the registrar or registry user where the Accuracy level is inadequate? Attempting to quantify losses may be helpful in determining an adequate level of Accuracy. The third question looks at the issue from the user's point of view. A user will consider several factors in assessing the Accuracy of the data and how much they can rely on it. If the liability for errors in the data lies with the registrar, the user may be satisfied to assume high Accuracy or may not be overly concerned with its Accuracy. In this case, the registrar will have very high standards to ensure adequate Accuracy. Factors that would influence the assessment of data Accuracy include data provenance, such as when the data was uploaded,[68] who uploaded it, the history of modifications, whether the data was independently audited or verified by the registrar, and whether penalties apply to the person who uploaded the data if it is not adequately accurate. Once these three interrelated questions are addressed, the registrar can design the registry system and supporting processes appropriately.

To illustrate how the business and legal environment influences Accuracy requirements, three examples are provided below. They clarify how international and regional instruments currently impact the required level of Accuracy for beneficial ownership (BO) information, which is collected by business registries in some jurisdictions, and a national legal instrument authorising the registrar to adopt a more proactive approach in ensuring Accuracy to prevent abuse of UK corporate structures.

Firstly, the importance of data Accuracy is emphasised in FATF Recommendation 24 'Transparency and beneficial ownership of legal persons' and Recommendation 25 'Transparency and beneficial ownership of legal arrangements', whereby jurisdictions must ensure adequate, accurate, and up-to-date information on basic and BO of legal persons and legal arrangements, and that such information shall be accessible to a competent authority in a timely manner.

Jurisdictions are required to have mechanisms that ensure BO information remains accurate and updated within a reasonable period following any change or restated at periodic intervals. Thus, information must be accurate when the legal person is initially registered and promptly updated throughout the life of the legal entity.

Secondly, the AML package in the EU, particularly Article 30 of Directive 2015/849/EU, mandates EU Member States to guarantee that corporate and other legal entities incorporated within their territories are required to obtain and hold adequate, accurate and current BO information, including the details of the beneficial interests held. It emphasises that the accuracy of data in BO registers is fundamental for all competent authorities, obliged entities, and other persons allowed access to that data, and for informed and lawful decision-making.

[68] Some data such as director addresses may change with time whereas other data, such as a snapshot of the financial status of the company at a particular point in time, will not.

Thirdly, the Economic Crime and Corporate Transparency Act aims to enhance the accuracy and quality of data on UK registries to combat economic crime and boost confidence in the UK economy. It introduces new statutory objectives and grants the registrar of companies new and enhanced powers to fulfil their mandate effectively.[69] The registrar's new objectives are: (i) to ensure that anyone who is required to deliver a document to the registrar does so (and that the requirements for proper delivery are complied with); (ii) to ensure information contained in the register is accurate and that the register contains everything it ought to contain; (iii) to ensure that records kept by the registrar do not create a false or misleading impression to members of the public; and (iv) to prevent companies and others from carrying out unlawful activities or facilitating the carrying out by others of unlawful activities. This Act redefines the role of registrar of companies, providing it with a broader authority to analyse and share data, marking a shift from a passive role in accepting 'duly delivered' documents to a more active role in ensuring the accuracy and integrity of UK company registers, granting it powers to reject, remove, or amend information on the register.

More generally, the UNCITRAL Legislative Guide, paragraph 12, defines a 'good quality and reliable' business registry as one that maintains registered information as current and accurate as possible, presenting a positive evaluation in terms of performance and security. Measures should be taken to collect accurate and reliable data in the registry and encourage the timely submission of updated data to the registry. According to Recommendation 30, requirements should include: (a) sending automated requests to registered businesses to prompt them to report whether the information maintained in the registry continues to be accurate or to state what changes should be made; (b) displaying notices of the required updates in the registry office and sub-offices and routinely publishing reminders on the registry website and social media and in national and local electronic and print media; (c) identification of sources of information on the registered businesses that would assist in maintaining the currency of the registry; and (d) updating the registry as soon as practicable following the receipt of amendments to registered information and, in any event, without undue delay thereafter.

Both FATF Recommendation 24 and Directive 2015/849/EU Article 30 establish the possibility and necessity of imposing sanctions for the failure to submit data in a timely manner. An effective system of sanctions and enforcement, if appropriate, helps to ensure that accurate and timely BO information is provided to authorities.

The International Business Registers Report also reveals that jurisdictions are taking various steps to ensure that the data contained in registers is accurate, as can be seen in Figure 3, below.

[69] UK Government. Economic Crime and Corporate Transparency Act 2023, Chapter 56, Part 1, Section 1081A, Objective 2. https://www.legislation.gov.uk/ukpga/2023/56 (last accessed 7 February 2025)

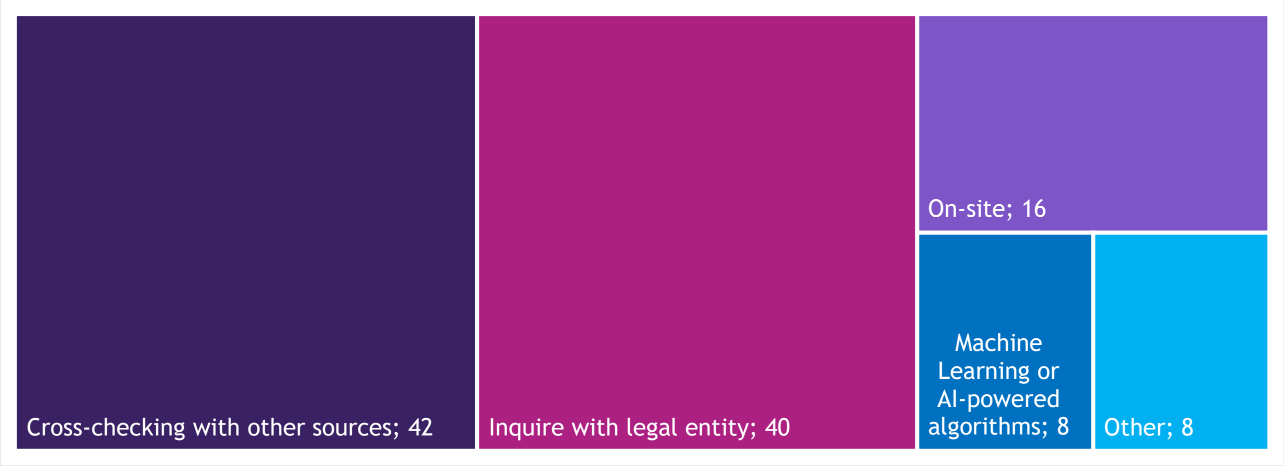


Figure 3. Measures that business registries take to check the Accuracy of the data contained in the register.[70] The figure has been redrawn by the authors for clarity.

Maintaining high standards of Accuracy in business registries not only supports regulatory and compliance efforts but also enhances overall confidence in the business sector.

Technical

Technical design of the EBR should identify the specific Accuracy requirements of each data item and put appropriate controls in place for these purposes. EBRs should adopt electronic verification systems that automate ongoing validation, detect inconsistencies, and verify data with great precision and speed. By leveraging these technologies, registries can reduce human error and ensure that information remains current, accurate, and reflective of any changes in real time. Providing detailed information to a user on the data provenance and penalties allows that user to assess its level of Accuracy.

Legal

The UNCITRAL Legislative Guide paragraph 52 indicates that, depending on the legal and institutional framework of the enacting State, a fundamental role and objective of business registries is to keep the information on registered businesses as current and accurate as possible, thereby ensuring its value for all registry users.

With a significant focus on the accuracy of data on BOs of legal entities, Directive 2015/849/EU mandates Member States to transfer the requirement that the information held in the central registry is adequate, accurate, and current into national law. This reinforces the critical role that accurate data plays in supporting transparency and regulatory oversight.

To promote compliance, FATF Recommendation 35, Directive 2015/849/EU Article 30, and Recommendation 46 of the UNCITRAL Legislative Guide provide for the imposition of sanctions on a business for breaching its obligations to submit information to the registry in an accurate and timely fashion.

It may be necessary for the registrar to update or remove data to improve Accuracy. In accordance with the UNCITRAL Legislative Guide, if the applicable law grants the registrar the authority to directly make changes, the registrar may be empowered or obligated to do so. In case of deregistration, Recommendation

[70] Business Registry Insights, Data Verification Survey 2024, Data Verification (2024) - Business Registry Insights (last accessed 7 May 2025).

48 suggests that the law should outline specific conditions under which a business can request deregistration and mandate the registrar to do so when those conditions are met. Alternatively, Recommendation 49 emphasises the importance of the law specifying the conditions under which a registrar can deregister a business involuntarily.

4. Authentication

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

As described in CPF 1 on Access Control, access can be granted only after the users who interact with a registry have been verified and authenticated; thus, Authentication consists of two major elements. The first element of Authentication involves establishing that 'a person is who they claim to be' through verifying their identity, and second, 'that a user is the person they claim to be' through the verification of the credentials which are associated with that identity.

The first element of Authentication occurs upon requesting the creation of a user account. Examples of Authentication techniques which verify identity include:

(i) Verifying a user's identity against a national ID database;

(ii) Verifying a user's identity employing biometrics, for example, facial recognition to compare a live capture with a photo of the government-issued ID;[71]

(iii) Verifying a user's identity through a remote identity management (IdM) system that provides pre-authenticated user credentials;[72] and

(iv) Verifying a user's identity through electronic certificates, i.e., electronic attestations that link signature-verification data to a person and confirm the identity of that person, or digital identity, i.e., a profile or set of information used to identify a specific user, machine, or other entity. Governments or other third parties often provide these services. In some cases, a notary may verify the identity of the person, but in such cases, the data would be provided to the business registry through a notary.

The second element of Authentication, once a user has been provided with access as above, involves the user presenting their credentials (or a token) every time they log in to interact with the EBR. Examples of strong Authentication techniques include requiring confirmation of receipt of an email to authenticate a

[71] This technique is used by the Global Aircraft Trading System (GATS), see Aviation Working Group, *Site Terms of Use* art. 12.4 (June 1, 2020), https://documents.e-gats.aero/SiteTermsOfUse.pdf (last accessed 26 February 2025).

[72] Remote IdM has been rapidly evolving in the past years from traditional centralised authentication models to more advanced, decentralised frameworks. Governments and the private sector are adopting biometric authentication, decentralised identity (DID), and verifiable credentials (VCs) to enhance security, privacy, and interoperability. Electronic KYC (e-KYC) systems, compliant with FATF guidelines, have been adopted in India, South Africa, Gulf countries, and Latin America. The EU's eIDAS 2.0 framework is facilitating cross-border authentication, while Zero Trust Architecture (ZTA) is an emerging security model that integrates identity verification. See Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024, https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng (last accessed 26 February 2025); see also, European Union Agency for Cybersecurity (ENISA), Remote Id Proofing Good Practices, 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/Remote%20ID%20Proofing%20Good%20Practices_en_0.pdf (last accessed 26 February 2025); see also Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials OpenID Foundation, 2023, https://openid.net/wp-content/uploads/2023/10/Human-Centric_Digital_Identity_Final-v1.1.pdf (last accessed 26 February 2025).

login attempt, biometrics, one-time token codes or passwords (OTPs), or using an authentication application.

Different levels and methods of Authentication are used by EBR systems depending on whether they relate to verifying identity or credentials. Regarding credentials, while the use of a username and password remains prevalent, multi-factor authentication (MFA) should always be used where possible. MFA requires more than one distinct authentication factor for successful authentication (generally two or three factors). These factors include something you 'know' (e.g., passwords or pin codes), something you 'have' (e.g., certificates, token codes), and something you 'are' (e.g., biometrics such as fingerprints or facial recognition). To the extent feasible, the Authentication process should be automated and employ advanced technologies (see CPF 14 on Interoperability).

Authentication may also occur when searching an EBR. Though the system could also be designed to require both an account and login for conducting searches, it does need to accommodate one-time users. Some Authentication is conducted when the search is subject to a fee, requiring the user to enter payment details. This ensures that access to data remains controlled.

The figure below gives an overview of the various requirements imposed by business registries in relation to verifying the identity and signatures of users when they submit information to business registries electronically. Digital Identity and Notaries are examples of methods used to verify identity, while Usernames and Passwords, Electronic Certificates and Two-Factor Authentication (a subset of MFA) are all methods of verifying credentials:

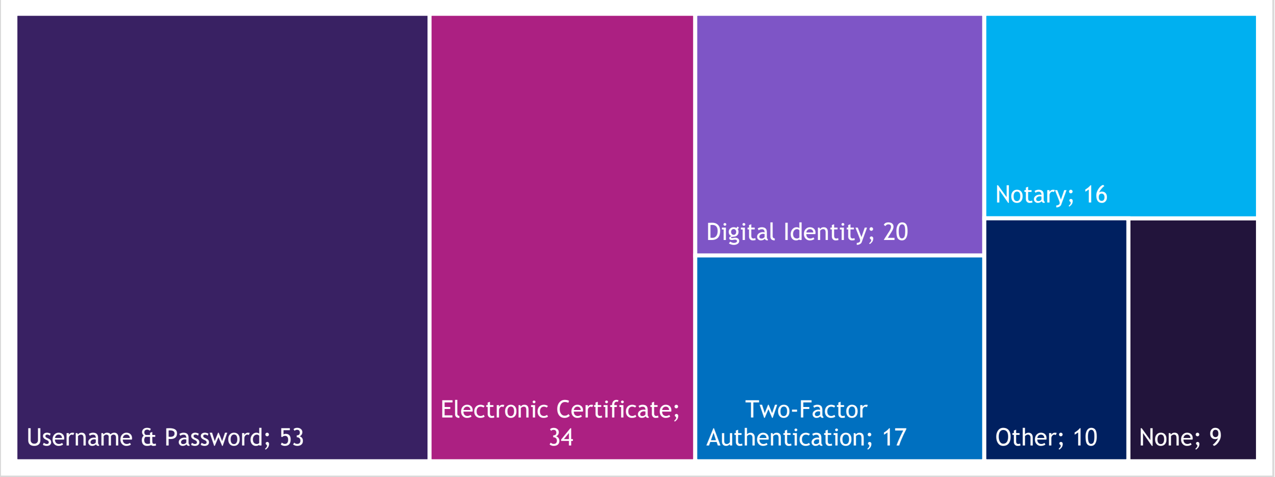


Figure 4. Methods of Filers' Identification.[73] The figure has been redrawn by the authors for clarity.

An appropriate Authentication system must be developed based on a risk assessment: what is the damage caused by a user if it bypasses the authentication mechanism, and what is the benefit for the user that might drive it to attempt such a breach? It is not always appropriate to have the most extreme authentication mechanism. At one end of the spectrum, when a user must pay for a service, they are less likely to misuse the system. At the other end of the spectrum, if access allows financial gain for the user, a

[73] The International Registers Survey Report, 2022 Interactive dashboard, https://ebra.be/survey-results/ (last accessed 7 April 2025).

highly robust authentication system should be adopted. As with all system components, technical decisions will be based on the context and, in particular, the registry's security posture and risk appetite.

In today's dynamic environment, where businesses operate beyond national borders, it is essential to have tools for reliable identification at both the national and international level. Therefore, it is necessary to create conditions for non-resident natural and legal persons to be able to access and benefit from registry services. Jurisdictions are looking to simplify the onboarding processes for digital identity and digital signature requirements, making business registration accessible for domestic and foreign founders and investors. Alternatively, business registries can have recourse to Know Your Customer (KYC) platforms, which are sophisticated systems designed to verify users' identities through a combination of biometric data, official documents, and other identifying information. Some jurisdictions also explore solutions employing blockchain for digital business identity and AI/ML for identity validation.[74]

In the context of the EU, the eIDAS 2.0 Regulation (EU) 2024/1183 established the European Digital Identity Framework. This framework mandates that Member States provide European Digital Identity (or Digital ID) Wallets to citizens, residents, and businesses, among which a dedicated EU Business Wallet is being considered. These wallets are to be designed to ensure accessible, secure cross-border digital identification according to stringent technical and security standards, incorporating advanced encryption, secure access protocols, and zero tracking policies. By ensuring interoperability, the wallets can enable digital credentials issued in one Member State to be recognised across the entire EU.[75] Directive (EU) 2019/1151,[76] in line with the eIDAS 2.0 Regulation, allows Member States to recognise only those electronic ID (eID) systems that meet high-security requirements for cross-border transactions. Despite the existence of numerous national eID systems, only a few of the systems meet the requirements for the highest level of assurance.

In any case, Authentication should not hinder Accessibility (CPF 2). Accordingly, the administrative and technical burden of the Authentication processes should be designed and adjusted in light of the user base.

Technical

ISO 9798-1 describes a variety of Authentication protocols that use security techniques to ensure that a person's identity is as claimed to be, by the collection of the relevant information and, where appropriate, verification with a trusted third party.[77]

ISO 27001 Annex A highlights the secure management of Authentication data (tokens, passwords, biometrics) through encryption, secure transmission, and regular updates to prevent unauthorised access and ensure compliance with information security standards.

[74] Marusic, Vranic "Is the Self-Sovereign Digital Identity the Future Digital Business Registry?" (blog), 2021, https://blogs.worldbank.org/psd/self-sovereign-digital-identity-future-digital-business-registry (last accessed 7 February 2025).

[75] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

[76] The formal legal name is Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law, https://eur-lex.europa.eu/eli/dir/2019/1151/oj/eng (last accessed 26 February 2025). The second part of the Company Law Package, Directive (EU) 2019/2121 of the European Parliament and of the Council of 27 November 2019 amending Directive (EU) 2017/1132 as regards cross-border conversions, mergers and divisions, was signed six months later, https://eur-lex.europa.eu/eli/dir/2019/1151/oj/eng (last accessed 26 February 2025).

[77] See ISO/IEC 9798-1 Information technology — Security techniques — Entity authentication, 2010, https://www.iso.org/obp/ui/#iso:std:iso-iec:9798:-1:ed-3:v1:en (last accessed 7 February 2025).

ISO/IEC 24760-1 provides a framework for IdM.[78] The standard specifies fundamental concepts and operational structures of Identity Management with the purpose of realising information system management to meet business, contractual, regulatory and legal obligations.

Legal

Recommendation 21 of the UNCITRAL Legislative Guide requires the registry to request and maintain information about the identity of the registrant(s). Unlike the approach adopted for registrants, the registry should not request and maintain evidence of the identity of a user as a precondition to obtaining access to the information on the business registry, since a user is merely retrieving information contained in the public registry record. Identification should be requested of users only if it is necessary for the purposes of collecting any fees applicable to the retrieval of such information.[79]

5. Availability

Definition: The property of being accessible and usable upon demand

In general, EBR systems should be accessible 24 hours a day, every day, which requires both robust technological infrastructure and the necessary human personnel (e.g., IT support personnel) to be available continuously. Advancements in technology, particularly automated solutions and AI, offer viable alternatives to traditional human intervention, such as system monitoring and user support, providing immediate assistance to users with common inquiries, basic troubleshooting, and, when necessary, referring complex issues to human personnel.

While aiming for maximum Availability, occasional downtime is necessary for scheduled maintenance and updates and the inevitability of technical and security interruptions. The UNCITRAL Legislative Guide provides recommendations for organising system maintenance and repair services, discussed below.

Security that ensures the Integrity of data should generally take priority over Availability, but as with Accessibility and Authentication, an appropriate balance must be struck.

Availability is a measure of the total amount of uptime that can be expected over a given period. Availability can be calculated as follows:

Availability = uptime / (uptime + downtime)[80]

The result can be expressed as the percentage of time that the EBR is available. Alternatively, it can be thought of as the probability that the EBR will be available at any given time.[81] For example, Availability of an EBR 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

[78] https://www.iso.org/standard/77582.html.

[79] UNCITRAL Legislative Guide, para. 180.

[80] Byron Radle & Tom Bradicich, What is Availability?, (National Instruments 2019), https://www.ni.com/en- us/innovations/white-papers/13/what-is-availability-.html#section--1867287128 (last accessed 7 February 2025).

[81] Id.

ISO 27000 (3.7) defines Availability as the ‘property of being accessible and usable on demand by an authorised entity.’ This standard underlines the importance of maintaining system accessibility as a core component of information security management systems.[82]

Legal

Recommendation 32 of the UNCITRAL Legislative Guide stipulates that if access to the services of the business registry is provided electronically, access should be available at all times. However, while acknowledging this recommendation, the business registry may suspend access to the services, either wholly or partially, in order to conduct maintenance or provide repair services to the registry. It is essential that: (i) the period of suspension of registration services is as short as practicable; (ii) notification of the suspension and its expected duration is widely publicised; and (iii) such notice should be provided in advance and, if not feasible, as soon after the suspension as is reasonably practicable.

6. Confidentiality and Privacy

Definitions:

Confidentiality - The property that information is not made available or disclosed to unauthorised persons.

Privacy – The property of protecting personally identifiable information

In their design and operation, EBRs implement controls to allow access to data only to authorised individuals, processes, and entities. This Guide draws a distinction between Confidentiality and Privacy; the former concerns commercially sensitive information, whereas the latter covers personally identifiable information (PII). Both should be embedded into the registry’s design and operation, reinforced by dedicated policies and supported by technical controls.

Confidentiality refers to the measures taken by the registry to protect commercially sensitive data from unauthorised disclosure, whether intentional or accidental. This includes implementing access controls, encryption protocols, and authentication mechanisms. The exact scope and definition of commercially sensitive information within the business registry are subject to the provisions of applicable national laws. Examples of such commercially sensitive data include information found in payment details. An EBR system design must avoid the unnecessary collection or disclosure of commercially confidential information.

Privacy, is a key principle when handling PII, ensuring compliance with data protection regulations and the safeguarding individuals’ rights. Data protection laws, such as the EU’s General Data Protection Regulation (GDPR), impose strict requirements on how PII may be collected, stored, processed and disclosed.[83] Data collection about individuals should be purpose-specific and not excessive. For example, collecting data beyond what is necessary for the registry's stated purpose, such as user preferences or unrelated demographic details, should be avoided unless there is a clear operational justification. Depending on the

[82] ISO/IEC 27000:2018 § 3.7. – Information Security Management Systems, https://www.iso.org/standard/73906.html (last accessed 7 February 2025).

[83] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (last accessed 26 February 2025).

types of personal data collected and stored, appropriate mechanisms for disclosing this data to the subject to the data, upon request, must be available.

Even in cases where data is necessary and its collection and storage are permitted by legislation, it is essential for the business registry to properly implement data protection provisions. While EBRs are generally designed for making the information public, certain personal data — such as BO information — may require restricted access to protect individuals' rights. Given this, access to some personal data may be granted based on demonstrated legitimate interest rather than being universally available.

A thorough analysis of the legal framework applicable to each EBR is essential to determine which types of data must be public and which are protected. See Annex I to this Guide for international and regional legal frameworks and recommendations, jurisdiction-specific examples, and more details on the scope of publicly accessible information.

The Privacy and Confidentiality of ancillary data and metadata must also be considered. Metadata, such as user IP addresses, access logs, or timestamps, may be used to infer sensitive information and should be subject to the same protections. For instance, IP addresses can be linked to geographic locations or used to track user behaviour over time, which can reveal patterns or associations not intended for disclosure. Without specific controls, such data may be misused or exposed.

While the legislation that establishes EBRs generally does not specify necessary security measures to protect commercially sensitive data and PII from unauthorised access, registries should adopt a confidentiality-by-design and privacy-by-design approach. These principles require that Confidentiality and Privacy are considered at the inception phase and built into the EBR system design.

Confidentiality and Privacy policies should be enforced through robust technical controls with security protocols, advanced Access Control frameworks, and Authentication mechanisms,[84] encryption technologies for data at rest and in transit, and audit logs. In this context, the use of privacy-enhancing technologies, for example, pseudonymisation, homomorphic encryption, and differential privacy,[85] can play a role in minimising the exposure of PII while preserving functionality. Decentralised IdM could also allow users to retain control over their identity information, reducing the risks associated with centralised data storage. Searching mechanisms should also be carefully designed to avoid enabling unintended exposure of registry data.

Other examples of technical and policy controls include conducting risk assessments, restricting database access to authorised personnel, educating personnel about Confidentiality and Privacy policies, and implementing disciplinary measures regarding information misuse and other breaches of security.[86]

[84] Implementing Zero Trust Architecture (ZTA) can ensure that every request for data access is authenticated and authorised, reducing the risk of insider threats and credential compromise. Attribute-Based Access Control or Policy-Based Access Control can be used to define precise access rights based on contextual factors.

[85] Pseudonymisation refers to the replacement of identifiers with pseudonyms in order to hide the identity of individuals. Homomorphic encryption is a type of encryption that permits operations on ciphertexts without decryption, preserving confidentiality of the underlying plaintext data during computation. Differential privacy is a property of a mechanism that, when applied to a dataset, makes it difficult to determine whether any individual's information is included in the input to the mechanism, within a specified level of probability. See more: ISO/IEC 20889, Privacy-enhancing data de-identification terminology and classification of techniques, https://www.iso.org/standard/69373.html, and ISO/IEC 18033- IT Security Techniques — Encryption Algorithms, https://www.iso.org/standard/67740.html (last accessed 25 June 2025).

[86] Although these examples are taken from the context of credit registries (a type of credit referencing system), they equally apply to electronic business registries. See World Bank, Responsible Use of Technology in Credit Reporting: White Paper (2022), http://hdl.handle.net/10986/38312 (last accessed 26 February 2025).

Transparency is also essential for all EBR users to understand how their data is collected, processed, and protected. This may be achieved through clearly written privacy notices, data use dashboards, or other mechanisms that enable individuals to view and control how their information is managed. CPF 22 on Transparency covers this in greater detail and outlines the measures necessary to foster trust and accountability.

Technical

ISO 27000 (§3.10) defines Confidentiality as the 'property that information is not made available or disclosed to unauthorised individuals, entities, or processes.'[87] Together with information Integrity and Availability, it constitutes the foundation of information security — the CIA triad. Enabling accurate and complete information to be available in a timely manner to those with an authorised need is a catalyst for business efficiency and can be achieved through the implementation of an appropriate set of security controls, including policies, processes, procedures, and infrastructure to protect information assets.[88]

Building upon the above-mentioned standard, ISO/IEC 29100 provides a privacy framework for information and communication technology systems. It clarifies privacy safeguarding requirements as part of the overall privacy risk management process, that are influenced, *inter alia*, by legal, regulatory, contractual, and business factors. According to ISO/IEC 29100, ICT systems should establish an appropriate privacy policy and implement privacy controls, adhering to ten key privacy principles.[89]

NIST Special Publication 800-122 is a practical, context-based guide to identifying PII, determining what level of protection is appropriate and how to provide it.[90] The guide outlines considerations that should be addressed when developing operational and privacy-specific safeguards, which include policies, raising awareness and training for personnel, as well as practices to minimise PII collection, use, and retention, conducting privacy impact assessments, and setting up security controls. The publication also provides recommendations for developing response plans for incidents involving PII. 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, Security and Privacy Controls for Information Systems and Organizations. The latter addresses privacy and provides controls from a functionality perspective and from an assurance perspective to ensure that IT systems are sufficiently trustworthy.[91]

Legal

[87] ISO/IEC 27000, § 3.10. – Information Security Management Systems, https://www.iso.org/standard/73906.html (last accessed 7 February 2025).

[88] ISO/IEC 27000 – Information Security Management Systems, https://www.iso.org/standard/73906.html (last accessed 7 February 2025).

[89] ISO/IEC 29100 - Information technology — Security techniques — Privacy framework (2024), https://www.iso.org/standard/85938.html (last accessed 14 March 2025).

[90] 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 7 February 2025). See also Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017, Rev 5: 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

[91] See Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017, Rev 5: 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

While Recommendation 35 of the UNCITRAL Legislative Guide specifies a general rule that 'all registered information is fully and readily available to the public unless it is protected under the applicable law', Recommendation 36 establishes guidelines for cases where information within the business registry remains confidential. According to this Recommendation, the law should:

(a) Establish which information concerning the registered business is subject to the applicable law on public disclosure of protected data and which types of information cannot be publicly disclosed; and

(b) Specify the circumstances in which the registrar may use or disclose information that is subject to confidentiality restrictions.

In the EU, Article 5(1)(f) of the GDPR, entitled 'Principles relating to processing of personal data', mandates that personal data should be processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[92] Other GDPR principles relevant to Privacy in EBRs include lawfulness, fairness, transparency, purpose limitation, accuracy, storage limitation, and accountability.

EBRs in the Asia-Pacific region are recommended to follow the APEC Privacy Framework, which is consistent with the core principles of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data.[93]

7. Continual Improvement

Definition: The process of systematically identifying areas for improvement, making changes, and monitoring the results to ensure that they lead to positive outcomes

EBRs can adhere to the principle of Continual Improvement by implementing systematic processes aimed at enhancing their operations, services, and offerings over time. This approach involves setting up a cycle of planning, implementing, monitoring, and correcting any issues that arise as the registry refines its design and operations. Key elements include establishing feedback mechanisms to gather input from stakeholders, conducting regular evaluations to identify areas for enhancement, benchmarking against industry standards, and providing ongoing staff training. Embracing new technologies, monitoring key performance indicators, and fostering a culture of iterative improvement are also crucial to maintaining a dynamic and responsive registry. Areas for Continual Improvement may also be identified when issues arise, such as operational non-conformance, leading to unexpected or unacceptable outcomes. Performing a root cause analysis[94] will assist in identifying causal factors and corrective actions to be taken to prevent reoccurrence.

[92] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (last accessed 26 February 2025).

[93] APEC Privacy Framework, 2015, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (last accessed 14 March 2025).

[94] Root cause analysis is the quality management process by which an organisation searches for the root of a problem, issue or incident after it occurs. See more at: https://www.ibm.com/think/topics/root-cause-analysis (last accessed 16 July 2025).

Given that every improvement represents a change, it is essential to integrate robust change control and management methodologies into Continual Improvement initiatives. The commitment of senior management is necessary to ensure that these changes are effectively implemented and sustained over time.

Continual Improvement in EBRs should maintain a customer-centric focus. Regular benchmarking against industry standards and ongoing stakeholder feedback help ensure that improvements align with user needs. Fostering a culture that promotes commitment to learning and knowledge sharing ultimately ensures adaptability and relevance in a dynamic landscape.

Continual improvement is not only essential for enhancing operational efficiency and service quality – it is also critical for avoiding technological or functional obsolescence. As digital technologies evolve rapidly, underlying registry systems must undergo regular assessment and upgrades to remain current and competitive. Given their role in the business environment, EBRs need to avoid functional and technical degradation. By regularly refreshing their infrastructure and integrating emerging technologies, registries can ensure they remain viable, secure, and aligned with evolving stakeholder expectations.[95]

Technical

To uphold the principle of Continual Improvement, EBRs should implement their quality management processes in alignment with ISO 9001 standards. This involves understanding the needs and expectations of stakeholders and then establishing feedback mechanisms to gather input from stakeholders to inform improvements, conducting regular evaluations to identify areas for enhancement, benchmarking against industry standards such as ISO 27001 for information security management, implementing tools (for example, user analytics and error log monitoring) to assess system performance, and providing ongoing training for staff to ensure compliance with these standards.

Legal

The ability of a business registry to implement Continual Improvement measures is shaped by the legal environment in which it operates. In practice, registries often face a structural tension between rapid technological advancement and statutory regimes that lag in responsiveness. For instance, a law not recognising electronic signatures can act as a constraint on innovation rather than its enabler. Paragraph 236 of the UNCITRAL Legislative Guide recognises that implementing reforms in business registration can require amendments to various aspects of the law to facilitate transparency and procedural flexibility. Recommendation 58 further emphasises the need for a legislative approach that accommodates technological evolution.[96] This entails establishing provisions on electronic transactions within the law that are future-proof and adaptable. It is therefore essential that registries, when involved in legislative development, advocate for language that is technologically neutral, if not expressly enabling, to allow for Continual Improvement of their design and operations.

8. Continuity

[95] See more at Foster Moore, Registers The New Frontier: A Proposal for the development of a new target operating model for registers (2023), https://www.fostermoore.com/hubfs/PDF/Registers-The-New-Frontier-05-2023.pdf (last accessed 15 April 2025).

[96] UNCITRAL Legislative Guide, Recommendation 58.

Definition: The property of delivering registry services at acceptable levels within acceptable timeframes during and following a disruptive incident

This CPF encompasses the resilience required to manage and recover from minor disruptions, such as a system failure or a loss of power, to more severe events, such as a software or cloud service provider terminating operations. Continuity is differentiated from Availability by its focus on ensuring the provision of registry services during and after a disruptive event, whereas Availability relates to the percentage of time that the registry's services are available under normal operating conditions.[97]

To address catastrophic events (for instance, loss of power or infrastructure malfunctions), disaster recovery (DR) processes should be in place. The EBRs that employ cloud-based solutions should adopt resilient designs that ensure Continuity, for example, by storing multiple copies of the data in different geographic zones, having an off-cloud backup, or using a multi-cloud approach. For EBRs using on-premises infrastructure, robust back-up procedures should be in place, together with DR plans that enable the registry to immediately failover to a second (or third) data centre, which is geographically and politically diverse, with the aim of preventing total outage scenarios across all DR sites. Back-ups should be periodically tested to ensure data restoration will be successful.

DR processes would ideally achieve a recovery point objective (RPO) of zero (i.e., no loss of data or Integrity[98]) and a recovery time objective (RTO) of zero (i.e., immediate recovery or no reduction of Availability). However, such zero targets are often cost-prohibitive, and a business rationale should be used to select appropriate and realistic RPO and RTO values.

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. A key element of Continuity planning is performing a business impact analysis (BIA). This is the process of analysing activities and the effect that a business disruption might have upon them. An EBR should identify the systems, data, suppliers, resources, and processes necessary for the proper functioning of the registry. Each critical item should have a dedicated recovery plan which considers the internal and external impact for each critical item and provides for RPO and RTO objectives as outlined above. For example, easily replaceable components (e.g., electricity supplier) may require a simpler plan, while personnel or specialised vendor services might need more complex measures.

Disruptions caused by cyberattacks and software failures can severely impact the Continuity of registry services. It is therefore essential to incorporate robust cybersecurity measures and proactive software management strategies as integral parts of the Continuity framework. Such measures should include a multi-layered security strategy with real-time monitoring tools, vulnerability assessments, regular software updates, and the development of incident response and recovery plans. It is vitally important that appropriate information security practices are maintained *during* an accident.

Data portability is essential, especially for cloud-based environments. Portability enables the registry to move and adapt its applications and data between its own systems and cloud services, between cloud

[97] See Availability – CPF 5, supra.

[98] See Integrity – CPF 13, infra.

services from different cloud service providers, and potentially under different cloud deployment models.[99] In addition to facilitating more rapid and less costly migration, this measure reduces the risk of vendor lock-in.[100] It is important to note that portability is not a binary concept and that transforming EBR data from its form on the source system to the form required by the target system may still require considerable effort.[101] Portability is especially valuable in multi-cloud strategies and DR planning, where flexibility and responsiveness are essential.

In addition to DR, the registry should prepare transitional plans that identify the elements necessary to ensure Continuity and prepare it for any contingencies. Such plans might include holding the source code to the system in escrow; legal protection of the EBR's intellectual property where the operator becomes insolvent; and establishing a contingency fund.

When the registry relies on outsourced services, such as cloud hosting, payment gateways, or data verification, it should establish contingency measures for each. These include ensuring the technical and legal capacity to retrieve registry data, adapt software for compatibility with an alternative provider's system, and maintain core functionality in case third parties' services become unavailable.

When a registry's software is procured from a third-party provider, the registry should secure its legal rights to ensure service continuity without unexpected costs or service degradation, for instance, through transitional licensing or exit clauses. Such rights become especially relevant in cases of disputes or vendor insolvency. Notably, the right to access and retrieve the data in the EBR should always prevail over a licence to operate the underlying system in which the data is stored.

Outsourcing agreements should enable the registry to make and implement decisions related to outsourced functions, continuously monitor service provider performance, and manage outsourcing arrangements.[102] Clarity in terms of roles and responsibilities is equally essential. For example, in the Canadian province of Saskatchewan, the Operation of Public Registry Statutes Act[103] governs how service agreements between the government and private-sector companies should be concluded, outlining the division of powers and responsibilities over public registries.

While Continuity relates to the uninterrupted provision of services of the registry system itself, it also requires sufficiently skilled personnel. In view of this, business registries should develop knowledge management practices and cross-training programmes to mitigate the impact of personnel changes. Continued operation of a registry system should be ensured, even in a situation where the operator becomes insolvent (in any case, a low risk for EBRs, which typically operate under governmental agencies).

Technical

[99] See CSCC, Interoperability and Portability for Cloud Computing: A Guide Version 3.0, 6, (Cloud Standards Customer Council (CSCC), Dec. 2022), https://www.omg.org/cgi-bin/doc?mars/2022-12-13 (last accessed 7 February 2025).

[100] See ISO 19941 Cloud computing - Interoperability and Portability, Introduction, https://www.iso.org/standard/66639.html (last accessed 7 February 2025).

[101] Id.

[102] See Final Report on EBA Guidelines on Outsourcing Arrangements, §§ 40.a.

[103] Operation of Public Registry Statutes Act, O-4.2, S.S. 2013 (last updated in 2023), https://publications.saskatchewan.ca/#/products/67707 (last accessed 7 February 2025).

ISO 22301[104] specifies requirements to implement, maintain and improve a business continuity management (BCM) system[105] and can be used to assess an organisation's ability to meet its own Continuity needs and obligations. Other BCM standards include ISO/IEC 27001 on information security management systems and the NFPA 1660 Standard for Emergency, Continuity, and Crisis Management: Preparedness, Response, and Recovery.[106]

Legal

Paragraph 235 of the UNCITRAL Legislative Guide identifies that, due to user expectations of the business registry's reliable operation, the registrar must ensure that any interruptions are brief, infrequent, and minimally disruptive to users and governments. To achieve this, governments should implement suitable measures to safeguard the registry. One such measure could involve developing a business continuity plan outlining necessary arrangements for managing operational disruptions and ensuring uninterrupted services to users.

Regulations and standards often govern the implementation of a BCM plan.[107] Some jurisdictions require a plan for handling business-critical operations. [108] 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.

9. Correctability

Definition: The process of identifying and rectifying errors in a timely, accurate, and legally sound manner

The concept of Correctability in an EBR requires establishing a clear definition of what constitutes an error. In this context, errors encompass deviations from accurate information, including grammatical or typographical inaccuracies during data entry, incomplete provision of required information, and submission of false or incorrect data. It is important to distinguish between errors and outdated information. While outdated information in the registry record indicates that the data held is not accurate, it does not necessarily qualify as an error unless it results from failure to comply with statutory updating obligations. Considerable attention is devoted to data accuracy in CPF 3 on Accuracy, above.

The responsibility to update and correct any errors or omissions in the information included in an application for registration or a request for an amendment submitted to the registry lies primarily with the data provider, i.e., the registrant.

EBRs should adopt robust mechanisms for detecting and correcting errors, ensuring the accuracy and trustworthiness of the data they provide to stakeholders. When registering data into the registry, it is crucial to verify that the pieces of information provided are consistent with each other and with the accompanying

[104] ISO 22301:2019 - Security and Resilience — Business Continuity Management Systems — Requirements, https://www.iso.org/standard/75106.html (last accessed 7 February 2025).

[105] See Chapter IV, infra.

[106] NFPA 1660: Standard for Emergency, Continuity, and Crisis Management: Preparedness, Response, and Recovery, 2024, https://www.nfpa.org/codes-and-standards/nfpa-1660-standard-development/1660 (last accessed 25 February 2025).

[107] See ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements (ISO, 2019), https://www.iso.org/standard/75106.html (last accessed 25 February 2025).

[108] See Monetary Authority of Singapore, Guidelines on Business Continuity Management (2022) https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management (last accessed 25 February 2025).

documents. The Data Input Validation (CPF 10) and Error Detection (CPF 11) processes are interrelated, focusing on maximising the accuracy of registered data, while Accuracy (CPF 3), in turn, highlights the importance of continuous evaluation and improvement of information quality within the EBR, reflecting the trust and reliability associated with registries.

Registrars should be authorised to correct computer-generated errors autonomously if appropriate or, if necessary, seek judicial approval through court orders. They should also inform users about policies and error correction processes in their jurisdiction. CPF 16 on Legal Authority of the Registrar underlines the importance of having regulations that grant registrars the right to correct human or computer-generated errors, ensuring legal authority to maintain accurate records. According to the UNCITRAL Legislative Guide, a registrar should have the authority to rectify its own errors and any incidental errors found in the supporting documentation submitted for business registration.[109] However, this authority should be exercised within clearly established conditions and limitations in a transparent manner. This ensures that any corrections made by the registrar uphold the integrity and accuracy of the registry's records while maintaining transparency in the registration process.

Corrections should be made exclusively through the registry’s application interface rather than via direct database manipulation. This method ensures systematic logging of changes, rigorous verification and auditing, thus reducing the risk of inadvertent changes to registry records. Notwithstanding the cost, error correction functionality should be built into the EBR system.

In the event of errors, EBRs must have clearly defined procedures, such as:

(a) Correction procedures and clarifying processes for rectifying information by the registrants, which include submitting error correction forms or requests;

(b) Verification processes, ensuring the accuracy and legitimacy of corrections, which may involve verification checks or document reviews;

(c) Audit trails and records documenting changes made to registered information, which facilitates tracking modifications and ensures transparency and accountability; and

(d) Communication channels offering accessible mechanisms for stakeholders to report errors, seek assistance with correcting information, and be informed when corrections are implemented.

EBRs should also employ appropriate mechanisms to enforce rectification of detected inaccuracies by data providers. As demonstrated by Figure 5 below, such measures often include penalties (administrative and/or financial), suspension of the business’s status on the register, and limitation of participation in business activities.

[109] UNCITRAL Legislative Guide, para. 147.

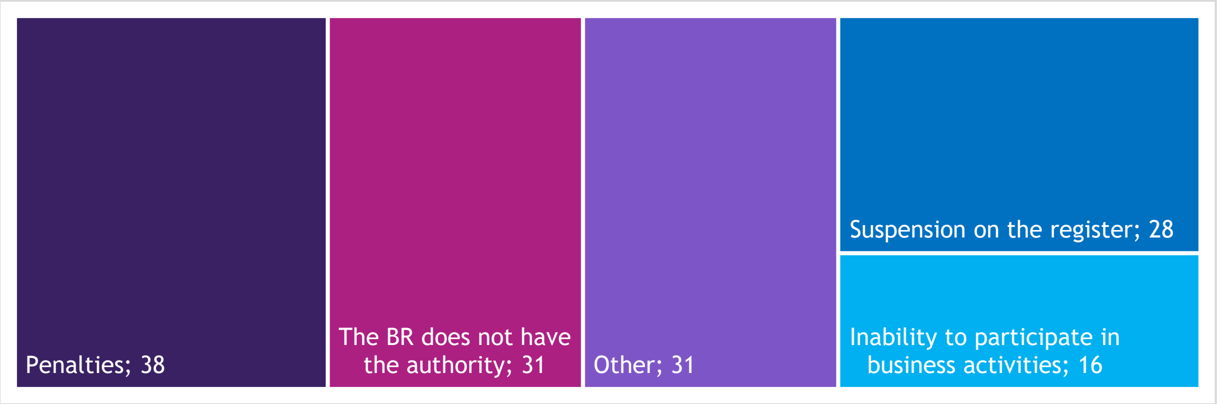


Figure 5. Mechanisms to enforce rectification of detected data inaccuracies by the entities.[110] The figure has been redrawn by the authors for clarity.

Errors may also result from unauthorised alterations through cyberattacks or technical malfunctions. Identifying such errors involves proactive approaches, such as employing public reporting and feedback mechanisms, which allow stakeholders to flag discrepancies, and advanced technical tools like anomaly detection algorithms to detect unauthorised changes. Automated data input validation checks can also ensure the internal consistency of submitted entries. Additionally, regular data audits are instrumental in identifying and resolving persistent or systemic issues. More about these mechanisms is elaborated in CPF 11 on Error Detection.

Technical

ISO/IEC 25012,[111] also known as Software Product Quality Requirements and Evaluation (SQuaRE), specifies data quality models and metrics, encompassing aspects related to error detection and correction as integral components of data quality assurance. NIST Special Publication 800-55 Volume 2[112] offers guidance on establishing procedures that enhance an organisation's ability to identify, assess, and rectify errors, covering continuous monitoring and improvement, feedback mechanisms, and thorough documentation and reporting.

Legal

The UNCITRAL Legislative Guide clearly states that the law should establish that the registrar may not alter or remove registered information, except as specified by law, and that any change to that information must be made in accordance with the applicable law. A similar approach should be taken in jurisdictions where information submitted electronically to the business registry must be entered manually by registry staff into the registry record, which naturally exposes such entry to error.

In accordance with Recommendation 27 of the UNCITRAL Legislative Guide, the law should grant the registrar the authority to correct its own errors as well as any incidental errors that may appear in the information submitted in support of the registration of the business, provided that the conditions under which the registrar may exercise this authority are clearly established.

[110] IBRR, Data Verification Survey (2024), https://br-insights.org/reports-dashboards/data-verification-2024/ (last accessed 14 April 2025).

[111] ISO/IEC 25012 Software engineering Software product Quality Requirements and Evaluation (SQuaRE) Data quality model; https://www.iso.org/standard/35736.html (last accessed 7 February 2025)

[112] NIST SP 800-55 v2 Measurement Guide for Information Security, 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v2.pdf (last accessed 7 February 2025).

10. Data Input Validation

Definition: The process of assessing that the data meets the established criteria for its purpose in the registry

Data Input Validation is a systematic process aimed at assessing compliance of entered data with criteria established by the EBR, focusing on structure and logical consistency. Validation of data inputs improves the quality of data in a registry by rejecting submissions that do not conform to required data specifications. It is a critical measure in EBRs that reduces the likelihood of errors, inconsistencies and incomplete entries, supporting seamless processing and reducing the risk of injection attacks, such as SQL injection, cross-site scripting, and command injection, by rejecting malformed or malicious input at the point of entry.[113]

Data Input Validation involves several layers of control that occur before data is stored or processed. It checks that the data submitted is, first, syntactically and, second, semantically valid before using it in any way, including displaying it back to the user. Syntactic validation checks that the data is in the expected format and structure. For example, ensuring that a required field (e.g., to enter share capital data) has not been left blank or that the required number of digits (e.g., for an ID number identifying the grantor) has been entered. Semantic validation verifies that the submitted data is logically consistent within the context of the rules of the EBR.[114]

Data Input Validation can be implemented on the front end, also known as client-side, and on the server-side before any data is processed by the system's functions. Front-end Data Input Validation occurs within the browser or local software client, before the data is submitted to the server. It improves user experience and can correct errors in the input early on, but it does not act as a security feature and can be bypassed or manipulated by users. It helps the honest user to avoid mistakes in data entry, but it can be circumvented by a dishonest and skilled user. After the data is submitted, back-end validation, which is a security feature, checks the inputs and rejects those that do not pass the required validation tests. Implementing both front-end validation for user experience and server-side validation for security is a recommended approach, increasing the EBR system's usability and safety.

Real-time data validation, as outlined in the World Bank's report on data-driven company registries,[115] reinforces the approach that errors should be flagged immediately at the point of entry. This mechanism allows for faster correction of errors, minimises manual oversight, reduces processing times, and ensures data quality from the outset, making it an essential component of modern EBRs.

Validation remains relevant in post-registration activities as well, such as amendments, renewals, or deregistrations. For example, if appropriate, it can preclude the registration of an amendment of a registration that has already been cancelled. The specific business rules for each registry will be based on its legal framework.

[113] See OWASP, C3: Validate Input and Handle Exceptions, in OWASP Top 10 Proactive Controls 2024, https://top10proactive.owasp.org/archive/2024/the-top-10/c3-validate-input-and-handle-exceptions (last accessed 7 February 2025).

[114] Id.

[115] World Bank Group, Data-Driven Company Registry, Guidance note (2022), https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf (last accessed 7 February 2025).

The UNCITRAL Legislative Guide[116] encourages implementing a series of checks and control procedures to ensure the provision of necessary information for business registration. For example, an electronic data submission service enables the identification of mandatory designated fields. Accordingly, if the required data is not entered, the system will automatically identify improperly filled or unfilled fields, prompting the applicant to make necessary corrections. This mechanism allows registries to maintain a high degree of operational efficiency and transparency, facilitating smoother business registration procedures while reducing administrative burden.

As registries move towards more automated systems, the human role in reviewing and correcting data decreases due to reliance on automation. This emphasises the need for more precise, layered Data Input Validation, which is perceived not just as a support function but a critical control in automated self-service systems. Such an approach requires validation rules to be designed to cover complex rules that have previously been managed by personnel within a manual process and should be regularly reviewed and updated as automation in systems expands.

As EBRs become increasingly interconnected through cross-border data exchanges, API-based verifications, or integration with other national authorities and databases, cross-registry Data Input Validation becomes ever more essential — this involves using common data standards and taxonomies, validation rules, and coherent electronic filing systems (see CPF 14 on Interoperability).

Technical

International standards like ISO/IEC 27001 and ISO/IEC 27002 emphasise the importance of implementing controls to validate input against system-defined rules, ensuring compliance before further processing, for the purposes of information security management. ISO/IEC 27034[117] reinforces this by integrating input validation mechanisms into application-level security to protect software from unauthorised or malformed input. Similarly, NIST SP 800-53,[118] under control SI-10 (Information Input Validation), highlights the need for the systems to validate input to meet specified syntax, type, and format requirements before processing, while NIST SP 800-218[119] promotes input validation as a foundational practice in secure software development. These standards underscore the importance of validation not just as a data quality mechanism but as a security and risk mitigation strategy.

The Open Worldwide Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.[120] Among its resources for assisting developers are the OWASP Top Ten Proactive Controls — a list of defensive techniques and controls that should be considered for every software

[116] UNCITRAL Legislative Guide, para. 146.

[117] ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security, 2011, https://www.iso.org/standard/44378.html (last accessed 7 February 2025)

[118] Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017, last updated 2020), App. D., https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

[119] Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities: NIST SP 800-218, 2022, https://csrc.nist.gov/pubs/sp/800/218/final (last accessed 7 February 2025)

[120] See the Open Worldwide Application Security Project (OWASP), https://owasp.org/ (last accessed 7 February 2025).

development project.[121] Ranked in order of importance, Input Validation is third on the list,[122] emphasising its critical role in preventing vulnerabilities.

Legal

The UNCITRAL Legislative Guide outlines guidelines for handling rejection due to errors in registration applications. In a registry system that allows registrants to submit applications and relevant information directly to the registry electronically, the system should be designed, when permitted by the State's technological infrastructure, so as to automatically require correction of the application if it is submitted with an error, and to automatically reject the submission of incomplete or illegible applications, displaying the reasons for the rejection on the registrant's screen.

11. Error Detection

Definition: The process of detecting discrepancies, inaccuracies, or wrongful information within the registry data

Detection of errors in the EBR plays a significant role in maintaining the data's reliability and accuracy. Inaccurate or incorrect data can involve operational and reputational risks that may undermine efficient business registration systems and erode stakeholders' trust. Error Detection is distinct from Data Input Validation. While Data Input Validation attempts to prevent errors at the point of entry (i.e., a protective control), Error Detection tackles issues arising at later stages in the data lifecycle (i.e., a detective control), identifying errors that have bypassed initial checks or emerged post-entry due to technical faults or external interference.

Error Detection can be achieved in different ways, depending on the nature of the error. Firstly, cryptographic controls can allow the system to detect if the data has become false, for instance, due to hard disk corruption or incomplete data replication. These controls are particularly valuable in identifying silent data corruption and tampering by malicious actors.

Secondly, some errors may require more advanced detection logic than standard Data Input Validation. These can include implausible dates of birth, incongruent fields, or role misassignments (for instance, a date of birth as 1900 instead of 1990, or a seven-year-old being listed as a professor). Such errors can be identified through rule-based detection engines that flag outliers and illogical combinations. These checks are developed over the years as errors are found manually, and then detection controls are introduced, in fact embodying a process of Continual Improvement (CPF 7).

Thirdly, other errors can be detected by cross-referencing authoritative external databases into EBRs' validation workflows. For instance, a business registration system can cross-check the directors' identification numbers against a national identification database, identifying any mismatches or fraudulent entries. Address verification can be enabled through geolocation APIs[123] and national postal services to

[121] See OWASP Top 10 Proactive Controls, https://top10proactive.owasp.org/the-top-10/ (last accessed 7 February 2025).).

[122] See OWASP Top 10 Proactive Controls, https://top10proactive.owasp.org/the-top-10/c3-validate-input-and-handle-exceptions/ (last accessed 7 February 2025).

[123] Esri Geocoding Services, https://developers.arcgis.com/rest/geocode/ (last accessed 7 February 2025).

correct address representation and standardise location data. Such cross-system workflows allow for the reduction of errors that otherwise persist within isolated systems.

Data science and machine learning models provide additional capabilities for detecting anomalies and predicting potential issues. Such models analyse historical data and allow EBRs to act earlier by recognising patterns deviating from the expected trend. For instance, the Danish Business Authority uses machine learning on interlinked datasets to detect abnormalities in business registrations for accuracy and compliance.[124]

Audit trails and version control systems that keep a complete history of all changes made on the register enable retrospective error detection. Such logs allow administrators to track changes, verify authorisations, and provide forensic insight in the event of cyberattacks or internal misuse. Additionally, real-time monitoring of access logs, automated alerts and deep analytics permit registrars to identify and respond promptly to anomalies and suspicious activities.

It is important to acknowledge that some errors, such as those resulting from unintentional human input, deliberate data manipulation or systemic flaws, may not always be immediately detectable. Therefore, the process of Continual Improvement again applies here, so that each data error detected manually or with ML tools is then reviewed and new protective and detective controls are introduced to reduce the risk of reoccurrence (again, see CPF 7 on Continual Improvement).

Technical

ISO/IEC 25012[125] defines a general data quality model for data retained in a structured format within a computer system. This data quality model presents a framework for defining and measuring data quality attributes, like completeness, accuracy, and validity, which are crucial for detecting errors and taking corrective action. ISO 8000-8 defines characteristics of information and data that determine its quality and specifies criteria for measuring data quality on three levels: syntactic, semantic, and pragmatic.[126]

ISO/IEC 27002[127] provides guidance for security controls, such as logging and anomaly detection, to ensure unauthorised changes are promptly detected. ISO/IEC 7064 specifies a set of ‘check character systems’ capable of protecting strings against errors that occur when people copy or type data.[128] NIST SP 800-53[129] completes this guidance by providing details of mechanisms for integrity checking using cryptographic techniques and monitoring system activities for discrepancies.

12. Evidentiary Value

[124] World Bank Group (2022), Data-Driven Company Registry, Guidance note, https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf (last accessed 7 February 2025).

[125] ISO/IEC 25012 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model, 2008, https://www.iso.org/standard/35736.html (last accessed 26 February 2025).

[126] ISO 8000-8 Data quality Part 8: Information and data quality: Concepts and measuring, 2015, https://www.iso.org/standard/60805.html (last accessed 7 May 2025).

[127] ISO 27002 Information Technology, Security Techniques, Code of Practice for Information Security Management, 2022, https://www.iso.org/standard/75652.html (last accessed 26 February 2025).

[128] ISO/IEC 7064 Information technology — Security techniques — Check character systems, 2003, https://www.iso.org/standard/31531.html (last accessed 7 May 2025).

[129] Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017, last updated 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

Definition: The property of constituting evidence or having the quality of evidence

Ensuring the Evidentiary Value of registry data is fundamental to maintaining legal certainty, regulatory compliance, and effective dispute resolution. To maintain the accuracy, integrity, and legal standing of their records over time, business registries should implement a robust set of legal, technical, and operational safeguards. Key components such as Data Input Validation (CPF 10), Integrity (CPF 13) and Reliability (CPF 17) are all integral to the concept of Evidentiary Value.

Business registries should align their operational frameworks with the specific legal and regulatory standards of their respective jurisdictions to ensure the evidentiary value of their data. Various technological and administrative methods should be implemented to guarantee the evidentiary value of EBR data and support the evidentiary integrity of register records. These precautions should include data change control procedures, extensive logging systems, reliable long-term storage options, and mechanisms for forensic evidence collection.

The implementation of data change control procedures is a key procedural step. Records must stay entire and unaltered, with stringent controls over any modifications, following the ISO 15489 standard.[130] Any modifications to registry data must be subject to formal approval processes, with details of the reasons for the change, the parties involved, and the exact modifications made. Maintaining a complete audit trail is essential to ensure that historical records and metadata remain accessible and verifiable. Logs must capture both automated and manual changes, documenting the identity of the user making the change, the context of the change, and the timestamps. This ensures transparency and provides an authoritative record for legal scrutiny. In disputes or regulatory investigations, detailed logs and records provide essential evidence to substantiate the reliability and validity of registry data. While not all logs need to be retained indefinitely, those relevant to incident detection (e.g., cybersecurity events) should be kept for a period appropriate to risk exposure (e.g., 18–24 months), with longer retention for data supporting legal evidence, and such logs should be tamper-resistant where possible.

Technical measures are essential in preserving data integrity. Qualified electronic signatures, electronic seals, and electronic ledgers (as outlined, for example, in the revised eIDAS 2.0 Regulation (No. 2024/1183)) allow for verifying the records' origin, integrity and legal status as evidence.[131] Complementing this, timestamping[132] serves to enhance data integrity by detecting modifications and establishing an immutable and verifiable chronological sequence for record creation and updates.

Equally important, a chain of custody protocol[133] ensures accountability by creating a transparent and secure trail regarding how the records have been accessed, transferred, or modified. Such protocols help prevent unauthorised modifications, provide user accountability, and support litigation and regulatory review.

[130] ISO 15489-1 Information and documentation — Records management, 2016, https://www.iso.org/standard/62542.html (last accessed 26 February 2025).

[131] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0 Regulation), http://data.europa.eu/eli/reg/2024/1183/oj (last accessed 5 May 2025).

[132] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0 Regulation), http://data.europa.eu/eli/reg/2024/1183/oj (last accessed 5 May 2025).

[133] Guide to Integrating Forensic Techniques into Incident Response, NIST, Special Publication 800-86, 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (last accessed 7 February 2025).

As a general rule, according to the UNCITRAL Legislative Guide, paragraph 227, registries should retain information indefinitely unless otherwise specified by law, ensuring their availability for legal and regulatory purposes. Identifying critical records and logs required for legal and regulatory purposes allows systems to be configured to capture and retain this information effectively (see CPF 18 on Retention and Disposition).

Technical

The Evidentiary Value of data housed within the business registry can be supported through adoption of internationally recognised frameworks. ISO 15489 provides criteria for detailed documentation and audit trails that ensure transparency and accountability for changes made to the data.[134] ISO/IEC 27001 deals with data integrity and security issues and provides mainly long-term storage principles and possible actions against technological obsolescence.[135] ISO/IEC 32000-2 provides guidance on digital signature validation and long-term validation formats (e.g., XAdES, PAdES).[136] Timestamping protocols and time-stamp token profiles are also elaborated in standard ETSI EN 319 422.[137] NIST SP 800-53[138] addresses privacy - and security-related controls; NIST SP 800-92[139] and NIST SP 800-86[140] address audit log management and cryptographic techniques to ensure data integrity. Together, these standards form the foundation of a chain of custody, safeguarding records and ensuring their evidentiary value.

13. Integrity

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

The 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 a reliable and authoritative source of information. The data Integrity of the EBR directly reflects on the reputation of the registrar.[141]

Integrity relates to the system, the data, and any decision-making of the registrar and registry staff. Ensuring Integrity is an ongoing objective that requires regular reviews and updates of security measures, risk assessments in light of emerging threats, and periodic audits of system access and user activity.

The registrar plays a key role in Integrity assurance, ensuring that submissions are not altered or corrupted after submission. Importantly, even invalid or incorrect data and documents submitted to the registrar must not be deleted or changed without preserving a complete and transparent record. This approach allows any

[134] ISO 15489-1 Information and documentation — Records management, 2016, https://www.iso.org/standard/62542.html (last accessed 6 May 2025).

[135] ISO/IEC 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022, https://www.iso.org/standard/27001 (last accessed 6 May 2025).

[136] ISO 32000-2, Document management — Portable document format, 2020, https://www.iso.org/standard/75839.html (last accessed 6 May 2025).

[137] ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, 2016, https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf (last accessed 6 May 2025).

[138] NIST Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53 Revision 5, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

[139] Guide to Computer Security Log Management, NIST SP 800-92, https://csrc.nist.gov/pubs/sp/800/92/final (last accessed 7 February 2025). See also NIST SP 800-92 (Initial Public Draft), Cybersecurity Log Management Planning Guide, 2023, https://csrc.nist.gov/pubs/sp/800/92/r1/ipd (last accessed 25 February 2025).

[140] Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, https://csrc.nist.gov/pubs/sp/800/86/final, (last accessed 7 February 2025).

[141] Foster Moore, Registers the New Frontier: A proposal for the development of a new target operating model for registers, https://www.fostermoore.com/white-papers/proposed-new-target-operating-model-for-registers-white-paper (last accessed 7 February 2025).

submission to be traced back to its initial state, thus increasing confidence in the system and strengthening the evidentiary value of registry records, an essential factor in ensuring legal certainty (see CPF 12 on Evidentiary Value).

Integrity relates not only to the data submitted by registrants but also to internally generated metadata. The registry should apply timestamps to all registrations and state changes in the EBR, to ensure the reliability of registered data and when disclosing information to third parties. Such timestamps should be cryptographically secured to prevent any tampering with the order in which changes occur. A forensic audit trail of chronologically ordered events should also be maintained.

Integrity depends heavily on access controls in EBR design. The EBR should also appropriately segregate the duties of registry staff and ensure that access authorisation does not exceed what is necessary for an employee's assigned tasks (see CPF 1 on Access Control). For instance, database permissions necessary for the registrar to correct registry errors should be restricted to staff acting under the legal authority of the registrar (see also CPF 16 on Legal Authority of the Registrar).

Integrity may further be dependent on the systems and controls of users who transact with the registry. This is particularly relevant for high-volume users who may transact through an API. If such users' systems are compromised due to malicious attacks or staff errors, many registrations might be impacted. To mitigate such risk, clear internal controls around API-based access should be in place, such as a suitable whitelisting mechanism through which the users connecting to the API are known in advance. This should allow system administrators to cut access should there be a compromise of a client's API channel or if the client's link is degrading the performance of the registry. In the absence of such a whitelist facility, the registry should have the capacity to blacklist API users where necessary (see also CPF 14 on Interoperability).

An example of a deliberate Integrity breach is the 2020 SolarWinds supply chain attack.[142] In this case, state-linked attackers infiltrated SolarWinds' software development environment and used malware to alter the build process of the company's Orion IT monitoring software. The attackers replaced legitimate source files with malicious versions containing a backdoor. These malicious versions were then compiled into signed software updates for distribution, while the original files were restored to conceal the tampering.[143] These compromised updates were distributed to over 18,000 SolarWinds customers, including critical US government agencies, major corporations, and infrastructure providers. The attackers manipulated trusted software artefacts at source, resulting in an attack on the Integrity of the software supply chain. The resulting updates looked authentic and passed signature checks but embedded malicious code into critical IT systems. Once installed, the compromised software further manipulated system configurations and logs, allowing it to establish a longer-term presence. The victims' systems appeared operational, but their underlying trust and correctness had been subverted. This case demonstrates how Integrity attacks can fundamentally erode confidence in trusted digital services. For EBRs, a comparable compromise could result in unauthorised filings, falsified records, or the insertion of malicious functionality into core services. Even

[142] Nakashima, E., A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (last accessed 25 June 2025).

[143] CrowdStrike, SUNSPOT Malware: Technical Analysis, https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/ (last accessed 25 June 2025).

without visible data theft, such a breach would severely undermine the Integrity, Evidentiary Value and Trustworthiness of registry operations.

Technical

The ISO 27000 family of standards provides useful reference points for various cryptographic methods, including encryption and algorithm standards. ISO 27002[144] Control 8.24 outlines the use of cryptography to protect information confidentiality, integrity, and authenticity. Control 8.24 is a preventive type of control that requires organisations to establish rules and procedures for the effective use of cryptographic techniques and thus eliminate and minimise risks to the compromise of information assets when they are in transit or at rest.[145] ISO/IEC 27701 Clause 6.7 relies on the same guidance notes from ISO 27002 Control 8.24 to provide a cryptographic framework within which organisations can operate. Specifically, ISO 27701 Clause 6.7 requires organisations to implement cryptographic controls to protect PII by developing a cryptographic policy, managing encryption keys, and ensuring compliance with regulatory requirements.[146]

ISO 27001 Annex A 8.27, Secure System Architecture and Engineering Principles, includes guidance on tamper-proofing to ensure that systems remain secure and impervious to malicious interference and emphasises that tamper resistance techniques can detect both logical and physical manipulation of information systems, preventing unauthorised access to data. In some cases, the control can prevent the successful extraction of data through its destruction (e.g., device memory can be deleted).[147]

ISO 27040 provides an overview of the design and implementation of storage security, related concepts and definitions. It includes guidance on the threat, design, and control aspects associated with storage technology.[148] In addition, it provides references to other standards that address practices and techniques relevant to storage security, such as IEEE 1619.1-2007 and NIST-FIPS 197, which formally define the Advanced Encryption Standard and provide authenticated encryption to protect the Integrity of stored data.[149] NIST SP 800-53 devotes special attention to software, firmware, and information integrity. It elaborates on several controls supporting Integrity, among which: integrity checks, automated notifications of and automated responses to integrity violations, cryptographic protections, and integrity verifications.[150]

Legal

Recommendation 10 of the UNCITRAL Legislative Guide underscores the importance of safeguarding the integrity of information contained within registry records as a core function and intended goal of business

[144] ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls, 2-022, https://www.iso.org/standard/75652.html (last accessed 7 May 2025).

[145] Max Edwards, ISO 27002 — Control 8.24 —Use of Cryptography, (ISMS.Online, Feb. 17, 2025), https://www.isms.online/iso-27002/control-8-24-use-of-cryptography/ (last accessed 7 May 2025).

[146] Max Edwards, ISO 27001 — Clause 6.7 — Cryptography, (ISMS.Online, Feb. 26, 2025), https://www.isms.online/iso-27701/clause-6-7-cryptography/ (last accessed 7 May 2025).

[147] ISO/IEC 27001, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, https://www.iso.org/standard/27001 (last accessed 7 February 2025).

[148] See ISO/IEC 27040 Information technology — Security techniques — Storage security § 7, Second Edition 2024, https://www.iso.org/standard/80194.html (last accessed 26 February 2025).

[149] IEEE 1619.1-2019 - IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices, 2019, https://ieeexplore.ieee.org/document/8637991 (last accessed 7 February 2025); NIST-FIPS 197 Advanced Encryption Standard (AES), 2001, updated 2023, https://csrc.nist.gov/publications/detail/fips/197/final (last accessed 7 February 2025).

[150] Security and Privacy Controls for Information Systems and Organizations: Special Publication 800-53, NIST (2017, last updated 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed 7 February 2025).

registries. Ensuring the integrity of registry data involves protecting the identity and accuracy of registered businesses.

In line with this recommendation, governments should maintain backup copies of registry records to mitigate the risk of loss, physical damage, or destruction.[151] In addition to these risks, EBRs face threats from criminal activities facilitated by technology. Therefore, implementing effective enforcement measures within the legislative framework is crucial to support the adoption of electronic solutions for business registration.[152]

These measures are essential for maintaining trust and confidence in the integrity of business registry systems and are reinforced in Recommendation 54 of the UNCITRAL Legislative Guide, which addresses the protection of business registry records against loss or damage.

14. 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 an automated manner and transparently for its users. It may be mandated by law or enabled by the system provider as a service to users. In EBRs, interoperability enables data sharing between different systems involved in the business registration, such as tax authorities, social security institutions, business regulators, the natural persons register, the address register, or commercial banks. This capability allows correct, timely, and cost-efficient reuse of registration data and is essential for maintaining data quality, streamlining procedures, and improving user experiences.[153]

In the EU, the European Interoperability Framework (EIF) advances public sector interoperability. The EIF distinguishes four dimensions of interoperability: legal, organisational, semantic, and technical (see Table 2).[154]

[151] UNCITRAL Legislative Guide, para. 233.

[152] UNCITRAL Legislative Guide, para. 234.

[153] World Bank Group (2022), Data-Driven Company Registry, Guidance note, https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf (last accessed 7 May 2025).

[154] New European Interoperability Framework 2017, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (last accessed 26 February 2025).

Legal interoperability	Organisational interoperability
Ensuring that organisations operating under different legal frameworks, policies, and strategies can work together. Common service terms and conditions, data-sharing principles, interoperability agreements on governance, accessibility, and data quality improve access to data.	Modelling business processes, aligning information architectures with organisational structures, and helping business processes to cooperate. Robust data management processes and service-level policies are critical for reliable sources of information.
Semantic interoperability	**Technical interoperability**
Ensuring that the precise meaning of exchanged information is understandable by any other application not initially developed for this purpose. Semantic assets, such as vocabularies, code lists, glossaries, and identifiers, can improve semantic interoperability.	Focusing on technical aspects of networks for data transport, interconnection architecture, standards for data exchange, and security. Adopting API-first principles and standardised data formats enhances data exchange and interoperability.

Table 2. Four dimensions of interoperability.

Interoperability governance refers to the oversight of interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements, and other aspects of ensuring and monitoring interoperability at different jurisdictional levels.[155] For example, the Interoperable Europe Act establishes the Interoperable Europe Board (the Board), composed of one representative designated by each Member State and the Commission.[156] The Board is responsible for monitoring the overall coherence of the recommended interoperability solutions at the national, regional, and local level.[157] Additionally, any EU entity responsible for regulating, providing, or managing trans-European digital public services shall designate an interoperability coordinator to provide support with regard to establishing or adapting internal processes to implement interoperability assessments.[158]

Interoperability is vital to facilitating cross-border business activities. For instance, the Business Register Interoperability System (BRIS)[159] allows for the simplification of cross-border transfer of a company's seat through a cooperative framework among EU business registries. Directive (EU) 2025/25 on digital tools in company law further strengthens interoperability in the EU.[160] It connects three systems, namely: BRIS; the Beneficial Ownership Register Interconnection (BORIS), linking national BO registries;[161] and the Insolvency Registers Interconnection (IRI) system. This way, the EU aims to improve access to and enable the carrying out of cross-checks on business information while respecting the access regime for information in each interconnected system.

[155] Enabling Digital Government: Interoperability and Data Exchange Between Registries, The benefits of a connected landscape, Bill Clarke, VP Business Development, Teranet Inc., John Murray, VP European Operations, Foster Moore International Limited, 2023, https://www.teranet.ca/wp-content/uploads/2023/02/Teranet-Foster-Moore_Interoperability-and-Data-Exchange-Between-Registries-01.30.23.pdf (last accessed 26 February 2025).

[156] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), Article 15.

[157] Id.

[158] Id., Art 18.

[159] European e-Justice Portal, Business registries at European level, 2017, https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do (last accessed 7 February 2025).

[160] Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law (Text with EEA relevance), http://data.europa.eu/eli/dir/2025/25/oj (last accessed 6 May 2025).

[161] European e-Justice Portal, Beneficial Ownership Interconnection System BORIS, https://e-justice.europa.eu/38590/EN/beneficial_ownership_registers_interconnection_system_boris (last accessed 26 February 2025).

Canada's Multi-Jurisdictional Registry Access Service (MRAS) is another example, connecting federal, provincial, and territorial business registries to reduce red tape and trade barriers for businesses nationwide. MRAS streamlines business registration by enabling real-time transactions where businesses can retrieve core information from their home jurisdiction to register in another. Moreover, it facilitates the communication of changes made by a business in one jurisdiction to other jurisdictions, in which the business is registered. Additionally, MRAS allows the public to search for businesses across registries, eliminating the need to search each registry individually.

In its publication "Digital Public Infrastructure and Development", the World Bank has underlined the importance of registries, including business registries, identifying them as a key element or 'building block' in the ecosystem of integrated digital public services. Implementing the interoperability principle is essential to ensure that data from registries is accessible.[162]

Insufficient Interoperability can lead to fragmentation and inconsistency, data duplication, outdated information, and lack of transparency in business transactions. This inconsistency breaches the 'once-only' principle, which holds that the same information should be provided by citizens and businesses to public administrations only once, and that that information be reused where permitted to achieve efficiency and increase user-friendliness.

Some jurisdictions designate business registries as base registries, such as in Denmark, where the Danish Business Authority manages such functions.[163] Base registries are trusted and authentic sources of information under the control of a public administration or organisation appointed by the government, and they are central to implementing the once-only principle. All other registries or information systems that require data about businesses should cross-check against the data in the respective base registry. To be authoritative, base registries should show the correct status, be up-to-date, and be of the highest possible quality and integrity. For this purpose, the EIF recommends that: (i) information should be made available while implementing access control mechanisms to ensure security and privacy (Recommendation 37); (ii) semantic and technical means and documentation needed for others to connect and reuse available information should be developed (Recommendation 38); (iii) each base registry should be associated with appropriate metadata, including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries (Recommendation 39); and (iv) data quality assurance plans should be created and followed (Recommendation 40).[164]

[162] Clark, J., Marin, G., Ardic Alper, O.P., Galicia Rabadan, G.A. 2025. Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1, Washington, DC: World Bank, p. 28, https://openknowledge.worldbank.org/server/api/core/bitstreams/93b2a6ef-d819-4cf4-b4d3-fb3387f5ec7a/content (last accessed 7 May 2025).

[163] *Danish law states that the central Business Registry (1) is the body which is responsible for the maintenance and development of the base registry, (2) cooperates with Customs, Tax and Statistics organisations for the registration and maintenance of certain basic data and activities and (3) is obliged to record: basic data on legal entities (e.g. a natural person in its capacity as employer or self-employed, a legal entity or a branch of a foreign legal person, an administrative entity, a region, a municipality, a municipal association); a unique numbering for legal entities; basic data available to public authorities and institutions, as well as private ones.* See more ABR Factsheet 2017, Denmark, European Commission, https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Denmark%20Factsheet%20Final_DIGST_everis.pdf (last accessed 2 April 2025).

[164] New European Interoperability Framework, Promoting seamless services and data flows for European public administrations, European Union, 2017, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (last accessed 5 May 2025).

FATF also strongly recommends data exchange at both the national and international level. Recognising the significance of sharing basic and BO information, countries are urged to rapidly, constructively and effectively provide the widest possible range of international cooperation in relation to basic and BO information, on the basis set out in Recommendations 37 and 40.[165]

Where Interoperability is mandated by the law, appropriate communications and governance protocols for managing Interoperability and data sharing agreements with the other databases should be established. Service-level agreements should govern the specific terms and conditions of service, including, among other things, service availability, advance downtime notification, service response time, IT support, and problem reporting and escalation procedures.[166]

A key enabler of Interoperability is standardisation, which serves as a form of normalisation that allows data to be shared seamlessly across systems. Standardised data formats and taxonomies are foundational to ensuring that disparate systems can communicate effectively.

Processing vast amounts of financial and non-financial business data, a growing number of registries adopt the XBRL (eXtensible Business Reporting Language)[167] format for statutory reporting and annual accounts. XBRL helps to automate and streamline the collection and validation of company data to reduce manual work and time of data processing, and enhance shareability and transparency with the public.

In the EU, iXBRL, an XBRL version with rendering capabilities, is used as a single electronic format for financial reporting by all issuers whose securities are admitted to trading on EU-regulated markets. Sustainability data reporting is also standardised using the same format according to the European Sustainability Reporting Standards XBRL Taxonomy.[168] Over 70 countries have adopted XBRL for financial transparency and regulatory purposes.[169]

The XBRL taxonomies enable the reuse of well-defined business concepts across different reporting domains. For example, XBRL taxonomies developed by the Danish Business Authority are used for mandatory reporting by companies but also for data sharing with cooperating agencies, as well as by other authorities in Denmark in different reporting scenarios, e.g., for tax and statistics purposes. Another example is the taxonomy developed by the South African Register (CIPC) as part of its Financial Reporting Digitisation Programme.[170]

When it comes to standardising BO data in registers, Open Ownership, a UK non-governmental organisation, has developed the Beneficial Ownership Data Standard as an open standard offering guidance for collecting,

[165] The FATF Recommendations, 2012, Updated 2025, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (last accessed 26 February 2025).

[166] 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://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/GRAInformationSharingEnterpriseService-LevelAgreement-Final11April2011.pdf (last accessed 7 February 2025). See also NIST SP 800-47 Managing the Security of Information Exchanges (2021), https://doi.org/10.6028/NIST.SP.800-47r1 (last accessed 26 February 2025).

[167] XBRL, managed by a global non-profit consortium (XBRL International), is a standardised data exchange format which enables the financial and non-financial reporting requirements to be made available for the companies in unambiguous, digital manner. The reporting requirements are represented in structured dictionaries (called 'XBRL taxonomies') which reduce confusion in interpretation of requirements, and ensure that that the data reported by companies is comparable and fit for automated quality verification and analysis. Such taxonomies are published among others by the IFRS Foundation.

[168] European Securities and Markets Authority (ESMA), Sustainability Reporting, https://www.esma.europa.eu/esmas-activities/sustainable-finance/sustainability-reporting (last accessed 26 February 2025).

[169] More information is available here: https://www.xbrl.org/the-standard/why/xbrl-project-directory/ (last accessed 2 April 2025)

[170] The paper includes contributions and sections consulted with BR-AG P.S.A. (formerly Business Reporting-Advisory Group).

sharing, and utilising high-quality BO data. It enables the capture of detailed information about the connections linking individuals with corporate entities and other entity types.

Adopting ISO standards 8000-115 and 20275 for generating unique company identifiers can improve the consistency of company identification across jurisdictions and platforms. An important milestone in this endeavour is the Entity Legal Forms (ELF) Code List released by the Global Legal Entity Identifier Foundation. This list categorises the legal structures of companies worldwide, proving particularly beneficial for organised databases containing portfolios of international companies. The ELF list contains legal forms in their native language, such as Gesellschaft mit beschränkter Haftung (GmbH), or Société Anonyme (SA), and assigns a unique code to each entity legal form. The code list simplifies the classification of legal forms, making it easier to manage and access information in the database.

Technical[171]

Some of the relevant ISO standards that can enhance Interoperability include ISO 2382, which defines Interoperability;[172] ISO 19941, which provides standards for transferring data between non-cloud and one or more cloud services and between cloud services;[173] ISO 8000-115 on unique identifiers; and the ISO 20275 ELF Code List. Moreover, standards such as the Beneficial Ownership Data Standard facilitate the collection, sharing, and utilisation of high-quality BO data, enhancing transparency and reliability in registry operations.

By implementing APIs that adhere to industry-standard protocols (for instance, REST), EBRs can support compatibility and Interoperability between their systems and external systems or services. APIs commonly support various data formats, such as JSON (JavaScript Object Notation) or XML (eXtensible Markup Language), which further enhance Interoperability by accommodating flexible data exchange requirements. Public APIs may serve external users (e.g., notaries or banks), while private APIs enable back-end integrations with government systems. The Australian PPSR and the Texas UCC filing office both provide SOAP APIs that businesses can integrate into their software to access the system more efficiently.[174] IACA (International Association of Commercial Administrators) supports a standard XML format recommended for transmitting electronic registrations to UCC filing offices.[175] UCC filing offices that support this filing method enable bulk processing to register multiple notices contained within each XML file.[176]

Legal

The UNCITRAL Legislative Guide emphasises that, when an electronic registry is adopted, interoperability should be considered. The registry should be designed to allow, even at a later stage, integration with other

[171] Sections of this chapter discussing the API were prepared in consultation with NRD Companies.

[172] See ISO/IEC 2382 Information technology — Vocabulary, 2015, https://www.iso.org/standard/63598.html (last accessed 26 February 2025), 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.'

[173] See ISO/IEC 19941, Information technology — Cloud computing — Interoperability and portability, 2017 (reviewed in 2023), https://www.iso.org/standard/66639.html (last accessed 7 February 2025).

[174] See Austl. Gov't, B2G Hub, https://www.ppsr.gov.au/b2g-hub (last accessed 7 February 2025); see also Tex. Sec'y of State, UCC Web Service Help, https://direct.sos.state.tx.us/help/help-ucc.asp?pg=ucc_ws (last accessed 7 February 2025).

[175] 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 7 February 2025).

[176] See, for instance, Texas and Louisiana. See https://direct.sos.state.tx.us/help/help-ucc.asp?pg=ucc_ws (last accessed 7 February 2025); and see Louisiana UCC Bulk Filings API Integration Guide 1.6 (2022), https://static.sos.la.gov/UCC/UCC_Bulk_API_Guide.pdf (last accessed 27 February 2025).

automated systems, such as other governmental authorities operating in the jurisdiction, and online or mobile payment portals.[177]

The UNCITRAL Legislative Guide highlights the importance of a unique identifier and its role in the data exchange process to ensure reliable and accurate data sharing among different information systems. Recommendation 17 of the UNCITRAL Legislative Guide emphasises the significance of interoperability between the technological infrastructure of the business registry and other public authorities (tax authorities, social security authorities and other public entities) that share information linked to the identifier.

Directive 2017/1132[178] emphasises interoperability among business registers within the EU. Article 22 mandates Member States to ensure the seamless integration of their registers within the interconnected system via the designated platform. Regulation (EU) 2024/903 further promotes the interoperability of digital public services encompassing essential services that are relevant for major life events for natural persons and for legal persons in their professional lifecycle.[179] In light of these instruments, the EBR design should take into account the likelihood that the requirement for cross-border and cross-sector Interoperability will increase over time due to policy direction. Therefore, EBRs should be designed with the ‘interoperability by default’ principle and be able to facilitate Interoperability at legal, organisational, semantic, and technical levels to support cross-border and cross-sector data exchange.

15. Legal Authority and Compliance

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

The legal framework provides the authority under which the business registry is established and sets the boundaries for its design and operation, which outline its scope, responsibilities, limitations and liabilities, as well as mechanisms for oversight and accountability. This framework consists not only of primary legislation such as commercial codes and company laws, but also of implementing regulations, case law, procedural instruments, and, where applicable, service-level agreements (for registries operated by private companies) and terms and conditions of use.[180] Less formal instruments, such as registrars’ practice statements and rulebooks,[181] also play an important role in operationalising the legal framework within the defined administrative discretion.

A comprehensive evaluation of the applicable legal framework is necessary at an early stage of the EBR design, ideally before selecting a registry system vendor. While the registrar may have the authority to revise operational procedures and technical features in the EBR to meet future objectives, the law typically defines the registry’s core functions to prevent regulatory inconsistencies.

[177] UNCITRAL Legislative Guide on Key Principles of a Business Registry (2019), para. 70.

[178] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification), http://data.europa.eu/eli/dir/2017/1132/2022-08-12 (last accessed 26 February 2025).

[179] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), http://data.europa.eu/eli/reg/2024/903/oj (last accessed 5 May 2025).

The EBR must comply with its full legal and regulatory mandate, including obligations related to data retention, Confidentiality, Integrity, and Availability. This extends to compliance with provisions of other laws, such as those that regulate data protection (see CPF 6 on Confidentiality and Privacy), security, archiving standards (see CPF 18 on Retention and Disposition), insolvency, and labour law.

National legal systems reflect different policy choices regarding the degree of ensuring the Accuracy and Reliability of registered data by different models of the EBRs. In the German model, business registries are incorporated in the judicial process overseen by commercial courts, providing users with extracts of data presumed to accurately reflect reality. In common law systems, the registrar's role is primarily administrative, and the accuracy of the registered information is contingent upon the good faith of those filing.[182] The Spanish model, also adopted by many South American countries, employs agents to conduct due diligence prior to registration, thereby enhancing the reliability of registered data, similar to the Italian notarial system. In certain Middle Eastern countries, where central tax authorities may be absent, business registries also serve as revenue collection and licensing entities.[183]

Although different jurisdictions have distinct legal regulations of business registries, they do not operate in isolation from the international legal environment. EBRs are increasingly required to adhere to continually evolving international frameworks that set standards for data protection, information security, and financial compliance. Effective cross-border coordination is beneficial for the seamless functioning of EBRs in supporting international transactions. When legal and regulatory frameworks allow for this, EBRs should be able to facilitate efficient access to accurate and up-to-date business information across jurisdictions (see more in CPF 14 on Interoperability).

Legal

The laws and regulations that govern registry design and operation also shape the implementation of other CPFs. The extent to which information must be validated, retained, or disclosed depends on the applicable laws and the institutional authority of the registrar (see more in CPF 16 on the Legal Authority of the Registrar). A clear legal mandate, combined with appropriate oversight and compliance mechanisms, is essential for ensuring trustworthiness of EBRs.

16. 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 correcting detected errors

The registrar is a natural or legal person appointed pursuant to domestic law to supervise and administer the operation of the business registry. The relevant laws typically specify the process for appointing and removing the registrar, outline their responsibilities, and identify the authority responsible for monitoring the registrar’s performance in carrying out these duties.

[182] Recently, the UK has been shifting its approach and is investing heavily in updating business processes to ensure data accuracy through verification. See more at: https://www.gov.uk/government/publications/corporate-transparency-and-register-reform/corporate-transparency-and-register-reform-accessible-webpage.

[183] UNIDROIT Foundation, BPER 7th Workshop, Summary Report for the Seventh Meeting of the Best Practices in the Field of Electronic Registry Design and Operation Project, para. 107 (2024), https://ctcap.org/wp-content/uploads/2024/05/BPER-Report-of-the-7th-Workshop.pdf (last accessed 26 February 2025).

This CPF relates to the authority of the registrar under the applicable legal framework to take certain actions that may affect risks and liability. It does not refer broadly to any authority, including all discretionary actions to enhance the registry's user-friendliness. The scope of the registrar's legal authority and its proper application is an important confidence factor for users. As with the broader CPF on Legal Authority and Compliance, the applicable legal framework should define the registrar's duties, powers, and limits. The powers of the registrar that could affect customers should always be clearly stated and logged for evidence purposes, and customers should be notified when these powers have been exercised.

Generally, registrants submit applications and documentation for business registration, amendments, or deregistration. However, there are instances when the registrar should intervene, e.g., to reject a submitted application for registration, correct an error, or register data amendments, in accordance with the relevant legislation.

In some jurisdictions, the registrar is authorised to reject a business registration only if the application does not meet the requirements prescribed by the applicable law.[184] To ensure transparency and prevent any misuse of this authority, the registrar should provide a written notice detailing the reasons for rejection of the registration application. Further, the registrant should also be granted an opportunity to challenge this decision through an appeal process and, if appropriate, resubmit the application.

Regarding corrective actions, this CPF applies only to situations where the error is not attributable to the user. Errors may occur either in the registry system itself or in the publicly disclosed data. Errors in the registry system that do not affect existing registrations should fall under the registrar's unrestricted authority and ability to correct such errors. Errors in data that have been made publicly available, however, are more difficult to address since they may have already affected those who relied on the inaccurate information. In such cases, any corrective action would need to take into account the legal implications and interests of affected parties (see more in CPFs 9 and 11 on Correctability and Error Detection, respectively).

Beyond error correction, this CPF also covers the authority of the registrar to deregister businesses under specific legal conditions. This authority may be exercised if a court decision is obtained for the compulsory liquidation of the business, or if a decision is made to deregister the company from the registry due to non-compliance with registration requirements. Such non-compliance could include, for example, failure to fulfil legal obligations to register or update BO information, annual financial statements, or other mandatory data stipulated by legislation. The legal consequences of deregistration, such as termination of legal personality, or restrictions on business activity, are governed by the applicable legal framework.

Legal

Recommendation 27 of the UNCITRAL Legislative Guide outlines provisions regarding the registrar's powers. Firstly, the law should stipulate that the registrar must reject an application for the registration of a business only if the application fails to meet the specified requirements. Secondly, the registrar is mandated to furnish the registrant with written reasons for any such rejection. Additionally, the law should grant the registrar the authority to rectify its own errors, as well as any incidental errors found in the information submitted for business registration, under clearly defined conditions.

[184] UNCITRAL Legislative Guide, para. 149.

In the EU, registries have the authority to collect basic information on businesses in line with the requirements of the Directive 2017/1132.[185] However, this authority does not extend to verification of the data, such as the financial statements of the company. Unlike in the EU, some registries in Asia have the responsibility to go further than merely accepting the filing. Compliance with the filing requirements is enforced by the establishment of penalties for the failure to file data, as well as the filing of false, incomplete or inaccurate data.

17. Reliability

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

Reliability reflects a system's ability to maintain its functionality and expected performance consistently over time. Given the importance of EBRs for digital public infrastructure and their role in supporting commercial activities and regulatory oversight, user expectations regarding the business registry's Reliability are particularly high. Not only is the reliability of the EBR itself important, but so is the reliability of automated processes. Tracking reliability through incident management is crucial for continual improvement in this area.

Reliability is typically measured through indicators such as mean time between failures (MTBF), calculated by dividing the total operational time by the number of failures, or as a failure rate, where the number of failures is divided by the total operational time. A higher MTBF indicates less frequent failures and, consequently, greater Reliability.[186]

Although closely related, Reliability and Availability measure different performance characteristics. Reliability refers to a system's ability to function correctly and minimise system failures and downtime, while Availability concerns the system's ability to remain operational and accessible even if it may not be functioning correctly. For instance, one failure per annum may suggest high Reliability, but if that single failure resulted in a week of downtime, its impact would be captured as poor Availability. Similarly, frequent minor failures that require users to reconnect to the system but last only a few seconds would reflect poorly on Reliability but would not greatly impact Availability.

EBR systems should be designed with Reliability as a core requirement. This entails designing a system capable of detecting and correcting anomalies and errors, isolating faults and reporting them to the higher-level recovery mechanisms, and potentially halting the affected operations and transparently reporting the corruption. These functions are critical not only to minimise disruption but also to safeguard public confidence in the registry.

System reliability can be improved through various measures, including routine maintenance scheduled to keep the system up-to-date and resilient to evolving threats or operational demands, and architectural redundancy to prevent single points of failure from halting processes. Comprehensive quality control and testing after each update or system change help identify and mitigate potential vulnerabilities. Data collection and analysis allow for identifying common failure patterns and refining the system (see also CPF

[185] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017L1132 (last accessed 25 February 2025).

[186] See Byron Radle & Tom Bradicich, supra note 89.

7 on Continual Improvement). Effective incident communication further supports responses and decreases recovery time.

While technological measures in EBR design are fundamental, the human factor remains equally relevant to ensure Reliability. Skilled, well-trained personnel are indispensable for monitoring and maintaining reliable systems. Organised maintenance operations, backed by institutional leadership and a culture of accountability, ensure that EBRs are not only technically sound but also operationally sustainable.

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'.[187] ISO 25010 addresses the quality of systems and software, including Reliability, which it considers more broadly as encompassing sub-characteristics of maturity (minimising failure frequency), availability, fault tolerance, and recoverability.[188] The standard defines maturity as the degree to which a system meets the need for Reliability under normal operation.[189] Fault tolerance is the degree to which a system operates as intended in spite of infrastructure faults (i.e., without adversely affecting Availability).[190] 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).[191] Also, NIST Special Publication 800-160, Volume 2[192] refers to Reliability as to an aspect of trustworthiness and within a paradigm of reliability, maintainability, and availability (RMA), essential for cyber resiliency. Notably, Reliability focuses on the degradation and failure of systems and their components, rather than on potential threats and harms.

18. Retention and Disposition

Definitions:

Retention – The process of preserving data in a system for a specified period of time

Disposition – The process of archiving, destroying or transferring data at the end of the retention period

In EBRs, the retention and disposition of records is critical to ensuring legal compliance, operational efficiency, data integrity and to minimise risk. Retention supports historical accountability and transparency, while disposition addresses data lifecycle management and regulatory obligations for data minimisation and privacy.

[187] ISO/IEC 27040: Information technology — Security techniques — Storage security, §3.36, 2024, https://www.iso.org/standard/80194.html (last accessed 26 February 2025). See also ISO/IEC 2382 Information technology — Vocabulary, 2015 (last reviewed in 2025), https://www.iso.org/standard/63598.html (last accessed 26 February 2025), defining reliability as the 'ability of a functional unit to perform a required function under given conditions for a given time interval.'

[188] ISO/IEC 25010 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, 4.2.5, https://www.iso.org/standard/78175.html (last accessed 26 February 2025); and see ISO/IEC 25010, https://www.iso.org/standard/78175.html (last accessed 26 February 2025).

[189] ISO/IEC 25010 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model, at 4.2.5.1., https://www.iso.org/standard/78175.html (last accessed 7 February 2025).

[190] Id. at 4.2.5.3.

[191] Id. at 4.2.5.4.

[192] NIST Special Publication 800-160, Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, 2021, https://doi.org/10.6028/NIST.SP.800-160v2r1.

Retention of registration data in EBRs is generally easier and more cost-effective than maintaining paper records,[193] as it eliminates the need for physical storage space. Even registries still reliant on paper archives are addressing this issue by digitising documents and transitioning to electronic archives, subsequently destroying the paper versions after the expiry of a minimum legal period for their preservation.

Providing prospective users with long-term access to information maintained in the registry is of key importance, not only for historical reasons but also to provide evidence of past legal, financial, and management issues relating to a business that might still be relevant. Although it may be technically possible to store records indefinitely, legal requirements, such as the general law on retention of records, may limit the length of time that certain records may be maintained within the registry and the conditions under which they may be transferred. However, in the absence of such laws, and as a general rule, the information in the business registry should be kept indefinitely.[194]

Disposition covers processes and policies related to archiving, destroying, or transferring records once the retention period expires or when continued storage is no longer justified. Disposition does not create new records other than in an activity log documenting an action. Disposition policies and processes 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 and should thus be removed. 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.

In addition to being archived or deleted, 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 a different location. The ability to transfer data from the EBR to another platform may facilitate portability (see CPF 8 on Continuity).

Disposition does not overwrite or erase corrected records. If the record is corrected, such as due to an error identified by the registry, an original record of the registration prior to its correction may be important to determine liability when a searcher relied on it before the correction was made.[195]

Ensuring that the format and storage medium for EBR records remain current is essential. As technology advances, the methods used for storing data should be regularly reviewed and updated to ensure continuous access. For instance, transitioning from obsolete storage devices like floppy disks, microfilm, or hard disk drives with limited lifespan, to modern solutions such as cloud-based storage, guarantees long-term accessibility and prevents data loss due to technological obsolescence. However, the format of the records is also important, as some older file formats may no longer be readable with the latest software. Therefore, the EBR should periodically review the readability of stored records and reformat them into a currently readable format, if necessary. Such proactive management maintains the integrity and usability of records, supporting reliable long-term access and safeguarding against data loss and security risks.

Data retention and disposition practices in EBRs are also subject to privacy regulations. While such regulations typically do not apply to legal entities registered with a business registry, they do affect the

[193] UNCITRAL Legislative Guide, para. 230.

[194] UNCITRAL Legislative Guide, para. 227.

[195] UNCITRAL Legislative Guide, para. 231.

handling of PII, including personal data of managers and directors. This may require, for example, limiting the retention of PII not necessary for ongoing legal obligations, or providing mechanisms for exercising the right to be forgotten.

However, under Article 16(5)(d) of Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017, certain information about the managers and directors of an enterprise should be made publicly accessible.[196] This creates a need to balance transparency obligations with privacy compliance (see CPF 6 on Confidentiality and Privacy, and Annex on the scope of publicly available information).

Technical

Several international standards provide guidance for the secure and compliant retention and disposition of electronic records. ISO 15489-1 Information and documentation — Records management, § 3.8, defines disposition as the 'range of processes associated with implementing records retention, destruction or transfer decisions'.[197] ISO/IEC 27001 specifies requirements for assessing security risks affecting information storage and for establishing, implementing, maintaining and continually improving an information security management system, which includes controls related to record retention and destruction.[198] Similarly, ISO/IEC 27040 sets out standards for data storage security, focused on protecting data against unauthorised disclosure, modification, or destruction while assuring Availability to authorised users.[199] The standards apply to controls that prevent, detect, or deter harmful events or unauthorised acts, as well as to those that correct or recover affected data.[200] Also relevant to EBRs, ISO 17068 specifies requirements for a trusted third party repository (TTPR) to safeguard the Integrity and authenticity of digital records and serve as a source of reliable evidence. It also supports the legal requirement to preserve audit trails and corrected records.[201]

Legal

Paragraph 227 of the UNCITRAL Legislative Guide establishes the general principle that information within the business registry should be retained indefinitely. The state determines the appropriate duration for retaining such information, with the option to apply its standard regulations governing the preservation of public documents.

Furthermore, Recommendation 52 of the UNCITRAL Legislative Guide stipulates that the law should mandate the preservation of documents and information submitted by registrants and registered businesses, including data concerning deregistered businesses, within the registry. This preservation ensures that the registry and other relevant parties can retrieve the information as needed.

[196] Article 16(5)(d) of the Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Codification), https://eur-lex.europa.eu/eli/dir/2017/1132/oj/eng (last accessed 26 February 2025).

[197] ISO 15489-1, Information and documentation — Records management, 2016, https://www.iso.org/standard/62542.html (last accessed 7 February 2025).

[198] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements, 1, https://www.iso.org/standard/27001 (last accessed 7 February 2025).

[199] ISO/IEC 27040 Information technology — Security techniques — Storage security, 3.49, https://www.iso.org/standard/80194.html (last accessed 7 February 2025).

[200] Id.

[201] ISO 17068 - 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 7 February 2025).

In relation to the general retention of records, the law may require the complete deletion of certain records from the database, including any backup or archived copies, to ensure compliance with legal and regulatory requirements. This is particularly relevant in cases involving PII collected during the account creation process for a business registry. For instance, personal details such as names, contact information, or identification numbers provided by individuals to register or access the system may fall under such regulations.

19. Risk Management

Definition: The process of identifying, assessing, and managing threats and vulnerabilities to registry design and operations

The EBR should undertake Risk Management as a systematic process that identifies and assesses threats and vulnerabilities, i.e., conditions or events with negative consequences on its operations. It involves making decisions to avoid, mitigate, transfer or accept the corresponding risks and monitoring the implementation and effectiveness of such decisions over time. Risk Management is a perpetual and adaptive process that enables registries to preserve legal certainty, data integrity, operational continuity and public trust in the face of evolving threats.

Given its public function and role in safeguarding legally significant business data, an EBR must approach Risk Management as a core governance priority. The failure of an EBR, notwithstanding the cause, can generate wide-ranging repercussions on the national economy and international commerce, particularly when registries are interconnected or facilitate cross-border services.

The EBR’s Risk Management framework must be tailored to its legal mandate, institutional model, technological configuration, and level of integration with other systems. For instance, a registry offering fully digital real-time registration services will have different risk dynamics than one operating a hybrid model with manual validation levels. Accordingly, the EBR’s Risk Management should be calibrated to its specific threat landscape, operational dependencies, and resource capacity.

The EBR should consider its risk appetite for each category of risk. This is the level and type of risk it is willing to accept in pursuit of its strategic objectives. Effective Risk Management requires a distinction between risks and vulnerabilities. Risks represent the potential events or conditions with adverse effects, while vulnerabilities refer to existing internal weaknesses in the registry’s systems that can be exploited to realise those risks. For example, while a cyberattack is a risk, the lack of robust firewalls or insufficient encryption measures would be a vulnerability. Sound risk assessment requires identifying vulnerabilities that increase the registry’s exposure to risks, followed by prioritising and implementing mitigation strategies.

Risks faced by EBRs span multiple domains, including technological, operational, reputational, financial, geopolitical, and supply-chain dimensions. Technological risks encompass threats to the confidentiality, availability, and integrity of data and systems. Cybersecurity threats (for instance, ransomware, DDoS attacks) can affect system and data integrity. System design flaws, lack of adequate IT infrastructure or outdated legacy systems may result in disruptions in service delivery. Poor interoperability with external systems may cause inefficiencies and data silos, while dependency on proprietary software may limit flexibility and increase costs for EBR operations. Inadequate testing and quality assurance during development can introduce defects that compromise usability, while poorly managed data structures and governance frameworks can result in inefficiencies and inaccuracies. Moreover, the lack of robust back-up, disaster recovery and business continuity strategies increases the risk of extended system failures, loss of data, or operational paralysis due to unexpected circumstances.

Operational risks relate to deficiencies in internal processes, governance, and staffing. Inadequate human resources, particularly in IT and legal functions, can increase exposure to errors or fraud. Insufficient staff training and internal controls undermine service quality and reliability. Additionally, non-compliance with changing legal and regulatory requirements can expose the business registry to legal penalties or reputational damage, diminishing its effectiveness and trustworthiness.

Reputational risks refer to potential adverse events, such as data breaches, fraud, or publicised operational failures, that harm the business registry's reputation and erode public trust and relationships with stakeholders. Weak implementation of global AML frameworks, leading to vulnerabilities in combatting illicit financial flows, and delayed or ineffective crisis communication can exacerbate reputational risks.

Financial risks may manifest themselves when adequate funding is not ensured for the maintenance and support of the registry's operations. If the business registry is publicly funded, budget allocations may be inadequate or delayed; if the business registry is financed through customer fees, the government may set insufficient pricing for the cost recovery of services. Registries operating across currency zones may be exposed to exchange rate fluctuations in procurement. Sustainable financial planning is therefore essential for the EBR's Continuity and Reliability.

Geopolitical risks may affect EBRs indirectly, particularly through increased exposure to politically motivated cyberattacks,[202] regulatory fragmentation, or restrictions on cross-border data transfers.[203] As digital public infrastructure becomes more strategically significant, registries may find themselves targeted in the context of broader geopolitical tensions. Given their increasing interconnection with international databases, EBRs should proactively monitor global trends and assess their potential impact on service continuity, data exchange frameworks, and technical compliance.

Supply chain risks affect the availability and security of goods and services for EBRs. EBRs frequently rely on external vendors, including cloud service providers, payment processors, or identity verification platforms. Disruptions due to vendor insolvency, cyberattacks on supply chain components, and capacity constraints may have a cascading impact on services required by EBRs. To address such supply fluctuations, robust vendor management, fallback arrangements, and contract governance are essential.[204]

To address these risks, the EBR should establish a Risk Management framework for (i) risk identification, recognising internal and external factors that may harm the registry operations; (ii) assessment, evaluating the likelihood and potential impact of each risk; (iii) treatment, implementing controls to mitigate, transfer, accept, or avoid risk; (iv) monitoring and review, regularly reassessing both the risks and the effectiveness

[202] Geopolitical risk dashboard, https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard (last visited 15 May 2025).

[203] How to factor geopolitics into technology strategy, (EY Parthenon, Sep. 10, 2021), https://www.ey.com/en_gl/insights/geostrategy/how-to-factor-geopolitical-risk-into-technology-strategy (last visited 15 May 2025).

[204] Ivan Stechynskyi, Major Supply Chain Cybersecurity Concerns and 7 Best Practices to Address Them (Sytec-a, Jan. 15, 2025), https://www.syteca.com/en/blog/supply-chain-security (last visited 15 May 2025).

of mitigation strategies; and (vi) communication and response, ensuring transparent and timely communication with users and stakeholders during risk events. Given that data is the key asset of the registry, special priority and resources should be allocated to risks and vulnerabilities that might compromise the housed data. This includes using secure backup, encryption protocols, and comprehensive disaster recovery plans. Clear lines of accountability, periodic audits, strong system change control procedures and integration with business continuity plans are also vital. A comprehensive Risk Management framework ensures the registry's resilience against adverse events, maintains stakeholder trust, and upholds its reputation as a reliable institution in the business ecosystem.

Chapter III on Evaluation of Risks to Electronic Business Registries will discuss a risk management framework suitable for EBRs and the impact of CPF non-performance on the registry.

Technical

The ISO 27000 series, notably ISO/IEC 27005,[205] is a valuable resource for information security risk management, offering insights into risk assessment and treatment processes. ISO/IEC 27001 provides a benchmark for implementing and maintaining an information security management system, enabling organisations to systematically manage risks and protect sensitive data and operational integrity. ISO 22301, the standard for business continuity management systems, offers a structured approach to resilience, helping organisations ensure the continuity of critical services during disruptions. Furthermore, ISO 31000[206] provides overarching guidelines for risk management across various sectors and organisational contexts.

In addition to these frameworks, SOC 2[207] (System and Organization Controls 2), focused on North American practices, provides critical guidance for organisations managing customer data, particularly in cloud-based environments. SOC 2 focuses on operational and security controls that align with the trust service criteria, which include security, availability, processing integrity, confidentiality, and privacy.

Although designed for US federal systems, NIST Special Publication 800-37[208] provides instrumental insight in guiding risk management processes, and EBRs can adapt and implement those principles to fortify technical risk management frameworks in other contexts.

Legal

The UNCITRAL Legislative Guide outlines the measures to be taken to protect the business registry record.[209] Recommendation 54 emphasises the necessity of protecting business registry records against loss or damage. Furthermore, the registry should establish and maintain backup mechanisms capable of facilitating the reconstruction of registry records in the event of any unforeseen circumstances.

Additionally, Recommendation 55 underscores the importance of safeguarding against accidental destruction of registry records. To this end, the law should stipulate the establishment of appropriate

[205] ISO/IEC 27005 "Information security, cybersecurity and privacy protection" Guidance on managing information security risks, 2022, https://www.iso.org/standard/80585.html (last accessed 7 February 2025).

[206] ISO 31000 "Risk management", 2018, last updated 2023, https://www.iso.org/standard/65694.html (last accessed 7 February 2025).

[207] AICPA "SOC for Service Organizations", available at https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report (last accessed 7 February 2025).

[208] NIST Special Publication 800-37 "Risk Management Framework for Information Systems and Organizations", 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (last accessed 7 February 2025).

[209] UNCITRAL Legislative Guide, Recommendations 54 and 55.

procedures to mitigate risks stemming from force majeure events, natural hazards, or other accidents. These procedures should encompass measures designed to mitigate potential disruptions to the processing, collection, transfer, and protection of data within the registry.

At the regional level, the NIS2 Directive provides a unified framework to enhance cybersecurity and operational resilience in critical sectors, including public services. [210] Its emphasis on risk-based security measures, incident reporting, and cross-sectoral cooperation complements the principles outlined by UNCITRAL and aligns with international standards such as ISO/IEC 27001 and ISO 22301. By integrating these requirements, business registries in the EU can bolster data protection and enhance the reliability and security of their data, recognising the legal, operational, and reputational considerations.

20. System Validation

Definition: The process of confirming, using objective evidence and testing, that the requirements for the intended use have been fulfilled by the system

System Validation is a systematic process of ensuring that EBRs operate in a way that is aligned with their intended purpose, meet defined functional requirements, and address the specific needs of their operational environments. Its objective is to ascertain that the registry system is designed and implemented to perform effectively within its context, considering the inherent risks and operational demands unique to business registries.

The concept of System Validation goes beyond the technical domain, focusing on the suitability of a system for its intended purpose. This involves a holistic assessment of operational functionality, reliability, and usability, as well as integration capacity under realistic working conditions. For business registries, this may include high transaction volumes, ensuring regulatory compliance, managing sensitive data, and enabling seamless interoperability with external systems. Validation processes, therefore, incorporate these variables to evaluate the system's capacity to support legal certainty, transparency and operational efficiency in the registry ecosystem.

The System Validation process typically encompasses a range of testing methodologies, including functional, performance, stress, security, and integration testing. These exercises are often conducted using simulated or anonymised data to replicate real-world scenarios without compromising sensitive information. Validation also extends to interface usability and accessibility testing, ensuring the system is suitable for diverse stakeholders.

Rigorous System Validation should address the risks and challenges intrinsic to the registry’s design and operational context. This includes accounting for potential vulnerabilities in data integrity and confidentiality, ensuring the system’s resilience under peak operational loads or system failure events, and addressing the complexities of inter-system dependencies. By grounding the validation process in the registry’s specific operational realities, the outcome is not merely a technically compliant system but one

[210] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 (NIS2 Directive), https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (last accessed 26 February 2025).

capable of fulfilling its role reliably, securely, and efficiently within a variable and often demanding environment.

Importantly, System Validation is not a one-time endeavour conducted at deployment, but a continuous process embedded throughout the EBR system's lifecycle. It also requires that, whenever the system changes, test cases be reviewed and adjusted to match the latest system behaviour and requirements, removing tests that are no longer useful and developing new ones for added or modified functionality. For instance, if the registry adds a new user role, existing tests for Access Control may no longer suffice. If test cases are not kept up to date, there is a risk that the system validation process, even if conducted continuously throughout the system's lifecycle, may overlook some malfunctions or security vulnerabilities. Such a comprehensive approach ensures that validation is responsive to system updates and modifications and maintains confidence in the registry's reliability and compliance.

Continuous monitoring, coupled with periodic reassessment and regression testing, allows for proactively identifying potential issues, ensuring the system remains aligned with its performance expectations and legal obligations. Comprehensive documentation of the validation process and its outcomes contributes to transparency and accountability, providing a valuable audit trail for oversight bodies, internal reviews, and future system enhancements.

Technical

ISO/IEC 25010[211] is a comprehensive quality model designed to evaluate systems and software against key quality characteristics and sub-characteristics. It addresses how well a system meets the needs of stakeholders by focusing on aspects such as functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, portability, and safety. Each characteristic is broken down further to assess specific attributes, such as functionality completeness, resource utilisation, fault tolerance, or adaptability, offering a structured foundation for evaluating whether a system fulfils its intended purpose.

Another internationally recognised standard, ISO/IEC/IEEE 29119, establishes a comprehensive framework for software testing.[212] This standard provides a systematic approach to managing, designing, executing, and documenting testing processes, which are essential attributes for the validation of EBRs. Compliance with ISO/IEC/IEEE 29119 enables business registry systems to adopt rigorous testing practices, ensuring high-quality software solutions that meet stakeholder expectations and enhance trust in the registry's outputs.

21. Timeliness

Definition: The process of considering time in the context of system design and operations

Timeliness is an important factor for EBRs, essential for maintaining transparency and facilitating business transactions. It has three distinct dimensions: *processing time*, which refers to the time taken to process an application or submission; *absolute time*, which refers to the precise time a registration or other event

[211] ISO/IEC 25010 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, https://www.iso.org/standard/78175.html (last accessed 26 February 2025).

[212] ISO/IEC/IEEE 2911 Software and systems engineering — Software testing, 2022, https://www.iso.org/standard/81291.html (last accessed 7 February 2025).

occurs, since in some instances, there may be a tax or statutory reason that a business has to be registered on one day rather than the next; and *relative time*, which determines the order of competing registrations or transactions where priority has legal effect, for instance, in registering intellectual property such as trademarks. These dimensions translate into three operational objectives: (i) responsiveness to customer needs, (ii) accurate time sources, and (iii) reliable order of registrations and other transactions. Each aspect must be considered in system design and operational management.

Firstly, Timeliness requires responsiveness to user needs through careful business process design and strong operations management. An efficient EBR ensures that registration, updates, corrections, publications and other transactions are processed swiftly, reducing delays and providing almost instant, accurate and up-to-date information to users. This aspect of Timeliness refers to the expectation of accessibility of information within a reasonable time,[213] which can be measured as latency, or the time delay, between when information is expected to be accessible and when it actually becomes accessible.[214] Ideally, information should become accessible in real time as registrations occur, or within a timeframe that preserves its legal relevance. When information in the registry does not reflect the current legal or factual status of a business due to delays in processing or publication, data quality and the Reliability of the system are compromised.

To achieve a high level of responsiveness, the registry should define targets for processing and publication times, monitor and publish performance metrics against the set targets, and seek periodic user feedback. Different business registries have also introduced user-facing tools to communicate the processing times. For instance, the Swedish business registry offers live updates about the expected processing time and specific dates by which a business can expect its requests to be performed, with updates about such dates and processing times being published three times per week.[215]

Automation increasingly enables real-time or near-real-time business registration, where transactions are processed by algorithms without human intervention. For instance, Greece has implemented real-time company registration, enabling fully automated application processing and the issuance of registration decisions immediately upon submission of required documentation (see Figure 7).[216]

[213] See David Loshin, Data Quality and Master Data Management, 5.3.5, (Elsevier, 2008), https://search.worldcat.org/en/title/424595637 (last accessed 7 February 2025).

[214] Id.; and see generally Laura Sebastian-Coleman, Measuring Data Quality for Ongoing Improvement, Ch. 5, (Elsevier, 2013) https://www.sciencedirect.com/book/9780123970336/measuring-data-quality-for-ongoing-improvement (last accessed 7 February 2025).

[215] Bolagsverket, Swedish Companies Registration Office, https://bolagsverket.se/en/omoss/varverksamhet/varservice/varahandlaggningstider.2081.html (last accessed 9 April 2025).

[216] World Bank Group (2022), Data-Driven Company Registry, Guidance note, https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf (last accessed 26 March 2025).

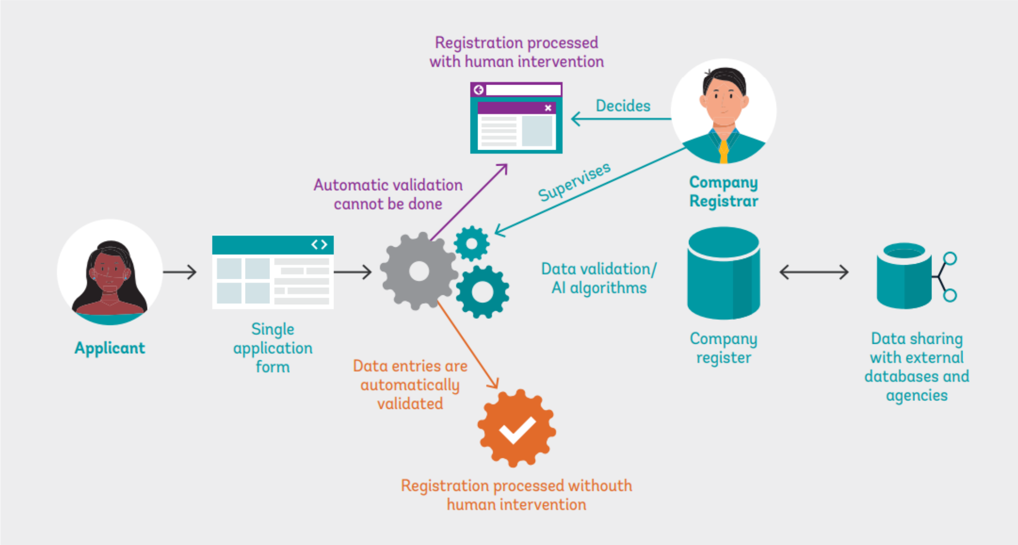


Figure 7. Illustration of real-time company registration.

Some decisions, particularly those involving complex legal or regulatory considerations, cannot yet be fully automated. Therefore, a balanced approach is needed, taking into account the speed and comprehensiveness of human oversight, often dictated by the risks involved.

Timeliness is also important when the registry rejects a registration submission or search request. Prompt feedback enables the registrant or searcher to take timely corrective action, prevents unnecessary delays in establishing legal rights, and supports predictable and efficient user interaction with the registry. Similarly, when EBRs are integrated with other systems, delays in those systems may affect the overall responsiveness of the registry. Thus, Timeliness should be considered as part of broader system design, risk planning, and service-level management.

Secondly, Timeliness requires accurate and reliable time sources. An EBR system should derive its time from secure, authoritative sources, such as Internet Network Time Protocol servers, satellite clocks, and atomic clocks, which are often maintained by national standard authorities.[217] With the proliferation of cloud computing, combined time sources can deliver accurate time readings and are simple to integrate into EBRs.[218] Each EBR system element should be synchronised to the same time source and use consistent settings, typically based on UTC. Accurate time sources matter where the absolute time of a transaction affects its legal validity, for example, where statutory deadlines apply. The level of precision required is a design decision that considers cost, practicality, and the size of the timestamp being stored. For instance, a Caesium Fountain Clock is accurate to one second per 300 million years. This level of precision may not be necessary for an EBR.

Thirdly, Timeliness encompasses ensuring that registrations and other transactions are recorded in the correct order. When competing interests are being registered, the order of registration can determine legal priority, for instance, when registering intellectual property or business names. Modern EBR systems often

[217] See more at: https://www.rte.ie/news/business/2023/0919/1406003-irelands-first-ever-national-timing-grid-launches/ (last accessed 1 July 2025)

[218] For instance, the AWS cloud service uses “a fleet of satellite-connected and atomic reference clocks in each AWS Region to deliver accurate and current time readings of the Coordinated Universal Time (UTC) global standard.” Precision clock and time synchronisation on your EC2 instance, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html (last accessed 1 July 2025).

process transactions in parallel on multiple application servers to spread the computing load and offer resilience should one server fail. Good design must resolve the situation where registration A arrives at the application server before registration B, but then arrives at the database server just after registration B. System design should therefore ensure that the timestamps are applied to each transaction when it is fully stored on the database and made searchable – not when it is first received by the application server (unless the law has an alternative provision, in which case other design considerations would be more appropriate).[219]

Another challenge with relative time is the situation where the time on a database server is changed, for instance, during daylight saving time changes. The time design of the EBR must ensure that the time on one server cannot be rolled back inadvertently by manual intervention. Good design of the time system should be sufficient, but it is a best practice that the EBR application detect time changes, particularly rollbacks, in case the underlying infrastructure design is flawed. The registry application should enforce sequential integrity and not allow a registration to be entered into the database with an earlier timestamp than that of the most recently stored record. This is a defence-in-depth approach and should be adopted for critical system components such as time.[220]

Technical

As such, no specific standard exists for Timeliness; however, ISO/IEC TS 25011 defines timeliness as the 'degree to which an IT service (3.3.2) delivers outcomes within time limits',[221] linking it in the IT service quality model as a part of IT service responsiveness.

Careful operational and technical design of the registry is essential to guarantee Timeliness, i.e., the responsiveness of the EBR, the accuracy of its timestamps and the order of transactions. The technical design will apply to both the software and hardware components of the registry's infrastructure, and the EBR's time system should be considered a discrete element requiring design, maintenance and monitoring.

Legal

Recommendation 26 of the UNCITRAL Legislative Guide addresses the time and effectiveness of registration, indicating that the law should require the business registry to record the date and time of receipt for registration applications, process them promptly and in the order received, ensuring minimal delay. Additionally, the law should clearly define the moment when business registration becomes effective and specify that the registration must be promptly entered into the business registry after approval, without unnecessary delay, ensuring efficient management of registration procedures.

In some jurisdictions, businesses may apply for the protection of certain rights prior to registration. For example, the provisional registration of the name of the business to be registered may protect that name from being used by any other entity until the registration of the business is effective. In such cases, the

[219] If the law bases the time of a registration on the time the application is received rather than when it has been processed and made searchable, the system design will have to include a queuing mechanism where a registration cannot go live and become searchable until all registrations with earlier time stamps are processed. This could cause delays. Other mechanisms are also possible, but the system design must directly address the issue.

[220] The designs discussed in this section are illustrative. Systems must be considered individually based on their legal and technical context.

[221] ISO/IEC TS 25011, Information technology — Systems and software Quality Requirements and Evaluation (SQuaRE) — Service quality models, 3.2.6.1, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:25011:ed-1:v2:en (last accessed 9 April 2025).

UNCITRAL Legislative Guide provides that the applicable law should be equally clear to establish the moment at which such pre-registration rights are effective and the period of their effectiveness.[222]

Further, in line with paragraph 144 of the UNCITRAL Legislative Guide, if the registry is designed to enable users to submit or amend registered information electronically without the intervention of registry staff and to use online payment methods for the registration, the registry software should ensure that the information becomes effective immediately or nearly immediately after it is transmitted.[223]

Beyond registration efficiency, Timeliness is also a critical factor for AML and CFT compliance. FATF Recommendations 24 and 25 indicate that countries should ensure that competent authorities have timely access to adequate, accurate and up-to-date basic and BO information. Business registries, as primary repositories of such data, are essential in meeting these requirements. Delays in registration or updates can compromise the availability of reliable information, impeding investigations and weakening compliance with international AML/CFT standards.[224]

22. Transparency

Definition: The process of disclosing, in an open and understandable manner, how a system or process operates, including how it produces and presents data

Transparency, in the context of EBRs, refers to providing appropriate information to the users of the EBR about the work of the system and the processes employed in executing tasks and producing an outcome. This includes making available, in an understandable manner, appropriate information about the registry's features, performance, limitations, components, policies, procedures, terminology, design choices, and assumptions. [225] It is important to note that Transparency does not presuppose disclosure of all information since such a measure may compromise the security, confidentiality or privacy of the EBR.[226]

The goal of Transparency is to facilitate informed decision-making, as information on how the registry operates enables users and other stakeholders to understand the registry and decide how much to rely on it. This involves understanding not only the data retrieved but also the underlying processes, technologies, and rules that shape that data. Transparency supports accountability by clarifying what the registry does, how it does it, and what can reasonably be expected from it.

In many jurisdictions, Transparency is mandated by law, requiring the publication of specified information about the registration process, access conditions, data categories, and service standards governing registry operations. Even when disclosure of certain information about EBR processes may not be required, it is a best practice to publish key information about the EBR's functioning, such as the roles and responsibilities of the registrar and registrants, expected processing time for applications, and availability of services, since they enable users to better understand and interact with the registry. Similarly, providing downloadable

[222] UNCITRAL Legislative Guide, para. 143.

[223] Id., para. 144.

[224] FATF Interpretive Note to Recommendation 24, paras. 9-11, and Recommendation 25, paras. 6-9.

[225] Such information typically includes data protection policies, verification processes, and system security measures, as well as information about the accuracy, reliability, and limitations of the data stored in the registry, and information about legal obligations and compliance requirements associated with using the registry.

[226] ISO/IEC 22989:2022 (en) (2022), Information technology — Artificial intelligence — Artificial intelligence concepts and terminology, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en:sec:5.15.8 (last accessed Mar. 12, 2025).

reports in multiple visualisation formats and metadata describing datasets (including their purpose, source, and update frequency) increases the interpretability and usability of registry data.

The transparency-by-design principle requires that registry systems and processes be developed with openness and accountability from the outset. This implies that systems are built to support scrutiny of data and procedures, to automate the disclosure of registry procedures in line with the predefined transparency policies, and to offer user documentation in clear, non-technical language.

Transparency is a particular concern for AI systems, and research in that area is useful in considering EBRs.[227] As EBRs increasingly adopt emerging technologies and AI solutions, maintaining Transparency becomes even more critical. Lessons from the AI domain emphasise the need to explain how automated processes function, their limitations, and how outcomes are generated. For instance, if AI tools are employed in data validation or fraud detection, registries should disclose, at least in very general terms, how these systems influence decision-making and the extent of human oversight applied.

Another example of where EBRs should consider Transparency is in search algorithms. When users search an EBR, they are presented with a response. By explaining the search algorithm used, the EBR allows the user to understand any limitations of the response and how they can tailor their query to best serve their needs. Given the centrality of search functionality, this simple measure is considered a best practice for enhancing Transparency in EBRs.

Transparency also enhances Interoperability with other systems by increasing the willingness of parties to allow their systems to be interoperable with the EBR. A system that clearly explains how data is processed and governed is more likely to be considered a reliable partner for integration and data-sharing with other systems, including national and international business registries, tax authorities and regulatory bodies. Similarly, disclosing security measures, data protection policies, and cybersecurity practices can help users engage with the registry with a clear understanding of the associated level of risk. By implementing cybersecurity transparency measures, such as security ratings, compliance certifications, or warnings about potential threats, the registry can strengthen trust while maintaining confidentiality safeguards.

Transparency is closely related to several other CPFs, including Accessibility, Accuracy, Continual Improvement, Correctability, Interoperability, Legal Authority and Compliance, Risk Management, Trustworthiness, and User-Centred Design. Whilst Transparency is most closely related to CPF 23 on Trustworthiness, the two differ in scope: Transparency focuses on the openness of process and functions of the registry, answering ‘how’ the registry operates, while Trustworthiness concerns the perception of Integrity and Reliability demonstrated by the outcomes and performance of registry functions, answering ‘what’ the registry delivers. Both are crucial in fostering trust in the EBR.

Adopting the best practices outlined in this Guide contributes to the overall Transparency of the registry. For example, Accuracy, Correctability and Error Detection measures ensure that the data disclosed is complete and reliable; User-Centred Design principles support the clear presentation of information; and Risk Management ensures that disclosures do not inadvertently create vulnerabilities.

[227] AI systems provide information to users, but, as they are not deterministic, it is important to allow a user to understand how the response was generated, for instance, by explaining the nature of the training data used in the case of large language models.

Technical

ISO/IEC TS 5723[228] defines *transparency of information* as the open, comprehensive, accessible, clear and understandable presentation of information, and *transparency of a system* as the property of a system or process to imply openness and accountability. As per this standard, accountability implies being answerable for actions, decisions and performance. It can therefore be demonstrated through regular audits and compliance checks on data management practices.

In the field of AI systems, which generally require greater scrutiny of transparency given the typically non-deterministic nature of this technology, ISO/IEC DIS 12792[229] and ISO/IEC 22989[230] emphasise transparency as the property of a system that stakeholders receive relevant information to help understand its features, limitations, data, system design and design choices.

Legal

The UNCITRAL Legislative Guide reflects the definition of Transparency as the ability of relevant stakeholders to access information and understand the functioning of the registry. Recommendation 7 stipulates that Transparency of registration procedures is ensured when the rules, procedures and service standards that are developed for the operation of the business registry are made public.[231] Further measures to enhance Transparency of the registry include the determination of the moment at which the registration of a business or any later change made to the registered information is effective,[232] as well as the determination of the time at which changes to the registered information are effective.[233]

While promoting Transparency, the Legislative Guide also acknowledges privacy and confidentiality concerns. States and, subsequently, registries should adopt a balanced approach that achieves both Transparency and the need to protect access to sensitive information maintained in the registry.[234] See more in the Annex on the scope of publicly available information, providing an overview of international instruments and jurisdictional examples.

23. Trustworthiness

Definition: The property of providing confidence to users and third parties that the registry performs its core functions in accordance with legal and technical expectations

Trustworthiness is of paramount importance for EBRs, facilitating a reliable business environment. An EBR's Trustworthiness is not a static feature but a multifaceted quality which results from the level of implementation of several independent CPFs described above. The key CPFs contributing to an EBR's Trustworthiness include: Availability, System Validation, System Reliability, Continuity, Access Control,

[228] ISO/IEC TS 5723:2022 (en) (2022), Trustworthiness — Vocabulary, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:5723:ed-1:v1:en:term:3.2.19 (last accessed Mar. 27, 2025).

[229] ISO/IEC DIS 12792 (en) (2024), Information technology — Artificial intelligence — Transparency taxonomy of AI systems, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:12792:dis:ed-1:v1:en (last accessed 7 March 2025).

[230] ISO/IEC 22989:2022 (en) (2022), Information technology — Artificial intelligence — Artificial intelligence concepts and terminology, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en:sec:5.15.8 (last accessed 12 March 2025).

[231] UNCITRAL Legislative Guide, paras. 44-45.

[232] Ibid., Recommendation 26.

[233] Ibid., Recommendation 31.

[234] Ibid., para 185.

Confidentiality and Privacy, Risk Management, Transparency, Interoperability, Legal Authority and Compliance, Continual Improvement, and User-Centred Design. Therefore, a comprehensive, holistic approach should be taken to build and maintain the registry's Trustworthiness. No single CPF can ensure Trustworthiness alone; rather, it is the combined and coherent performance across these domains that builds user confidence.

A registry's Trustworthiness is underpinned by its functionality and assurance.[235] Functionality embodies the features, functions, and services provided by the registry.[236] Assurance is the measure of confidence that registry functionality is implemented correctly, operating as intended, and producing the desired result.[237] System Validation plays a key role here, ensuring that functional requirements are not only met during development but continuously upheld during operation. System Reliability, Continuity, and Availability demonstrate the registry's capacity to process requests, operate without critical failure, and recover from adverse events in a timely manner.

Another key factor affecting the registry's Trustworthiness is its Integrity, largely derived from its ability to protect its systems and data from compromise with the help of its Access Control, Confidentiality and Privacy, and Risk Management processes. To instigate trust, the EBR should implement robust security frameworks that include encryption, authentication, auditing and other mechanisms to mitigate evolving risks, including unauthorised access, PII disclosure, data corruption, loss of processing capacities, and personnel expertise.

Additionally, Transparency supports trust in the registry by enabling users to inform themselves of the registry's processes and procedures, making them more understandable for users. Interoperability enhances the EBR's usability and integrity by enabling cross-checking of the data submitted to it, allowing system integrations through API, and improving alignment with international data exchange protocols.

Undoubtedly, Legal Authority and Compliance is indispensable for the registry's Trustworthiness, since trust is corrupted when legal authority is unclear or regulatory obligations are not met. As elaborated in CPF 15 on Legal Authority and Compliance, compliance with the national and international regulatory framework and adherence to data protection, AML/CFT, and cybersecurity regulations are all essential for trust.

Trustworthiness is maintained over time through the process of Continual Improvement, which allows for the identification of any underperforming registry elements that require attention.[238] Regular assessments, monitoring tools, and user feedback mechanisms are essential to achieving the goal of Continual Improvement, maintaining user trust towards the registry and staying abreast of developing technology and evolving threats.

User-Centred Design complements the above-mentioned factors and improves the overall usability of the registry's system and perception of its reliability. It allows users to understand the registry's services, learn

[235] NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, §2.6, 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (last accessed 7 February 2025).

[236] Id.

[237] Id.

[238] ISO 16363 Space Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories, (2012, Edition 2 in 2025) at § 1.6., https://www.iso.org/standard/87472.html (last accessed 26 May 2025).

how to use them; the registry should be able to be operated intuitively owing to the visual design of the services, appropriate documentation and multilingual support (where necessary) of the registry.

Finally, effective governance is key to maintaining Trustworthiness. Governance should include regular risk assessments, control effectiveness evaluations, service delivery and compliance reviews, and clear lines of accountability. Accordingly, when designing and implementing a registry, it is important to consider the types of features and functions that should be built into the system to enable the registrar or administrator to periodically assess the effectiveness of controls and registry performance and implement corrective actions, for example, removing inefficient controls or implementing new ones. The system should assist in the governance of the registry function, and users need to have confidence that the EBR is not only functionally reliable but institutionally responsible.

A declaration of Trustworthiness is insufficient on its own; an objective process of certification is required.[239] Providing users with the results of external audits and certification that the registry meets international standards not only provides assurance but also creates transparency and engenders trust among registry users.[240] Additionally, independent professional training and certification of EBR staff in skillsets required to manage and operate the EBR enhances its Trustworthiness, demonstrates competency, and contributes to its reputation.

Technical

The ISO/DIS 16363 technical standard addresses Trustworthiness directly from the perspective of Space Data and Information Transfer Systems (particularly, the Audit and Certification of Trustworthy Digital Repositories), and it defines procedures suitable for objectively auditing and certifying the trustworthiness of registries.[241] A regular cycle of audits and certification is required to maintain trustworthy status.[242] Where the registry can demonstrate that it has implemented practices required by related standards, this may serve to satisfy similar requirements of the audit (e.g., by employing the relevant standards and practices found in the ISO 27000 series of standards developed for Information Security Management Systems, and ISO 9000 series of standards for Quality Management Systems, ISO 15489-1 and -2 for Records Management).[243]

The scope of ISO 16363 is broad: it encompasses IT systems including infrastructure, communications equipment and firewalls, as well as supporting physical assets, personnel, management and administrative procedures. This covers, among other things, fire protection and flood detection systems, management procedures to assess staff skill levels relative to evolving relevant technology, and the registry's intellectual property rights practices.[244] Disaster preparedness and recovery plans are also assessed.[245]

[239] Id. at § 1.3.

[240] Id. at § 2.1.

[241] Id. at § 1.1, stating that the scope of the document is 'the entire range of digital repositories',

[242] Id. at § 2.1.

[243] Id. at § 2.3, 5.2.

[244] Id.

[245] Id. § 5.2.4.

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.[246]

The ITIL, now a stand-alone term but originating from the Information Technology Infrastructure Library developed in 1989, defines the organisational structure and skill requirements of an IT organisation and a set of standard operational management procedures and practices designed to manage an IT operation and associated infrastructure, such as an EBR.[247] ITIL 4, rolled out in 2023, focuses on digital transformation and addresses matters of cloud computing, hybrid cloud, AI and other technologies. In Canada and some US states, public registries and managed IT services use ITIL as the industry standard and sometimes also require ITIL certification for IT personnel maintaining EBRs. Implementing ITIL allows EBRs to create predictable IT environments and deliver the best service possible to their users, all while improving efficiency.

24. User-Centred Design

Definition: The property by which the design and development of the registry system aims to make the registry more usable by considering how the registry is used and applying human factors, ergonomic, and usability principles

Ergonomics and usability are central to the concept of User-Centred Design (UCD). According to ISO, ergonomics is the scientific discipline concerned with the understanding of interactions among human and other elements of a system, and applying theory, principles, data and methods to design in order to optimise human well-being and overall system performance.[248] Usability is defined as the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction.[249] Thus, UCD is concerned with not only functional adequacy but also the qualitative experience of interacting with the system. It aims to optimise user interaction and enhance user satisfaction and overall system performance by ensuring that user needs, behaviours, and contexts are considered throughout the system's lifecycle.

In some jurisdictions, UCD principles are recommended or mandated as a part of broader public digital services design standards. For instance, the United Kingdom's Government Digital Service Design Principles contain the fundamental principle 'Start with user needs', the Italian Design Guidelines for websites and digital services for public administration require ease of reference and user experience, and the Australian Digital Service Standard operates by the 'Know your user' criterion.[250]

At the international level, the OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age echo this approach, emphasising the building of accessible, ethical and equitable public services that prioritise user needs, rather than government needs. The Principle of 'Understand users and their needs' requires engaging users on an ongoing basis to identify insights for iterating the design of services, simplifying underlying procedures and increasing access for all user groups. It calls for documenting the user

[246] See NIST Recommended Security Controls for Federal Information Systems: SP 800-53, supra note 251, at Appendix E.

[247] See Information Technology Infrastructure Library (ITIL), www.itlibrary.org (last accessed 7 February 2025).

[248] ISO 9241-210 §3.5, Ergonomics of human-system interaction, 2019, https://www.iso.org/standard/77520.html (last accessed 26 February 2025).

[249] Id. at §3.13.

[250] See more here: https://oecd-opsi.org/toolkits/government-digital-service-design-principles/, https://www.agid.gov.it/en/guidelines, and https://www.digital.gov.au/policy/digital-experience/digital-service-standard.

journeys, data flows, and organisational responsibilities, identifying opportunities to apply the 'once-only' principle as widely as possible, and empowering users to manage their personal data.[251]

Applying UCD in the EBR context requires adopting the *design thinking* approach that views system development from the perspective of end users. As a result, the navigation, content presentation, and interactivity are based on user expectations and cognitive behaviour, the number of interactions required to complete a task is minimal, and the level of satisfaction is monitored throughout the user journey to further improve the user's experience. Services delivered are intuitive, context-appropriate, and accessible to a diverse population without legal or technical assistance.[252]

Effective UCD requires early and repeated user engagement to identify system requirements and to understand not just what users do, but why they do it.[253] The iterative process of research, design, redesign, and adaptation should integrate user feedback at every stage of the design and development process. Often, users do not use a system in the expected manner, and the UCD process should continue after the deployment of the EBR and throughout its lifetime, integrating inputs from helpdesk logs, analytics, beta testing, surveys, and stakeholder meetings.[254]

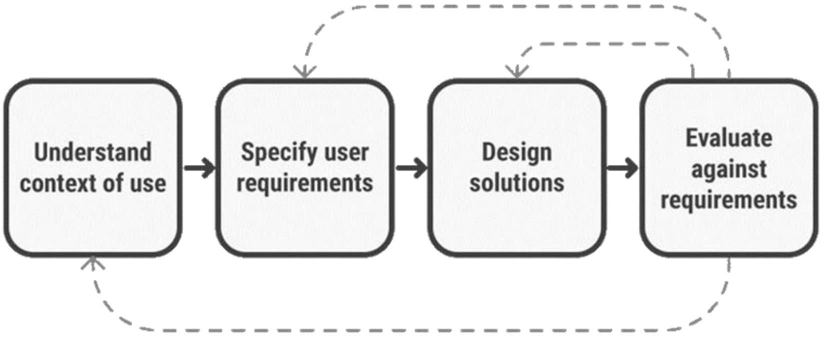

Understand context of use
Specify user requirements
Design solutions
Evaluate against requirements

Figure 8. User-Centred Design is an iterative process that focuses on an understanding of the users and their context in all stages of design and development.[255]

An EBR should be designed around the diverse needs and expectations of its users.[256] Some users (for instance, intermediaries) may conduct highly specialised tasks repeatedly, such as creating user accounts for clients, while others may interact with the registry only once. Designing only for the 'average user' risks overlooking important user segments. Therefore, user segmentation and task analysis are critical tools in tailoring services to different use cases.

In addition to usability, UCD also addresses User Experience (UX), which includes a user's perception of the EBR and response to using it. Poorly designed systems are difficult to understand, frustrate users and

[251] OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age, 2022, OECD Public Governance Policy Papers, No. 23, OECD Publishing, Paris, https://doi.org/10.1787/2ade500b-en (last accessed 31 July 2025).

[252] NRD Companies, Practical Guidelines for Starting the Digitalization of Public Services "Measure. Target. Act." https://www.nrdcompanies.com/app/uploads/2023/08/nrd-white-paper-e-services.pdf (last accessed 7 February 2025).

[253] See ISO 9241-210 Ergonomics of human-system interaction — Part 210:Human-centred design for interactive systems at 3.7, https://www.iso.org/standard/77520.html, (last accessed 7 February 2025); 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 7 February 2025).

[254] See User Centred Design, Interaction Design Foundation, https://www.interaction-design.org/literature/topics/user-centered-design (last accessed 7 February 2025); and see User-Centered Design: a Beginner's Guide, (Justin Mind, Jul. 14, 2020), https://www.justinmind.com/blog/user-centered-design/ (last accessed 7 February 2025).

[255] See User Centred Design, Interaction Design Foundation, https://www.interaction-design.org/literature/topics/user-centered-design (last accessed 7 February 2025);

[256] Id.

undermine user trust. In contrast, user-friendly systems have intuitive interfaces and helpful features that efficiently accomplish system functions and enhance the registry's reputation. UX is shaped by a combination of the registry's interface, functionality, performance, interactive behaviour, assistive capabilities, and alignment with user expectations.[257]

Furthermore, effective UCD reduces the likelihood of user error and thereby supports the accuracy of information on the registry, whereas inadequate system design may contribute to inaccurate filings or failed registrations, with legal or reputational consequences for registrars.

Technical innovation, increased digital literacy, and market and regulatory developments mean that user needs and expectations evolve over time. To stay effective, the UCD should be dynamic, i.e., interfaces and processes should evolve with user feedback; proactive, i.e., anticipating user needs where possible rather than responding to complaints; and strategic, i.e., incorporated as a part of broader registry operations, not just an IT consideration. For example, an alert that registrations are about to expire assists users in ensuring the effectiveness of their registration is extended where necessary, and autofill suggestions save time for users in completing the registration.[258]

Technical

UCD is supported by a range of internationally recognised technical standards and guidance. ISO 9241, 'Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems', provides detailed guidance on human-centred design for interactive systems. It includes principles and methods to enhance usability to help those responsible for managing infrastructure design and re-design processes.[259] It provides requirements and recommendations for UCD principles and activities throughout the lifecycle 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 and emphasises that systems must be designed based on an explicit understanding of users, tasks, and environments, and that user involvement should be continuous.

ISO/IEC 25010 offers a model for software product quality, including usability, accessibility, and user experience. It identifies 'quality in use' attributes like effectiveness and satisfaction as essential to software evaluation.

The principles set out in the WCAG[260] stipulate that the user interface be perceivable, operable, understandable, and robust, to meet the needs of all users, including those with disabilities (see CPF 2 on Accessibility). These are inherently user-friendly and complement UCD principles.

Apart from the standards, User Interface design heuristics (for instance, Jakob Nielsen's ten principles) are widely used as a practical evaluation method to evaluate and improve UCD. These heuristics include principles such as user control and freedom, error prevention, recognition rather than recall, and consistency.

[257] See ISO 9241-210, supra note 383, at 3.15.

[258] Id.

[259] See ISO 9241-210 §3.7.

[260] See WCAG 2.2 at a Glance, https://www.w3.org/WAI/standards-guidelines/wcag/glance/ (last accessed 7 February 2025).

III. EVALUATION OF RISKS TO ELECTRONIC BUSINESS REGISTRIES

Chapter II identified 24 CPFs essential for EBRs to carry out their functions reliably and efficiently. While CPF 19 already introduced the concept of risk management and provided a general overview of risks facing EBRs, the nature of these risks demands a more systematic and leadership-driven risk management approach. Risk in EBRs cannot be reduced to cybersecurity or ICT concerns alone; it extends to legal, operational, organisational, and reputational dimensions. Consequently, risk management must be treated as a strategic governance function, embedded in leadership decision-making, and not merely a compliance checkbox. Effective risk management enables proactive rather than reactive responses to threats, builds resilience, and maintains stakeholder trust.

To this end, this Chapter outlines a structured framework for evaluating and managing risks to EBRs, based on internationally recognised standards and best practices. It distinguishes between the general approaches to organisational risk management, drawing on ISO 31000 and the Three Lines of Defence model (3Lod), and specific methodologies for information security and system-related risks, drawing on the NIST Risk Management Framework (RMF) and the CIA triad.

A. CONTEXTUALISING RISK IN EBRs

The risk that the EBR may not 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. It is influenced by implementation decisions, required features, and the physical and digital environment in which the registry operates. As a result, it is generally not possible to reduce risk to zero. Instead, risk must be managed to an acceptable level using structured methodologies.

Risk management of an information system has been defined by NIST as 'the process of managing risks to organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals resulting from the operation of an information system, and includes: i) conducting a risk assessment; ii) implementing a risk mitigation strategy; and iii) employing techniques and procedures for the continuous monitoring of the security state of the information system.'[261] This definition makes clear that risk is not static; risk evolves, and so must the response mechanisms employed by EBRs.

B. RISK AS A LEADERSHIP FUNCTION: ISO 31000 AND THREE LINES OF DEFENCE

ISO 31000 provides a high-level, principle-based framework for risk management applicable to any organisation, including EBRs, which vary significantly in function, stakeholder landscape, and legal

[261] NIST, Minimum Security Requirements for Federal Information and Information Systems, FIPS Publication 200, March 2006, pp. 17, https://doi.org/10.6028/NIST.FIPS.200 (last accessed 7 February 2025). See also NIST Risk Management Framework, https://csrc.nist.gov/projects/risk-management (last accessed 7 February 2025).

context.[262] Its core elements (particularly, principles, framework, and processes) can be embedded in an EBR's governance, design and operations. ISO 31000 emphasises that risk management should be:

(i) integrated into organisational governance and decision-making;

(ii) structured and comprehensive;

(iii) based on best available information and tailored to the external and internal context;

(iv) dynamic, iterative, and responsive to change.

Of particular relevance is Clause 5.4.3, which addresses the need to clearly assign organisational roles, authorities, responsibilities, and accountabilities in risk management. This requirement aligns closely with the 3LoD model, originally developed by the Institute of Internal Auditors (IIA) and widely adopted across governance, risk, and compliance frameworks.[263]

The 3LoD model structures an organisation's internal governance into three coordinated layers:

(i) the First Line (Operational Management) is responsible for owning and managing risks directly – in EBRs, this includes registry staff managing data inputs, system users, and ICT operations on daily basis;

(ii) the Second Line (Risk and Compliance Functions) oversees and monitors risk – in an EBR, this function may include compliance officers, legal advisers, or IT security teams responsible for developing policies, standards, and monitoring tools;

(iii) the Third Line (Independent Assurance) provides objective assurance on the effectiveness of governance and risk management – for EBRs, this is typically an internal audit function assessing the control measures in place and providing suggestions for improvement.

Some organisations adapt the model to include a fourth or fifth line, such as external stakeholders, regulators, or supervisory bodies, who provide additional oversight and accountability. These adaptations are also appropriate for EBRs to further promote accountability. ISO 31000 principles, particularly leadership commitment (Principle 1), Integrated risk management (Principle 5) and Continual improvement (Principle 8) are directly applicable to each line of defence.

Deploying the 3LoD model in EBRs supports proactive risk identification and control, helps mitigate internal and external threats, and reinforces trust among users and stakeholders. For registries operating in jurisdictions where the regulatory environment includes GDPR, NIS2, or MiFID II,[264] such structured models are not just best practices but rather implicit or explicit requirements.

C. INFORMATION SECURITY TRIAD AND NIST

[262] ISO 31000 Risk management — Guidelines, 2018, https://www.iso.org/standard/65694.html (last accessed 25 May 2025).

[263] The IIA's Three Lines Model: An Update of the Three Lines of Defense, 2024, https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf (last accessed 26 May 2025).

[264] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, http://data.europa.eu/eli/dir/2014/65/oj (last accessed 26 May 2025).

Given the electronic nature of EBRs, risks to information security form a crucial part of overall risk management. The foundation of information security evaluation is the Confidentiality, Integrity, and Availability (CIA) triad, a model widely endorsed by NIST and embedded in ISO/IEC 27001.[265] These three principles form the backbone of secure system design and are indispensable to the secure and reliable operation of EBRs. Failure in any one of these dimensions compromises not only technical operations but also the legal and reputational integrity of the registry.[266]

Confidentiality
THE CIA TRIAD
Integrity
Availability

Figure 9. Model of the security triad in information systems.

Importantly, the performance of the CIA triad and, respectively, corresponding three CPFs is dependent on many of the other CPFs, creating interdependencies that compound risk. For instance, Confidentiality (not to mention Privacy) requires Access Control to prevent unauthorised access to specific data (e.g., a user's PII, login credentials, or billing information). Integrity requires, *inter alia*, consistent performance of Accuracy, Reliability, Retention and Disposition, Data Input Validation, and Access Control to maintain the legal validity of registrations and ensure confidence in search results. Availability requires Accessibility, Reliability, and Continuity, and, in certain cases, Interoperability to ensure that systems and data are accessible when needed.

Legal Authority and Compliance provides the rules that define the requirements for the CIA triad. Trustworthiness and Risk Management are dependent on its effectiveness in securing the registry from potential risks.[267]

[265] See, e.g., 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 7 February 2025).

[266] For cloud computing, a similar well-established triad consists of security, portability, and interoperability. See generally, NIST Cloud Computing Standards Roadmap: SP 500-291 Version 2, 2013, http://dx.doi.org/10.6028/NIST.SP.500-291r2 (last accessed 7 February 2025); and see OMG, Interoperability and Portability for Cloud Computing: A Guide Version 3.0, 2022, https://www.omg.org/cgi-bin/doc?mars/2022-12-13 (last accessed 7 February 2025).

[267] See Recommended Security Controls for Federal Information Systems: Special Publication 800-53, at 308, defining Trustworthiness as: 'The degree to which an information system (including the information technology components that are used to build the system)

To translate these principles into operational practice, registries may employ the NIST Risk Management Framework (RMF), which provides a structured process for information systems risk management. While ISO 31000 emphasises principles and organisational integration, NIST RMF is prescriptive and phased, guiding entities through: (i) categorisation of information systems, (ii) selection and implementation of security controls, (iii) assessment and authorisation, and (iv) continuous monitoring.

In support of this, NIST FIPS 199 Standards for Security Categorisation 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. In Table 3 below, the expected adverse effect is classified as low, moderate, or high, depending on the consequences for registry functionality, assets, and financial standing. For EBRs, these categories can be adapted to reflect the registry's unique functions and legal responsibilities, thereby enabling risk prioritisation and proportionate allocation of resources.

Potential Impact	Extent of adverse effect on registry operations and assets
Low	Limited, such as (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, such as (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, such as (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 3. Classification of Potential Impact (Adapted from NIST FIPS 199) [268]

Taken together, the CIA triad, NIST RMF, and impact classification provide a coherent framework for addressing the specific information security risks inherent in EBRs. They complement broader governance-oriented approaches such as ISO 31000 and the 3LoD, ensuring that information security is embedded within the wider risk management architecture of the registry.

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.'

[268] NIST SP 800-60 Vol. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, 2008.

D. RISK MAPPING OF CPF NON-PERFORMANCE

A key application of risk evaluation is to understand how non-performance of each CPF affects the registry's operation. Table 4 identifies the result of non-performance for each of the CPFs and suggests the level of impact (low, moderate, or high) this may have on an EBR.

CPF	Result of non-performance	Impact
1. Access Control	Privileged access is not restricted; unauthorised data manipulation, tampering or deletion possible	High
2. Accessibility	Registry or parts of it are unavailable to users with limited abilities	Moderate to High
3. Accuracy	Inaccurate records undermine legal value and user trust to EBR	High
4. Authentication	Users are not properly verified, enabling unauthorised submissions or access, undermining integrity	High
5. Availability	Registry cannot be queried or used for registration by users, disrupting business and legal processes	Moderate to High
6. Confidentiality and Privacy	Confidential or personal information is disclosed to unauthorised entities	High
7. Continual Improvement	Registry fails to adapt or respond to evolving needs, vulnerabilities, or user expectations	Moderate
8. Continuity	System downtime impairs operational resilience and public access	Moderate to High
9. Correctability	Errors cannot be rectified, potentially leading to legal disputes, financial harm and compliance issues	Moderate to High
10. Data Input Validation	Invalid, erroneous or incomplete submissions are accepted into the system	High
11. Error Detection	Systemic or user errors are unnoticed, creating persistent inaccuracies	High
12. Evidentiary Value	Registry data is not admissible in court or deemed unreliable	High
13. Integrity	Altered or corrupted data misrepresents legal or factual status	High
14. Interoperability	Registry is unable to interact effectively with other systems	Low to High
15. Legal Authority and Compliance	Registry fails to align with laws and regulations, leading to legal sanctions or nullified acts	High
16. Legal Authority of the Registrar	Registrar acts outside established mandate, registration outcomes are void or challengeable	High

17. Reliability	Inconsistent service or performance results compromise user confidence	High
18. Retention and Disposition	Data is retained or deleted inconsistently with legal requirements	Low to High
19. Risk Management	Vulnerabilities remain unmanaged, registry becomes more exposed to systemic threats	High
20. System Validation	Failures in design and validation cause operational breakdowns and regulatory breaches	High
21. Timeliness	Registration or update delays affect legal certainty and market operations	Moderate to High
22. Transparency	Lack of clarity in operations erodes public trust and legitimacy	High
23. Trustworthiness	Perceived unreliability or opacity leads to reputational damage, reduced usage, and stakeholder disengagement	High
24. User-Centred Design	Interface complexity leads to input errors or user exclusion	Moderate to High

Table 4. Risks and impacts of CPF non-performance.

In summary, given their critical role in enabling legal certainty and commercial transparency, EBRs must adopt structured, principle-based risk management approaches, such as ISO 31000, the 3LoD, and the NIST RMF. Risk in EBRs is contextual and cannot be eliminated entirely, but it can be managed within acceptable thresholds. The registrar, as the governance authority, should ensure clear assignment of roles and responsibilities, supported by models like the 3LoD and subject to oversight by external bodies, often governmental.

Embedding risk management in day-to-day operations enables EBRs to maintain trust, fulfil legal obligations, and remain efficient in evolving technical and regulatory environments.

IV. CONCLUSION

Business registries have always played an important role in supporting economic activity, legal certainty, and transparency. With the rapid digital transformation underway in many jurisdictions, their role has expanded beyond the traditional function of recordkeeping to become a cornerstone of modern commercial infrastructure. EBRs are now expected to combine legal authority with technological resilience, ensuring that data is accurate, accessible, secure, and usable across increasingly interconnected systems.

This Guide was developed to assist registry designers and operators at different stages of digitalisation, whether transitioning from paper-based systems, modernising legacy platforms, or establishing new registries. It builds upon the framework of CPFs first elaborated by the BPER Project for electronic collateral registries, re-examining them through the prism of business registry needs and the opportunities and risks brought by technological advancement. In doing so, it adapts a tested framework to a broader institutional context, while adding new CPFs and perspectives specific to EBRs.

The 24 CPFs presented in this Guide define the key dimensions of an effective and trustworthy EBR, ranging from legal authority and compliance to access control, interoperability, and user-centred design. Taken together, they represent a practical framework to eliminate or mitigate risks, reinforce reliability, and improve usability. Complementing these CPFs, the Guide incorporates international standards and reference materials, offering registries a comprehensive resource base when evaluating their unique challenges and opportunities.

The Guide has also benefitted from the collective expertise of practitioners, legal and technical experts, ensuring that it reflects both theory and practice, as well as a wide range of comparative experiences. By drawing on this knowledge, it seeks to provide not only a toolkit of practical measures but also a source of "food for thought" for those charged with strengthening their registries.

Ultimately, the value of this Guide lies in its ability to support registries as they evolve in line with broader digital transformation, helping them to remain reliable, resilient, and responsive to the needs of businesses, governments, and society at large.

V. GLOSSARY

Term	Definition
Accountability	The principle according to which a person or institution is responsible for a set of duties and can be required to give an account of their fulfilment to an authority that is in a position to issue rewards or punishment.[269]
Accuracy	The extent to which the data recorded in a business registry reliably reflects the information provided by registrants.
Application Programming Interface (API)	A means by which two or more computer programmes can communicate with each other.[270]
Authenticated	The state of having one's identity verified through a process that ensures the person, device, or entity attempting access is who or what they claim to be. It is typically done using credentials such as passwords, security tokens, biometric data, or cryptographic methods. Authentication establishes the legitimacy of the identity but does not grant or define the permissions associated with that identity.
Authorised	The state of having permissions applied to an authenticated identity about what actions or level of access a given user or system has in the registry. Authorisation defines the extent to which the user or system can perform certain activities in the registry, as implemented through predefined roles, attributes, or policies.
Auxiliary Data	The supplementary data that accompanies the primary data collected by electronic systems. It is often automatically collected for operational, security, or transparency purposes and can include metadata, audit trails, and technical logs.
Beneficial Owner (BO)	In the context of legal persons, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person (such as a company or arrangement such as a trust). Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.

[269] Britannica Dictionary, https://www.britannica.com/topic/accountability (last accessed 2 Mar. 2025).

[270] Glossary of Registry Terms, Foster Moore https://www.fostermoore.com/glossary-of-registry-terms-and-acronyms (last accessed 2 Mar. 2025).

Business Registry The State’s mechanism for receiving, storing and making accessible to the public certain information about businesses, as required by domestic law.

Digital Identity A set of electronically captured and stored attributes and credentials that can uniquely identify a person.[271]

Digital Signature An electronic signature that relies on cryptographic techniques to secure a message or document. It provides strong security features such as non-repudiation and data integrity verification.

Electronic Record Information that is born-digital or transformed into a structured digital format that enables dynamic interaction, processing, and analysis. Unlike scanned paper documents, electronic records are inherently digital, allowing users to edit the data, ensuring accuracy, integrity, and compliance with regulatory requirements.

Error An error refers to inaccuracies or deviations from the correct, expected, or intended data. Unlike updates, errors signify incorrectness and require correction to restore accuracy.

Escrow A legal arrangement to store the source code of the registry system with a neutral third party for protection against vendor insolvency.

Extensible Markup Language (XML) A versatile markup language designed for storing, transmitting, and reconstructing arbitrary data. It serves as a standardised way to share structured information between different systems and applications.

Open Data Information that is made public in a machine-readable format, free of restrictions in use, redistribution, or sharing. It typically involves non-sensitive information and may enable stakeholders like businesses, researchers, and regulators to make decisions by using and analysing the data for innovation and increased trust and transparency in the business environment.

Real-time Data Processing The ability to process and validate data immediately as it is received, which enables instantaneous decision-making and automated actions without human intervention.

Responsiveness Capacity of a system to respond to incidents, with *incident response* referring to actions taken in order to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilising or disruptive events and to recover to a normal situation.[272]

Unique Identifier A single unique business identification number is assigned to a business entity at the time of its registration. This identifier is allocated only once and remains

[271] World Bank Group (2017), Technical Standards or Digital Identity, DRAFT FOR DISCUSSION, https://thedocs.worldbank.org/en/doc/579151515518705630-190022018/original/ID4DTechnicalStandardsforDigitalIdentity.pdf (last accessed 25 Mar. 2025).

[272] ISO/DIS 22300, Security and resilience (2016), https://www.iso.org/obp/ui/#iso:std:iso:22300:dis:ed-2:v1:en (last accessed 25 Mar. 2025).

	associated with the entity throughout its entire lifecycle. Public authorities consistently use it to identify the legal entity uniquely across various systems and processes.
Validated	The state of having the legitimacy of a user or system confirmed before access to the registry is granted. Validation involves checking that a user or system meets specific criteria, such as providing valid credentials, agreeing to terms and conditions, or adhering to predefined standards.
Vulnerability	Weakness of an asset or control that can be exploited so that an event with a negative consequence occurs.[273]

[273] ISO/IEC 27005 Information security, cybersecurity and privacy protection — Guidance on managing information security risks https://www.iso.org/standard/80585.html (last accessed 7 February 2025).

ANNEX I: SCOPE OF PUBLICLY AVAILABLE INFORMATION

The design and operation of EBRs shall be grounded in a comprehensive understanding of the legal frameworks that govern both the disclosure and protection of business-related information. In this context, registries serve a dual role: they function as a key transparency mechanism, allowing the public, investors, and authorities to access essential business data, while at the same time, they safeguard certain categories of information to uphold confidentiality, privacy, and security, as elaborated in the CPFs on Access Control and Confidentiality and Privacy. The distinction between information that should be made publicly accessible and that which should remain protected is particularly critical in light of diverging national approaches and evolving legal standards, including those arising from data protection laws and international efforts to combat illicit financial flows.

Taking this context into consideration, the present Annex aims to assist business registrars in conducting a comprehensive legal analysis and outlines guidance provided by relevant international and regional instruments regarding publicly available business information. It also illustrates how these principles are applied in practice, drawing on examples from the Survey on Data Registration and Disclosure Practices in Business Registries conducted by the BPER Project team in December 2024 (the Survey).

Several existing international and regional instruments, such as the ***UNCITRAL Legislative Guide on Key Principles of a Business Registry (2018)***, *Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 Relating to Certain Aspects of Company Law* (EU Directive 2017/1132), and the ***Financial Action Task Force (FATF) Recommendations***, specify the types of data that should be registered in a business registry and establish principles for the disclosure of information.

Registration and disclosure of information on companies

The UNCITRAL Legislative Guide sets out the minimum information required for business registration in Recommendation 21.

Recommendation 21: Minimum information required for registration

The law should establish the required information and supporting documents for the registration of a business, including at least:

a) The name of the business;
b) The address at which the business can be deemed to receive correspondence or, in cases where the business does not have a standard form address, the precise description of the geographical location of the business;
c) The identity of the registrant(s);
d) The identity of the person or persons who are authorized to sign on behalf of the business or who serve as the business's legal representative(s); and
e) The legal form of the business being registered and its unique identifier, if such an identifier has already been assigned.

Depending on the jurisdiction and form of business organisation, other information might be required for registration:[274]

a) the names and addresses of the persons associated with the business, which may include managers, directors and officers of the business;
b) the rules governing the organisation or management of the business;
c) information relating to the capitalisation of the business;
d) proof of share capital;
e) information regarding the nature of business activities that the organisation performs;
f) contracts for non-cash property; and
g) shareholder details and any changes in those details.

For statistical purposes and in a strictly voluntary manner, registries may request additional details, such as gender identification, ethnicity or language group of the registrant and other persons associated with the business.[275]

Information required at a post-registration stage may include:[276]

a) Amendments to any of the information that was initially or subsequently required for the registration of the business as set out in Recommendation 21;
b) changes in the name(s) and address(es) of the person(s) associated with the business;
c) financial information, depending on the legal form of the business; and
d) information concerning insolvency proceedings, mergers or winding-up.

The Survey results demonstrated that most registries collect the minimum information required for registration listed in Recommendation 21. Going beyond minimum requirements, many business registries collect annual accounts and BO information. This is reflected in the responses from the registries operating in Estonia, Ireland, Italy, Belize, Ghana, Tunisia, and Jamaica.

The public availability of registered information and related restrictions are stipulated in Recommendations 35 and 36.

Recommendation 35: Public availability of information

The law should specify that all registered information is fully and readily available to the public unless it is protected under the applicable law.

Recommendation 36: Where information is not made public

In cases where information in the business registry is not made public, the law should:

a) Establish which information concerning the registered business is subject to the applicable law on public disclosure of protected data and which types of information cannot be publicly disclosed; and

[274] UNCITRAL Legislative Guide, paras. 129 and 131.
[275] UNCITRAL Legislative Guide, para. 130.
[276] UNCITRAL Legislative Guide, para. 156.

b) Specify the circumstances in which the registrar may use or disclose information that is subject to confidentiality restrictions.

Similarly, Article 14 of the EU Directive 2017/1132 stipulates that Member States shall take the measures required “to ensure the compulsory disclosure by companies of at least the following documents and particulars:

a) The instrument of the constitution and the statutes if they are contained in a separate instrument.
b) Any amendments to the instruments referred to in point (a), including any extension of the duration of the company.
c) After every amendment of the instrument of constitution or statutes, the complete text of the instrument or statutes as amended to date.
d) The appointment, termination of office, and particulars of the persons who, either as a body constituted pursuant to law or as members of any such body:
   (i) Are authorised to represent the company in dealings with third parties and in legal proceedings. The disclosure must specify whether these persons may act alone or are required to act jointly.
   (ii) Take part in the administration, supervision, or control of the company.
e) At least once a year, the amount of subscribed capital, where the instrument of constitution or statutes mention an authorised capital, unless any increase in the subscribed capital necessitates an amendment of the statutes.
f) The accounting documents for each financial year that are required to be published.
g) Any change of the registered office of the company.
h) The winding-up of the company.
i) Any declaration of nullity of the company by the courts.
j) The appointment of liquidators, particulars concerning them, and their respective powers, unless such powers are expressly and exclusively derived from law or the statutes of the company.
k) Any termination of liquidation and, in Member States where striking off the register entails legal consequences, the fact of any such striking off.”

Article 16 of the EU Directive 2017/1132 requires Member States to ensure that the disclosure of the documents and information referred to in Article 14 is effected by making them publicly available in the register.

According to the survey results, business registries generally make the company name and address publicly available. The names of directors and officers and annual accounts are also commonly disclosed. However, public access to BO information remains limited, with only Estonia and Ghana reporting that this data is publicly accessible.

Disclosure of beneficial ownership information

According to FATF Recommendation 24, countries should ensure that adequate, accurate, and up-to-date information on the BO and control of legal persons can be obtained or accessed rapidly and efficiently by competent authorities through a BO register or an alternative mechanism.

The FATF Interpretive Note to Recommendation 24 provides further details on the requirements for company registries regarding BO identification. The minimum basic information about a company to be recorded by the registry and made public includes:[277]

a) the company name;
b) proof of incorporation;
c) the legal form and status of the company;
d) the address of the registered office;
e) basic regulating powers (e.g., memorandum and articles of association);
f) a list of directors; and
g) a unique identifier (e.g., tax identification number, where applicable).

BO information shall include information that is sufficient to identify:

- The natural person(s) who are the beneficial owner(s): full name, date and place of birth, nationality, residential address, national identification number and document type, and the tax identification number or equivalent in the country of residence; and

- The nature and extent of the means and mechanisms to exercise ownership or control: ownership structure information, means to exercise control (e.g., votes, shares or other interests).

As exemplified by the survey, in jurisdictions where business registries are responsible for collecting BO data, typically, comprehensive personal and structural details are required: date of birth, place of birth, nationality, residential address, passport number, tax identification number, ownership structure information, and means to exercise control. However, verification is limited — only Ireland, Estonia, and Tunisia reported verification of submitted BO data as a responsibility of the registration authority.

Transparency and Public Access Restrictions

In the EU, the tension between transparency and privacy came to the fore with the 2022 judgment of the Court of Justice of the European Union (CJEU) in ***WM and Sovim SA v Luxembourg Business Registers***. The CJEU ruled that not all information concerning ultimate BOs should be freely accessible to the public. It determined that providing unrestricted public access to personal data held in BO registers contravenes Articles 7 (Respect for private life) and 8 (Protection of personal data) of the European Union Charter of Fundamental Rights.

While reaffirming the importance of transparency in tackling money laundering and terrorist financing, the CJEU emphasised the need to strike a balance, taking into account the protection of privacy rights. Access to data in business registries should be granted based on a legitimate interest, with individuals or entities

[277] FATF Interpretive Note to Recommendation 24, paras. 4-5.

required to demonstrate a valid reason for accessing different data sets. The principle of proportionality was highlighted, ensuring that the level of access granted aligns with the demonstrated legitimate interest. This decision called for a careful recalibration of registry practices within EU Member States to ensure transparency obligations align with robust data protection principles.

Following this court decision, many registries had to reassess access to BO data and evaluate which information could be accessible to which entities. The later-adopted sixth AML Directive[278] seeks to provide more clarity regarding which third parties have access to BO information of legal entities and legal arrangements. According to this Directive, competent authorities shall have immediate, unfiltered, direct and free access to registers across the European Union. In addition, persons of the public with legitimate interests can also access this information. Such persons include, for instance, journalists, civil society organisations, and third-country competent authorities. These rules on access to persons of the public aim to reconcile the transparency goals of AML initiatives with the fundamental rights affirmed by the CJEU.

It is important to remember that the GDPR, the AML Directive, and the CJEU ruling apply only to EU Member States. Other jurisdictions rely on their own legal frameworks to determine the extent and nature of information accessible to third parties.

Around the world, business registries take different approaches to safeguarding protected data while maintaining transparency and public access to registry data. For example, open data bulk files provided by the EBR in Estonia exclude personal identification codes, ensuring some level of privacy protection. In Ghana, the dates of birth and residential addresses of directors are withheld from public access according to the Data Protection Act. Similarly, in Hong Kong, the habitual residential addresses and full identification numbers of directors, company secretaries and other relevant persons are categorised as protected information and are only accessible to specified persons upon application; instead, correspondence addresses and partial identification numbers are available to the public. In Tunisia, personal data is disclosed only to competent authorities or through judicial request.

Notably, in Mexico, while the information registered in the Public Registry of Commerce is public, access to the information is classified as follows: i) general inquiries, accessible to any person, ii) inquiries by notaries and public officials, who may access detailed records, iii) access by financial institutions, which may request financial data of registered companies to assess credit risk, iv) access for research and statistical purposes, provided that no individualised data is disclosed, and v) other types of access, which require explicit authorisation from the Ministry of Economy. Such a multi-level approach clearly reflects considerations of transparency and privacy of the registry data.

Given the particular sensitivity of BO information, EBRs in jurisdictions collecting BO data implement various Access Control measures to ensure that such information is accessible only to authorised individuals. For example, in Ireland, BO information is accessible only to competent authorities via dedicated, IP-restricted access, while obliged entities receive limited BO data through a user account system, ensuring strict control

[278] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, accessible at http://data.europa.eu/eli/dir/2024/1640/oj.

and prohibiting public searches. The EBR system in Tunisia monitors and tracks all interactions with BO data by authorised users. In Jamaica, access requests must be submitted electronically and vetted to confirm the requestor's identity and legal eligibility, while in Ghana, BO data is provided upon request to competent authorities free of charge, through formal letters. Interestingly, in the Canadian province of Saskatchewan, the EBR limits public searches only to specific business entities, preventing searches by individual names.

Conclusion

In conclusion, the design and operation of EBRs should strike a careful and dynamic balance between Transparency and the protection of Confidentiality and Privacy. As illustrated by international standards and evolving regional regulations, registries should be built on principles that enable public access to essential business information while implementing appropriate legal and technical safeguards for data sets subject to Confidentiality, Privacy, or security considerations. The variety of legal approaches across jurisdictions, especially in the fields of data protection and AML, underlines the need for EBRs to carefully calibrate Access Controls that can respond to jurisdiction-specific mandates. As legal standards evolve, it is essential to establish mechanisms for the regular review and adjustment of EBR operations in light of evolving jurisprudence, legislative reforms, and international commitments. Ensuring compliance while upholding the goals of Transparency and Confidentiality and Privacy requires continuous legal monitoring and technical responsiveness from modern EBRs.

ANNEX II: RELEVANT TECHNICAL STANDARDS

Modern EBRs incorporate a wide array of functionalities, starting with access control, cybersecurity, and information security, to data quality, interoperability, confidentiality, privacy, record management, and risk management. Table 5 below represents a non-exhaustive list of relevant technical standards, grouped by scope and, more broadly, functional category, while acknowledging that some may span multiple domains.

Category	Standard	Scope
Access Control	INCITS 359-2012 (R2022)	Role Based Access Control (RBAC)
	ISO/IEC 9798-1	Entity Authentication
	ISO/IEC 24760	Framework for Identity Management
	NIST SP 800-162	Attribute Based Access Control (ABAC)
Business Continuity	ISO 22301	Business Continuity Management System (BCMS)
	NFPA 1660	Emergency, continuity, and crisis management
Cybersecurity	ISO/IEC 27034	Application security
	ISO/IEC 27040	Storage security
	ISO/IEC TR 27103	Cybersecurity and ISO and IEC Standards
	NIST SP 800-160, Vol. 2	Developing cyber-resilient systems
	NIST SP 800-161	Cybersecurity supply chain risk management practices
	NIST SP 800-207	Zero Trust Architecture
	NIST SP 800-50	Cybersecurity and privacy learning programmes
	NIST SP 800-92	Cybersecurity log management
Data Quality	ISO 8000-8	Information and data quality fundamental concepts
	ISO 9001	Quality management systems
	ISO/IEC 25012	Data quality model
	ISO/IEC 7064	Check character systems
	NIST SP 800-218	Data Input Validation
Electronic Signatures	ETSI EN 319 422	Electronic signatures and infrastructures
Encryption	IEEE 1619.1-2019	Cryptographic units for storage device encryption
	NIST-FIPS 197	Advanced Encryption Standard (AES)

Human-Computer Interaction	ISO 9241-210	Human-centred design of interactive systems
Information Security	ISO/IEC 27000	Information Security Management Systems (ISMS)
	ISO/IEC 27001	ISMS Requirements
	ISO/IEC 27002	Information security controls
	ISO/IEC 27005	Managing information security risks
	NIST SP 800-100	Comprehensive guide for managers on information security management
	NIST SP 800-12	Information security concepts for federal information systems
	NIST SP 800-47	Secure information exchanges between organisations
	NIST SP 800-55	Measuring information security performance
	NIST SP 800-137	Information Security Continuous Monitoring
Interoperability	ISO 19941	Cloud computing interoperability and portability
Privacy	ISO/IEC 29100	A high-level privacy framework
	NIST SP 800-122	Protecting Personally Identifiable Information
	NIST SP 800-53	Security and privacy controls for information systems
Record Management	ISO 15489-1	Records management concepts and principles
	ISO/TR 17068	Trusted third-party repository for digital records
	ISO 32000-2	Portable Document Format (PDF) version 2.0.
Risk Management	ISO 31000	Principles and guidelines on risk management
	NIST SP 800-37	Risk Management Framework (RMF) for security and privacy
Software Quality	ISO/IEC 25010	Systems and software quality requirements and evaluation
	ISO/IEC TS 25011	Service quality models for software evaluation
	ISO/IEC/IEEE 2911	Framework for software testing
	NIST SP 800-218	Secure Software Development Framework
Trustworthiness	ISO/DIS 16363	Requirements for auditing trustworthy digital repositories.

Table 5. Standards supporting the CPFs.

As clarified in Chapter I.E. LIMITATIONS OF TECHNICAL STANDARDS AND SELECTIVE ADOPTION', technical standards underpin most of the CPFs and inform the best practices discussed throughout this Guide. However, they are to be understood as reference material, not prescriptive practices *per se*. Their application must be context-specific and aligned with each registry's legal, technological, and operational environments.

While a comprehensive understanding of the standards listed requires an extensive analysis of each of them, which is beyond the scope of this document, a brief annotation of some of them can be provided to help explain these standards function and can be applied to EBRs. For instance, in information security and risk management, ISO/IEC 27001 defines the requirements for an information security management system, while NIST SP 800-53 offers a catalogue of security and privacy controls especially suited for public sector registries, and ISO 31000 provides principles and guidelines for risk management adaptable to any context, including EBRs. When it comes to Data Quality and Software Quality, ISO/IEC 25010 defines system and software quality models, including attributes such as reliability, security, and usability, ISO/IEC IT 25011 focuses on service quality aspects of IT services, and, eventually, ISO/IEC 25012 covers data quality characteristics, crucial for trustworthy EBR.

1. INDUSTRY AND COMMUNITY-LED BEST PRACTICES

Best practices and standards developed by industry- and community-driven guidelines complement international standards. Developed by experts from industry, governments, academia, and other organisations, they provide valuable insights, particularly in areas where formal standards may lag behind innovation or deployment realities.[279]

Industry organisations often develop and publish best practices for their industry or segment of interest. Examples include the Data Management Association (DAMA), Object Management Group (OMG), and Storage Networking Industry Association (SNIA). Some vendors and manufacturers (e.g., Microsoft and Amazon Web Services (AWS)) also publish best practices that may be specific to their products or more general but targeting markets that their products serve.

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 the configuration and installation of their products. The value of these publications is 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.

Publisher	Title
American Institute of Certified Public Accountants (AICPA)	System and Organization Controls (SOC) 2[280]

[279] See ISO, ISO in Brief, 10, (ISO, 2019), https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf (last accessed 7 February 2025).

[280] See at https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services (last accessed 7 May 2025).

AWS	AWS Well-Architected Framework (2020)[281]
DAMA	DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) (2017)[282]
OWASP	OWASP Top Ten[283]
OMG	Interoperability and Portability for Cloud Computing: A Guide[284]
SNIA	Data Protection Best Practices (2025)[285]
World Wide Web Consortium (W3C)	Web Content Accessibility Guidelines[286]

Table 6. Examples of industry and community-led publications

2. INFORMATION SECURITY CONTINUOUS MONITORING (ISCM) AND CYBERSECURITY FRAMEWORKS

Beyond technical standards which specify controls, requirements, or metrics to be implemented, EBRs should also consider operational frameworks such as Information Security Continuous Monitoring (ISCM), the NIST Cybersecurity Framework (CSF), and ISO/IEC 27103. Such frameworks are not only complementary to technical standards, but they also allow EBRs to ensure that implemented controls remain effective, responsive to threats, and aligned with their institutional, regulatory, and operational realities.

Ongoing monitoring of information security is a critical component of risk management.[287] Information security does not end with the infrastructure setup or with the issuance of a security policy.[288] Instead, continuous monitoring and management are required to protect the confidentiality, integrity, and availability of information over time.[289]

With evolving technology come new threats and vulnerabilities that must be identified and addressed.[290] Information security continuous monitoring (ISCM) is defined as 'maintaining ongoing awareness of information security, vulnerabilities, and threats to support organisational risk management decisions'.[291]

[281] AWS Well-Architected Framework, AWS (2024), https://docs.aws.amazon.com/pdfs/wellarchitected/latest/framework/wellarchitected-framework.pdf#welcome (last accessed 7 February 2025).

[282] See the Global Data Management Community (DAMA), Data Management Body of Knowledge, 2017, https://www.dama.org/cpages/body-of-knowledge (last accessed 7 February 2025).

[283] See https://owasp.org/www-project-top-ten/ (last accessed 7 May 2025).

[284] See OMG Cloud Working Group, Cloud Interoperability and Portability: A Guide, Version 3.0, https://www.omg.org/cgi-bin/doc?mars/22-12-13.pdf (last accessed 7 May 2025).

[285] See SNIA, Data Protection Best Practices, Version 2.0, 2025, https://www.snia.org/sites/default/files/2025-03/SNIA-Data-Protection-Best-Practice-2025-01-27-v2.pdf (last accessed 7 May 2025).

[286] See https://www.w3.org/WAI/standards-guidelines/wcag/ (last accessed 7 May 2025).

[287] NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, 2011, at vi, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf (last accessed 27 February 2025). See also NIST IR 8212, ISCMA: An Information Security Continuous Monitoring Program Assessment, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8212.pdf (last accessed 27 February 2025).

[288] NIST SP 800-12 Rev 1: An Introduction to Information Security, 2017, § 2.7, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (last accessed 7 February 2025).

[289] Id.

[290] Id.

[291] Kelley Dempsey et al., at vi.

This approach is codified in NIST Special Publication 800-137, which offers guidelines to assist organisations in developing an ISCM strategy and implementing a programme to monitor threats and vulnerabilities, the effectiveness of deployed security controls, and overall risk posture.[292] A registry's ISCM strategy must be based on a clear understanding of the specific security risks faced by the registry and should provide meaningful metrics on security effectiveness and compliance with the regulatory, organisational, and policy requirements.[293] By providing actionable information on security status, ISCM enables the transition from compliance-driven to data-driven risk management.[294] Input from ISCM can also be used to monitor the CPFs' performance across time and prioritise the registry's resources accordingly.

The NIST's Cybersecurity Framework (CSF) provides a high-level, technology-neutral approach to managing security risk. It is particularly suited to institutions like EBRs, given its flexibility, modularity, and alignment with global standards, guidelines, and practices. Developed originally for the critical infrastructure sector, the CSF has now been widely adopted across both public and private sectors and across jurisdictions. It structures cybersecurity procedures around a core framework of six concurrent and continuous functions:

i) Govern – The organisation's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored;

ii) Identify – The organisation's current cybersecurity risks are understood;

iii) Protect – Safeguards to manage the organisation's cybersecurity risks are used;

iv) Detect – Possible cybersecurity attacks and compromises are found and analysed;

v) Respond – Actions regarding a detected cybersecurity incident are taken; and

vi) Recover – Assets and operations affected by a cybersecurity incident are restored. [295]

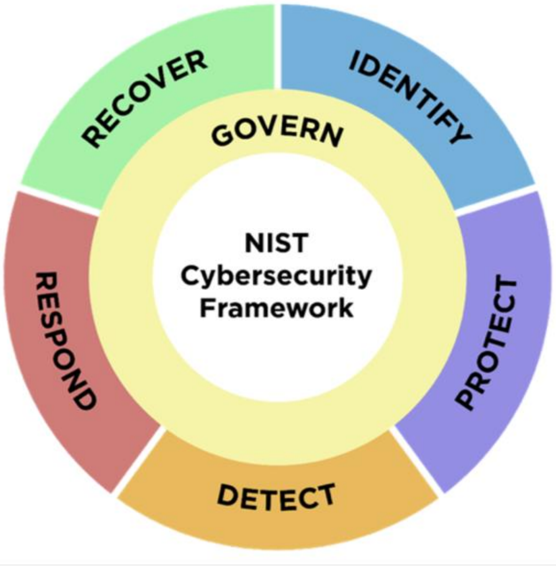


Figure 10. NIST Cybersecurity Framework Functions[296]

[292] Id. at 3.

[293] Id. at vi.

[294] Id. at vii.

[295] NIST Cybersecurity Framework 2.0, 2024, pp. 3-4, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last accessed 27 February 2025).

[296] The NIST Cybersecurity Framework (CSF) 2.0, 2024, https://doi.org/10.6028/NIST.CSWP.29 (last accessed 27 February 2025).

Each function is broken down into categories and subcategories, which represent more specific outcomes of technical and management activities.[297] For example, the ‘Protect’ function is divided into five categories, which are further divided into subcategories (i.e., ‘Users, services, and hardware are authenticated’ is one of six subcategories under the category ‘Identity management, Authentication and Access Control’).[298] For each subcategory, the CSF provides informative references and implementation examples on the dedicated website. Notably, earlier versions of the CSF included only five functions (Identify, Protect, Detect, Respond, Recover). Version 2.0 added Govern as a core function, further reinforcing its relevance for the EBR oversight.

Similarly, ISO/IEC TR 27103 offers guidance on how to use a cybersecurity framework aligned with ISO/IEC standards, particularly for organisations that wish to integrate international best practices.[299] ISO/IEC TR 27103 incorporates a risk-based, prioritised, flexible, outcome-focused, and communications-enabling framework consisting of five core functions: Identify, Protect, Detect, Respond, and Recover.[300] Mirroring the structure of the NIST CSF, within each function, there are also categories and sub-categories that are important for achieving the specified outcomes, as well as references demonstrating how to leverage existing ISO and IEC standards, such as ISO/IEC 27001 on Information Security Management, ISO/IEC 27002 on Security Controls, and ISO/IEC 27005 on Risk Management, to better support the implementation of relevant activities.[301] This report facilitates standard-to-framework mapping, enabling EBRs to build cohesive systems using both strategic frameworks and detailed standards.

[297] Id. at Table 1: CSF 2.0 Core Function and Category names and identifiers. The CSF is available as a free download from the NIST website https://www.nist.gov/cyberframework (last accessed 26 February 2025).

[298] See NIST Cybersecurity Framework 2.0, 2024, p.19, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last accessed 27 February 2025).

[299] See ISO/IEC TR 27103, Information technology — Security techniques — Cybersecurity and ISO and IEC Standards, https://www.iso.org/standard/72437.html (last accessed 7 February 2025).

[300] Id., § 6.2.

[301] Id. at Annex A.