GUIDE ON
BEST PRACTICES FOR

Electronic Business Registries

MAY 2026

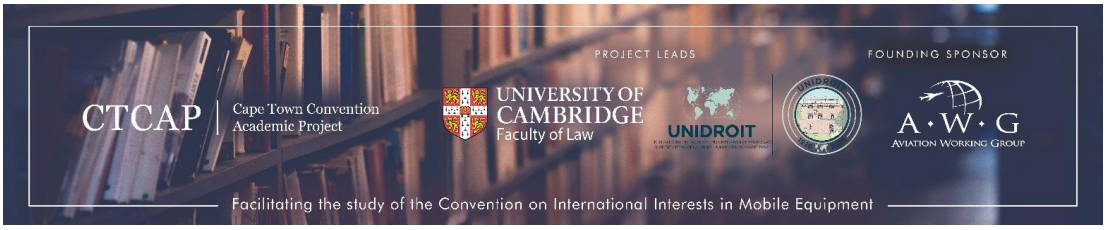
CTCAP | Cape Town Convention Academic Project

Guide on Best Practices for Electronic Business Registries

CTCAP – Cape Town Convention Academic Project

Rome, 2026

ISBN: 978-88-86449-80-9



THE UNIDROIT FOUNDATION
SUPPORTING THE WORK OF UNIDROIT

aviareto

ACKNOWLEDGEMENTS

This Guide on Best Practices for Electronic Business Registries has been prepared by the Project Group on Best Practices in the Field of Electronic Registry Design and Operation (BPER), which is managed under the auspices of the Cape Town Convention Academic Project (CTCAP).

The CTCAP is a joint undertaking of 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 is supported by the UNIDROIT Foundation and Aviareto.

Particular recognition is due to Rob Cowan (Aviareto) for his technical expertise, generous funding support, and the insights provided by his team, including Caroline O'Brien, Michael Choi, and Denis Finnegan. The Project also profoundly relied on the expertise and dedication of its expert consultants, Paul Farrell (2021–2022) and Ieva Tarailienė (2023–2024), whose guidance significantly shaped the practical recommendations in the Guide.

The BPER Project Group greatly benefited from the involvement of representatives of various international and national organisations and institutions engaged in establishing and operating electronic business registries, including Andrea August, Goran Vranic, Aris Molfetas-Lygkiaris (World Bank Group); Monica Canafoglia (UNCITRAL); Pier-Olivier Turcot, Marla Weinstein, Silverio Espinola (ICAO); Kathy Hillman-Weir, Laurel Garven (Information Services Corporation); Justin Hygate, Julian Lamb, John Murray (Foster Moore); Marco Vianello (Infocamere, European Business Registry Association); Maureen O'Sullivan (Companies Registration Office, Ireland); Alexis Lupo (IACA (Michigan)), Jaime Weddle Jones (IACA (Oregon)); Declan Geaney (Seapoint); and Katarzyna Connell (Enterprise Registry Solution).

Gratitude is further extended to Teresa Rodríguez de Las Heras Ballell (Universidad Carlos III de Madrid) and Siew Huay Tan (Civil Aviation Authority of Singapore) for their valuable insights. During the consultation phase, the Corporate Registers Forum and the Registre National des Entreprises in Tunisia, which hosted the 2025 Annual Meeting, contributed to gathering industry feedback on the Guide.

Contributions to the survey on publicly accessible information have further enriched the Guide, including input from the Corporations Division in the Commonwealth of Massachusetts, the Estonian Business Registry, the Corporations Division in the State of Michigan, the Belize Companies and Corporate Affairs Registry, the One-Stop Business Facilitation Centre of the Ministry of Trade and Industry of Lesotho, the Companies Office of Jamaica, the Samoa International Finance Authority, and the Office of the Registrar of Companies in Ghana. These insights were complemented by meaningful feedback provided during the targeted consultation phase by Stephen Abbott Pugh (Beneficial Ownership Data Standard expert), Joel Vicente (CoreFiling), Zvonko Obradović (Former Director of the Serbian Business Registry Agency (2007-2019)), Hayley Thompson (Code Management Association (ECCMA)), Ana Gómez Adeva (Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España), Assad Hijjah (DAI), Tomasz Tomczak (University of Opole), Kersti Rätsep (Centre of Registers and Information Systems), and Julia Naedts (Justiz NRW Mitarbeiterin der Verfahrenspflegestelle RegisSTAR und Projektgruppe AuRegis).

Finally, the CTCAP is deeply grateful to the UNIDROIT Secretariat, particularly Kateryna Bovsunovska, Benedetta Mauro and Hamza Hameed for their exceptional management of this specific project at various times, as well as Anna Veneziano, William Brydie-Watson, Myrte Thijssen and Theodora Kostoula for their contributions to the development of the Guide. It also appreciates the work of UNIDROIT interns Yara Boehlen (Germany), Maria Arancia Simiuc (Romania/Austria), Ze Yuan (China), and Nia Gabunia (Georgia) on this project.

MESSAGE FROM THE DIRECTORS

Electronic business registries are foundational infrastructure for modern economies. By transparently recording the legal existence, structure, and key information of business entities, they underpin commercial activity, legal certainty, and regulatory compliance across every jurisdiction in which they operate. Where registries are unreliable, poorly designed, or outdated, the consequences are wide-ranging: public trust erodes, reputational damage ensues, and significant economic harm is inflicted on market participants. Investors, both domestic and foreign, are deprived of the trustworthy business data they need to assess market risks; suppliers are unable to connect to global value chains; and governments risk losing the data quality on which sound economic policy and effective regulation depend.

The transformation of business registries from paper-based administrative systems to interconnected digital infrastructure has significantly expanded both their potential and their complexity. Modern electronic business registries are now often expected to support cross-border interoperability, beneficial ownership transparency, anti-money laundering compliance, and integration with broader public digital services. This expansion of functions also increases the responsibility for those charged with designing and operating these systems, and a corresponding need for guidance on how to meet it.

This Guide on Best Practices for Electronic Business Registries responds to that need. It offers registry designers and operators a structured framework, built around 24 Critical Performance Factors, each combining practical operational measures, legal analysis, and internationally recognised technical standards, to help registries at any level of digital maturity evaluate and strengthen their practices. It is the product of several years of research and dialogue among legal and technical experts and registry operators from across the world, reflecting both the diversity of approaches found in different jurisdictions and the common principles underpinning sound registry design.

This Guide is the second major publication of the BPER Project, which began with the Guide on Best Practices for Electronic Collateral Registries (published in 2021) and has committed to extending its framework to other types of electronic registries. That commitment is fulfilled here. The framework initially developed for collateral registries has been thoroughly re-examined, adapted, and expanded to account for the distinct legal, institutional, and technical features of business registries, producing a Guide that stands on its own terms while building on the rigour of its predecessor.

As Directors of the CTCAP, we are pleased to endorse the publication of this Guide. We believe it makes a significant contribution to the broader mission of advancing understanding of the electronic registry systems on which modern commerce depends. We hope it will serve as a practical and enduring resource for all those working to ensure that electronic business registries fulfil their functions with reliability, integrity, and trust.

Professor Louise Gullifer K.C. (hon) FBA

Professor Ignacio Tirado

Professor Jeffrey Wool

FOREWORDS

Recent Subnational Business Ready studies conducted across the European Union under the World Bank's B-READY methodology consistently identify digital public services (Pillar II) as the area of weakest performance, a finding echoed by the World Bank's B-READY 2025 report.

Business registries sit at the intersection of economic development and digital governance. As gatekeepers of formal economic activity, they are expected to deliver sovereign, secure, and compliant digital services to both businesses and governments, yet they operate in an environment of accelerating change. The BPEBR Guide arrives at a pivotal moment, offering a practical, technology-neutral, and legally grounded framework developed by international business registry experts to meet precisely these demands.

Business registration reform is foundational to any broader business environment agenda, placing registries at the frontline of national development. The imperative to digitalise is inseparable from rising requirements for data protection, traceability, and authentication - demands that cannot be addressed through piecemeal solutions.

The Guide is directly relevant to the World Bank's Subnational B-READY agenda; by identifying the critical performance factors (CPFs) of electronic business registers, it helps to translate diagnostic findings into actionable digital and institutional reforms and supports cross-regional comparability.

As a team working on improving and measuring business registration efficiency, we welcome the Guide as a coherent toolkit for building registries that are not only compliant but genuinely capable. Looking forward to seeing the Guide's CPFs measurable and adopted in practice - shifting the emphasis, where it belongs, from formal rules to functional outcomes and overall better economic performance of countries.

Andrea August
World Bank Group, Regulatory Efficiency
Senior Consultant and Business Entry
Topic Lead – Subnational Projects

Over the past two decades, business registries have moved from largely administrative functions to central components of national and international economic infrastructure. This evolution has been shaped by advances in technology and rising expectations around transparency, data quality, and the integrity of corporate information.

Through engagement with registry communities across multiple jurisdictions, many of the challenges faced by registrars are shared: managing the increasing volume and complexity of data, responding to evolving regulatory demands, and maintaining public trust in an environment where digital systems are both critical and exposed. While legal frameworks and institutional models differ, the underlying issues of governance, risk, and system design are remarkably consistent.

A recurring lesson from international practice is that successful registries are those that approach their role as system stewards rather than system operators. This requires a deliberate focus on data integrity, resilience, and user outcomes, supported by clear governance and a strong understanding of risk. It also requires the ability to adapt to technological change and shifting policy expectations in areas such as beneficial ownership transparency, interoperability, and cross-border information exchange.

The global registry community has developed a significant body of practical knowledge, often through experience gained in implementation rather than theory. Capturing that knowledge in a way that can be applied across jurisdictions is an important step in supporting more consistent and effective outcomes.

This Guide reflects that effort. It translates international experience into a form that is practical and adaptable, recognising that there is no single model for success. It provides a reference point against which registries can assess their own systems, identify priorities, and make informed decisions based on their specific context.

From the perspective of a registrar operating within an international financial centre, the importance of robust registry systems is evident. Confidence in the integrity of corporate information is fundamental to market participation, regulatory effectiveness, and international reputation. The ability to demonstrate that systems are well-governed, secure, and reliable is therefore both an operational requirement and a strategic one.

This publication will be of value to those responsible for registry systems at all stages of development. It supports a more structured approach to design and operation, while reinforcing the importance of leadership, collaboration, and continuous improvement.

I commend the contributors for their work and the global registry community for the experience and insight that underpin it.

Julian Lamb, CDIR, FCCA, FCSI
Registrar-General, IFC Oman
Former Executive Director and Registrar of Companies, Jersey Financial Services Commission (JFSC)
Former Board Member: IACA, EBRA, EBR, CRF

مـركـز عُـمـان المـالي العـالمي
International Financial Centre of Oman

Jersey Financial Services Commission

Much of the work of the public sector lies in giving practical effect to law. This is achieved not only through policy and regulation, but through the systems that enable those laws to operate in practice. Registers sit at the centre of this effort. They are the mechanisms through which legal identity is conferred, obligations are recorded, and transparency is delivered.

In the twenty-first century, these systems are no longer paper-based. They are increasingly digital, interconnected, and expected to operate in real time. Electronic business registries are now critical national infrastructure. They underpin economic activity, support regulatory oversight, and enable trusted data exchange across government and with the private sector.

This guide has been developed to support those responsible for the design, delivery, and operation of these systems. Its central aim is to ensure that jurisdictions embarking on this journey are able to benefit from the experience of others, avoiding common pitfalls and building on proven approaches. Too often, registry modernisation efforts repeat the same challenges. This Guide seeks to reduce that risk by capturing the practical lessons, insights, and accumulated wisdom of those who have already delivered electronic registry systems.

Building on the success of the Best Practices for Electronic Collateral Registries (2021), this Guide addresses the greater complexity of electronic business registries. It brings together legal, operational, and technical perspectives, and provides a structured toolkit for policymakers, registry leaders, and technology practitioners. Whether establishing a new register, modernising an existing one, or benchmarking current capability, this Guide is intended to support better decisions and more effective outcomes.

Ultimately, well-designed electronic business registries do more than record information. They enable trust, strengthen markets, and form a foundational component of a modern digital economy.

Justin Hygate
Chief Registry Officer – Foster Moore International Limited
Former Manager of the New Zealand Companies Office
Former Board Member of IACA

Foster Moore
The registry people

CONTENTS

LIST OF FIGURES

LIST OF TABLES

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
AICPA	American Institute of Certified Public Accountants
ALEI	Authoritative Legal Entity Identifier
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
BORIS	Beneficial Ownership Register Interconnection System
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
CFT	Combating the Financing of Terrorism
CIA	Confidentiality, Integrity, and Availability
CIPC	South Africa's Companies and Intellectual Property Commission
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
eID	electronic ID

EIF	European Interoperability Framework
ELF	Entity Legal Forms
ELI	European Law Institute
ETSI	European Telecommunications Standards Institute
EU	European Union
FATF	Financial Action Task Force
GATS	Global Aircraft Trading System
GDPR	European Union's General Data Protection Regulation
GmbH	Gesellschaft mit beschränkter Haftung
IACA	International Association of Commercial Administrators
ICT	Information and Communications Technology
idf	Interoperable Data Format
IdM	Identity Management
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFC	International Finance Corporation of the World Bank Group
IIA	Institute of Internal Auditors
IRI	Insolvency Registers Interconnection System
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
iXBRL	Inline eXtensible Business Reporting Language
JSON	JavaScript Object Notation
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
NIS2 Directive	European Union's Network and Information Security 2 Directive
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development

OWASP	Open Web Application Security Project
PAdES	PDF Advanced Electronic Signatures
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoLP	Principle of Least Privilege
RBAC	Role-Based Access Control
REST	Representational State Transfer
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	Société Anonyme
SNIA	Storage Networking Industry Association
SOAP	Simple Object Access Protocol
SOC 2	System and Organization Controls 2
SoD	Segregation of Duties
SP	Special Publication
SPOF	Single Point of Failure
TTPR	Trusted Third Party Repository
UBO	Ultimate Beneficial Owner
UCC	Uniform Commercial Code
UCD	User-Centred Design
UNCITRAL	United Nations Commission on International Trade Law
UNIDROIT	International Institute for the Unification of Private Law
UNODC	United Nations Office on Drugs and Crime
UX	User Experience
WCAG	Web Content Accessibility Guidelines
WS Security	Web Services Security
XAdES	XML Advanced Electronic Signature
XBRL	eXtensible Business Reporting Language
XML	Extensible Markup Language

CHAPTER ONE

Introduction

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 (CTCAP), supported by the UNIDROIT Foundation and Aviareto.[1] The CTCAP 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 Protocols to the Convention. 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 work. This Guide aims to extend the existing framework, which has already been successfully utilised to identify best practices for electronic collateral registries (ECRs), to encompass electronic business registries (EBRs). This expansion addresses core issues and considerations relating to their design, operation, and technological infrastructure taking into account the diversity of their operational and legislative environments.

This Guide is not a legislative guide and does not provide recommendations to legislators on reforming substantive business registration laws or institutional arrangements within individual jurisdictions. Rather, it is intended as an operational and technical reference framework. Its primary target audience consists of business registry operators, registrars, system architects, information technology specialists and other professionals involved in the design, implementation, management, and oversight of EBR systems. While policymakers and legislators may find the analysis informative, the Guide does not purport to prescribe legislative models or mandate specific institutional structures.

The nature of the Guide is therefore practical and implementation-oriented. It identifies a set of Critical Performance Factors (CPFs) that collectively form a comprehensive framework for evaluating and strengthening the performance of EBRs. The CPFs are designed to be technologically neutral and adaptable to different legal traditions, levels of digital maturity, and institutional configurations. By articulating internationally informed best practices, the Guide aims to support registry authorities in improving operational effectiveness, mitigating legal and technical risks, strengthening data quality, and reinforcing public trust while preserving flexibility for jurisdictions to tailor solutions to their domestic contexts.

A. SCOPE: ELECTRONIC BUSINESS REGISTRIES

Digital transformation has fundamentally impacted both the public and private sectors. Governments increasingly adopt electronic service delivery for business registration in response to growing demands from residents and businesses for faster, more accessible, and more convenient services. Electronic

[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).

registries have emerged as a cornerstone of systems that collect, store, and disseminate data, and, in some cases, establish and transfer property rights. Even where domestic laws do not specify the use of best practices, registry operators may be liable for system failures that result in losses to their users.

While not all business registries are fully electronic, most 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 EBRs, covering 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 enable the electronic processing, validation or automated exchange of structured data that are defining operational characteristics of EBRs. Registries operating in these models may nonetheless find the framework useful as a reference when planning their transition to electronic services.

Accordingly, the purpose of this Guide is to provide guidance to the designers and operators of EBR 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, which enhances efficiency, accessibility,[4] and transparency. 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 tax authorities, 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 managed by an administrative authority, like in the United Kingdom, Australia, and Canada, or placed under a judicial system, like in Paraguay, France, or Germany.

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, as seen in Paraguay and the Netherlands.

---

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

[3] United Nations Commission on International Trade Law, *UNCITRAL Legislative Guide on Key Principles of a Business Registry* (2018) 28 <https://uncitral.un.org/en/texts/msmes/legislativeguides/business_registry> accessed 3 April 2026 ('UNCITRAL Legislative Guide').

[4] To enhance Accessibility, electronic business registration should be designed and operated in accordance with the dedicated Accessibility principles. On an international level, these principles are outlined in the Web Content Accessibility Guidelines. See CPF 2 on Accessibility.

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, whereas the Greek 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 and electronic Trade Register extracts are available free of charge, while fees are charged for other data, financial statements, translated extracts, and organisation rules (articles of association, partnership agreements, by-laws, or rules). Certain jurisdictions impose restrictions on the reuse of registry data or limit access to commercial service providers.

Centralised or Decentralised Registry

- In a centralised model, such as in Belgium, Chile, Singapore, and Bangladesh, a single national authority manages the entire registration lifecycle, database, and legal enforcement for the whole country. Decentralisation occurs when the authority to register businesses and maintain records is distributed across sub-national entities or different administrative layers. In countries with a federalist structure, where provinces or states have independent legislative power, jurisdictional decentralisation takes place. For instance, a business registered in Ontario, Canada, is not automatically registered in Quebec, Canada. Decentralisation can also occur administratively, where the registration powers are delegated to the local level rather than performed by a central agency. In Spain, each province maintains its own business register ('Registro Mercantil') with the registrars responsible for registering companies, while a Central business register ('Registro Mercantil Central') coordinates name reservations and publishes business information nationwide.

1.1. Registry Functions

The traditional role of a business registry is to provide businesses with a legal personality that is recognised by the jurisdiction and to serve as an official repository of information related to registered businesses accessible to the public.[5]

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

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

[5] Depending on the jurisdiction, some legal forms of the business may have legal personality without mandatory registration with the business registry, and, should such a business choose to get registered, the registry's main purpose is then to publicise its legal status.

(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.[6]

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.

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.

Table 1: Registry functions.

1.1.1. Data collection

The business registry is responsible for collecting and, in many cases, verifying data related to registered entities. This may include 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 typically 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 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 the information recorded in them.

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

[6] UNCITRAL Legislative Guide, Recommendation 10.

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. Considering 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.

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 scope of information that EBRs make publicly available varies considerably across jurisdictions, which are shaped by divergent privacy and transparency requirements (see Annexe I to this Guide for an overview).

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.

1.2. The evolving role of business registries

In today's dynamic business landscape, the traditional role of business registries has transitioned from record-keepers into efficient service providers with multifaceted responsibilities. Contemporary business registries are increasingly significant for economic development and governance. They achieve this, in part, by leveraging their vast datasets to provide transparency and generate valuable insights that benefit policymakers, researchers, financial institutions, and businesses, as described in Section 1.1.3.

Furthermore, business registries are instrumental for economic growth and investment facilitation by enabling online business registration, once the requirements set by the applicable law are fulfilled, and by providing accessible, reliable, and up-to-date data.[7] 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.

[7] 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: United Nations Conference on Trade and Development, World Investment Report 2024 (2024) ch 4 'Investment Facilitation and Digital Government' <https://unctad.org/system/files/official-document/wir2024_ch04_en.pdf> accessed 3 April 2026.

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 transparency. The World Bank's Data-Driven Company Registry Guidance Note[8] highlights this expanded role, underlining the prevention of fraud as an imperative for modern business registries. To effectively meet this challenge, registries not only integrate data from various governmental and financial systems but also employ 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 early detection of non-compliance and actively contribute to fostering a culture of tax responsibility among businesses.

1.3. The evolving role of business registrars

In parallel with the transformation in the role of the business registry, a similar evolution is altering the responsibilities of the registrar. The traditional perception of the registrar as an administrator of records has shifted to encompass strategic oversight and adept navigation of dynamic legal, regulatory, technological, and business frameworks shaped by national laws and international and regional practices.

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, legally informed approach, exercising its functions with due diligence and transparency.[9] This transformative leadership 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 a wide range of 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.

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 a best practice for EBRs.

Essentially, automation refers to actions carried out by computer systems without the necessary review or intervention of a natural person.[10] 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.[11] For instance, automated checks and alerts monitoring changes within the registry and relevant external data

---

[8] World Bank Group, Data-Driven Company Registry: Guidance Note (2022) <https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf> accessed 3 April 2026.

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

[10] United Nations Commission on International Trade Law, UNCITRAL Model Law on Automated Contracting (2025) <https://uncitral.un.org/en/mlac> accessed 3 April 2026.

[11] Investment Climate Advisory Services (World Bank Group), Innovative Solutions for Business Entry Reforms: A Global Analysis (2012) <https://documents1.worldbank.org/curated/en/196211468137721462/pdf/770990WP0inves0B00PUBLIC00july02012.pdf> accessed 3 April 2026.

sources, or 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 contribute to transparent and predictable EBR operation and increase businesses' trust.

Automation may also be viewed from the perspective of registry users. Where reliable information is already available to the registry through trusted external sources, automation can reduce or eliminate the need for users to repeatedly submit the same data (see 'once-only' principle in CPF 14 on Interoperability). Through interoperability with population registers, tax authorities, or other public databases, certain registration or change events may be generated and processed automatically. For example, a change in the legal name of a natural person recorded in a population registry may trigger an automated update in the business registry without requiring a separate application. Such approaches can reduce administrative burden for users, improve data consistency across public systems, and further mitigate the risk of inaccurate or outdated registry records.

Legislation directly impacts the level of automation of business registries. Clear and 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.[12]

Despite its advantages, automation may also introduce challenges. Often, automated and interactive machine-to-machine Access Control is introduced in an *ad hoc* manner by system administrators, vendors, or integrators, leading to a lack of formal lifecycle management processes.[13] This underlines the need for a systematic approach to automating processes and systems, ensuring that automation is implemented with robust design, testing, maintenance and risk management. This is particularly relevant for company registries, where, according to a 2025 survey conducted by Business Registry Insights with 84 participating jurisdictions, only 28.57% of registration applications are fully automated, 54.76% are partly automated, and 16.67% are manually processed — highlighting a significant opportunity to systematise and secure these operations.[14] 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.[15] 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.[16] In these cases, phased implementation is advisable, starting with basic electronic services and progressively integrating more advanced functionalities as infrastructure improves.[17]

---

12 Innovative Solutions for Business Entry Reforms (n 11).

13 National Institute of Standards and Technology, Security of Interactive and Automated Access Management Using Secure Shell (SSH) (NIST IR 7966, 2015) <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf> accessed 3 April 2026.

14 Business Registry Insights, 'E-Services' (2025) <https://br-insights.org/reports-dashboards/e-services-2022/> accessed 3 April 2026.

15 Innovative Solutions for Business Entry Reforms (n 11).

16 John R Willie and others, 'Business Regulation – Leveraging Technology to Support Business Registration Reform: Insights from Recent Country Experience' (World Bank, Investment Climate in Practice 2011) <https://openknowledge.worldbank.org/server/api/core/bitstreams/3c6df1c2-0bcd-5f45-92b8-996e935c7ab7/content> accessed 3 April 2026.

17 UNCITRAL Legislative Guide.

Significant automation of business registration procedures can be achieved, requiring minimal intervention from the registrar to process applications and issue decisions on initial registrations or registration changes. The advanced level of automation may allow EBRs to take *decision-making* actions carried out by computer systems with limited oversight by a natural person,[18] for instance, facilitating 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 shifts the registrar's focus from checking and processing registration applications to continuously monitoring and improving EBR data management and algorithms.[19]

The broad term 'automated system' encompasses, among 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.[20] Such technologies, including AI and ML, are increasingly used by EBRs and have the potential to further enhance their functionality. These technologies can be used for decision-making and optimising various registry functions, from automating document verification, customer support, and predictive analytics for identifying potential fraud or non-compliance, to refining backup management.[21] A 2025 survey reflects this trend, showing a 25.60% increase in respondents developing, using, or planning to use new digital services since 2022.[22] However, given the emerging nature of these technologies and the wide variety of standards and regulatory frameworks surrounding them, the present Guide does not examine 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 a recommended infrastructure solution for EBRs, offering scalability, efficiency and enhanced reliability through, for instance, elastic storage, automated disaster recovery, centralised hosting, and instantaneous data backup, capabilities particularly valuable for registries that must maintain continuous public availability and handle variable demand.[23] Cloud adoption in the EBR context, however, raises specific considerations that operators should address; these include jurisdictional requirements governing where registry data may be stored and processed, multi-tenancy risks in shared cloud environments, and dependency on third-party service continuity. Cloud security standards such as ISO/IEC 27017 and the Security Guidance from the Cloud Security Alliance 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. All CPFs defined in this Guide apply regardless of the technological infrastructure adopted.

---

18 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 (n 10) and European Law Institute, 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> accessed 3 April 2026.

19 World Bank Group, Data-Driven Company Registry: Guidance Note (n 8).

20 UNCITRAL Model Law on Automated Contracting (n 10) para 29.

21 Organisation for Economic Co-operation and Development, Governing with Artificial Intelligence: Are Governments Ready? (OECD Artificial Intelligence Papers No 20, OECD Publishing 2024) <https://doi.org/10.1787/26324bc2-en> accessed 3 April 2026.

22 Business Registry Insights, 'E-Services' (n 14).

23 A.P. Amadi-Echendu and J.E. Amadi-Echendu, 'A Study on Data and Information Integration for Conveyancing, Cadastre and Land Registry Automation' in Proceedings of PICMET' 16: Technology Management for Social Innovation (2016) <https://ieeexplore.ieee.org/document/7806611> accessed 3 April 2026. See more World Bank Group, Institutional and Procurement Practice Note on Cloud Computing: Cloud Assessment Framework and Evaluation Methodology (Equitable Growth, Finance and Institutions Insight, World Bank Group) <http://documents.worldbank.org/curated/en/099114503072319732> accessed 3 April 2026; Khuram Farooq, Joseph Huntington La Cascia, Knut J Leipold, Bertram Boie, Data Classification Matrix and Cloud Assessment Framework: Cloud Assessment Framework and Evaluation Methodology (English) (Equitable Growth, Finance and Institutions Insight, Report No 180672, World Bank Group) <http://documents.worldbank.org/curated/en/099114503072340316> accessed 3 April 2026.

Automation and cloud computing are best practices for modern EBRs, augmenting their operational efficiency, reducing errors, and promoting transparency. Nevertheless, their effectiveness is contingent upon a sound governance framework, ongoing risk assessments, and reliable infrastructure.

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

This Guide applies the best practices identified in the context of ECRs to EBRs and identifies additional best practices specific to this type of registry. In this context, 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.[24] Beyond mitigating operational risks and liabilities, best practices also ensure that the systems are continuously available, accessible to all users, transparent and efficient.

Prior to the 2022 survey on e-services conducted by International Business Registry Report, few studies had explored best practices for EBRs.[25] With responses from 88 jurisdictions, the survey results 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 planned to adopt digital identity authentication to better perform and secure their services. The updated 2025 survey illustrates developments since 2022, with more recent data showing a 2% increase in respondents accepting electronic applications, along with a 2.44% rise in those intending to transition to fully electronic services. These trends underscore the continued momentum toward digitalisation and reaffirm the pressing need for a comprehensive best practices framework.[26]

The concept of best practice most commonly arises in organisational and manufacturing management, where a set of actions can be related to resulting outcomes.[27] Determining a best practice, therefore requires a comparison of actions and outcomes where there is a known causal relationship between the two.[28] Moreover, to identify the best practice, the comparison must include all relevant cases; otherwise, the best practice might be overlooked.[29] Importantly, to be comparable, whether statistically or based on human judgment, the causal relationship between actions and outcomes must be scientifically quantifiable.[30] In practice, the above conditions are rarely all met simultaneously.[31] Different styles of research, whether economic or technical, tend to produce incomplete or divergent insights and conclusions.[32]

Given these challenges, the Guide draws on authoritative standards of recommended or mandated practices, rather than solely comparing existing industry practices. These include standards issued by international standards bodies, such as the International Organization for Standardization (ISO); government agencies, such as the National Institute of Standards and Technology (NIST); industrial organisations, such as the Institute of Electrical and Electronics Engineers (IEEE); and other

---

24 *Cambridge Dictionary*, 'best practice' <https://dictionary.cambridge.org/us/dictionary/english/best-practice> accessed 3 April 2026.

25 The 2022 survey conducted by International Business Registry Report 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 International Business Registry Report, 'E-Services' (2022) < https://br-insights.org/reports-dashboards/e-services-2022/> accessed 3 April 2026.

26 The 2025 edition collected responses from 84 jurisdictions and maintains broadly consistent regional coverage, with 59 jurisdictions participating in both the 2022 and 2025 surveys, enabling a comparative analysis of E-Services progress between the years. See more Business Registry Insights, 'E-Services' (n 14).

27 S Bretschneider and others, '"Best Practices" Research: A Methodological Guide for the Perplexed' (2005) 15(2) Journal of Public Administration Research and Theory 307.

28 Bretschneider and others, '"Best Practices" Research' (n 27) 310.

29 Bretschneider and others, '"Best Practices" Research' (n 27).

30 Bretschneider and others, '"Best Practices" Research' (n 27) 311.

31 Bretschneider and others, '"Best Practices" Research' (n 27).

32 Michael Cusumano, *In Search of Best Practice: Enduring Ideas in Strategy and Innovation* (Oxford University Press, 2010) 11.

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.[33] Respondents reported that the most stringently controlled best practices were those related to database security, high availability resilience, and disaster recovery.[34] 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.[35]

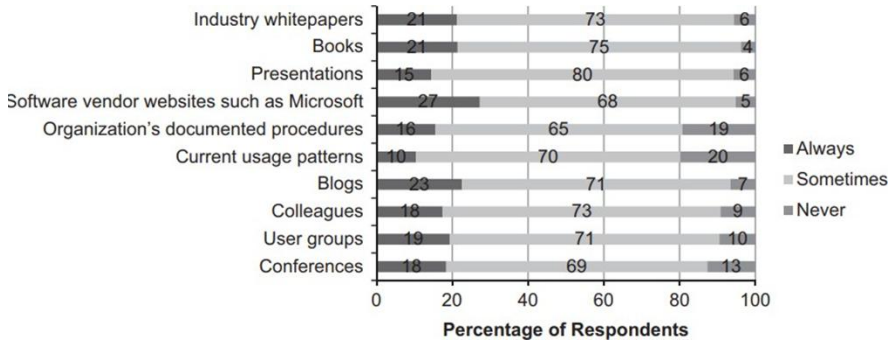


Figure 1: Responses to the question: Where do you personally find database best practice guidelines to follow? [36]

The ECR Guide identified 17 CPFs, which are registry system properties and processes essential to a collateral registry's ability to perform its core functions at a level that meets the reasonable expectations of relevant market participants. While all of those 17 CPFs remain largely applicable and reusable in the context of EBRs, two of them have been merged into one for clarity (new CPF 18 on Retention and Disposition), and eight additional CPFs have been specifically identified for EBRs. Importantly, although the EBR Guide is informed by the ECR Guide framework, it is structured as a self-contained document with some terminology and aspects of best practices from the ECR Guide adjusted for the specificities of EBRs.

The diligent implementation of the practices set out in the CPFs would result in a registry that is:

- authenticated and governed by robust access control, with identities verified and interactions validated through secure methods, and clearly defined roles determining who may read, modify or delete data;
- accessible to all users, including persons with disabilities, through usable, inclusive, and publicly searchable interfaces and services;
- accurate in its records, with data validated at the point of entry, errors detected as they arise, and corrections made through defined and auditable processes;
- available, reliable, and continuously operational, with consistent performance, adequate capacity during peak usage, and redundancy mechanisms that prevent single points of failure;

33 Victoria Holt and others, 'The Usage of Best Practices and Procedures in the Database Community' (2015) 49 Information Systems 163, 164–168 <http://dx.doi.org/10.1016/j.is.2014.12.004> accessed 3 April 2026.

34 Holt and others, 'The Usage of Best Practices' (n 33) 168, 170.

35 Holt and others, 'The Usage of Best Practices' (n 33) 163–181.

36 Holt and others, 'The Usage of Best Practices' (n 33) 169.

- capable of providing confidentiality and privacy, protecting stored and transmitted information from unauthorised disclosure in accordance with applicable legal requirements;
- committed to continual improvement, informed by lessons learned, feedback, and performance assessments, consciously avoiding legacy systems;
- capable of ensuring evidentiary value and integrity of its records, with entries that are tamper-proof, auditable, and meet the standards required for reliance by courts and authorities;
- interoperable, using open standards and APIs to exchange data with other systems efficiently and securely;
- operating within the mandate of its legal authority and compliant with applicable legal and regulatory requirements;
- retaining the records for as long as legally required and able to dispose of them in a manner that preserves the registry's historical integrity;
- governed by a structured risk management framework, actively managing internal and external threats, including unauthorised access, tampering, malware, and denial of service attacks;
- operating systems that have been validated against defined performance and security requirements and continue to be monitored throughout their deployment;
- timely in processing registrations, updates, and responses, ensuring that delays do not undermine legal certainty or business transactions;
- transparent and trusted by users and authorities alike, with clear and accessible information provided about its processes and maintaining a demonstrated record of reliability, security, and legal soundness; and
- user-centred in its design, with interfaces and workflows that are intuitive and minimise the risk of user error.

Following best practices is important not only to implement the registry's legal mandate but also to enhance its performance and credibility. Globally, adherence to shared best practices creates conditions for interoperability and cross-border collaboration. At the same time, best practices should not be applied in a rigid manner; their implementation must be contextual, thoughtfully tailored to the specific legal, economic, and technological environment of each jurisdiction. The CPF framework in this Guide is designed to support this balance between international standards and contextually grounded application.

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 are 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 enhances 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.[37] 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.[38] 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. As the British Computer Society (BCS) points out, 'it is perfectly possible to be fully compliant with the standard, but be insecure'.[39] 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.

Independent validation is a practical complement to standard adoption. EBRs are encouraged to commission annual security audits by information security professionals, with progress reviews to track remediation of identified issues. This external perspective helps verify whether selected controls are performing as intended in the specific operational context of the registry. This Guide does not make recommendations regarding the pursuit of formal certification in any of the standards it references; certification decisions remain a matter for each registry to assess in light of its legal obligations and resources available.

To guide selective and responsible adoption of proposed best practices and recommended standards, 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 supports informed and responsible decision-making.

F. LEGAL RELEVANCE OF BEST PRACTICES

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

[37] International Organization for Standardization, ISO/IEC 27002: Information Security, Cybersecurity and Privacy Protection — Information Security Controls (2022).

[38] ISO/IEC 27002 (n 37).

[39] Id. BCS, 'Why ISO 27001 Is Not Enough' (2009) <https://www.bcs.org/articles-opinion-and-research/why-iso-27001-is-not-enough/> accessed 3 April 2026.

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), the NIS2 Directive (Network and Information Security Directive) affects the implementation of security measures in EBRs operating in EU Member States.

EBR operations are 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 AML and CFT policies,[40] while the EU develops binding legal instruments, such as the Company Law Directive 2017/1132[41] and Directives 2019/1151[42] and 2025/25[43] 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. 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 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.[44] Therefore, registrars should carefully consider how liability arises in their jurisdiction and use this understanding to conduct risk assessments that determine how the registry should be designed, built and operated.

At the same time, it is important to recognise that a gap may exist between adherence to *best practices* and the threshold for legal liability under domestic law. In many legal systems, liability is triggered only where a registry or registrar fails to meet a standard of *reasonable or ordinary care*, rather than by reference to best practices as such. As a result, the legal consequences of non-compliance with best practices may be limited or indirect, even where such practices represent a higher benchmark for performance, security, and trustworthiness.

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:

---

40 Financial Action Task Force, The FATF Recommendations (2012, updated 2025) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> accessed 3 April 2026.

41 Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law [2017] OJ L169/46.

42 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 [2019] OJ L186/80.

43 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 [2025] OJ L 25.

44 Liability regimes applicable to EBRs vary considerably across jurisdictions. In Austria, the Federal Government is subject to a statutory strict liability regime for damage caused by errors in the use of information and communication technologies in public registers, irrespective of fault, subject to limited exceptions for unavoidable events (Act on the Organisation of the Courts (GOG), Austria, § 89e). By contrast, in the United Kingdom, registry liability is assessed primarily under general principles of negligence, with courts recognising a duty of care in respect of clerical or ministerial errors, requiring proof that reasonable care was not exercised (Companies Act 2006, ss 1080 and 1098; *Sebry v Companies House* [2015]). In Estonia, compensatory damages are awarded only where the registrar acted unlawfully and with culpability (Commercial Register Act, Estonia, § 67), while in Singapore, qualified immunity is provided to registry officials acting in good faith and with reasonable care (Accounting and Corporate Regulatory Authority Act 2004, Singapore, s 11).

(i) errors or omissions by the registry officers/employees and contracted third parties (operation only);
(j) infrastructure failure attributable to hardware (design and operation);
(k) infrastructure failure attributable to software (design and operation); and
(l) unexpected outcomes or unexpected actions (design and operation).

Category (d) may encompass, for example, outputs generated by automated decision-making systems that produce legally consequential results not anticipated by the system's designers or the applicable regulatory framework. Unlike category (d), where the treatment of unforeseen consequences is still evolving,[45] liability arising from events in the first three categories is typically based on error or negligence, on the basis of an avoidable failure. Examples of avoidable failures in these categories include:

1. human error by an officer manually entering a court order discharging a registration or selecting the wrong company which has gone into liquidation;
2. failure of a hardware component of infrastructure that could have been prevented by implementing a redundancy principle in design; and
3. error in the programming of a software component of infrastructure 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 known 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 vulnerability, resulting in unauthorised access to, and the modification and deletion of, registry data. While the underlying software design flaw (category (c) above) could not, for the purposes of this example, have been prevented, the registrar's failure to react to the notification may constitute an error or omission (category (a) above), and the registrar may incur liability for damages caused by the cyberattack, subject to the applicable legal framework.

In an even more extreme scenario, a system error or inadequacy (e.g., in the process of authenticating registrants) may not be discovered until legal proceedings are underway. Such an event may raise uncertainty not only about registrations performed by a particular user but also about all past registrations in the registry system, undermining the evidentiary value of the registry as a whole.[46]

The legal relevance of best practices in the context of EBRs is therefore nuanced. 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. International instruments and standards, such as those set by the FATF, the EU, and the UNCITRAL, help to delineate the scope of the registrar's responsibilities and potential exposure to liability. 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. Reliance solely on minimum legal standards of care may address immediate exposure to liability but can undermine data quality, public confidence, and the evidentiary value of the registry over time. Accordingly, the adoption of best practices should be understood not as a legal obligation in itself, but as a strategic and preventative measure that supports the registrar's duty of diligence, strengthens institutional resilience, and mitigates legal, operational, and reputational risks across different liability regimes.

---

[45] 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 (n 10); Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (n 18); 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 [2024] OJ L2853. UNIDROIT has also included a new 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> accessed 3 April 2026.

[46] Rob Cowan and Donal Gallagher, 'The International Registry for Aircraft Equipment—The First Seven Years: What We Have Learned' (2014) 45 UCC Law Journal 225, 249 <https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan- Gallagher.pdf> accessed 3 April 2026.

I. INTRODUCTION

This Guide draws on the earlier work of the Project[47] 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 risk management in EBRs in more detail. Chapter IV presents a conclusion for the Guide, followed by a Glossary of terms. Annexe I provides an overview of the international framework on the scope of publicly disclosed information by EBRs, and Annexe II provides a detailed summary of identified relevant technical standards, which may be used as a reference for the CPFs in the present Guide.

[47] See Aaron Ceross, Practices in Electronic Registries (Interim Report, Spring 2018) prepared 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 <https://www.law.ox.ac.uk/best-practices-in-the-field-of-electronic/best-practices-field-electronic-registry-design-and> accessed 3 April 2026.

CHAPTER TWO

Critical Performance Factors

II. CRITICAL PERFORMANCE FACTORS

This Chapter provides definitions and detailed descriptions of the CPFs and explains their relevance to EBRs. Table 2 lists each CPF along with its definition. Most CPFs combine descriptions with a technical discussion that references international standards and a legal discussion that references relevant laws and legal standards. For other CPFs, the discussion is limited to either technical or legal aspects.

CRITICAL PERFORMANCE FACTORS

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 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 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 property of considering time in the context of system design and operations.

Transparency

The property 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 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.

Table 2: CPF definitions (in alphabetical order).[48]

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 (for more details, see CPF 4 on Authentication), to arrangements where only specific users can access resources requiring verified credentials.

Upon authentication, 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)[49], which ensures that 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 do not

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

[49] ISO/IEC 27002 (n 37) 27, 5.15 'Access control': see also National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Rev 5, 2020) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> accessed 3 April 2026.

have access, for instance, to the data intended for the registry staff. This reduces the risk of accidental or malicious misuse of registry data or functions. In addition, segregation of duties (SoD)[50] 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.

Modern Access Control paradigms include role-based access control (RBAC),[51] attribute-based access control (ABAC),[52] zero-trust architecture,[53] and discretionary access control (DAC).[54] For EBRs, RBAC is generally the most appropriate baseline approach, given that registry user roles are typically stable (public users, registrants, intermediaries, registry staff, and system administrators). RBAC maps cleanly onto these categories and supports auditability. ABAC provides a useful complement when contextual factors are relevant, for example, restricting certain Application Programming Interfaces (APIs) access by jurisdiction, time of day, or volume thresholds. Zero-trust architecture, which assumes no user or system is inherently trusted and requires continuous verification, is particularly appropriate for internal staff access and machine-to-machine integrations, where the consequences of a compromised trusted account are most severe. DAC, which allows resource owners to grant access at their discretion, may be less suitable for registries operating under regulatory frameworks, where access policies must be uniformly applied and auditable rather than delegated to users.

Entities are authorised, and access rights and privileges are managed by issuing credentials or tokens to designated entities. Upon each attempt to access registry functions, for example, 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 accessible on the European e-Justice Portal through the Business Register Interconnection System (BRIS) is available without authentication. Access Control levels depend on the EBR's policy and relevant legislation, which is further elaborated in CPF 6 on Confidentiality and Privacy.

Access Control applies to all interactions with registry, including direct user access to a registry function or data, interoperability with other registries, APIs,[55] and intermediaries. It also extends to physical access to registry locations and infrastructure, such as the use of identification badges, biometric sensors, closed-circuit television, locks, or other security measures. Physical Access Control prevents unauthorised actors from gaining material access to registry data or its infrastructure.[56]

Various controls can be implemented to counter attempts to gain unauthorised access, including automatically terminating sessions that are inactive for a certain period and deploying bot-detection and automated-access-deterrence measures. Simple Completely Automated Public Turing test to tell

---

50 ISO/IEC 27002 (n 37) 27, 5.3 'Segregation of Duties'.

51 InterNational Committee for Information Technology Standards, INCITS 359-2012 (R2022): Information Technology — Role Based Access Control (2012, revised 2022) <https://webstore.ansi.org/standards/incits/incits3592012r2022?source=blog&_gl=1*16xxwwu*_gcl_au*NzAyOTA1OTE2LjE3NDA2OTgwNDU> accessed 3 April 2026.

52 National Institute of Standards and Technology, Guide to Attribute Based Access Control (ABAC) Definition and Considerations (NIST Special Publication 800-162, 2014) <https://csrc.nist.gov/pubs/sp/800/162/upd2/final> accessed 3 April 2026.

53 Scott W Rose, Oliver Borchert, Stuart Mitchell and Sean Connelly, Zero Trust Architecture (NIST Special Publication 800-207, National Institute of Standards and Technology 2020) <https://www.nist.gov/publications/zero-trust-architecture> accessed 3 April 2026.

54 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

55 Amazon Web Services, 'What Is an API (Application Programming Interface)?' <https://aws.amazon.com/what-is/api/> accessed 3 April 2026. 2025 Survey data reflects that many registries are moving in this direction: approximately half currently offer API access to both public and private users, while 21.43% restrict it to government agencies or other public organisations. See Business Registry Insights, 'E-Services' (n 14).

56 See International Finance Corporation, Secured Transactions, Collateral Registries and Movable Asset-Based Financing (IFC Knowledge Guide 2019) 84 <https://documents1.worldbank.org/curated/en/193261570112901451/pdf/Knowledge-Guide.pdf> accessed 3 April 2026.

Computers and Humans Apart (CAPTCHA)[57] mechanisms can be used together with behavioural analytics which analyse mouse movement and typing rhythm to distinguish human users from automated scripts, and risk-based authentication which adjusts verification based on device, location, or access history, or device fingerprinting. Governance policies and arrangements should underpin all these controls, including 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. The 2024 Insider Threat Report, based on responses 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 11-20 incidents. When asked to estimate the average cost of remediation after an insider attack, the most common response, reported by 32% of organisations, was estimated as $100K to $499K.[58] Organisational measures, such as pre-employment screening and regular training for trusted insiders (including employees, contractors, and vendors who have access to the registry), are essential. The PoLP mentioned above serves to minimise such risks, ensuring that access authorisations do not exceed what is strictly necessary for employees' tasks. The 'super-users' who have administrative rights to access data, even temporarily, should be subject to greater levels of scrutiny.[59]

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. The deterrent effect of audit logging is strongest where logs are demonstrably tamper-resistant and where users and staff are aware that their access is recorded.

Technical

ISO/IEC 27000 defines Access Control as ensuring that access to assets is authorised and restricted based on business and security requirements.[60] ISO/IEC 27001 provides a framework for organisations to establish appropriate authorisation mechanisms as part of their broader information security management practices.[61] Annex A of ISO/IEC 27001 contains a set of Access Control measures, 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. Each control in Annex A is associated with a specific security objective which contributes to the principles of confidentiality, integrity and availability of information.

NIST also recommends that all United States (US) federal government information systems enforce Access Control policies that limit access to authorised users.[62]

Legal

National legislation, usually company laws and regulations, provides a framework for implementing Access Controls and security measures within the registry to prevent corporate identity theft or unauthorised individuals from acting on behalf of the entity. For example, it is often a legal requirement that data submitted to the business registry must come from a legal entity acting through its

57 With a simple CAPTCHA, users must correctly identify numbers or letters contained in randomly generated CAPTCHA images to continue their session.

58 Cybersecurity Insiders and Gurucul, 2024 Insider Threat Report (2024) <https://gurucul.com/2024-insider-threat-report/> accessed 3 April 2026.

59 For instance, monitoring measures could include capture and review of access activities associated with exceptional access to demonstrate compliance with Access Control policies.

60 International Organization for Standardization, ISO/IEC 27000 family — Information Security Management (2022).

61 International Organization for Standardization, ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements (2022).

62 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

management or 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.

Similarly, according to Recommendation 21 of the UNCITRAL Legislative Guide,[63] 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).

2. Accessibility

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

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.[64] To this end, a registry system and registry services should be designed considering a range of physical and intellectual abilities, as well as cultural and linguistic diversity,[65] 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.[66] In some jurisdictions, equal access is also a legal obligation; for example, accommodations may be required for sight-impaired users and users with intellectual disabilities.

From a technological perspective, Accessibility implies that 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.

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 operates within the boundaries established by Access Control measures (see CPF 1 on Access Control). In other words, Accessibility governs how easily eligible users can reach and use the services they are entitled to, while Access Control governs who is entitled to access what, and on what terms.

63 UNCITRAL Legislative Guide, Recommendation 21.

64 UNCITRAL Legislative Guide, Recommendation 4.

65 For EBRs operating in jurisdictions with more than one official language, it is recommended that the publicly available registry information be available in all such languages, in accordance with applicable language laws. At the same time, registrants should be permitted to submit information or documentation in only one language. The provision of registry data, forms, and user instructions in additional languages may further enhance Accessibility and may be supported, where appropriate, using machine translation tools. Registries should clearly publicise which language(s) they accept for information and documentation, and which character sets are used by the system. Accuracy across languages could be supported by the acceptance of certified translations where required. See more UNCITRAL Legislative Guide, paras. 133 -135, 194, 197.

66 UNCITRAL Legislative Guide, Recommendation 33.

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
• Maximise **compatibility** with current and future user tools.

Figure 2: The four WCAG Principles.[67]

The Web Content Accessibility Guidelines (WCAG) developed by the World Wide Web Consortium (W3C) provide a widely adopted framework with recommendations for making web pages accessible to a broad range of people with disabilities (see Figure 2 above). These guidelines are based on four foundational principles, that information, user interface, and navigation must be: (i) perceivable, (ii) operable, (iii) understandable, and (iv) robust.[68] Following the WCAG also often makes web content more usable in general (see CPF 24 on User-Centred Design).

Access to EBRs is generally provided through the internet. Where access is provided through intermediaries, the registrar should ensure that the intermediaries grant registry access equivalent to that available to direct users of the registry. Additional access to the registry can be provided via telephone services, subscription services, ordering services to enable access to various products, and delivery services of various products, such as transcripts of publicly available registered information on business.[69]

In light of this, 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 with limited digital literacy skills are not excluded from

[67] World Wide Web Consortium (W3C), Web Content Accessibility Guidelines (WCAG) 2.2 (2024) <https://www.w3.org/TR/WCAG> accessed 3 April 2026.

[68] World Wide Web Consortium (W3C), 'WCAG 2 at a Glance' <https://www.w3.org/WAI/standards-guidelines/wcag/glance> accessed 3 April 2026.

[69] UNCITRAL Legislative Guide, para. 193.

essential registry services.[70] 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

ISO/IEC 40500 is an approved international standard developed based on the WCAG 2.0 and updated to reflect WCAG 2.2 principles, guidelines, success criteria, and sufficient and advisory techniques.[71] These guidelines cover a wide range of disabilities, including visual, auditory, physical, speech, cognitive, language, learning, and neurological impairments in a non-technology-specific way. They also aim to make web content more usable for older individuals with changing abilities due to ageing.[72]

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.[73]

Recommendation 39 of the UNCITRAL Legislative Guide further sets out that the law should ensure easy access to public information about registered businesses.[74] 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.

In the EU, the Web Accessibility Directive (Directive (EU) 2016/2102) creates binding legal obligations for public sector bodies to ensure that their websites and mobile applications meet Accessibility standards of WCAG 2.1 Level AA.[75] Under the Directive, registries should publish and maintain an Accessibility statement describing the conformance status of their digital services, identifying any content that does not meet the standard and the reasons for the exemption, and providing a mechanism for users to report Accessibility failures and request accessible alternatives.

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

[70] OECD, OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age (OECD Public Governance Policy Papers No 23, OECD Publishing 2022) <https://doi.org/10.1787/2ade500b-en> accessed 3 April 2026.

[71] See WCAG 2.2 (n 67).

[72] International Organization for Standardization and International Electrotechnical Commission, Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.2 (ISO/IEC 40500, 2012).

[73] UNCITRAL Legislative Guide, Recommendations 32, 33, 35.

[74] UNCITRAL Legislative Guide, Recommendation 39.

[75] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies [2016] OJ L327/1.

a business that has been independently audited in accordance with the appropriate accounting standards with only immaterial errors allowed, which do not need to be corrected.[76] Other registered data may, of course, be located at a different point on the Accuracy spectrum.

Accuracy requires the registrar to consider three interrelated questions in designing and operating an EBR: (i) what is the purpose of the data, (ii) how accurate does the data need to be, given its purpose, and (iii) how can a user of the data assess its Accuracy.

In addressing the first question, the registrar should consider the relevant legislation, regulatory policy concerns, who is entitled to access the information and for what legal purpose. If business accounts published on the register are accurate enough for their purpose, they are sufficient. Other data may be less accurate but still adequate 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 during an audit, there may be periods 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.

The second question should be addressed through the lens of CPF 19 on 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 a required 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 registrar will have very high standards to ensure adequate Accuracy. In this case, the user may be satisfied to assume high Accuracy of the registry data. Otherwise, it would need to assess the data Accuracy; the factors that would influence the assessment would include data provenance, such as when the data was uploaded,[77] 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 legislation authorising the registrar to adopt a more proactive approach in ensuring Accuracy to prevent abuse of UK corporate structures. While Accuracy operates as a spectrum, international legal instruments establish minimum compliance thresholds, below which legal obligations are triggered regardless of context.

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.[78] Jurisdictions are required to have mechanisms that ensure BO information remains accurate and updated within a reasonable period

[76] For a discussion of materiality under International Auditing Standards, see Financial Reporting Council, ISA (UK) 320: Materiality in Planning and Performing an Audit (May 2022) <https://media.frc.org.uk/documents/ISA_UK_320_Updated_May_2022_aJAQtFV.pdf> accessed 3 April 2026.

[77] 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.

[78] The FATF Recommendations (n 40).

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 ensure 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.[79]

Thirdly, the Economic Crime and Corporate Transparency Act aims to promote the integrity of UK registries to combat economic crime and boost confidence in the UK economy. It introduces new statutory objectives and grants the registrar of companies enhanced powers to fulfil their mandate.[80] The registrar's new objectives include, *inter alia*, ensuring that information contained in the register is accurate and that the register contains everything it ought to contain, and ensuring that records kept by the registrar do not create a false or misleading impression to members of the public. This Act redefines the role of the registrar of companies, giving it a more active role in ensuring the accuracy and integrity of UK company registers and 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: (i) 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; (ii) 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; (iii) identification of sources of information on the registered businesses that would assist in maintaining the currency of the registry; and (iv) updating the registry as soon as practicable following the receipt of amendments to registered information and, in any event, without undue delay thereafter.

The International Business Registers Report reveals that jurisdictions are taking various steps to ensure that the data contained in registers is accurate (see Figure 3 below). The most widely adopted measures include cross-checking submitted data against external sources such as business name, population or address registers, and direct inquiries with the legal entities. A significant proportion of registries also report on-site verifications of business information. Fewer registries currently report using advanced analytical tools, such as ML/AI-powered algorithms, to proactively identify inconsistencies in existing records, though this is a growing area of development. Taken together, these measures reflect a shift from reactive correction toward more proactive data quality management, consistent with the growing expectations of Accuracy of the EBR data.

[79] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73.

[80] Economic Crime and Corporate Transparency Act 2023 (United Kingdom) s 1081A.

Figure 3: Measures that business registries take to check the Accuracy of the data recorded in the register. [81]

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. It may be necessary for the registrar to update or remove data to improve Accuracy (see CPF 16 on Legal Authority of the Registrar).

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.

To promote compliance, FATF Recommendations 24 and 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 manner.

[81] Business Registry Insights, 'Data Verification Survey' (2024) <https://br-insights.org/reports-dashboards/data-verification-2024/> accessed 3 April 2026. The figure has been redrawn by the authors of this document for clarity.

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;[82]
(iii) Verifying a user's identity through a remote identity management (IdM) system that provides pre-authenticated user credentials;[83] 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. A notary may also 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. While the use of a username and password remains prevalent, multi-factor authentication (MFA) should always be used where possible, as it reduces the risk of unauthorised access through compromised credentials alone. MFA requires more than one distinct factor for successful authentication (generally two or three factors): something you 'know' (e.g., passwords or pin codes), something you 'have' (e.g., certificates, token codes, one-time passwords or authentication applications), 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 apply when searching an EBR, for example, when searches are subject to a fee. In such cases, requiring payment details serves as a practical Access Control measure, though systems should also accommodate one-time users who do not create user accounts.

---

[82] This technique is used by the Global Aircraft Trading System (GATS), see Aviation Working Group, *Site Terms of Use* art. 12.4 (1 June 2020), <https://documents.e-gats.aero/SiteTermsOfUse.pdf> accessed 3 April 2026.

[83] 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] OJ L 1183; 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> accessed 3 April 2026; see also Eve Maler Garber and Mike Haine (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> accessed 3 April 2026.

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:

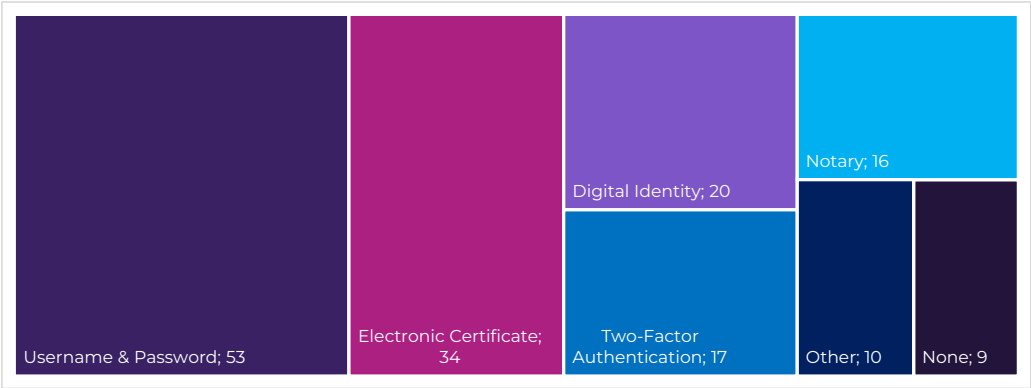


Figure 4: Methods of Filers' Identification.[84]

An appropriate Authentication system must be developed based on a risk assessment: what damage would occur if a user bypasses the authentication mechanism, and what benefit might drive them to attempt such a breach? It is not always appropriate to have an extreme authentication mechanism. For instance, when a user must pay for a service, they are less likely to misuse the system, whereas if access allows financial gain for the user, a 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 (i.e., its overall cybersecurity readiness and the strength of its existing controls relative to its threat landscape) 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 national and international levels. Therefore, it is often 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 use identity verification platforms that employ Know Your Customer (KYC) techniques, 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.[85]

Authentication should not hinder Accessibility, since its administrative and technical processes should be designed and adjusted in light of the user base (see CPF 2 on Accessibility).

[84] European Business Registry Association (EBRA), 'International Registers Survey Report 2022: Interactive Dashboard' <https://ebra.be/survey-results/> accessed 3 April 2026. The figure has been redrawn by the authors of this document for clarity.

[85] Goran Vranic and Andreja Marusic, 'Is the Self-Sovereign Digital Identity the Future Digital Business Registry?' (World Bank Blogs, 2021) <https://blogs.worldbank.org/psd/self-sovereign-digital-identity-future-digital-business-registry> accessed 3 April 2026.

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.[86]

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.

ISO/IEC 24760-1 provides a framework for IdM.[87] 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.[88]

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, with a dedicated EU Business Wallet under development. These wallets are to be designed to ensure accessible and 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.[89] Directive (EU) 2019/1151,[90] 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.

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.

86 International Organization for Standardization, ISO/IEC 9798-1: Information Technology — Security Techniques — Entity Authentication (2010).

87 International Organization for Standardization, ISO/IEC 24760-1:2019, IT Security and Privacy — A Framework for Identity Management — Part 1: Terminology and Concepts (2019).

88 UNCITRAL Legislative Guide, para. 180.

89 Regulation (EU) 2024/1183 (n 83).

90 The formal legal name is Directive (EU) 2019/1151 (n 42). 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 [2019] OJ L186/80, was signed six months later.

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, which will be discussed in the Legal section below.

Security that ensures the Integrity of data should generally take priority over Availability, but this priority should be applied consistently. The trade-off is most acute when a security vulnerability requires immediate remediation and the patch cannot be applied without taking the registry system offline, or when a security incident requires suspending the system to prevent further damage or data loss. In these cases, a documented incident response protocol should specify who can authorise downtime, what evidence is required, how long the suspension may last, and what notifications must be issued. Outside these scenarios, the priority of security over Availability should not be used to justify routine or extended downtime. Security improvements should generally be implemented without service interruption, such as through rolling updates or shadow deployments.

Availability is a measure of the total amount of uptime that can be expected over a given period. Availability can be calculated as follows, with the result expressed as the percentage or time that EBR is available or as the probability that the EBR will be available at any given time:

$$\text{Availability} = \text{uptime} / (\text{uptime} + \text{downtime})$$[91]

For example, the Availability of an EBR not available for a total of 24 hours (1 day) during the course of 365 days would be:

$$\text{Availability} = 364 / (364 + 1) = 0.997 \text{ (or } 99.7\%)$$

While the formula above allows any Availability level to be calculated, the EBRs, as a digital public infrastructure, should target a minimum of 99.9% Availability, commonly referred to as 'three nines'. At this level, total permitted unplanned downtime is approximately 8.7 hours per year. Planned maintenance downtime should be calculated separately and communicated in advance in accordance with the established notification requirements.

Technical

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.[92]

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.

[91] Byron Radle and Tom Bradicich, 'What Is Availability?' (National Instruments, 2019) <https://www.ni.com/en/shop/electronic-test-instrumentation/application-software-for-electronic-test-and-instrumentation-category/systemlink/automate-data-analysis/what-is-rasm/what-is-availability-.html> accessed 3 April 2026.

[92] International Organization for Standardization, ISO/IEC 27000: Information Security Management Systems — Overview and Vocabulary (2018) 3.7.

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 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. 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 in handling PII, ensuring compliance with data protection regulations and 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.[93] 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 types of personal data collected and stored, appropriate mechanisms for disclosing this data to the subject of 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 Annexe 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 to avoid its misuse or inadvertent exposure.

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

[93] Regulation (EU) 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) [2016] OJ L 119/1.

confidentiality-by-design and privacy-by-design approach, which requires 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,[94] 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,[95] can play a role in minimising the exposure of PII while preserving functionality. Decentralised Identity Management (IdM) could also allow users to retain control over their identity information, reducing the risks associated with centralised data storage. The design of searching mechanisms should avoid enabling unintended exposure of registry data.

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.'[96] 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 can be achieved with appropriate security controls, including policies, processes, procedures, and infrastructure, which protect information assets.[97]

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, which 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 the ten key privacy principles.[98]

NIST SP 800-122 is a practical, context-based guide to identifying PII, determining what level of protection is appropriate and how to provide it.[99] The guide outlines considerations for developing operational and privacy-specific safeguards, which include policies, raising awareness and training for personnel, practices minimising 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. It references other NIST publications that cover each element of data privacy protection in more detail, such as SP 800-47, Security Guide for

---

94 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.

95 *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: International Organization for Standardization, ISO/IEC 20889: Privacy-Enhancing Data De-Identification Terminology and Classification of Techniques (2018); and International Organization for Standardization, ISO/IEC 18033: Information Technology — Security Techniques — Encryption Algorithms (2010).

96 ISO/IEC 27000 (n 60)3.10.

97 ISO/IEC 27000 (n 60).

98 International Organization for Standardization, ISO/IEC 29100: Information Technology — Security Techniques — Privacy Framework (2024).

99 McCallister E, Grance T and Scarfone K, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (National Institute of Standards and Technology Special Publication 800-122, 2010) <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990> accessed 3 April 2026. See also NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

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.[100]

Legal

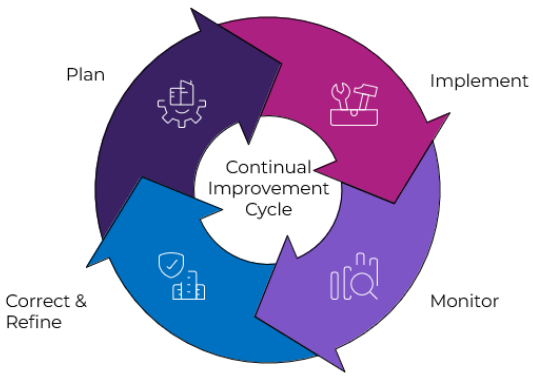
In the EU, Article 5(1)(f) of the GDPR, entitled 'Principles relating to processing of personal data', mandates that personal data should be processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[101] 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,[102] which is consistent with the core principles of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data.

For a more comprehensive overview of the international and regional legal frameworks and recommendations on the scope of publicly accessible information, see Annexe I to this Guide.

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, particularly registrants, 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 knowledge sharing and 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,

100 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

101 General Data Protection Regulation (n 93).

102 Asia-Pacific Economic Cooperation, APEC Privacy Framework (2015) <https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015)> accessed 3 April 2026.

leading to unexpected or unacceptable outcomes. Performing a root cause analysis[103] assists in identifying causal factors and corrective actions to be taken to prevent reoccurrence.

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 is not only essential for enhancing operational efficiency and service quality; it is also critical for avoiding technological or functional legacy, or obsolescence. As digital technologies evolve rapidly, underlying registry systems must undergo regular assessment and infrastructure and technological upgrades to remain current and competitive, avoid functional and technical degradation, remain secure, and meet the evolving stakeholder expectations.[104]

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, establishing feedback mechanisms 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.[105] 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.

[103] 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 IBM, 'What Is Root Cause Analysis?' <https://www.ibm.com/think/topics/root-cause-analysis> accessed 3 April 2026.

[104] 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> accessed 3 April 2026.

[105] UNCITRAL Legislative Guide, Recommendation 58.

8. Continuity

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 (see CPF 5 on Availability).

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 (see CPF 13 on Integrity), 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 these activities. 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 DR plans. It is vitally important that appropriate information security practices are maintained *during* a disruptive incident.

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 services from different cloud service providers, and potentially under different cloud deployment models.[106] In addition to facilitating more rapid and less costly migration, this measure reduces the risk

[106] Cloud Standards Customer Council (CSCC), Interoperability and Portability for Cloud Computing: A Guide (Version 3.0, December 2022) 6 <https://www.omg.org/cgi-bin/doc?mars/2022-12-13> accessed 3 April 2026.

of vendor lock-in.[107] It is important to note that portability is not a binary concept, and transforming EBR data from its form in the source system to the form required by the target system may still require considerable effort. 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. The latter needs to account for the situations where the registry relies on outsourced services, such as cloud hosting, payment gateways, or data verification, or the registry is operated by a private company. In such cases, the plans should 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-party services become unavailable or the registry operator becomes insolvent.

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, source code escrow, 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.[108] For example, in the Canadian province of Saskatchewan, the Operation of Public Registry Statutes Act[109] 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 depends on sufficiently skilled personnel. To address this, EBRs 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 (a lower risk when EBRs are operated directly by governmental agencies). The identification and systematic assessment of the conditions that give rise to such disruptive events is addressed in CPF 19 on Risk Management.

Technical

ISO 22301[110] is the primary international standard for business continuity management (BCM). It specifies requirements for establishing, implementing, maintaining, and continually improving a BCM system, and can be used to assess an organisation's ability to meet its own Continuity needs and obligations through identifying continuity risks, defining recovery objectives, and testing continuity plans. Other BCM standards include ISO/IEC 27001, which addresses information security continuity as part of the broader information security management system, and the NFPA 1660 Standard for Emergency, Continuity, and Crisis Management provides further guidance on preparedness, response, and recovery in the context of broader organisational resilience.[111]

---

107 International Organization for Standardization, ISO/IEC 19941: Information Technology — Cloud Computing — Interoperability and Portability (2017) Introduction.

108 See European Banking Authority, Final Report on Guidelines on Outsourcing Arrangements (2019) para 40(a).

109 Operation of Public Registry Statutes Act, SS 2013, c O-4.2 <https://publications.saskatchewan.ca/#/products/67707> accessed 3 April 2026.

110 International Organization for Standardization, ISO 22301: Security and Resilience — Business Continuity Management Systems — Requirements (2019).

111 National Fire Protection Association, NFPA 1660: Standard for Emergency, Continuity, and Crisis Management — Preparedness, Response, and Recovery (2024).

NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, introduces a structured seven-step process for contingency planning. It includes a policy statement, business impact analysis, preventive controls, contingency strategies, contingency plan development, testing, training and exercise, and plan maintenance — each of which maps directly onto the Continuity requirements described in this CPF.[112]

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.[113] Some jurisdictions require a plan for handling business-critical operations.[114] 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 transfer to an alternate provider upon contract termination.

In the EU, the NIS2 Directive (Directive 2022/2555) imposes binding obligations on essential and important entities regarding service continuity and resilience.[115] Business registries may fall within its scope depending on their classification under national legislation. Article 21 requires covered entities to implement BCM measures, including backup management, disaster recovery, and crisis management procedures capable of ensuring service restoration within defined timeframes. Article 23 requires that significant incidents be reported to the competent national authority within 24 hours of detection, with a more detailed report within 72 hours. These obligations make documented continuity governance, including defined RPO and RTO targets and regularly tested recovery plans, a legal requirement rather than merely a best practice for in-scope registries.

9. Correctability

Definition: The process of 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 no longer accurate, it does not necessarily qualify as an error unless it results from failure to comply with statutory updating obligations. Considerable attention to data accuracy is given in CPF 3 on Accuracy, above.

---

112 National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34 Rev 1, 2010).

113 ISO 22301 (n 110).

114 See Monetary Authority of Singapore, Guidelines on Business Continuity Management (2022) <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management> accessed 3 April 2026.

115 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) [2022] OJ L333/80.

In certain legal systems, a further distinction is drawn between information that is factually accurate but legally invalid (for example, where an appointment is duly recorded but was made in breach of mandatory corporate law requirements) and information that is both factually and legally incorrect. In such cases, the defect lies not in the data itself, but in its legal validity, which may require a different corrective response.

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, legal validity, and trustworthiness of the data they provide to stakeholders. When registering data in the registry, it is crucial to verify that the pieces of information provided are consistent with each other and with the accompanying 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.

Registrars should be authorised to correct computer-generated or clerical errors autonomously where 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 authority to correct human or computer-generated errors 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.[116] However, this authority should be exercised within clearly established conditions and limitations in a transparent manner.

In some jurisdictions, particularly where registries form part of the judicial system, registrars or courts may also be empowered to act *ex officio* to delete, correct, or refuse to maintain information that is legally inadmissible or invalid, even in the absence of a correction request by the registrant. Such powers serve to protect the integrity of the registry and the legitimate reliance interests of third parties.

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 associated 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 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, document reviews, and court procedures;
(c) audit trails and records documenting changes made to registered information, facilitating tracking modifications and ensuring transparency and accountability; and
(d) communication channels offering accessible mechanisms for stakeholders to report errors, seek assistance with correcting information, and be notified when corrections are implemented.

Since the primary responsibility to correct errors typically lies with registrants as data providers, EBRs should also employ appropriate mechanisms to enforce the rectification of detected inaccuracies on them. Where voluntary compliance is not achieved, such measures may include penalties (administrative and/or financial), suspension of the business's status on the register, and limitation of participation in business activities (see Figure 5 below).

[116] UNCITRAL Legislative Guide, para. 147.

Figure 5: Mechanisms to enforce rectification of detected data inaccuracies by the entities. [117]

Errors may also result from unauthorised alterations through cyberattacks or technical malfunctions. To limit potential damage to the public, EBRs need to proactively identify such errors by 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 also support 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,[118] 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[119] 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.[120]

---

117 Data Verification Survey (n 81). The figure has been redrawn by the authors of this document for clarity.

118 International Organization for Standardization, ISO/IEC 25012: Software Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Data Quality Model (2008).

119 National Institute of Standards and Technology, Security Metrics Guide for Information Security (NIST Special Publication 800-55 Rev 2, 2024).

120 UNCITRAL Legislative Guide, Recommendation 27.

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 the 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.[121]

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 registrant) has been entered. Semantic validation verifies that the submitted data is logically consistent within the context of the rules of the EBR.[122]

Data Input Validation should 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. 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 security (see CPF 24 on User-Centred Design).

Real-time data validation, as outlined in the World Bank's report on data-driven company registries,[123] 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 improves data quality from the outset, making it an essential component of modern EBRs.

Validation remains relevant in post-registration activities, such as amendments, renewals, or deregistrations. For example, if appropriate, it can preclude the registration of an amendment to a registration that has already been cancelled.

The UNCITRAL Legislative Guide encourages implementing a series of checks and control procedures to ensure the provision of necessary information for business registration.[124] 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.

---

121 See Open Worldwide Application Security Project (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> accessed 3 April 2026.

122 OWASP, 'C3: Validate Input and Handle Exceptions' (n 121).

123 World Bank Group, Data-Driven Company Registry: Guidance Note (n 8).

124 UNCITRAL Legislative Guide, para. 146.

As registries move towards more automated systems, the instances of manual reviewing and correcting data decrease 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. This approach requires validation rules to be designed to cover complex, nuanced rules that have previously been managed by registry personnel within a manual process. Such rules should be applied under human oversight with regular reviews and updates 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[125] reinforces this by integrating input validation mechanisms into application-level security to protect software from unauthorised or malformed input. Similarly, NIST SP 800-53,[126] 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[127] 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. 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]

The Open Worldwide Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.[129] 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 development project.[130] Ranked in order of importance, Input Validation is third on the list,[131] 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.[132]

---

125 International Organization for Standardization, ISO/IEC 27034-1: Information Technology — Security Techniques — Application Security (2011).

126 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

127 National Institute of Standards and Technology, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST Special Publication 800-218, 2022).

128 International Organization for Standardization, ISO/IEC 7064: Information Technology — Security Techniques — Check Character Systems (2003).

129 See Open Worldwide Application Security Project (OWASP) <https://owasp.org/> accessed 3 April 2026.

130 See Open Worldwide Application Security Project (OWASP), OWASP Top 10 Proactive Controls <https://top10proactive.owasp.org/the-top-10/> accessed 3 April 2026.

131 OWASP, 'C3: Validate Input and Handle Exceptions' (n 121).

132 UNCITRAL Legislative Guide, para. 148.

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 (see CPF 7 on Continual Improvement).

Thirdly, as is also set out in CPF 3 on Accuracy, 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[133] and national postal services to 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 ML 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.[134]

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.

---

133 Esri, 'Geocoding Services' <https://developers.arcgis.com/rest/geocode/> accessed 3 April 2026.

134 World Bank Group, Data-Driven Company Registry: Guidance Note (n 8).

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 (see CPF 7 on Continual Improvement). Registries should also periodically conduct rule reviews, examining correction histories and rejection patterns, to identify gaps in detection coverage before new errors become systemic.

Technical

ISO/IEC 25012 defines a general data quality model for data retained in a structured format within a computer system.[135] 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.[136]

ISO/IEC 27002 provides guidance for security controls, such as logging and anomaly detection, to ensure unauthorised changes are promptly detected.[137] NIST SP 800-53 completes this guidance by providing details of mechanisms for integrity checking using cryptographic techniques and monitoring system activities for discrepancies.[138]

12. Evidentiary Value

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. CPF 6 on Confidentiality and Privacy, CPF 10 on Data Input Validation, CPF 13 on Integrity and CPF 17 on Reliability are all integral to the concept of Evidentiary Value.

Subject to specific legal and regulatory standards of their respective jurisdictions, EBRs should implement various technological and administrative methods to support the evidentiary integrity of their records. Implementing data change control procedures is a key procedural step. Records must stay complete and unaltered, with stringent controls over any modifications, following the ISO 15489 standard.[139] 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 determined based on the EBR's risk

135 ISO/IEC 25012 (n 118).

136 International Organization for Standardization, ISO 8000-8: Data Quality — Part 8: Information and Data Quality — Concepts and Measuring (2015).

137 ISO/IEC 27002 (n 37).

138 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

139 International Organization for Standardization, ISO 15489-1: Information and Documentation — Records Management (2016).

exposure and applicable legal requirements (e.g., 18–24 months), with longer retention for data supporting legal evidence. All such logs should be tamper-resistant where possible.

Technical measures are essential in preserving data integrity. Qualified electronic signatures, electronic seals, and electronic ledgers (defined, for example, in eIDAS 2.0 Regulation (No. 2024/1183)) allow for verifying the records' origin, integrity and legal status as evidence.[140] Complementing this, timestamping[141] binds the date and time to the data to enhance data integrity by detecting modifications and establishing an immutable, verifiable, chronological sequence for record creation and updates.

Equally important, a chain of custody protocol[142] ensures accountability by creating a transparent and secure trail of how records have been accessed, transferred, or modified. Such protocols help prevent unauthorised modifications, provide user accountability, and support litigation and regulatory review.

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 such 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 registry data can be supported through the adoption of internationally recognised frameworks. For record authenticity and integrity verification, ISO/IEC 32000-2 provides guidance on digital signature validation and long-term validation formats, including XML Advanced Electronic Signature (XAdES) and PDF Advanced Electronic Signatures (PAdES), which enable the verification of signed documents over time.[143] Timestamping protocols and time-stamp token profiles are elaborated in ETSI EN 319 422.[144] It provides guidance for establishing an immutable, verifiable chronological sequence for record creation and updates.

Further, ISO 15489 provides criteria for documentation and audit trails that ensure transparency and accountability for changes made to the data.[145] NIST SP 800-92 addresses audit log management, covering log generation, protection, and retention to support both operational and forensic investigations.[146] NIST SP 800-86[147] elaborates on cryptographic techniques to ensure data integrity and forensic analysis.

ISO/IEC 27001 addressed data integrity and security issues and provides mainly long-term storage principles and actions against technological obsolescence.[148] NIST SP 800-53[149] addresses privacy- and security-related controls relevant to the protection and governance of records. Together, these standards form the foundation of a chain of custody, safeguarding records and ensuring their Evidentiary Value.

---

140 Regulation (EU) 2024/1183 (n 83).

141 Regulation (EU) 2024/1183 (n 83).

142 A chain of custody protocol refers to a documented and unbroken record of who has accessed, handled, or transferred data or evidence. See National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86, 2006).

143 International Organization for Standardization, ISO 32000-2: Document Management — Portable Document Format (2020).

144 European Telecommunications Standards Institute, ETSI EN 319 422 V1.1.1: Electronic Signatures and Infrastructures (ESI) — Time-Stamping Protocol and Time-Stamp Token Profiles (2016).

145 ISO 15489-1 (n 139).

146 National Institute of Standards and Technology, Guide to Computer Security Log Management (NIST Special Publication 800-92, 2006); see also National Institute of Standards and Technology, Cybersecurity Log Management Planning Guide (NIST Special Publication 800-92 Rev 1, Initial Public Draft, 2023).

147 NIST Guide to Integrating Forensic Techniques into Incident Response (n 142).

148 ISO/IEC 27001 (n 61).

149 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

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, the legal certainty of registry records erodes, and public trust cannot be placed in the registry as an authoritative source of information. Protection of the Integrity of the registry record also safeguards the legal identity and standing of the registered business. Data Integrity of the EBR directly reflects on its reputation.[150]

Integrity relates to the system, the data, and any decision-making of the registrar and registry staff. 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 (but accepted by the system, see CPF 10 on Data Input Validation) must not be deleted or changed without preserving a complete and transparent record. This approach allows any 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 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 could be impacted. To mitigate such risk, clear internal controls around API-based access should be in place, such as a suitable allowlisting mechanism through which the users connecting to the API are known in advance. This should allow system administrators to revoke 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 an allowlist facility, the registry should have the capacity to blocklist API users where necessary (see CPF 14 on Interoperability).

The 2020 SolarWinds supply chain attack exemplifies a deliberate Integrity breach.[151] State-linked attackers infiltrated SolarWinds' development environment, embedding malware in software updates by replacing legitimate source files with malicious ones containing a backdoor. These updates, distributed to over 18,000 customers including critical US government agencies and major

[150] Foster Moore, Registers: *The New Frontier — A Proposal for the Development of a New Target Operating Model for Registers* (2023) <https://www.fostermoore.com/white-papers/proposed-new-target-operating-model-for-registers-white-paper> accessed 3 April 2026.

[151] Dina Temple-Raston, '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> accessed 3 April 2026.

corporations, appeared authentic but contained malicious code. Once installed, they manipulated system configurations, logs, and established a long-term presence, undermining trust and the integrity of the software supply chain. This attack illustrates how breaches of the Integrity CPF can erode confidence in digital services and, in EBRs, could lead to unauthorised filings, falsified records, or malicious functionality in core services. Even without visible data theft, such a breach would severely undermine the Integrity, Evidentiary Value and Trustworthiness (see CPF 23 on 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[152] 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.[153] 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.[154]

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).[155]

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.[156] 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.[157] NIST SP 800-53 devotes special attention to software, firmware, and information integrity. It elaborates on several controls supporting Integrity, among which are: integrity checks, automated notifications of and automated responses to integrity violations, cryptographic protections, and integrity verifications.[158]

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 registries. It is reinforced in Recommendation 54 of the UNCITRAL Legislative Guide, which addresses the protection of business registry records against loss or damage.

---

152 ISO/IEC 27002 (n 37).

153 Max Edwards, 'ISO 27002 — Control 8.24 — Use of Cryptography' (ISMS.online, 17 February 2025) <https://www.isms.online/iso-27002/control-8-24-use-of-cryptography/> accessed 3 April 2026.

154 Max Edwards, 'ISO 27001 — Clause 6.7 — Cryptography' (ISMS.online, 26 February 2025) <https://www.isms.online/iso-27701/clause-6-7-cryptography/> accessed 3 April 2026.

155 ISO/IEC 27001 (n 61).

156 See ISO/IEC 27040, Information technology — Security techniques — Storage security (2nd edn, 2024) s 7.

157 IEEE, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices (IEEE 1619.1-2019, 2019); National Institute of Standards and Technology, Advanced Encryption Standard (AES) (FIPS PUB 197, 2001, updated 2023).

158 NIST Security and Privacy Controls for Information Systems and Organizations (n 49).

In line with this recommendation, governments should maintain backup copies of registry records to mitigate the risk of loss, physical damage, or destruction.[159] In addition to these risks, EBRs face threats from criminal activities facilitated by technology, such as unauthorised access or interference with the electronic registry; unauthorised interception of or interference with data; misuse of devices; fraud and forgery. Therefore, implementing effective enforcement measures within the legislative framework is crucial to support the EBRs.[160]

In the EU, GDPR Article 5 also establishes 'integrity and confidentiality' as one of the six core data protection principles. While this obligation falls primarily on data controllers, registries processing PII as part of their statutory function must implement technical and organisational measures commensurate with the risk, as further specified in Article 32. At the network and systems level, NIS2 (Directive (EU) 2022/2555) requires operators of essential and important entities to implement technical, operational, and organisational measures to manage risks to the security of network and information systems. Article 21 specifically requires measures addressing supply chain security, access control, and the integrity of systems and their data.

Together, these instruments create a layered legal obligation for the EBRs in the EU. They must protect data against external threats and be able to demonstrate, through audit trails and certified outputs, that the records they hold remain accurate, complete, and unaltered from their authoritative source.

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 and transparent manner for its users. It may be mandated by law or enabled by the system provider as a service to users. In EBRs, Interoperability enables correct, timely, and cost-efficient data sharing among different systems involved in business registration, such as tax authorities, social security institutions, business regulators, the natural persons register, the address register, or commercial banks, as prescribed by applicable laws.[161]

In its publication "Digital Public Infrastructure and Development", the World Bank has underlined the importance of registries, including business registries, as a key element or 'building block' in the ecosystem of integrated digital public services.[162] As building blocks of the digital public infrastructure, EBRs implement the once-only principle — the requirement that businesses and citizens provide information to public authorities only once, after which it is reused across systems and agencies rather than re-submitted. When established by the applicable law, the once-only principle has direct implications for EBR design, as registry data collected at the point of formation should be shareable with other authorities and registries without requiring re-submission.

159 UNCITRAL Legislative Guide, para. 233.

160 UNCITRAL Legislative Guide, para. 234.

161 World Bank Group, Data-Driven Company Registry: Guidance Note (n 8).

162 J Clark, G Marin, OP Ardic Alper and GA Galicia Rabadan, Digital Public Infrastructure and Development: A World Bank Group Approach (Digital Transformation White Paper vol 1, World Bank 2025) <https://hdl.handle.net/10986/42935> accessed 3 April 2026.

II. CRITICAL PERFORMANCE FACTORS

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 3).[163]

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 can be understood 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 3: 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.[164] 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.[165] The Board is responsible for monitoring the overall coherence of the recommended interoperability solutions at the national, regional, and local levels.[166] 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.[167]

Interoperability is vital to facilitating cross-border business activities. For instance, the Business Register Interoperability System (BRIS)[168] 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.[169] It connects three systems, namely: BRIS; the Beneficial Ownership Register Interconnection (BORIS), linking national BO

163 European Commission, 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> accessed 3 April 2026.

164 Bill Clarke and John Murray, Enabling Digital Government: Interoperability and Data Exchange Between Registries – The Benefits of a Connected Landscape (Teranet Inc and 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> accessed 3 April 2026.

165 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) art 15.

166 Regulation (EU) 2024/903 (n 165).

167 Regulation (EU) 2024/903 (n 165) art 18.

168 European Commission, 'Business registries at European level' (European e-Justice Portal, 2017) <https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do> accessed 3 April 2026.

169 Directive (EU) 2025/25 (n 43) article 22(7).

registries;[170] 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.

Another example of an interoperability infrastructure is the X-Road system, an open-source, centrally governed yet distributed data exchange layer that enables secure system-to-system communication. It is mandatory for public sector data exchange in Estonia and is also used in Finland, Japan, and several other jurisdictions. This framework enables EBRs and other public authorities to exchange data in real time through authenticated, logged and encrypted connections, without relying on centralised data storage. Business registry data between Estonian and Finnish authorities is exchanged automatically via X-Road services, supporting cross-border interoperability, information accuracy, and security.[171]

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.

Some jurisdictions designate business registries as base registries, such as in Denmark, where the Danish Business Authority manages such functions.[172] 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).[173]

FATF also strongly recommends data exchange at both the national and international levels. 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.[174]

---

170 European Commission, 'Beneficial Ownership Registers Interconnection System (BORIS)' (European e-Justice Portal) <https://e-justice.europa.eu/38590/EN/beneficial_ownership_registers_interconnection_system_boris> accessed 3 April 2026.

171 X-Road, 'The business registers of Estonia and Finland start cross-border interoperability' <https://x-road.global/xroad-case-studies-library/2024/10/21/the-business-registers-of-estonia-and-finland-start-cross-border-interoperability> accessed 3 April 2026.

172 *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 European Commission, ABR Factsheet 2017: Denmark – Access to Base Registries in Denmark (2017) <https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Denmark%20Factsheet%20Final_DIGST_everis.pdf> accessed 3 April 2026.

173 European Commission, 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> accessed 3 April 2026.

174 The FATF Recommendations (n 40).

Where Interoperability is mandated by the law, appropriate communications and governance protocols for managing Interoperability and data-sharing agreements with 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.[175]

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.

Over 70 countries adopt the XBRL (eXtensible Business Reporting Language) format for vast amounts of financial and non-financial business data used in statutory reporting and annual accounts.[176] XBRL helps automate the collection and validation of business data, reducing manual work and processing time and enhancing shareability and transparency with the public. In the EU, Inline XBRL (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.[177]

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 businesses, for data sharing with cooperating agencies, and by other authorities in Denmark in different reporting scenarios, e.g., for tax and statistical purposes. Another example is the taxonomy developed by the South African Register (CIPC) as part of its Financial Reporting Digitisation Programme.[178]

When it comes to standardising BO data in registers, Open Ownership, a UK non-governmental organisation, has developed the Beneficial Ownership Data Standard, an open standard offering guidance for collecting, 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.[179]

Technical[180]

A number of ISO standards can support the technical implementation of Interoperability. These include ISO 2382, which defines Interoperability;[181] while ISO 19941 provides standards for transferring data

---

175 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, April 2011) <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/GRAInformationSharingEnterpriseService-LevelAgreement-Final11April2011.pdf> accessed 3 April 2026. See also National Institute of Standards and Technology, Managing the Security of Information Exchanges (NIST SP 800-47r1, 2021).

176 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. See more XBRL International, 'XBRL Project Directory' <https://www.xbrl.org/the-standard/why/xbrl-project-directory/> accessed 3 April 2026.

177 European Securities and Markets Authority, 'Sustainability Reporting' <https://www.esma.europa.eu/esmas-activities/sustainable-finance/sustainability-reporting> accessed 3 April 2026.

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

179 Beneficial Ownership Data Standard it is the official data standard for the UK government; it has also received endorsements from the World Bank, OECD and UNODC. See more Open Ownership, 'Beneficial Ownership Data Standard (BODS) v0.4' <https://standard.openownership.org/> and Open Ownership, 'Beneficial Ownership Data Standard' <https://www.openownership.org/en/topics/beneficial-ownership-data-standard/> accessed 3 April 2026.

180 Sections of this CPF discussing the API were prepared in consultation with NRD Companies.

181 See International Organization for Standardization, Information technology — Vocabulary (ISO/IEC 2382, 2015), 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.'

between non-cloud and one or more cloud services and between cloud services.[182] The ISO 8000 family of standards addresses data quality in complex information systems and the use of unique identifiers. In particular, ISO 8000-114[183] specifies an interoperable data format (idf) that combines JavaScript Object Notation (JSON), with semantic encoding based on open technical dictionaries, as set out in ISO 22745.[184] ISO 8000-115 establishes principles for identifiers,[185] and ISO 8000-116 applies those principles specifically to identifiers issued by business registries.[186] In addition, ISO 25500-3, currently under development, is intended to specify the requirements for a request for the verification and a request for data of an Authoritative Legal Entity Identifier (ALEI) formatted in accordance with ISO 8000-116 and the response to the request.[187] Supporting standards such as ISO 8601 on date and time representations further contribute to consistency and interoperability across systems.[188]

The use of APIs based on widely adopted, industry-standard protocols (for instance, REST) can support compatibility and Interoperability between EBR systems and external systems or services. APIs commonly support various data formats, such as JSON and eXtensible Markup Language (XML), accommodating flexible and machine-readable data exchange. Public APIs may serve external users (e.g., notaries or banks), while private APIs typically enable back-end integrations with government systems. For instance, the Louisiana Secretary of State provides a REST API that businesses can integrate into their software to access the system more efficiently.[189] The International Association of Commercial Administrators (IACA) also recommends a standard XML format for transmitting electronic registrations to Uniform Commercial Code (UCC) filing offices.[190]

Adopting internationally recognised approaches to unique company identifiers can improve the consistency of business identification across jurisdictions and platforms. In this respect, the ISO 8000 family of standards provides guidance on the creation of globally unique identifiers while preserving the autonomy of national registries. In particular, ISO 8000-116[191] applies the principles of ISO 8000-115 to business registry identifiers by enabling the use of jurisdictional and registry-specific prefixes (for example, based on ISO 3166 country codes) without requiring any modification to the domestic registration number itself. This approach allows registries to retain full control over their identifiers while enabling international uniqueness and machine readability.

Complementary initiatives, such as the Entity Legal Forms (ELF) Code List released by the Global Legal Entity Identifier Foundation, support interoperability by standardising the classification of legal entity forms across jurisdictions. The ELF list assigns unique codes to legal forms in their native language, such as Gesellschaft mit beschränkter Haftung (GmbH), or Société Anonyme (SA), and simplifies the classification of legal forms, which is beneficial for databases containing information on international companies.

---

182 See ISO/IEC 19941 (n 107).

183 See International Organization for Standardization, Data quality — Part 114: Master data: Application of ISO/IEC 21778 and ISO 8000-115 to portable data (ISO 8000-114, 2024).

184 See International Organization for Standardization, Industrial automation systems and integration — Open technical dictionaries and their application to master data (ISO 22745, 2010).

185 See International Organization for Standardization, Data quality — Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements (ISO 8000-115, 2024).

186 See International Organization for Standardization, Data quality — Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 to authoritative legal entity identifiers (ISO 8000-116, 2019).

187 See International Organization for Standardization, Supply chain interoperability and integration — Part 3: Verification of trading entity identity (ISO/DIS 25500-3).

188 See International Organization for Standardization, Date and time — Representations for information interchange (ISO 8601-1, 2019).

189 See Louisiana Secretary of State Commercial API Guide (2022), <https://static.sos.la.gov/COAPI/Commercial_API_Guide.pdf> accessed 3 April 2026.

190 International Association of Commercial Administrators, XML Technical Specifications for Uniform Commercial Code Filings: Revised Article 9 (Version 4.00, 2019) <https://www.iaca.org/secured-transactions/xml-technical-specifications/> accessed 3 April 2026.

191 See ISO 8000-116 (n 186).

Legal

The UNCITRAL Legislative Guide emphasises that, when an electronic registry is adopted, Interoperability should be considered. The registry should be designed to allow, also at a later stage, integration with other automated systems, such as other governmental authorities operating in the jurisdiction, and online or mobile payment portals.[192]

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[193] 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. The Interoperable Europe Act (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.[194] 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. Less formal instruments, such as registrars' practice statements and administrative rules, 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.

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

192 UNCITRAL Legislative Guide, para. 70.
193 Directive (EU) 2017/1132 (n 41).
194 Regulation (EU) 2024/903 (n 165).

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 maintained by the ordinary courts. Registrations in the business registry, which can be accessed online, are presumed to be complete and correct (good faith of the business registry). 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.[195] In the Spanish model, also adopted by many South American countries, the registrar thoroughly examines the documents submitted prior to registration, thereby enhancing the reliability of registered data, similar to the Italian notarial system. In certain Middle Eastern countries, business registries may also serve as revenue collection and licensing entities.[196]

EBRs also 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 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 CPF 16 on the Legal Authority of the Registrar). A clear legal mandate, combined with appropriate oversight and compliance mechanisms, is essential for ensuring the 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.[197] 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.

---

195 In recent years, the UK has been shifting its approach and is investing heavily in updating business processes to ensure data accuracy through verification. See more Department for Business, Energy and Industrial Strategy, 'Corporate Transparency and Register Reform' (2022) <https://www.gov.uk/government/publications/corporate-transparency-and-register-reform/corporate-transparency-and-register-reform-accessible-webpage> accessed 3 April 2026.

196 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 (2024) para. 107 <https://ctcap.org/wp-content/uploads/2024/05/BPER-Report-of-the-7th-Workshop.pdf> accessed 3 April 2026.

197 This definition corresponds to the terminology provided in the UNCITRAL Legislative Guide on Key Principles of a Business Registry (2019), p.6. It is used solely for the purposes of this Guide and does not prescribe how the legal status of the registrar should be defined under domestic laws. In some jurisdictions, there is no single "registrar" entrusted with the entirety of registration system; instead, these functions may be allocated among several public or private entities. For example, in Poland, the "registrar" functions are split functionally: the Minister of Justice is responsible for the overall operation, maintenance, and technical administration of the registry system, while the District Courts (and specifically Judicial Registrars—referendarze sądowi) exercise the substantive legal authority to enter data, reject applications, and correct the register. Consequently, this CPF should be analysed based on the specific functions exercised by the relevant authorities within the domestic legal framework.

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 are important confidence factors 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 users should always be clearly stated and logged for evidentiary purposes, and users should be notified when these powers are exercised.

Generally, only 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 most jurisdictions, the registrar is authorised to reject a business registration application only if it does not meet the requirements prescribed by the applicable law.[198] To ensure transparency and prevent any misuse of this authority, the registrar should provide a written notice detailing the reasons for rejecting 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 in either 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 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. As mentioned above, 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.

In the EU, the scope of the registrar's authority should be understood within the legal framework established for business registries, *inter alia*, under Directive (EU) 2017/1132[199] and Directive (EU) 2025/25.[200] These instruments require mandatory preventive controls for the formation and subsequent filings of limited liability companies and commercial partnerships. However, EU law allows for flexibility in institutional arrangements for the exercise of such controls. Depending on the legal tradition of the

198 UNCITRAL Legislative Guide, para. 149.

199 Directive (EU) 2017/1132 (n 41).

200 Directive (EU) 2025/25 (n 43).

Member State concerned, preventive checks, such as verification of the identity and legal capacity of the applicant, authority to represent the entity, legality of the name and object, and appointment of directors, may be conducted by an administrative authority (including the registrar), a court, a notary, or a combination thereof. Consequently, the extent to which the registrar is empowered to perform substantive legality review is determined by domestic legislation transposing the Directive, which defines the limits and conditions of the registrar's authority.[201]

In some non-EU jurisdictions, including parts of Asia, registrars are granted broader authority to go beyond formally accepting the filing and to conduct substantive examination of compliance with corporate, commercial, or regulatory requirements. In these jurisdictions, compliance with the filing requirements is typically reinforced through a combination of penalties for the failure to file data, as well as the filing of false, incomplete or inaccurate data, and the registrar's corrective powers. This way, the registrar's corrective and supervisory functions form part of a more expansive model of administrative oversight.

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.

Reliability for registries as repairable systems is typically measured using the 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.[202]

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 day 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

---

201 Jessica Schmidt, 'The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers' (2024) 21 European Company and Financial Law Review 578–602 <https://www.degruyter.com/document/doi/10.1515/ecfr-2024-0023/html> accessed 3 April 2026.

202 See Byron Radle and Tom Bradicich (n 91).

quality control and testing after each update or system change help identify and mitigate potential vulnerabilities. Incident data collection and analysis allow for identifying common failure patterns and refining the system (see CPF 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,[203] 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'.[204] 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.[205] The standard defines maturity as the degree to which a system meets the need for Reliability under normal operation.[206] Fault tolerance is the degree to which a system operates as intended in spite of infrastructure faults (i.e., without adversely affecting Availability),[207] while recoverability is defined as the degree to which a system can recover from an interruption or failure, including restoring any affected data (i.e., restoring Availability).[208] Also, NIST Special Publication 800-160, Volume 2[209] refers to Reliability as 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

---

203 Culture of accountability should be understood as a culture where the organisation is accountable to its internal and external stakeholders for its decisions, conduct and outcomes. Such culture is characterised by consistency in behaviour and expected level of commitment, application of rules and procedures, feedback mechanisms, whistle-blowing policy, etc. See more on organisational culture John P Kotter, Leading Change (Harvard Business School Press 1996).

204 See ISO/IEC 27040 (n 156), §3.36. See also ISO/IEC 2382 (n 181) defining reliability as the 'ability of a functional unit to perform a required function under given conditions for a given time interval.'

205 See International Organization for Standardization, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models (ISO/IEC 25010, 2011) 4.2.5.

206 ISO/IEC 25010 (n 205) 4.2.5.1.

207 ISO/IEC 25010 (n 205) 4.2.5.3.

208 ISO/IEC 25010 (n 205) 4.2.5.4.

209 National Institute of Standards and Technology, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST Special Publication 800-160 vol 2, 2021) **<**https://doi.org/10.6028/NIST.SP.800-160v2r1**>** accessed 3 April 2026.

transparency, while Disposition addresses data lifecycle management and regulatory obligations for data minimisation and privacy.

Retention of registration data in EBRs is generally more cost-effective than maintaining paper records,[210] 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 preservation period. Yet registries should not underestimate the ongoing costs of digital infrastructure, which include server maintenance, cybersecurity, software licensing, data migration, and the staff dedicated to managing long-term digital preservation. EBR operations should include long-term preservation rather than treating digitisation as a one-time investment.

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.[211]

Disposition covers processes and policies for archiving, destroying, or transferring records when the retention period expires or continued storage is no longer justified. It does not create new records other than in an activity log documenting an action. 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.[212]

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 discs, microfilm, or hard disc drives with limited lifespans 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 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 of Directive (EU) 2017/1132 of the

210 UNCITRAL Legislative Guide, para. 230.

211 UNCITRAL Legislative Guide, para. 227.

212 UNCITRAL Legislative Guide, para. 231.

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.[213] This creates a need for registries to have a documented policy, reviewed against applicable privacy and transparency requirements, setting out which categories of personal data are subject to erasure requests and under what conditions, and should ensure that any partial erasure does not compromise the integrity or completeness of the historical business record. (see CPF 6 on Confidentiality and Privacy, and Annexe I 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'.[214] 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.[215] 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.[216] 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.[217] 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.[218]

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.

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.

213 Directive (EU) 2017/1132 (n 41) art 16(5).

214 See ISO 15489-1 (n 139).

215 See ISO/IEC 27001 (n 61).

216 See ISO/IEC 27040 (n 156) s 3.49.

217 See ISO/IEC 27040 (n 156) s 3.49.

218 See International Organization for Standardization, Information and documentation — Trusted third party repository for digital records (ISO 17068, 2017).

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 (see CPF 7 on Continual Improvement).

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.

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 and 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 (see CPF 17 on Reliability). 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 (see CPF 20 on System Validation). 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 (see CPF 8 on Continuity).

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 (see CPF 23 on 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,[219] regulatory fragmentation, or restrictions on cross-border data transfers.[220] 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.[221]

To address these risks, which vary depending on the EBR institutional model and operational context, the EBR should establish a structured Risk Management framework. It should include (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 of mitigation strategies; and (v) 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 (see CPF 13 on Integrity). 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

[219] BlackRock Investment Institute, 'Geopolitical Risk Dashboard' <https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard> accessed 3 April 2026.

[220] EY-Parthenon, 'How to factor geopolitics into technology strategy' (2021) <https://www.ey.com/en_gl/insights/geostrategy/how-to-factor-geopolitical-risk-into-technology-strategy> accessed 3 April 2026.

[221] Ivan Stechynskyi, 'Major Supply Chain Cybersecurity Concerns and 7 Best Practices to Address Them' (Syteca, 15 January 2025) <https://www.syteca.com/en/blog/supply-chain-security> accessed 3 April 2026.

resilience against adverse events, maintains stakeholder trust, and upholds its reputation as a reliable institution in the business ecosystem.

Chapter III on the Evaluation of Risks to Electronic Business Registries discusses 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,[222] 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[223] provides overarching guidelines for risk management across various sectors and organisational contexts.

In addition to the ISO/IEC standards referenced above, a private assurance framework SOC 2[224] (System and Organization Controls 2), focused on North American practices, provides critical guidance for organisations managing user data, particularly in cloud-based environments. Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 operational and security controls that align with the trust service criteria, which include security, availability, processing integrity, confidentiality, and privacy, are most relevant for registries procuring cloud or managed services from vendors who undergo SOC 2 audits as part of their contractual assurance obligations.

NIST Special Publication 800-37[225] 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 (see Chapter III for a more detailed overview).

Legal

The UNCITRAL Legislative Guide outlines the measures to be taken to protect the business registry record.[226] Recommendation 54 emphasises the necessity of protecting business registry records against loss or damage. Further, Recommendation 55 underscores the importance of safeguarding against accidental destruction of registry records. To this end, the law should stipulate the establishment of appropriate 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.[227] 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.

---

222 See International Organization for Standardization, Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005, 2022).

223 See International Organization for Standardization, Risk management — Guidelines (ISO 31000, 2018).

224 American Institute of Certified Public Accountants, 'SOC for Service Organizations' <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report> accessed 3 April 2026.

225 National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations (NIST Special Publication 800-37 Rev. 2, 2018).

226 UNCITRAL Legislative Guide, Recommendations 54 and 55.

227 Directive (EU) 2022/2555 (n 115).

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 manner aligned with their intended purpose, meet defined functional requirements, and address the specific needs of their operational environments, while 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 (see CPF 2 on Accessibility and CPF 24 on User-Centred Design).

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 (see CPF 8 on Continuity, CPF 19 on Risk Management and CPF 17 on Reliability). By grounding the validation process in the registry's specific operational realities, the outcome is not merely a technically compliant system but one capable of fulfilling its role reliably, securely, and efficiently in a variable, 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 (see CPF 1 on Access Control). 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. Continuous monitoring, coupled with periodic reassessment and regression testing, allows proactive identification of potential issues, ensuring the system remains aligned with its performance expectations and legal obligations.

As a standard process embedded in the EBR system, System Validation requires a dedicated staff with sufficient independence from the development team to ensure objectivity. 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 (see CPF 7 on Continual Improvement).

Technical

ISO/IEC 25010[228] 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, which includes managing, designing, executing, and documenting testing processes.[229] 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 property 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 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 users with almost instant, accurate and up-to-date information. This aspect of Timeliness refers to the expectation of Accessibility of information within a reasonable time,[230] which can be measured as latency, or the time delay, between when information is expected to be accessible and when it actually becomes accessible.[231] 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.

---

228 See ISO/IEC 25010 (n 205).

229 See International Organization for Standardization, International Electrotechnical Commission and Institute of Electrical and Electronics Engineers, Software and systems engineering — Software testing (ISO/IEC/IEEE 29119, 2022).

230 See David Loshin, Data Quality and Master Data Management (Elsevier 2008) 5.3.5 <https://search.worldcat.org/en/title/424595637> accessed 3 April 2026.

231 Loshin (n 230) 5.3.5; see generally Laura Sebastian-Coleman, Measuring Data Quality for Ongoing Improvement (Elsevier 2013) ch 5 <https://www.sciencedirect.com/book/9780123970336/measuring-data-quality-for-ongoing-improvement> accessed 3 April 2026.

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 for when a business can expect its requests to be processed, with these updates being published three times per week.[232]

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 6).[233] Still, some decisions involving complex legal or regulatory issues require balancing automation, timeliness and necessity of human oversight, often dictated by the risks involved and how they are treated under the applicable legal framework.

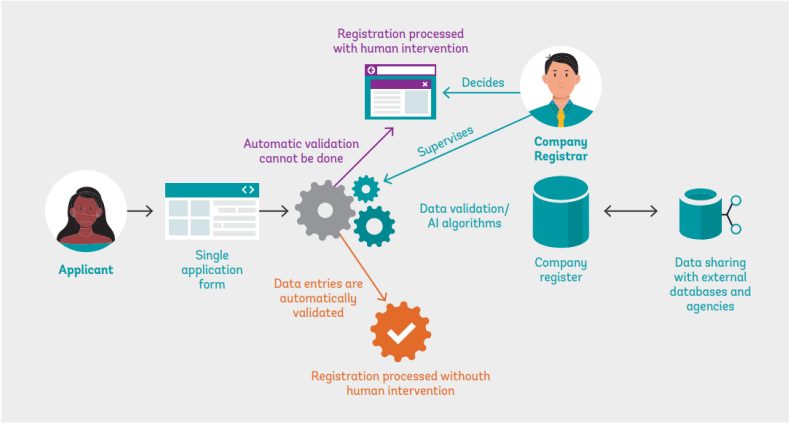


Figure 6: Illustration of real-time company registration.

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.[234] With the proliferation of cloud computing, combined time sources can deliver accurate time readings and are simple to integrate into EBRs.[235] Each EBR system element should be synchronised to the same time source and use consistent settings linked to the Coordinated Universal Time (UTC). Accurate time sources are important where the absolute time of a transaction affects its legal validity, for example, where

[232] Bolagsverket, 'Swedish Companies Registration Office' <https://bolagsverket.se/en/omoss/varverksamhet/varservice/varahandlaggningstider.2081.html> accessed 3 April 2026.

[233] World Bank Group, Data-Driven Company Registry: Guidance Note (n 8).

[234] See more Brian O'Donovan, 'Ireland's First National Timing Grid Launched' (RTÉ, 19 September 2023) <https://www.rte.ie/news/business/2023/0919/1406003-irelands-first-ever-national-timing-grid-launches/> accessed 3 April 2026.

[235] 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> accessed 3 April 2026.

statutory deadlines apply. The level of precision required is a design decision that considers cost, practicality, and the size of the timestamp being stored. Typically, UTC-synchronised timestamps accurate to the second should meet EBR requirements, while a Caesium Fountain Clock, which is accurate to one second per 300 million years, exceeds the level of precision 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 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).[236]

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 detects 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.[237]

Technical

ISO/IEC TS 25011 defines timeliness as the 'degree to which an IT service (3.3.2) delivers outcomes within time limits',[238] 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 protection of certain rights, such as a business name registration, prior to business entity registration. In such cases, the UNCITRAL Legislative Guide

---

236 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.

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

238 International Organization for Standardization and International Electrotechnical Commission, Information technology — Systems and software Quality Requirements and Evaluation (SQuaRE) — Service quality models (ISO/IEC TS 25011, 2017) 3.2.6.1.

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.[239]

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.[240]

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.[241] See CPF 3 on Accuracy, which addresses the relationship between the accuracy of registry data and legal compliance. Delays in registration or updates can compromise the availability of reliable information, impeding investigations and weakening compliance with international AML/CFT standards.

22. Transparency

Definition: The property 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 appropriate information about the registry's features, performance, limitations, components, policies, procedures, terminology, design choices, and assumptions available, in an understandable manner.[242] 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.[243]

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 the registry 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 reports in multiple visualisation formats and metadata describing

239 UNCITRAL Legislative Guide, para. 143.

240 UNCITRAL Legislative Guide, para. 144.

241 The FATF Recommendations (n 40) Interpretive Note to Recommendation 24 paras 9–11 and Recommendation 25 paras 6–9.

242 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.

243 See International Organization for Standardization and International Electrotechnical Commission, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology (ISO/IEC 22989, 2022) 5.15.8.

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 predefined transparency policies, and to offer user documentation in clear, non-technical language.

Transparency is a particular concern for AI systems,[244] and research in that area is useful as EBRs increasingly adopt emerging technologies and AI solutions. 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. As mentioned in CPF 3 on Accuracy, Transparency also extends to the provenance of registry data. Where registry records are derived from or validated against other authoritative data sources, the registry should disclose which source is authoritative for each data field and when it was last updated.

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.

[244] 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[245] 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[246] and ISO/IEC 22989[247] 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.[248] Further measures to enhance Transparency of the registry include defining the moment at which the registration of a business or any modification to the registered information becomes effective.[249] This also involves determining the time at which changes to the registered information become effective.[250]

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.[251] See Annexe I 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, 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

245 See International Organization for Standardization and International Electrotechnical Commission, Trustworthiness — Vocabulary (ISO/IEC TS 5723, 2022) 3.2.19.

246 See International Organization for Standardization and International Electrotechnical Commission, Information technology — Artificial intelligence — Transparency taxonomy of AI systems (ISO/IEC DIS 12792, 2024).

247 ISO/IEC 22989 (n 243) 5.15.8.

248 UNCITRAL Legislative Guide, paras. 44-45.

249 UNCITRAL Legislative Guide, Recommendation 26.

250 UNCITRAL Legislative Guide, Recommendation 31.

251 UNCITRAL Legislative Guide, para. 185.

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.[252] Functionality embodies the features, functions, and services provided by the registry.[253] Assurance is the measure of confidence that registry functionality is implemented correctly, operating as intended, and producing the desired result.[254] 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. Additionally, Transparency supports trust in the registry by enabling users to inform themselves of the registry's processes and procedures, making them more understandable. 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.

Legal Authority and Compliance is indispensable for the registry's Trustworthiness, since trust is undermined when legal authority and subsequent liability are 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.[255] Regular assessments, monitoring tools, and user feedback mechanisms are essential for Continual Improvement, maintaining user trust towards the registry and keeping 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 how to use them, reduce errors and build familiarity, all of which ultimately contribute to user trust.

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.[256] 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

252 See NIST Security and Privacy Controls for Information Systems and Organizations (n 49), 2.6.

253 NIST Security and Privacy Controls for Information Systems and Organizations (n 49), 2.6.

254 NIST Security and Privacy Controls for Information Systems and Organizations (n 49), 2.6.

255 See International Organization for Standardization, Space Data and Information Transfer Systems — Audit and Certification of Trustworthy Digital Repositories (ISO 16363, 2012; edn 2, 2025) 1.6.

256 ISO 16363 (n 255) 1.3.

among registry users.[257] 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 16363 technical standard addresses the Trustworthiness of EBRs indirectly from the perspective of Space Data and Information Transfer Systems (particularly, the Audit and Certification of Trustworthy Digital Repositories), but it is helpful in defining procedures for objectively auditing and certifying the trustworthiness of registries.[258] A regular cycle of audits and certification is required to maintain a trustworthy status.[259] 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).[260]

NIST Special Publication 800-53 provides an extensive and diverse list of controls focused on assurance, such as incident response training, security verification, continuous monitoring, and real-time analysis.[261]

The ITIL 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.[262] ITIL 4, launched in 2019, 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.[263] Usability is defined as the

257 ISO 16363 (n 255) 2.1.

258 ISO 16363 (n 255) 1.1, stating that the scope of the document is 'the entire range of digital repositories.'

259 ISO 16363 (n 255) 2.1.

260 ISO 16363 (n 255) 2.3, 5.2.

261 National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems: Special Publication 800-53 (NIST, 2017) Appendix E.

262 ITIL is now a stand-alone term, but originated from the Information Technology Infrastructure Library developed in 1989. See IBM, 'What is the IT Infrastructure Library (ITIL)?' <https://www.ibm.com/think/topics/it-infrastructure-library> accessed 3 April 2026.

263 See International Organization for Standardization, Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems (ISO 9241-210, 2019) 3.5.

extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction.[264]

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 '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 user 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.[265]

Applying UCD in the EBR context requires adopting the *design thinking* approach that views system and service 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.[266]

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.[267] The iterative process of research, design, redesign, and adaptation should integrate user feedback at every stage of design and development. 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.[268]

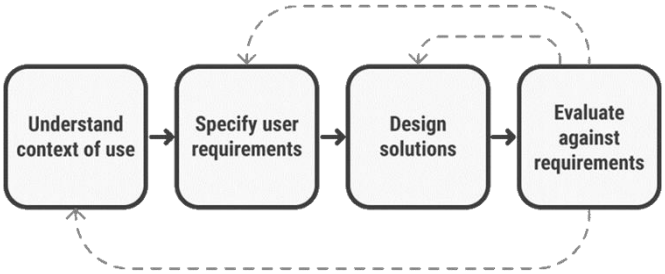


Figure 7: User-Centred Design is an iterative process that focuses on an understanding of the users and their context in all stages of design and development.[269]

An EBR should be designed around the diverse needs and expectations of its users.[270] 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

264 ISO 9241-210 (n 263) 3.13.

265 OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age (n 70).

266 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> accessed 3 April 2026.

267 See ISO 9241-210 (n 263) 3.7; see also UK Government Digital Service, '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/> accessed 3 April 2026.

268 See Interaction Design Foundation, 'User-Centred Design' <https://www.interaction-design.org/literature/topics/user-centered-design> accessed 3 April 2026; see also Justinmind, 'User-Centered Design: A Beginner's Guide' (15 October 2024) <https://www.justinmind.com/blog/user-centered-design/> accessed 3 April 2026.

269 Interaction Design Foundation (n 268).

270 Interaction Design Foundation (n 268).

'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, for instance, overburdened with complex legal and technical language, are difficult to understand, frustrate users and 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.[271]

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, progressive disclosure of complex business registration forms displays only the fields relevant to user needs without exposing them to additional unnecessary fields. An effective status dashboard provides real-time, plain-language updates that distinguish at minimum between received, under review, and completed, and, when a filing is queried, specifies precisely what requires attention and links directly to the correction workflow, reducing customer support inquiries.

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', includes principles and methods to enhance usability, requirements and recommendations for UCD principles and activities throughout the lifecycle of computer-based interactive systems.[272] It focuses on how 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[273] 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 practitioner guidance to evaluate and improve UCD. These heuristics include principles such as user control and freedom, error prevention, recognition rather than recall, and consistency.

Legal

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, a non-binding guidance, contain the fundamental principle 'Start with user needs', the Italian Design Guidelines for websites and digital services for public administration require ease of

271 See ISO 9241-210 (n 263) 3.15.

272 See ISO 9241-210 (n 263) 3.7.

273 World Wide Web Consortium (W3C), 'WCAG 2.2 at a Glance' <https://www.w3.org/WAI/standards-guidelines/wcag/glance/> accessed 3 April 2026.

reference and user experience, and the Australian Digital Service Standard, which has a contractual force for certain governmental services, operates under the 'Know your user' criterion.[274]

The EU Web Accessibility Directive (Directive (EU) 2016/2102) further reinforces the design obligations discussed here by requiring public sector bodies to publish accessibility statements and provide mechanisms for users to report barriers (see CPF 2 on Accessibility).

[274] See more OECD Observatory of Public Sector Innovation (OPSI), 'Government Digital Service Design Principles' <https://oecd-opsi.org/toolkits/government-digital-service-design-principles/>; Agenzia per l'Italia Digitale (AgID), 'Guidelines' <https://www.agid.gov.it/en/guidelines>; and Australian Government Digital Transformation Agency, 'Digital Service Standard' <https://www.digital.gov.au/policy/digital-experience/digital-service-standard> accessed 3 April 2026.

CHAPTER THREE

Evaluation of Risks to Electronic Business Registries

III. EVALUATION OF RISKS TO ELECTRONIC BUSINESS REGISTRIES

Chapter II identified the 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 requires a more detailed discussion. Risk in EBRs spans IT, legal, operational, organisational, and reputational dimensions, and risk management must be treated as a strategic governance function embedded in leadership decision-making, not merely a compliance function. Effective risk management enables proactive responses to threats, builds resilience, and maintains stakeholder trust.

To this end, this Chapter provides 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 Confidentiality, Integrity, and Availability (CIA) triad.

A. CONTEXTUALISING RISK IN EBRs

The risk that the EBR may not perform as intended by its designers and as expected by its users is inherently difficult to quantify. It is influenced by required features, implementation decisions, and the operating environment that evolves in ways that cannot be fully anticipated. 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.'[275]

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 context.[276] 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 activities and decision-making;
(ii) structured and comprehensive, contributing to consistent and comparable results;
(iii) customised and proportionate to the external and internal context;
(iv) inclusive, so that stakeholders are appropriately and timely involved;
(v) dynamic, able to anticipate, detect, acknowledge, and respond to risk changes and risk events;
(vi) based on the best available information and future expectations;

[275] National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems (FIPS Publication 200, March 2006) 17 <https://doi.org/10.6028/NIST.FIPS.200> accessed 3 April 2026; see also National Institute of Standards and Technology, 'Risk Management Framework' <https://csrc.nist.gov/projects/risk-management> accessed 3 April 2026.

[276] ISO 31000 (n 223).

(vii) subject to human behaviour and culture; and
(viii) continually improving through learning and experience.

Of particular relevance is Clause 5.4.3, which addresses the need to clearly assign and communicate organisational roles, authorities, responsibilities, and accountabilities in risk management. In an EBR context, this means that a registrar, or another authority in charge of the business registry, should treat risk management as a core institutional responsibility rather than delegating it solely to technical and/or compliance staff. Specifically, the registry should identify risk owners, i.e. individuals with both the authority and the accountability to manage specific categories of risk. The assignment of these roles and the registry's overall risk posture should be documented and reported regularly to the oversight body responsible for the registry, whether a supervisory authority, ministry, or another institution, in accordance with applicable law.

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.[277] 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 a 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.

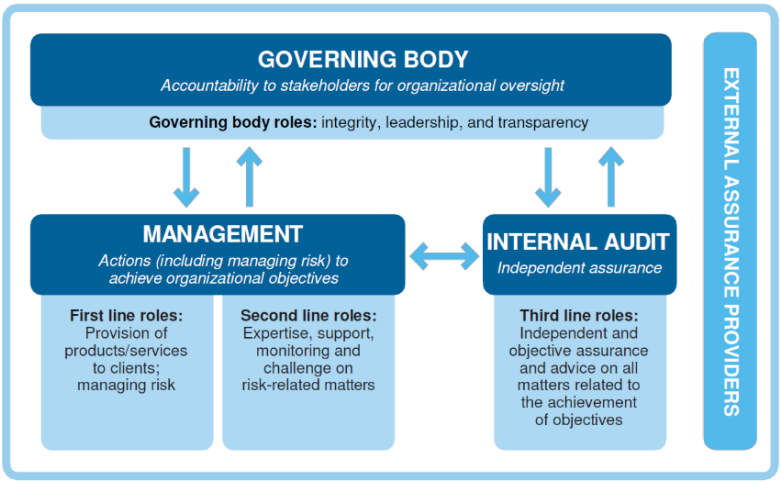


Figure 8: 3LoD Model.

[277] The Institute of Internal Auditors, 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> accessed 3 April 2026.

Some organisations extend the model to include external oversight bodies such as regulators or supervisory authorities as an additional accountability layer, an adaptation that is appropriate for EBRs subject to governmental oversight. ISO 31000 principles, particularly the structured and comprehensive approach, integration in all organisational activities, and continual improvement, 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 under GDPR and NIS2, or equivalent regulatory frameworks, such structured models are not just best practices but rather implicit or explicit obligations.

C. INFORMATION SECURITY TRIAD AND NIST

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 CIA triad, a model widely endorsed by NIST and embedded in ISO/IEC 27001.[278] These three principles form the backbone of secure system design; failure in any one of these dimensions compromises not only technical operations but also the legal and reputational integrity of the registry.[279]

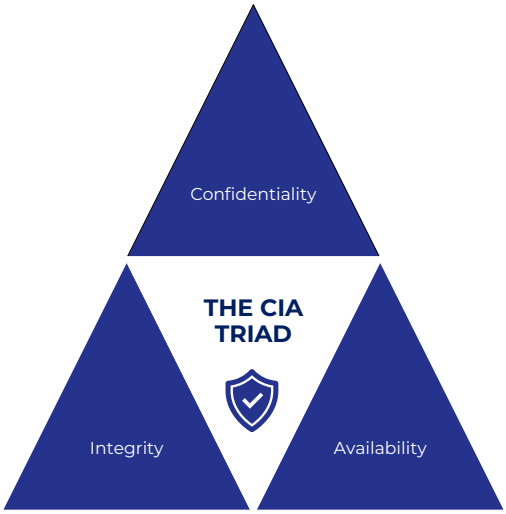


Figure 9: Model of the security triad in information systems.

Importantly, the performance of the CIA triad and, respectively, the corresponding three CPFs is dependent on many of the other CPFs, creating interdependencies that compound risk. For instance, Confidentiality requires Access Control to prevent unauthorised access to specific data (e.g., a user's PII or login credentials). Integrity requires, *inter alia*, consistent performance of Accuracy, Reliability, Retention and Disposition, Data Input Validation, and Access Control to maintain the legal validity of

[278] See, e.g., National Institute of Standards and Technology, NIST Special Publication 800-12 Rev 1: An Introduction to Information Security (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.'

[279] For cloud computing, a similar well-established triad consists of security, portability, and interoperability. See generally, National Institute of Standards and Technology, NIST Cloud Computing Standards Roadmap (Special Publication 500-291 Version 2, 2013); see also Object Management Group, Interoperability and Portability for Cloud Computing: A Guide (Version 3.0, 2022) <https://www.omg.org/cgi-bin/doc?mars/2022-12-13> accessed 3 April 2026.

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 normative foundation that defines what the CIA triad must achieve — the minimum standards for Confidentiality, Integrity, and Availability that the registry is legally required to uphold. Trustworthiness and Risk Management as CPFs are, in turn, contingent on how effectively those standards are met in practice: a registry that cannot secure its data, guarantee its Integrity, or ensure Availability cannot credibly claim to be Trustworthy, nor can its Risk Management be considered adequate.[280]

To translate these principles into operational practice, registries can 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) preparation to managing security and privacy risks, (ii) categorisation of system and information processed, stored, and transmitted based on an impact analysis, (iii) selection of security controls to protect the system based on risk assessment(s), (iv) implementation of security controls and deployment documentation, (v) assessment of security controls' operation and their results, (vi) authorisation of the system to operate, and (vii) continuous monitoring of control implementation and risks to the system.

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 4 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.

Impact Level	Extent of adverse effect on registry operations, assets and financial standing
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.

[280] See NIST Recommended Security Controls for Federal Information Systems (n 261) 308, defining Trustworthiness as: 'The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to 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.'

High	Severe or catastrophic, such as (i) severe degradation in or loss of registry capability to an extent and duration that the registry cannot perform one or more of its primary functions; (ii) major damage to registry assets; or (iii) major financial loss.

Table 4: Classification of Potential Impact (Adapted from NIST FIPS 199).[281]

D. RISK MAPPING OF CPF NON-PERFORMANCE

A key application of risk evaluation is to understand how the non-performance of each CPF affects the registry's operation. Table 5 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.

The risk mapping in Table 5 shows individual CPF risks, but registries should also consider the combined and cascading effects of multiple CPF failures. The EBR's risk assessment should evaluate how risks interconnect and amplify outcomes beyond single failures. IEC 31010, which supports ISO 31000 by providing risk assessment techniques, recommends scenario-based analysis. In an EBR, for example, a degradation in Data Input Validation combined with a failure of Error Detection may together produce Integrity failures that would not have arisen from either failure alone. Similarly, concurrent non-performance of Authentication and Access Control can affect the registry's Confidentiality and Privacy beyond their individual impact. Continuous monitoring enables registries to address degradation in a single CPF before it affects other CPFs.

CPF	Result of non-performance	Impact Level
1. Access Control	Privileged access is not restricted; unauthorised data manipulation, tampering or deletion is possible.	High
2. Accessibility	Registry or parts of it are unavailable to users with limited abilities, digital literacy, or connectivity.	Moderate to High
3. Accuracy	Inaccurate records undermine legal value and user trust in the registry.	High
4. Authentication	Users are not properly verified, enabling unauthorised submissions or access to the data.	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; failure is cumulative, immediate operational impact is limited
8. Continuity	System downtime impairs operational resilience and public access.	Moderate to High

[281] National Institute of Standards and Technology, Guide for Mapping Types of Information and Information Systems to Security Categories (NIST Special Publication 800-60 Vol. 1, 2008).

9. Correctability	Errors cannot be rectified, potentially leading to legal disputes, financial harm, and regulatory non-compliance.	Moderate to High
10. Data Input Validation	Invalid, erroneous or incomplete submissions are accepted into the system.	High
11. Error Detection	Errors are unnoticed, creating persistent inaccuracies and affecting the legal validity of registry records.	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, undermining reliance by third parties and courts.	High
14. Interoperability	Registry is unable to interact effectively with other systems.	Low to High; the impact depends on whether the registry operates in isolation or as part of an interconnected system
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 system performance erodes user confidence and disrupts time-sensitive legal or commercial processes.	High
18. Retention and Disposition	Data is retained or deleted inconsistently with legal requirements.	Low, where minor administrative records are disposed of incorrectly, to High, where legally required records are destroyed
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 legal challenges to registry records.	High
24. User-Centred Design	Interface complexity leads to input errors or user exclusion.	Moderate to High

Table 5: Risks and impacts of CPF non-performance.

III. EVALUATION OF RISKS TO ELECTRONIC BUSINESS REGISTRIES

Given their critical role in enabling legal certainty and commercial transparency, EBRs are encouraged to adopt structured, principle-based Risk Management approaches, such as ISO 31000, the 3LoD, and the NIST RMF. Structured Risk Management, embedded in governance and responsive to the registry's specific context, is the foundation on which the reliability and legitimacy of EBRs ultimately rest.

CHAPTER FOUR

Conclusion

IV. CONCLUSION

The 24 Critical Performance Factors presented in this Guide on Best Practices for Electronic Business Registries define a comprehensive framework for the design, operation, and governance of EBRs, integrating legal authority, technological resilience, interoperability, and usability within a single coherent architecture.

This Guide responds to the need for meaningful guidance to registry designers and operators across different legal environments, institutional arrangements, and stages of digital transformation, including those transitioning from paper-based systems, modernising legacy platforms, or establishing new registries. The CPF approach, first developed by the BPER Project for electronic collateral registries and now adapted and extended for business registries, is suited to that task precisely because it focuses on performance outcomes rather than prescribing specific technical or legal solutions, allowing registries to adapt the framework to their own institutional and legal context.

Complementing the CPFs in Chapter II, this Guide incorporates international standards and reference materials, offering registries a resource base for evaluating their specific legal, technical, or operational challenges. The Guide reflects both comparative legal analysis and practitioner experience, ensuring that the CPFs address challenges encountered in real-world registry operations rather than theoretical ideals. It seeks to provide both a practical toolkit and a foundation for further reflection and development for those charged with strengthening their registries.

A useful insight from this Guide is that the 'critical' nature of a CPF implies that its non-performance has not only a technical impact, but may also lead to legal, reputational, and operational consequences. It is illustrated by the risk mapping exercise in Chapter III, where the majority of CPFs, if neglected, produce high-impact outcomes that affect the registry's legal validity, its credibility as a public institution, or its ability to serve the economic and societal functions for which it was established.

Registries are encouraged to revisit this Guide as their institutional contexts develop, using it not as a static standard but as a basis for continuous evaluation and improvement, and helping them to remain reliable, resilient, and responsive to the needs of businesses, governments, and society at large.

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.[282]
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.[283]
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.
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.[284]
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.

[282] *Encyclopaedia Britannica*, 'Accountability' <https://www.britannica.com/topic/accountability> accessed 3 April 2026.

[283] Foster Moore, 'Glossary of Registry Terms and Acronyms' <https://www.fostermoore.com/glossary-of-registry-terms-and-acronyms> accessed 3 April 2026.

[284] World Bank, Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO) (2018) <https://hdl.handle.net/10986/31825> accessed 3 April 2026.

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 whereby source code, data, or documentation of the registry system is deposited with a neutral third party, to be released under specified conditions such as vendor insolvency or material breach of contract.
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, with no or minimal restrictions on 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.
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 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	In the context of data processing, the state of having submitted data confirmed as meeting the format, completeness, and logical consistency requirements of the registry system before it is accepted and recorded. Validation is distinct from Authentication, which concerns identity verification, and from Accuracy, which concerns the truthfulness of the data's content.
Vulnerability	A weakness of an asset or control that can be exploited so that an event with a negative consequence occurs.[285]

Table 6: Definition of terms.

[285] ISO/IEC 27005 (n 222).

ANNEXE I: SCOPE OF PUBLICLY AVAILABLE INFORMATION

The design and operation of EBRs should 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 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 Annexe 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:[286]

(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;

[286] UNCITRAL Legislative Guide, paras. 129 and 131.

(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.[287]

Information required at a post-registration stage may include:[288]

(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

(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, as amended by Directive 2025/25, 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;

287 UNCITRAL Legislative Guide, para. 130.
288 UNCITRAL Legislative Guide, para. 156.

(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; it shall be apparent from the disclosure whether the persons authorised to represent the company may do so 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 capital subscribed, where the instrument of constitution or statutes mention an authorised capital, unless any increase in the capital subscribed necessitates an amendment of the statutes;
(f) the accounting documents for each financial year which 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;
(l) the object of the company, describing its main activity or activities, which can be expressed using the relevant Statistical Classification of Economic Activities in the European Community (NACE) code, where such code is used for the purposes of the register pursuant to applicable national law, and where the object is recorded in the national register."[289]

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:[290]

(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:

289 Directive (EU) 2017/1132 (n 41).

290 The FATF Recommendations (n 40) Interpretive Note to Recommendation 24 paras 4–5.

- 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*.[291] 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 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 sixth AML Directive[292] seeks to provide more clarity on which third parties have access to the 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, members 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 with legitimate interest 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, 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

[291] Joined Cases C-37/20 and C-60/20 WM and Sovim SA v Luxembourg Business Registers [2022] ECLI:EU:C:2022:912.

[292] 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 [2024] OJ L.

partial identification numbers are available to the public. In Tunisia, personal data is disclosed only to competent authorities or through a 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 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 requester's identity and legal eligibility, while in Ghana, BO data is provided upon request to competent authorities free of charge, through formal letters. 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 be able to achieve a 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 proportional 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, registries should establish mechanisms for the regular review and adjustment of their disclosure and access practices in light of jurisprudence, legislative reforms, and international commitments. Ensuring compliance while upholding the goals of transparency and data protection requires continuous legal oversight and technical adaptability from modern EBRs.

ANNEXE 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 7 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 8000-114	Data quality: master data and data portability
	ISO 8000-115	Data quality: master data and exchange of quality identifiers
	ISO 8000-116	Data quality: master data, exchange of quality identifiers for authoritative legal entity identifiers
	ISO 9001	Quality management systems
	ISO/IEC 25012	Data quality model
	ISO/IEC 7064	Check character systems
	NIST SP 800-53	Data Input Validation

ANNEXE II: RELEVANT TECHNICAL STANDARDS

Category	Standard	Scope
Electronic Signatures	ETSI EN 319 422	Electronic signatures and infrastructures
Encryption	IEEE 1619.1-2019	Cryptographic units for storage device encryption
	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/IEC 19941	Cloud computing interoperability and portability
	ISO 22745	Open technical dictionaries for industrial automation systems and integration
	ISO/DIS 25500-3	Supply chain interoperability and integration, Verification of trading entity identity
	ISO 8601	Date and time — Representations for information interchange
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

Category	Standard	Scope
	ISO/IEC TS 25011	Service quality models for software evaluation (SQuaRE)
	ISO/IEC/IEEE 29119	Framework for software testing
	NIST SP 800-218	Secure Software Development Framework
Trustworthiness	ISO 16363	Requirements for auditing trustworthy digital repositories

Table 7: 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 how 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.[293]

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.

[293] See International Organization for Standardization, ISO in Brief (ISO 2019) 10 <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf> accessed 3 April 2026.

Publisher	Title
American Institute of Certified Public Accountants (AICPA)	System and Organization Controls (SOC) 2[294]
AWS	AWS Well-Architected Framework (2020)[295]
Cloud Security Alliance	Security Guidance for Critical Areas of Focus in Cloud Computing (v5, 2024)[296]
DAMA	DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) (2017)[297]
OWASP	OWASP Top Ten[298]
OMG	Interoperability and Portability for Cloud Computing: A Guide[299]
SNIA	Data Protection Best Practices (2025)[300]
World Wide Web Consortium (W3C)	Web Content Accessibility Guidelines[301]

Table 8: 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.[302] Information security does not end with the infrastructure setup or with the issuance of a security policy.[303] Instead,

294 See American Institute of Certified Public Accountants, 'System and Organization Controls (SOC) Suite of Services' <https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services> accessed 3 April 2026.

295 AWS, 'AWS Well-Architected Framework' (Amazon Web Services 2024) <https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html> accessed 3 April 2026.

296 Cloud Security Alliance, 'Security Guidance for Critical Areas of Focus in Cloud Computing' (v5, 2024) <https://cloudsecurityalliance.org/artifacts/security-guidance-v5> accessed 3 April 2026.

297 See DAMA International, 'Data Management Body of Knowledge' (2017) <https://www.dama.org/cpages/body-of-knowledge> accessed 3 April 2026.

298 See OWASP Foundation, 'OWASP Top Ten Web Application Security Risks' <https://owasp.org/www-project-top-ten/> accessed 3 April 2026.

299 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> accessed 3 April 2026.

300 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> accessed 3 April 2026.

301 See World Wide Web Consortium (W3C), 'Web Content Accessibility Guidelines (WCAG)' <https://www.w3.org/WAI/standards-guidelines/wcag> accessed 3 April 2026.

302 Kelley Dempsey and others, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST Special Publication 800-137, National Institute of Standards and Technology 2011) vi; see also Kelley Dempsey and others, ISCMA: An Information Security Continuous Monitoring Program Assessment (NIST Interagency/Internal Report (NISTIR) 8212, National Institute of Standards and Technology, March 2021).

303 NIST An Introduction to Information Security (n 278) 2.7.

continuous monitoring and management are required to protect the Confidentiality, Integrity, and Availability of information over time.[304]

With evolving technology come new threats and vulnerabilities that must be identified and addressed.[305] Information security continuous monitoring (ISCM) is defined as 'maintaining ongoing awareness of information security, vulnerabilities, and threats to support organisational risk management decisions'.[306] 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.[307] 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.[308] By providing actionable information on security status, ISCM enables the transition from compliance-driven to data-driven risk management.[309] 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. [310]

Figure 10: NIST Cybersecurity Framework Functions. [311]

304 NIST An Introduction to Information Security (n 278) 2.7.
305 NIST An Introduction to Information Security (n 278) 2.7.
306 See Kelley Dempsey and others, (n 301, 1) vi.
307 See Kelley Dempsey and others, (n 301, 1) 3.
308 See Kelley Dempsey and others, (n 301, 1) vi.
309 See Kelley Dempsey and others, (n 301, 1) vii.
310 National Institute of Standards and Technology, The NIST Cybersecurity Framework 2.0 (2024) 3–4 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> accessed 3 April 2026.
311 NIST, Cybersecurity Framework 2.0 (n 309).

Each function is broken down into categories and subcategories, which represent more specific outcomes of technical and management activities.[312] 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').[313] 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.[314] 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.[315] Similarly to 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.[316] The ISO/IEC TR 27103 standard facilitates standard-to-framework mapping, enabling EBRs to build cohesive systems using both strategic frameworks and detailed standards.

312 NIST, Cybersecurity Framework 2.0 (n 309) Table 1: CSF 2.0 Core Function and Category names and identifiers.

313 NIST, Cybersecurity Framework 2.0 (n 309) p 19.

314 See ISO/IEC TR 27103, Information Technology — Security Techniques — Cybersecurity and ISO and IEC Standards (2018).

315 ISO/IEC TR 27103 (n 313) 6.2.

316 ISO/IEC TR 27103 (n 313) Annex A.

BIBLIOGRAPHY

A. Legal Sources

1. Accounting and Corporate Regulatory Authority Act 2004 (Singapore)

2. Act on the Organisation of the Courts (Austria)

3. Commercial Register Act (Estonia)

4. Companies Act 2006 (United Kingdom)

5. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73

6. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies [2016] OJ L327/1

7. Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law [2017] OJ L169/46

8. 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 [2019] OJ L186/80

9. 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 [2019] OJ L 321/1

10. 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) [2022] OJ L333/80

11. 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 [2024] OJ L 2024/1640

12. 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 [2024] OJ L2853

13. 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 [2025] OJ L25

14. 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 [2014] OJ L173/349

15. Economic Crime and Corporate Transparency Act 2023 (United Kingdom) s 1081A

16. Operation of Public Registry Statutes Act, SS 2013

17. Regulation (EU) 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) [2016] OJ L 119/1

18. 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] OJ L 1183

19. 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) [2024] OJ L 2024/903

20. Sebry v Companies House [2015] EWHC 115 (QB))

21. Joined Cases C-37/20 and C-60/20 WM and Sovim SA v Luxembourg Business Registers [2022] ECLI:EU:C:2022:912

B. Intergovernmental, International, and Governmental Publications

22. Agenzia per l'Italia Digitale (AgID), 'Guidelines' <https://www.agid.gov.it/en/guidelines>

23. Asia-Pacific Economic Cooperation, APEC Privacy Framework (2015) <https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015)> accessed 3 April 2026

24. Australian Government Digital Transformation Agency, 'Digital Service Standard' <https://www.digital.gov.au/policy/digital-experience/digital-service-standard> accessed 3 April 2026

25. Australian Government, 'B2G Hub' <https://www.ppsr.gov.au/b2g-hub> accessed 3 April 2026

26. Clark J, Marin G, Ardic Alper OP and Galicia Rabadan GA, Digital Public Infrastructure and Development: A World Bank Group Approach (Digital Transformation White Paper vol 1, World Bank 2025) < https://hdl.handle.net/10986/42935> accessed 3 April 2026

27. Department for Business, Energy and Industrial Strategy, Corporate Transparency and Register Reform (CP 638, February 2022) <https://www.gov.uk/government/publications/corporate-transparency-and-register-reform/corporate-transparency-and-register-reform-accessible-webpage> accessed 3 April 2026

28. European Banking Authority, Final Report on Guidelines on Outsourcing Arrangements (2019)

29. European Commission, ABR Factsheet 2017: Denmark – Access to Base Registries in Denmark (2017) <https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Denmark%20Factsheet%20Final_DIGST_everis.pdf> accessed 3 April 2026

30. European Commission, 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> accessed 3 April 2026

31. European Law Institute, 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> accessed 3 April 2026

32. European Securities and Markets Authority, 'Sustainability Reporting' <https://www.esma.europa.eu/esmas-activities/sustainable-finance/sustainability-reporting> accessed 3 April 2026

33. 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> accessed 3 April 2026

34. Financial Action Task Force, The FATF Recommendations (2012, updated 2025) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> accessed 3 April 2026

35. International Finance Corporation, Secured Transactions, Collateral Registries and Movable Asset-Based Financing (IFC Knowledge Guide 2019) <https://documents1.worldbank.org/curated/en/193261570112901451/pdf/Knowledge-Guide.pdf> accessed 3 April 2026

36. Investment Climate Advisory Services (World Bank Group), Innovative Solutions for Business Entry Reforms: A Global Analysis (2012) <https://documents1.worldbank.org/curated/en/196211468137721462/pdf/770990WP0inves0B00PUBLIC00july02012.pdf> accessed 3 April 2026

37. Khuram Farooq, Joseph Huntington La Cascia, Knut J Leipold, Bertram Boie, Data Classification Matrix and Cloud Assessment Framework: Cloud Assessment Framework and Evaluation Methodology (English) (Equitable Growth, Finance and Institutions Insight, Report No 180672, World Bank Group) <http://documents.worldbank.org/curated/en/099114503072340316> accessed 3 April 2026

38. Monetary Authority of Singapore, Guidelines on Business Continuity Management (2022) <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management> accessed 3 April 2026

39. Organisation for Economic Co-operation and Development Observatory of Public Sector Innovation (OPSI), 'Government Digital Service Design Principles' <https://oecd-opsi.org/toolkits/government-digital-service-design-principles/> accessed 3 April 2026

40. Organisation for Economic Co-operation and Development, Good Practice Principles for Public Service Design and Delivery in the Digital Age (OECD Public Governance Policy Papers No 23, OECD Publishing 2022) <https://doi.org/10.1787/2ade500b-en> accessed 3 April 2026

41. Organisation for Economic Co-operation and Development, Governing with Artificial Intelligence: Are Governments Ready? (OECD Artificial Intelligence Papers No 20, OECD Publishing 2024) <https://doi.org/10.1787/26324bc2-en> accessed 3 April 2026

42. 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 (2024) <https://ctcap.org/wp-content/uploads/2024/05/BPER-Report-of-the-7th-Workshop.pdf> accessed 3 April 2026

43. UNIDROIT, Guide on Best Practices for Electronic Collateral Registries (Cape Town Convention Academic Project, 2021)

44. United Nations Commission on International Trade Law, UNCITRAL Legislative Guide on Key Principles of a Business Registry (2018) <https://uncitral.un.org/en/texts/msmes/legislativeguides/business_registry> accessed 3 April 2026

45. United Nations Commission on International Trade Law, UNCITRAL Model Law on Automated Contracting (2025) <https://uncitral.un.org/en/mlac> accessed 3 April 2026

46. United Nations Conference on Trade and Development, World Investment Report 2024 (2024) 'Investment Facilitation and Digital Government' <https://unctad.org/system/files/official-document/wir2024_ch04_en.pdf> accessed 3 April 2026

47. Willie RJ and others, 'Business Regulation – Leveraging Technology to Support Business Registration Reform: Insights from Recent Country Experience' (World Bank, Investment Climate in Practice 2011) <https://openknowledge.worldbank.org/server/api/core/bitstreams/3c6df1c2-0bcd-5f45-92b8-996e935c7ab7/content> accessed 3 April 2026

48. World Bank Group, Data-Driven Company Registry: Guidance Note (2022) <https://documents1.worldbank.org/curated/en/099435008302231899/pdf/P17553401702c10490be6e02112bae75050.pdf> accessed 3 April 2026

49. World Bank Group, Institutional and Procurement Practice Note on Cloud Computing: Cloud Assessment Framework and Evaluation Methodology (Equitable Growth, Finance and Institutions Insight, World Bank Group) <http://documents.worldbank.org/curated/en/099114503072319732> accessed 3 April 2026

50. World Bank, Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO) (2018) <https://hdl.handle.net/10986/31825> accessed 3 April 2026

51. World Bank, Responsible Use of Technology in Credit Reporting: White Paper (2022) <http://hdl.handle.net/10986/38312> accessed 3 April 2026

C. Technical Standards and Frameworks

52. DAMA International, 'Data Management Body of Knowledge' (2017) <https://www.dama.org/cpages/body-of-knowledge> accessed 3 April 2026

53. Dempsey K and others, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST Special Publication 800-137, National Institute of Standards and Technology 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf> accessed 3 April 2026

54. Dempsey K and others, ISCMA: An Information Security Continuous Monitoring Program Assessment (NIST Interagency/Internal Report (NISTIR) 8212, National Institute of Standards and Technology, March 2021) <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8212.pdf> accessed 3 April 2026

55. European Telecommunications Standards Institute, ETSI EN 319 422 V1.1.1: Electronic Signatures and Infrastructures (ESI) — Time-Stamping Protocol and Time-Stamp Token Profiles (2016)

56. Financial Reporting Council, ISA (UK) 320: Materiality in Planning and Performing an Audit (May 2022) <https://media.frc.org.uk/documents/ISA_UK_320_Updated_May_2022_aJAQtFV.pdf> accessed 3 April 2026

57. Global Standards Council, Global Reference Architecture (GRA) Information Sharing Enterprise Service-Level Agreement (US Department of Justice, Global Infrastructure/Standards Working Group, April 2011) <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/GRAInformationSharingEnterpriseService-LevelAgreement-Final11April2011.pdf> accessed 3 April 2026

58. IEEE, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices (IEEE 1619.1-2019, 2019)

59. International Association of Commercial Administrators, XML Technical Specifications for Uniform Commercial Code Filings: Revised Article 9 (Version 4.00, 2019) <https://www.iaca.org/secured-transactions/xml-technical-specifications/> accessed 3 April 2026

60. InterNational Committee for Information Technology Standards, INCITS 359-2012 (R2022): Information Technology — Role Based Access Control (2012, revised 2022) <https://webstore.ansi.org/standards/incits/incits3592012r2022?source=blog&_gl=1*16xxwwu*_gcl_au*NzAyOTA1OTE2LjE3NDA2OTgwNDU> accessed 3 April 2026

61. International Organization for Standardization and International Electrotechnical Commission, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology (ISO/IEC 22989, 2022)

62. International Organization for Standardization and International Electrotechnical Commission, Information technology — Artificial intelligence — Transparency taxonomy of AI systems (ISO/IEC DIS 12792, 2024)

63. International Organization for Standardization and International Electrotechnical Commission, Information technology — Security techniques — Cybersecurity and ISO and IEC Standards (ISO/IEC TR 27103, 2018)

64. International Organization for Standardization and International Electrotechnical Commission, Information technology — Security techniques — Storage security (ISO/IEC 27040, 2nd edn, 2024)

65. International Organization for Standardization and International Electrotechnical Commission, Information technology — Systems and software Quality Requirements and Evaluation (SQuaRE) — Service quality models (ISO/IEC TS 25011, 2017)

66. International Organization for Standardization and International Electrotechnical Commission, Trustworthiness — Vocabulary (ISO/IEC TS 5723, 2022)

67. International Organization for Standardization, Data quality — Part 114: Master data: Application of ISO/IEC 21778 and ISO 8000-115 to portable data (ISO 8000-114, 2024)

68. International Organization for Standardization, Data quality — Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements (ISO 8000-115, 2024)

69. International Organization for Standardization, Data quality — Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 to authoritative legal entity identifiers (ISO 8000-116, 2019)

70. International Organization for Standardization, Date and time — Representations for information interchange (ISO 8601-1, 2019)

71. International Organization for Standardization, Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems (ISO 9241-210, 2019)

72. International Organization for Standardization, Industrial automation systems and integration — Open technical dictionaries and their application to master data (ISO 22745, 2010)

73. International Organization for Standardization, Information and documentation — Trusted third party repository for digital records (ISO 17068, 2017)

74. International Organization for Standardization, Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005, 2022)

75. International Organization for Standardization, Information technology — Vocabulary (ISO/IEC 2382, 2015)

76. International Organization for Standardization and International Electrotechnical Commission, Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.2 (ISO/IEC 40500, 2012).

77. International Organization for Standardization, International Electrotechnical Commission and Institute of Electrical and Electronics Engineers, Software and systems engineering — Software testing (ISO/IEC/IEEE 29119, 2022)

78. International Organization for Standardization, ISO 15489-1: Information and Documentation — Records Management (2016)

79. International Organization for Standardization, ISO 22301: Security and Resilience — Business Continuity Management Systems — Requirements (2019)

80. International Organization for Standardization, ISO 32000-2: Document Management — Portable Document Format (2020)

81. International Organization for Standardization, ISO 8000-8: Data Quality — Part 8: Information and Data Quality — Concepts and Measuring (2015)

82. International Organization for Standardization, ISO in Brief (ISO 2019) <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf> accessed 3 April 2026

83. International Organization for Standardization, ISO/IEC 18033: Information Technology — Security Techniques — Encryption Algorithms (2010)

84. International Organization for Standardization, ISO/IEC 19941: Information Technology — Cloud Computing — Interoperability and Portability (2017)

85. International Organization for Standardization, ISO/IEC 20889: Privacy-Enhancing Data De-Identification Terminology and Classification of Techniques (2018)

86. International Organization for Standardization, ISO/IEC 24760-1: IT Security and Privacy — A Framework for Identity Management — Part 1: Terminology and Concepts (2019)

87. International Organization for Standardization, ISO/IEC 25012: Software Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Data Quality Model (2008)

88. International Organization for Standardization, ISO/IEC 27000 family — Information Security Management (2022)

89. International Organization for Standardization, ISO/IEC 27000: Information Security Management Systems — Overview and Vocabulary (2018)

90. International Organization for Standardization, ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements (2022)

91. International Organization for Standardization, ISO/IEC 27002: Information Security, Cybersecurity and Privacy Protection — Information Security Controls (2022)

92. International Organization for Standardization, ISO/IEC 27034-1: Information Technology — Security Techniques — Application Security (2011)

93. International Organization for Standardization, ISO/IEC 29100: Information Technology — Security Techniques — Privacy Framework (2024)

94. International Organization for Standardization, ISO/IEC 7064: Information Technology — Security Techniques — Check Character Systems (2003)

95. International Organization for Standardization, ISO/IEC 9798-1: Information Technology — Security Techniques — Entity Authentication (2010)

96. International Organization for Standardization, Risk management — Guidelines (ISO 31000, 2018)

97. International Organization for Standardization, Security and resilience (ISO/DIS 22300, 2016)

98. International Organization for Standardization, Space Data and Information Transfer Systems — Audit and Certification of Trustworthy Digital Repositories (ISO 16363, 2012; edn 2, 2025)

99. International Organization for Standardization, Supply chain interoperability and integration — Part 3: Verification of trading entity identity (ISO/DIS 25500-3)

100. International Organization for Standardization, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models (ISO/IEC 25010, 2011)

101. McCallister E, Grance T and Scarfone K, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (National Institute of Standards and Technology Special Publication 800-122, 2010) <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990> accessed 3 April 2026

102. National Institute of Standards and Technology, Advanced Encryption Standard (AES) (FIPS PUB 197, 2001, updated 2023)

103. National Fire Protection Association, NFPA 1660: Standard for Emergency, Continuity, and Crisis Management — Preparedness, Response, and Recovery (2024)

104. National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34 Rev 1, 2010)

105. National Institute of Standards and Technology, Cybersecurity Log Management Planning Guide (NIST Special Publication 800-92 Rev 1, Initial Public Draft, 2023) <https://csrc.nist.gov/pubs/sp/800/92/r1/ipd> accessed 3 April 2026

106. National Institute of Standards and Technology, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST Special Publication 800-160 vol 2, 2021)

107. National Institute of Standards and Technology, Guide for Mapping Types of Information and Information Systems to Security Categories (NIST Special Publication 800-60 Vol. 1, 2008)

108. National Institute of Standards and Technology, Guide to Attribute Based Access Control (ABAC) Definition and Considerations (NIST Special Publication 800-162, 2014)

109. National Institute of Standards and Technology, Guide to Computer Security Log Management (NIST Special Publication 800-92, 2006)

110. National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86, 2006)

111. National Institute of Standards and Technology, Managing the Security of Information Exchanges (NIST SP 800-47r1, 2021)

112. National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems (FIPS Publication 200, March 2006)

113. National Institute of Standards and Technology, NIST Cloud Computing Standards Roadmap (Special Publication 500-291 Version 2, 2013)

114. National Institute of Standards and Technology, NIST Special Publication 800-12 Rev 1: An Introduction to Information Security (2017)

115. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems: Special Publication 800-53 (NIST, 2017)

116. National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations (NIST Special Publication 800-37 Rev. 2, 2018)

117. National Institute of Standards and Technology, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (NIST Special Publication 800-218, 2022)

118. National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Rev 5, 2020)

119. National Institute of Standards and Technology, Security Metrics Guide for Information Security (NIST Special Publication 800-55 Rev 2, 2024)

120. National Institute of Standards and Technology, Security of Interactive and Automated Access Management Using Secure Shell (SSH) (NIST IR 7966, 2015)

121. National Institute of Standards and Technology, The NIST Cybersecurity Framework 2.0 (2024) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> accessed 3 April 2026

122. Open Ownership, 'Beneficial Ownership Data Standard' <https://www.openownership.org/en/topics/beneficial-ownership-data-standard/> accessed 3 April 2026

123. Open Worldwide Application Security Project (OWASP) <https://owasp.org/> accessed 3 April 2026

124. Open Worldwide Application Security Project (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> accessed 3 April 2026

125. Open Worldwide Application Security Project (OWASP), OWASP Top 10 Proactive Controls <https://top10proactive.owasp.org/the-top-10/> accessed 3 April 2026

126. OWASP Foundation, 'OWASP Top Ten Web Application Security Risks' <https://owasp.org/www-project-top-ten/> accessed 3 April 2026

127. Rose WS, Oliver Borchert, Stuart Mitchell and Sean Connelly, Zero Trust Architecture (NIST Special Publication 800-207, National Institute of Standards and Technology 2020) <https://www.nist.gov/publications/zero-trust-architecture> accessed 3 April 2026

128. World Wide Web Consortium (W3C), 'Web Content Accessibility Guidelines (WCAG)' <https://www.w3.org/WAI/standards-guidelines/wcag/> accessed 3 April 2026

129. XBRL International, 'XBRL Project Directory' <https://www.xbrl.org/the-standard/why/xbrl-project-directory> accessed 3 April 2026

D. Academic Works

130. Amadi-Echendu AP and Amadi-Echendu JE, '*A Study on Data and Information Integration for Conveyancing, Cadastre and Land Registry Automation*' in Proceedings of PICMET '16: Technology Management for Social Innovation (2016) <https://ieeexplore.ieee.org/document/7806611> accessed 3 April 2026

131. Bretschneider S and others, *"'Best Practices" Research: A Methodological Guide for the Perplexed*' (2005) 15(2) Journal of Public Administration Research and Theory

132. Business Registry Insights (BRI), 'Data Verification Survey' (2024) <https://br-insights.org/reports-dashboards/data-verification-2024/> accessed 3 April 2026

133. Business Registry Insights (BRI), 'E-Services' (2025) <https://br-insights.org/reports-dashboards/e-services-2022/> accessed 3 April 2026

134. Cowan R and Gallagher D, '*The International Registry for Aircraft Equipment—The First Seven Years: What We Have Learned*' (2014) 45 UCC Law Journal <https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan- Gallagher.pdf> accessed 3 April 2026

135. Cusumano M, *In Search of Best Practice: Enduring Ideas in Strategy and Innovation* (Oxford University Press 2010)

136. Holt V and others, '*The Usage of Best Practices and Procedures in the Database Community*' (2015) 49 Information Systems <http://dx.doi.org/10.1016/j.is.2014.12.004> accessed 3 April 2026

137. Kotter JP, *Leading Change* (Harvard Business School Press 1996)

138. Loshin D, *Data Quality and Master Data Management* (Elsevier 2008) <https://search.worldcat.org/en/title/424595637> accessed 3 April 2026

139. Schmidt J, '*The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers*' (2024) 21 European Company and Financial Law Review <https://www.degruyter.com/document/doi/10.1515/ecfr-2024-0023/html> accessed 3 April 2026

140. Sebastian-Coleman L, *Measuring Data Quality for Ongoing Improvement* (Elsevier 2013) <https://www.sciencedirect.com/book/9780123970336/measuring-data-quality-for-ongoing-improvement> accessed 3 April 2026

E. Reports and White Papers

141. American Institute of Certified Public Accountants, 'SOC for Service Organizations' <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report> accessed 3 April 2026

142. American Institute of Certified Public Accountants, 'System and Organization Controls (SOC) Suite of Services' <https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services> accessed 3 April 2026

143. AWS, 'AWS Well-Architected Framework' (Amazon Web Services 2024) <https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html> accessed 3 April 2026

144. BlackRock Investment Institute, 'Geopolitical Risk Dashboard' <https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard> accessed 3 April 2026

145. Ceross A, Practices in Electronic Registries (Interim Report, Spring 2018) prepared 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 <https://www.law.ox.ac.uk/best-practices-in-the-field-of-electronic/best-practices-field-electronic-registry-design-and> accessed 3 April 2026

146. Clarke B and Murray J, Enabling Digital Government: Interoperability and Data Exchange Between Registries – The Benefits of a Connected Landscape (Teranet Inc and 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> accessed 3 April 2026

147. Cloud Security Alliance, 'Security Guidance for Critical Areas of Focus in Cloud Computing' (v5, 2024) <https://cloudsecurityalliance.org/artifacts/security-guidance-v5> accessed 3 April 2026

148. Cloud Standards Customer Council (CSCC), Interoperability and Portability for Cloud Computing: A Guide (Version 3.0, December 2022) <https://www.omg.org/cgi-bin/doc?mars/2022-12-13> accessed 3 April 2026

149. Cybersecurity Insiders and Gurucul, 2024 Insider Threat Report (2024) <https://gurucul.com/2024-insider-threat-report/> accessed 3 April 2026

150. European Business Registry Association (EBRA), 'International Registers Survey Report 2022: Interactive Dashboard' <https://ebra.be/survey-results/> accessed 3 April 2026

151. EY-Parthenon, 'How to factor geopolitics into technology strategy' (2021) <https://www.ey.com/en_gl/insights/geostrategy/how-to-factor-geopolitical-risk-into-technology-strategy> accessed 3 April 2026

152. Garber E M 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> accessed 3 April 2026

153. International Business Registry Report, 'E-Services' (2022) <https://br-insights.org/reports-dashboards/e-services-2022> accessed 3 April 2026

154. Moore F, Registers: The New Frontier — A Proposal for the Development of a New Target Operating Model for Registers (2023) <https://www.fostermoore.com/white-papers/proposed-new-target-operating-model-for-registers-white-paper> accessed 3 April 2026

155. 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> accessed 3 April 2026

156. 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> accessed 3 April 2026

157. The Institute of Internal Auditors, 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> accessed 3 April 2026

F. Web Resources

158. Amazon Web Services, 'Precision clock and time synchronisation on your EC2 instance' <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html> accessed 3 April 2026

159. Amazon Web Services, 'What Is an API (Application Programming Interface)?' <https://aws.amazon.com/what-is/api/> accessed 3 April 2026

160. Aviation Working Group, GATS Site Terms of Use (1 June 2020) <https://documents.e-gats.aero/SiteTermsOfUse.pdf> accessed 3 April 2026

161. BCS, 'Why ISO 27001 Is Not Enough' (2009) <https://www.bcs.org/articles-opinion-and-research/why-iso-27001-is-not-enough/> accessed 3 April 2026

162. Bolagsverket, 'Swedish Companies Registration Office' <https://bolagsverket.se/en/omoss/varverksamhet/varservice/varahandlaggningstider.2081.html> accessed 3 April 2026

163. Cambridge Dictionary, 'best practice' <https://dictionary.cambridge.org/us/dictionary/english/best-practice> accessed 3 April 2026

164. CrowdStrike, 'SUNSPOT Malware: Technical Analysis' <https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/> accessed 3 April 2026

165. Edwards M, 'ISO 27001 — Clause 6.7 — Cryptography' (ISMS.online, 26 February 2025) <https://www.isms.online/iso-27701/clause-6-7-cryptography/> accessed 3 April 2026

166. Edwards M, 'ISO 27002 — Control 8.24 — Use of Cryptography' (ISMS.online, 17 February 2025) <https://www.isms.online/iso-27002/control-8-24-use-of-cryptography/> accessed 3 April 2026

167. Encyclopaedia Britannica, 'Accountability' <https://www.britannica.com/topic/accountability> accessed 3 April 2026

168. Esri, 'Geocoding Services' <https://developers.arcgis.com/rest/geocode/> accessed 3 April 2026

169. European Commission, 'Beneficial Ownership Registers Interconnection System (BORIS)' (European e-Justice Portal) <https://e-justice.europa.eu/38590/EN/beneficial_ownership_registers_interconnection_system_boris> accessed 3 April 2026

170. European Commission, 'Business registries at European level' (European e-Justice Portal, 2017) <https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do> accessed 3 April 2026

171. IBM, 'What is the IT Infrastructure Library (ITIL)?' <https://www.ibm.com/think/topics/it-infrastructure-library> accessed 3 April 2026

172. IBM, 'What Is Root Cause Analysis?' <https://www.ibm.com/think/topics/root-cause-analysis> accessed 3 April 2026

173. Interaction Design Foundation, 'User-Centred Design' <https://www.interaction-design.org/literature/topics/user-centered-design> accessed 3 April 2026

174. Justinmind, 'User-Centered Design: A Beginner's Guide' (14 July 2020) <https://www.justinmind.com/blog/user-centered-design/> accessed 3 April 2026

175. Louisiana Secretary of State, Louisiana UCC Bulk Filings API Integration Guide (Version 1.6, 2022) <https://static.sos.la.gov/UCC/UCC_Bulk_API_Guide.pdf> accessed 3 April 2026

176. Moore F, 'Glossary of Registry Terms and Acronyms' <https://www.fostermoore.com/glossary-of-registry-terms-and-acronyms> accessed 3 April 2026

177. Temple-Raston D, '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> accessed 3 April 2026

178. O'Donovan B, 'Ireland's First National Timing Grid Launched' (RTÉ, 19 September 2023) <https://www.rte.ie/news/business/2023/0919/1406003-irelands-first-ever-national-timing-grid-launches/> accessed 3 April 2026

179. Object Management Group, Interoperability and Portability for Cloud Computing: A Guide (Version 3.0, 2022) <https://www.omg.org/cgi-bin/doc?mars/2022-12-13> accessed 3 April 2026

180. Radle B and Bradicich T, 'What Is Availability?' (National Instruments, 2019) <https://www.ni.com/en/shop/electronic-test-instrumentation/application-software-for-electronic-test-and-instrumentation-category/systemlink/automate-data-analysis/what-is-rasm/what-is-availability-.html> accessed 3 April 2026

181. Stechynskyi I, 'Major Supply Chain Cybersecurity Concerns and 7 Best Practices to Address Them' (Syteca, 15 January 2025) <https://www.syteca.com/en/blog/supply-chain-security> accessed 3 April 2026

182. UK Government Digital Service, '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/> accessed 3 April 2026

183. Vranic G and Marusic A, 'Is the Self-Sovereign Digital Identity the Future Digital Business Registry?' (World Bank Blogs, 2021) <https://blogs.worldbank.org/psd/self-sovereign-digital-identity-future-digital-business-registry> accessed 3 April 2026

184. X-Road, 'The business registers of Estonia and Finland start cross-border interoperability' <https://x-road.global/xroad-case-studies-library/2024/10/21/the-business-registers-of-estonia-and-finland-start-cross-border-interoperability> accessed 3 April 2026

CTCAP | Cape Town Convention Academic Project

9 788886 449809