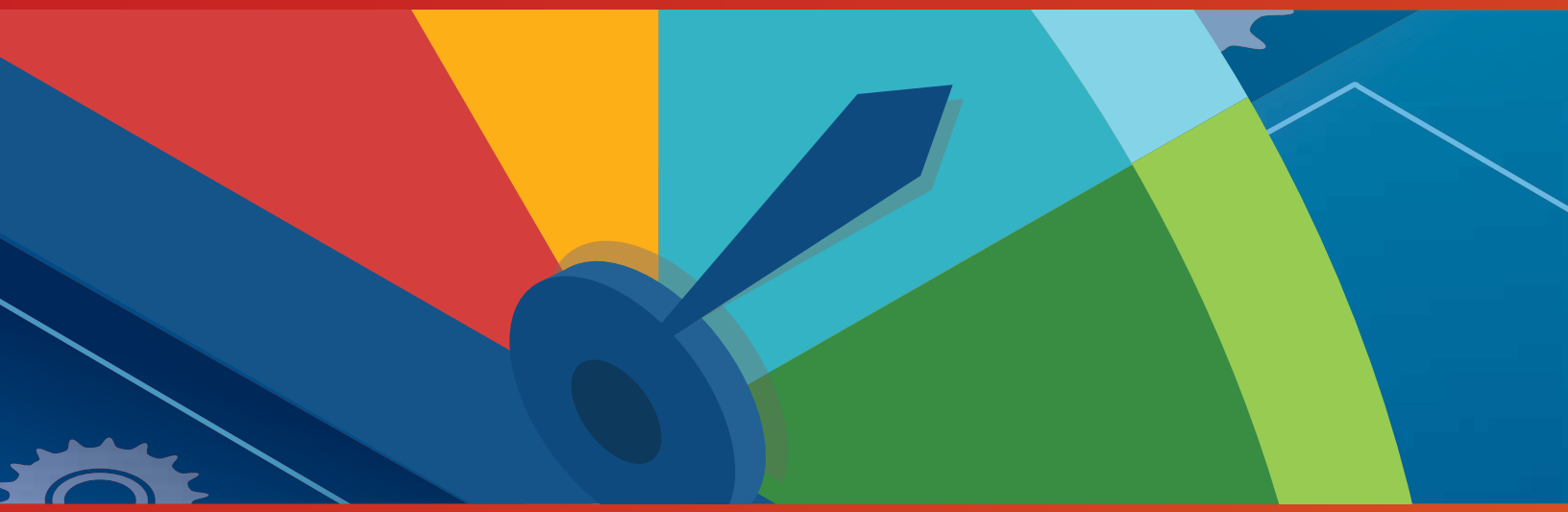
Key Principles for Effective Regulation and Supervision of Credit Reporting Service Providers

WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org



Key Principles for Effective Regulation and Supervision of Credit Reporting Service Providers

WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

TABLE OF CONTENTS

BOXES, FIGURES, and TABLES

ABBREVIATIONS

ACCIS	Association of Consumer Credit Information Suppliers
AI	Artificial intelligence
AISP	Account information service provider
API	Application program interface
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BoR	Bank of Russia
CFPB	Consumer Financial Protection Bureau
CRSP	Credit reporting service provider
DLT	Distributed ledger technology
EBA	European Banking Authority
ECB	European Central Bank
EDPB	European Data Protection Board
FCA	Financial Conduct Authority
FCRA	Fair Credit Reporting Act
Fintech	Technology-enabled financial services
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
GPCR	General Principles for Credit Reporting
ICCR	International Committee on Credit Reporting
IFC	International Finance Corporation
IMF	International Monetary Fund
LEI	Legal Entity Identifier
MAS	Monetary Authority of Singapore
MSME	Micro, small, and medium enterprise
ML	Machine learning
NPL	Nonperforming loan
OCC	Office of the Comptroller of the Currency
PBOC	People's Bank of China
P2P	Peer to peer
SME	Small and medium enterprise
UEMOA	West African Monetary and Economic Union

ACKNOWLEDGMENTS

This report is a product of the International Committee on Credit Reporting (ICCR) and the World Bank Group. The report was prepared by Dr. Talha Ocal (independent consultant) under the leadership and guidance of Collen Masunda, Secretariat of the ICCR and the ICCR Regulatory Oversight Framework Working Group, co-chaired by Neil Munroe (BIIA) and Jorge Laguna (Banco de México).

The document benefited from a consultation process and the contributions of plenary members, representative organizations, and peer reviewers. The committee gratefully acknowledges valuable inputs and comments from peer reviewers Hung Hoang Ngovandan (Lead Financial Sector Specialist, World Bank Group) and Nan Jiang (Senior Economist, World Bank Group).

The ICCR would also like to thank the Chairman of the ICCR, Mahesh Uttamchandani and Secretariat members Luz Maria Salamina and Collen Masunda for guiding the process. Susan Boulanger provided editorial services. The layout and design of the report was prepared by Naylor Design, Inc.

EXECUTIVE SUMMARY

Credit reporting systems have emerged to be a key part of the financial infrastructure, playing multiple supportive roles in areas such as sustainable access to credit, financial inclusion, prudential supervision, and financial stability. Credit reporting systems effectively support the sound and fair extension of credit in an economy as the foundation for robust and competitive credit markets. Hence, failure of the credit reporting infrastructure can significantly impact the effective functioning of credit markets and as a result impact domestic and global financial stability. Like any other activity, credit information sharing as facilitated by credit reporting service providers (CRSPs) has inherent risks and vulnerabilities. CRSPs face operational, cyber, reputation, model, regulatory, and compliance risks, among others. The adoption of innovative technologies and the use alternative data sources also increase the level of inherent risks. Further, the high levels of interconnectedness of the financial sector emphasizes the importance of effectively managing risks in credit reporting systems to avoid potential impact on the financial infrastructure.

Against this background, supervisory and regulatory authorities as well as other stakeholders in the credit reporting industry have renewed their attention to the regulation and supervision of credit reporting activities. There are vast differences in the existing frameworks across jurisdictions around the globe, however, and no global standard setting body (SSB) has as yet issued comprehensive guidance on regulating and supervising CRSPs. The General Principles on Credit Reporting (GPCR), published by the ICCR, provide guidance on risk management and legal and regulatory frameworks, as well as high-level recommendations for the effective oversight of credit reporting systems, but the need remains for comprehensive, granular guidance that builds on existing principles and other relevant guidance documents, taking into account the changes in the credit reporting environment resulting from technological innovations that bring in new risks and opportunities for regulatory arbitrage.

The first section of this report briefly introduces the topic and explains the role of credit reporting systems in the financial infrastructure. The second section briefly discusses the role of the different types of CRSPs and recognizes alternative credit reporting service providers as emerging players in the industry. It also sheds light on the use of new technologies in credit reporting and their potential implications.

The third section discusses GPCR as published by the ICCR in 2011. GPCR represents the only universal set of standards for credit reporting as included under the Financial Stability Board (FSB) noncore compendium of standards for the financial sector. GPCR's five principles describe the respective roles of key stakeholders, accompanying guidance, and recommendations for effective oversight. The section elaborates on the relevance of GPCR for developing key principles for the effective regulation and supervision of CRSPs. In doing so, it provides numerous examples of how GPCR applies in the regulatory frameworks of different jurisdictions around the globe.

The fourth section discusses the major types of risks related to credit reporting systems. These risks are not necessarily mutually exclusive and interrelate in many ways, but they can be termed strategic risk, operational risk, cyber risk, model risk, reputation risk, and legal and compliance risk, among others. The section focuses on the evolving role of credit reporting with a forward-looking approach to identify risks and vulnerabilities.

The fifth section discusses the key considerations for regulatory and supervisory principles. The section outlines the preconditions for developing and implementing an effective regulatory and supervisory framework and explains the scope of application of the key principles and the responsibilities of regulatory and supervisory authorities.

The sixth section then introduces twelve principles for safe and efficient credit reporting along with the roles and responsibilities of the supervisory authority. The objective of the key principles is to ensure the effective functioning of the credit reporting systems. The authority is expected to oversee the credit reporting system as a whole to accomplish the objective of the key principles. This can be achieved through a risk-based supervisory approach that makes proportionate use of the authority's powers, tools, and resources. The principles are as follows:

PRINCIPLE 1: Regulatory Framework. Credit reporting activities should be subject to regulation and supervision by authorities with clearly defined responsibilities and objectives. An appropriate regulatory framework should be in place for each authority responsible for supervision to provide the necessary legal powers to oversee credit reporting activities.

PRINCIPLE 2: The Authority. The authority should be granted, by an appropriate legal framework, operational independence, effective organizational structure, and adequate human capital and financial resources to discharge its duties. The authority should define, disclose, and review its objectives and be accountable for executing its duties and for the use of its resources.

PRINCIPLE 3: Supervisory Approach. The authority should adopt a risk-based supervisory approach to identify and assess risks related to credit reporting activities, evaluate these risks by on-site and off-site supervision tools as appropriate, and employ proportionate enforcement actions (with their corresponding dispute resolution mechanisms) to address these risks and ensure compliance.

PRINCIPLE 4: Cooperation and Collaboration. The authorities should coordinate and cooperate with each other, at both the jurisdictional and the international level, to promote the development, safety, and efficiency of credit reporting systems, as well as the cross-border exchange of credit information.

PRINCIPLE 5: Permissible Activities. The regulatory framework should define and cover permissible activities in credit reporting. Appropriate permission mechanisms, including market entry requirements, should be governed by the authority.

PRINCIPLE 6: Access and Transparency. Credit reporting systems should allow fair and open access to their services, on the basis of reciprocity, by data providers, data users, data subjects, and other relevant stakeholders. Credit reporting systems should be subject to a clearly defined disclosure framework to enable participants to have an accurate understanding of credit reporting activities.

PRINCIPLE 7: Governance. Credit reporting systems should be administered using a governance framework commensurate with the risks and the scope of the activities. The framework should establish policies and procedures, a proper internal control environment, and an appropriate organizational structure with clearly defined duties and responsibilities that ensures system efficiency and effectiveness in serving the markets.

PRINCIPLE 8: Risk Management. Credit reporting systems should be monitored within a comprehensive risk management framework and culture to identify, assess, evaluate, manage, and mitigate all risks related to credit reporting activities on an ongoing basis.

PRINCIPLE 9: Data Security. An appropriate information security framework should govern credit reporting activities to protect the confidentiality, integrity, and availability of information and ensure business continuity and operational resilience.

PRINCIPLE 10: Data Collection. Data providers should provide relevant, accurate, timely, and sufficient information on data subjects, including positive data, to CRSPs to enable a comprehensive credit information sharing mechanism. CRSPs can collect data from all legal, reliable, appropriate, and available sources and retain this information for a sufficient time for credit reporting.

PRINCIPLE 11: Personal Data. Personal data collection, processing, and distribution should be undertaken only for the purposes for which the data was collected, including creditworthiness assessment, credit risk analysis, indebtedness and repayment capacity, ID confirmation, fraud prevention, and prudential supervision.

PRINCIPLE 12: Consumer Rights. Consumers should have clear rights regarding the use of their personal data for credit reporting. These rights should include consent, dispute, notification, and access rights; right to restrict data use; and right to request transfer of data, as appropriate. Effective dispute resolution mechanisms should be established for handling consumer disputes related to credit reporting activities. Credit reporting products should be explainable, transparent, and fair.

The seventh section of the report discusses the suggested approach authorities should adopt in applying the principles. This discussion emphasizes the importance of maintaining holistic oversight of how the credit reporting system functions to ensure that the players in credit reporting activities are able to manage the risks related to credit information sharing. The section provides further guidance on the risk-based supervision approach followed by supervisory programs to be imple-

mented by authorities. The section also provides additional considerations with respect to different types of CRSPs, the oversight of artificial intelligence-based scoring models, and the role of industry associations.

Finally, the eighth section presents the methodology for assessing the regulatory and supervisory frameworks at the jurisdictional level. The assessment methodology is primarily intended for international financial institutions (IFIs), but it is also helpful for national authorities and other internal and external assessors. Assessment responsibility for observing adherence to the key principles primarily lies with individual countries' regulatory and supervisory authorities.

1

INTRODUCTION

Credit reporting systems, as facilitated by credit reporting service providers (CRSPs), represent one of the key pillars in global economies' financial infrastructures. Robust credit reporting systems promote access to credit, financial inclusion, prudential supervision, and financial stability. As the financial infrastructure is highly interconnected, failure of credit reporting systems could significantly hamper the effective functioning of credit markets, which in turn can impact financial stability.

CRSP activities present inherent risks and vulnerabilities. CRSPs face a number of risks, including operational, cybersecurity, reputational, legal, regulatory, compliance, and model risks. CRSPs are commonly technology-intensive operators dealing with multiple parties that provide and use very large amounts of data. Potential losses from operational and cybersecurity risks can thus be significant and can also lead to legal and reputational risks. Continuous innovations in technology, new business models, and emerging new players also increase the level of risk in CRSP activities.

Effective regulation and supervision are vital to ensuring that CRSPs can manage the risks related to credit reporting. Considering the importance of CRSPs, the need is growing for regulatory and supervisory oversight of credit reporting activities. Vast differences in existing frameworks across jurisdictions interfere with this process. Many countries have no specific regulations. In those cases, CRSPs are governed by general provisions and treated as regular businesses, subject mainly to personal data protection or data privacy regulations. Some countries do have CRSP regulations in place, but they focus more on licensing and less on supervising their activities. CRSPs in many jurisdictions operate under a voluntary code of conduct that aims to replicate regulatory requirements, but by their nature such codes lack oversight functions. Only in a handful of countries does a comprehensive approach to regulating and supervising CRSPs exist.

The International Committee on Credit Reporting (ICCR) issued its General Principles on Credit Reporting (GPCR) to address the need to ensure sound and effective credit reporting systems (see the Appendix). General Principle 3 on Governance and Risk Management identifies risks inherent in credit reporting activities. At the same time, General Principle 4 on Legal and Regulatory Frameworks provides high-level guidance on what such frameworks should cover. GPCR also includes high-level recommendations for the effective oversight of credit reporting systems. Since the introduction of the GPCR, the ICCR has published additional detailed guidance on various topics to complement the general principles (ICRR 2018, 2019a, 2019b).

Despite the growing recognition of the need for them, a coherent framework and comprehensive guidance on the regulation and supervision of CRSPs do not currently exist. Building on the existing principles and guidance documents developed by the ICCR, it is believed that a globally applicable, principles-based framework for effective regulation and supervision of CRSPs would help develop the credit reporting system. These principles should define the critical elements needed for a regulatory and supervisory framework that can support a sound, efficient, and effective credit reporting system. The framework should also take into account the ongoing innovations occurring in the credit reporting environment and the risks and opportunities that could result from these changes.

2

CREDIT REPORTING SYSTEMS IN THE FINANCIAL INFRASTRUCTURE

Credit reporting is facilitated by credit reporting service providers (CRSPs), which are entities that manage a credit information sharing system. CRSPs collect and compile permissible information on individuals and/or firms and provide this data to third-party users, as well as offering value-added products based on such data. Defined broadly, CRSPs encompass private credit bureaus, public credit registries, business information providers, and alternative credit reporting service providers.[1] While they all serve the common purpose of supporting credit risk management through credit reporting, their core focus can differ. They are categorized mainly based on these differences.

A private credit bureau is a credit information exchange with the primary objective of improving the quality and availability of data for creditors so they can make better-informed decisions. Private credit bureaus collect credit data from banks, nonbank financial institutions (NBFIs), and other financial or nonfinancial creditors. They generally focus on retail and MSME lending markets. A public credit registry is a model of credit information exchange the primary objective of which is to support prudential supervision and enable access to credit data by financial institutions to improve the quality of credit portfolios. Credit registries are typically owned and operated by central banks or other financial supervisors and mainly collect credit information from regulated financial institutions. Business information providers are entities that collect information on businesses, including sole proprietorships, partnerships, and corporations for credit risk assessment, credit scoring, or other business purposes, such as the extension of trade credit (World Bank 2011). While there are distinctions in the role of these entities, in many cases it is also possible to combine multiple functions within a single CRSP.

Alternative credit reporting service providers are emerging as a new type of CRSP. These entities use innovative methodologies and nontraditional data, such as digital footprints, social media data, phone data, and browser histories, to assess credit risk and produce credit scores. They often focus on developing credit reporting products in niche markets that traditional credit reporting systems do not cover. From a regulatory perspective, these entities do not generally fall under existing regulatory frameworks, and their activities have increasingly begun to attract the attention of regulatory authorities.

Credit reporting systems comprise the institutions, individuals, rules, procedures, standards, and technology that enable the information flows that support decision-making processes regarding extension of credit (World Bank 2011). They are a vital part of the financial infrastructure, playing multiple supportive roles in sustainable access to credit, financial inclusion, micro-prudential supervision, and financial stability. Developing an effective credit reporting system requires commitment from various stakeholders. The credit information-sharing cycle involves CRSPs, individuals, businesses, data providers, data users, regulators, and supervisors.

Over the years, advances in technology and growing market needs have enabled CRSPs to move beyond credit reports. As a result, CRSPs developed capabilities to process, analyze, and transform data to produce ready-to-use tools to support users and data subjects. In essence, value-added products apply to all differentiated credit reporting services. The range of such products is extensive and evolving, but they include tools such as consumer and commercial credit scores, ID verification and fraud detection, credit portfolio monitoring, behavioral scoring, debt collection services, business insights, marketing services, and personal financial management tools.

1. Credit bureaus can also be termed credit reference agencies, credit reference bureaus, consumer reporting agencies, or credit reporting agencies; business information providers can also be known as commercial credit reporting providers or business credit reporting agencies.

Technology is at the core of credit reporting systems. From the era of paper-based credit reports to automated lending systems, CRSPs have adopted technological advances and updated the way credit reports are created and delivered. In parallel to the innovations, the role of credit reporting has evolved, and CRSPs are transforming into technology-intensive entities that provide a wide range of data analytics solutions. Several new technologies have recently emerged in the credit reporting industry to improve capabilities for CRSPs. These include those listed below (World Bank 2019d), but there are many more.

i. Cloud computing technologies that allow CRSPs to facilitate efficient storing, processing, and transferring data, to lower costs, and to improve service delivery.

ii. Biometrics, national identity, and digital identity systems that improve the ability to authenticate identities of data subjects properly.

iii. Open data platforms that offer available "big data" for use.

iv. Distributed ledger technologies (blockchain) that allow transactions and data to be securely processed across a distributed network.

v. Electronic payment systems that create transactional data for payers and payment acceptors.

vi. Artificial intelligence (AI) techniques that make processing vast amounts of data easier, faster, and more cost-effective.

By adopting new technologies and business models, the credit reporting ecosystem has evolved significantly over the past decade. The accuracy, depth, and breadth of credit data has improved, and delivery of credit reports is much faster, if not instant. Where new technologies enabled CRSPs to enhance their services, alternative credit reporting service providers emerged as competitors. Despite its benefits, improved technologies present a source of risk for credit reporting systems, adding to the risks traditionally associated with credit reporting activities. Key risks associated with the emergence of financial technologies include strategic risk, operational risk, cyber risk, and compliance risk (BCBS 2019).

3

GENERAL PRINCIPLES RELATED TO REGULATION AND SUPERVISION

Since its publication in 2011 by the ICCR, GPCR has been the only set of universal standards for credit reporting included in the Financial Stability Board (FSB) noncore compendium of standards for the financial sector. GPCR has five principles (see the Appendix) describing key stakeholders' respective roles, accompanying guidelines, and recommendations for effective oversight. ICCR has also published guidelines to complement the general principles on topics such as cybersecurity, credit scoring approaches, and the use of alternative data. GPCR lists the following as key attributes of an effective credit reporting system:

i. Supports financial and nonfinancial creditors in accurately assessing creditworthiness, sound management of credit risk, and well-performing credit portfolios.
ii. Facilitates inclusive, sustainable, efficient access to finance in the economy on competitive terms.
iii. Supports authorities in supervising financial institutions to ensure the safety and soundness of the financial system and oversight of systemic risk.
iv. Encourages individuals and businesses to manage their finances responsibly by rewarding responsible behavior, avoiding overindebtedness, and contributing to financial literacy.

GPCR is extensively used by regulators, supervisors, and policy makers in decision-making processes regarding credit reporting systems and CRSPs. Box 1 provides an overview of the two main credit reporting regulatory approaches.

BOX 1

Overview of Credit Reporting Regulations

In general, two main approaches to regulating credit reporting systems are in use around the globe. Many countries regulate credit reporting activities using broad data protection laws, while others enact specific credit reporting laws or regulations.

The first group includes the European Union (EU), which enacted the General Data Protection Regulation (GDPR). GDPR covers credit reporting activities and any other business activities involving personal data management and data exchange. Specific legislation like the Consumer Credit Directive also covers credit reporting activities in the EU. Other countries following this data protection framework approach include Argentina, Chile, and Uruguay. In countries without specific credit reporting regulations, credit reporting systems may operate under self-regulatory mechanisms. In these countries, CRSPs usually have codes of conduct for good governance (for example, the Czech Republic and New Zealand).

The second group enacted specific credit reporting laws, mainly covering consumer credit reporting activities and credit bureaus. The US was a pioneer in this approach, passing the Fair Credit Reporting Act (FCRA) in 1971, amended in 2011 with the Dodd-Frank Wall Street Reform and Consumer Protection Act creating the Consumer Financial Protection Bureau (CFPB) as an oversight authority. Other countries with specific credit reporting laws include Russia, India, and the Bahamas; countries with credit reporting regulations include Vietnam, Egypt, and Morocco. Such specific laws or regulations generally focus on the entry and exit requirements for credit bureaus; data collection, retention, and security provisions; access, confidentiality, and permissible purposes rules; corporate governance rules; consumer rights and dispute resolution mechanisms; and oversight and enforcement.

3.1 The Five Principles

General Principle (GP) 1 on *data* outlines the following attributes of what constitutes properly collected and distributed data for credit reporting systems:

i. Accurate, to the extent possible, free of error, truthful, complete, and up to date.
ii. Systematically collected from all data providers using consistently applied, appropriate rules and procedures.
iii. Updated on a predefined schedule or at specific triggers, including prompt adjustment of errors and upon significant events like credit exposures, arrears, defaults, and fraud.
iv. Promptly accessible by data users to support their functions without delays.
v. Comprehensive, covering all relevant information, including negative and positive data, and any nontraditional information.
vi. Available to data users for defined purposes within a specified period of time.

Countries apply the attributes of GP1 in a variety of regulatory rules. From a broader viewpoint, natural tension exists between the rules that require systematic collection of personal data to provide effective financial services to the people and the rules that protect the privacy of personal data of the very same people. In this sense, credit reporting activities are under the scope of data protection laws in many countries. It is worth noting that consent and permissible purposes requirements of personal data protection are mainly applicable to consumer credit bureaus. In the case of credit registries, it is typically required by the relevant financial supervisor for all regulated creditors to share data with the registry. Also, for business information providers, the information related to business entities is generally not subject to data protection regulations, except for the data of business owners. Box 2 provides selected examples of jurisdictional approaches related to GP1.

GP2, addressing *data processing: security and efficiency*, stipulates the following as attributes of credit reporting systems that should be ensured:

i. Data is protected against any loss, corruption, destruction, misuse, or undue access.
ii. Precautions are taken to ensure business continuity and avoid disruptions in users' access to data.
iii. Efficient operations are maintained to provide cost-effective services that meet high standards.

BOX 2
Regulatory Examples of GP1

Most countries facilitate the reporting of both positive and negative information in credit reports. A few, however, have regulations allowing reporting negative credit information only (Spain, Costa Rica) and prohibit collecting and sharing positive information.

Regulations often require that CRSPs and data providers take all reasonable steps to ensure data are accurate, up-to-date, and valid. To avoid errors in data, regulations can determine the specific minimum inputs for consumer credit reports (Rwanda).

Many countries require the consent of individual data subjects for data collection and/or access to credit reports. In countries such as Australia and Panama, explicit borrower consent is required for a data provider to share information with a CRSP. Countries like the US do not require explicit borrower consent for information sharing in general but require explicit consent if the information is used for specific purposes, like employment.

Countries generally specify the length of time for which information can be stored and shared. Different types of data may have different retention periods. The majority of credit bureaus and credit registries share information for a period of five years or less (World Bank 2019a).

Countries generally allow CRSPs to collect all data relevant for creditworthiness assessment, including data in public records. To protect against discrimination, however, jurisdictions can prohibit collecting certain data types. Most regulations protect to some degree against discriminatory practices in credit scoring (US, EU). However, the use of artificial intelligence (AI) is a particular area of concern, because proprietary AI algorithms are black boxes with unclear decision-making methods, creating the potential for discrimination. As such, countries are considering the risks of AI from many perspectives and exploring ways to regulate it. The EU recently proposed a regulation to introduce harmonized rules on AI. In the US, AI models must address the adverse action notice requirements in the FCRA, which requires the CRSP to disclose key factors that adversely affect a credit score.[2] As a guideline, the Monetary Authority of Singapore (MAS) published principles to promote fairness, ethics, accountability, and transparency (FEAT) in the use of AI and data analytics for the financial sector.

2. A draft bill before the US Congress (the Algorithmic Accountability Act) requires entities to conduct impact assessments of high-risk automated decision systems to evaluate the impact of the system's design process and training data on accuracy, fairness, bias, discrimination, privacy, and security.

Data security is at the core of safe credit reporting systems, and authorities take an interest in the accuracy, confidentiality, and integrity of credit information databases. Countries apply the attributes of GP2 in a variety of regulatory rules. Box 3 provides selected examples of the jurisdictional approaches related to GP2.

GP3 on *governance and risk management* outlines the importance of proper governance to ensure risks associated with credit reporting systems are effectively managed. As such, CRSPS and their data providers should be subject to the following mechanisms:

i. Proper accountability with clearly defined management and board responsibilities as well as independent external audits.

ii. Procedures to ensure disclosure of relevant matters relating to the entity and/or its activities in a timely fashion to the respective authority.

iii. Appropriate risk management guidelines for effective governance of activities related to credit reporting activity.

iv. Assessment of all relevant risks by the entity management and reporting the assessment outcomes to the respective authority.

v. Sound internal control and risk management functions related to credit reporting activity within the entity.

vi. Procedures to ensure fair access to data by all users under proper conditions.

Sound governance is key to managing risks associated with credit reporting activities. Thus regulations in many countries include a broad range of governance rules for CRSPs. Box 4 provides selected examples on the jurisdictional approaches as related to GP3.

BOX 3

Regulatory Examples of GP2

The majority of countries have regulations to deal with cybersecurity and information security (ICCR 2019b). For example, the New York State Department of Financial Services (NYSDFS) introduced a cybersecurity regulation in 2018 that requires CRSPs to adopt the core requirements of a cybersecurity program and risk assessments, establish a cybersecurity policy to protect consumer and business data, install effective access privileges like multifactor authentication and encryption, conduct training and monitoring for authorized personnel, appoint a chief information security officer, and report known cyber breaches to the department within 72 hours.

Countries can introduce rules to avoid disruptions in credit reporting services. In Russia, qualified credit bureaus are expected to establish IT systems with the highest level of redundancy and reliability to ensure business continuity. The UK issued guidelines on operational resilience that require identifying critical business services; assessing impact tolerances; identifying key employees, processes, and technology to ensure uninterrupted operations; and conducting scenario analysis to plan communication strategies.

Countries can also regulate the use of cloud-based services by CRSPs. For example, regulations can include data localization rules for cloud services for the transfer of personal data outside the country (Australia) or prohibit personal data transfers abroad (Rwanda).

BOX 4

Regulatory Examples of GP3

Countries may regulate the shareholding requirements to restrict commercial banks' shares in a credit bureau (Nigeria).

The board of directors and senior management may be subject to minimum qualifications and/or fit and proper requirements, with their responsibilities stipulated in the regulations (India). Failure of employees, officers, and major shareholders to be "fit and proper" can be a condition for revoking a credit bureau's license (Singapore).

Countries can require that CRSPs establish effective internal controls and audit and risk management functions. While these governance functions may be mentioned explicitly in credit reporting regulations (Korea), most CRSPs are governed by general corporate laws and codes of conduct that cover the policies of these functions.

To complement the internal control and audit functions, regulators can also impose mandatory external audits to ensure the CRSPs' accountability and transparency (Rwanda).

GP4 on the *legal and regulatory environment* states that credit reporting systems should be subject to a legal and regulatory framework that is clear, predictable, nondiscriminatory, proportionate, and supportive of data subject and consumer rights, including effective judicial or extrajudicial dispute resolution mechanisms. In addition, the framework should have the following attributes:

i. Clear rules with consistent terminology and predictable consequences for CRSPs, data providers, data users, and data subjects for actions related to credit reporting activities.

ii. Nondiscriminatory rules that are applied equally and fairly regardless of the nature of the participants.

iii. Proportionate and practical rules that support an effective credit reporting system, ensure a high degree of compliance, avoid overly restrictive obligations, and include commensurate corrective actions.

iv. Protection of the rights of data subjects and consumers, including, at a minimum, the right to object to collection or use of their information for specific purposes and/or use, the right to be informed on the conditions of collection, processing, and distribution of data held about them, the right to access data held about them periodically at little or no cost, and the right to challenge the accuracy of information about them.

v. The data subjects' and consumers' privacy issues are addressed and/or subjects and consumers are referred to the relevant data protection regulations.

vi. Effective judicial and extrajudicial dispute resolution structures aim for expeditious solutions to disputes and provide appropriate enforcement and redress tools.

While attention to the need for a regulatory framework and supervisory oversight of credit reporting systems is growing, vast differences remain in the existing regulatory frameworks across jurisdictions. Countries apply a combination of credit reporting laws, banking laws, data protection laws, commercial laws, and consumer protection laws to credit reporting activities. These laws may be complemented with fair credit granting and consumer credit regulations and with corporate secrecy and bank secrecy provisions. In general, regulatory requirements that apply to consumer credit bureaus do not apply to business information providers that mainly deal with business-related information. Box 5 provides selected examples of jurisdictional approaches related to GP4.

BOX 5

Regulatory Examples of GP4

Market Entry

Several jurisdictions enacted provisions for entry and exit requirements, mainly for credit bureaus, in the form of licensing (Singapore) by or registration (South Africa) with the relevant regulator. Licensing regulations generally stipulate minimum paid-in capital, governance requirements, and operational and business standards for CRSPs. In countries with licensing requirements, conditions for revoking licenses can be stipulated in the regulation (Namibia). In the EU, approximately half of the CRSPs are subject to a specific regulatory procedure for entering the market, and a significant minority of the CRPSs are further subject to specific regulatory provisions. More than one-third of the CRSPs are subject to direct supervision by a national supervisory authority (ACCIS 2020).

Whereas multiple credit bureaus operate in many countries, most countries have a single credit registry founded by and operating under a specific law (Spain). Also, business information providers are not generally subject to entry requirements and are not within the scope of credit reporting regulations. They can, however, be subject to some degree of oversight by data protection agencies or commerce ministries.

Countries can also impose licensing requirements for specific activities related to credit reporting instead of licensing CRSPs. One notable example of the activity-based licensing approach is the account information service provider (AISP) licensing procedure in the EU. CRSPs with an AISP license in the EU can retrieve, process, and aggregate consumers' bank account and payment data seamlessly.

Alternative Credit Reporting Service Providers

From a regulatory perspective, these innovative entities do not generally fall under existing regulatory frameworks. Regulating new technologies necessitates a balanced approach that promotes innovation while overseeing their risk implications. Countries adopt varying approaches to regulating fintechs and new technologies, such as (i) observing and monitoring the implications of innovation before intervening where and when necessary; (ii) following a light-touch supervisory approach, with a "no objection letter" to allow entities to operate in a live environment, followed by a more stringent framework if deemed necessary; (iii) promoting innovation facilitators, such as innovation hubs or regulatory sandboxes; and (iv)

BOX 5, *continued*

introducing new laws, regulations, or licensing frameworks to cover either a broad range of fintech activities or specific activities (World Bank 2020c).

As an example, the People's Bank of China (PBOC) has issued the Measures for the Administration of Credit Reporting Services. The new measures clearly define the boundaries and scope of credit information, taking alternative data into regulation. (Source: PBOC).

Consumer Rights

Most countries enact consumer protection regulations that include requirements governing the lawful grounds or permissible purposes for data processing and for disclosing consumer data.

Most regulations also give consumers the right to dispute any inaccurate information in their files. Consumer complaints generally consist of claims for correcting factual inaccuracies, such as data entry or process errors, and claims on legal status and liability, such as mixed files, proof of transactions, and fraud or identity theft (World Bank 2019a).

Dispute Resolution

Many regulations establish dispute resolution mechanisms for consumers. The structures of these mechanisms can differ with regard to the type of dispute and the applicable legal framework. Examples of dispute resolution mechanisms include (i) internal complaints handling services of CRSPs, (ii) credit ombudsmen (South Africa), (iii) credit reporting review commissions (Bahamas), and (iv) alternative dispute resolution service providers (Singapore).

BOX 6

Regulatory Examples of GP5

Notwithstanding its technical difficulties, cross-border credit reporting is only possible where legal frameworks allow credit information to be shared across borders. In this respect, many countries impose data localization rules that require personal data be stored and processed in the country (India, Malaysia). Other than data sovereignty restrictions, practical challenges exist for cross-border credit reports, such as lack of unique identifiers for individuals and companies and absence of standard data formats.[3]

A legal framework that enables shared regional credit reporting only exists in the West African Monetary and Economic Union (UEMOA), which covers eight countries. Also, the AnaCredit Project aims to enable a credit information-sharing mechanism between national banks through the European Central Bank (ECB) in the EU. AnaCredit allows national central banks and financial supervisors to collect and share harmonized and standardized loan information at a granular level.

GP4 on *cross-border data flows* outlines the facilitation of cross-border data transfers, where appropriate, provided the following requirements are in place:

i. Transfers are feasible based on a cost-benefit analysis that considers the conditions of the credit markets, the level of economic and financial integration between the countries, the respective laws and regulations, and the CRSPs' needs for the data.
ii. Procedures are clearly identified, including standard data formats and transfer protocols.
iii. Potential sources of risk are adequately assessed and appropriately managed.
iv. A mutual agreement exists for cooperation and coordination between the relevant authorities.

Cross-border data sharing enables a data subject's credit history to be leveraged in multiple countries. It helps borrowers access credit in countries where they have no credit history despite having one in their country of origin. Globalization leads to the extensive migration of consumers and businesses from one country to another, whether digitally or in person, spurring the need for regionalized or globalized credit reporting. Box 6 provides selected examples of jurisdictional approaches related to GP5.

3. For more discussion on the legal and technical challenges for cross-border credit reporting and for policy recommendations for potential solutions, see ICCR 2021, "Cross-border Credit Reporting."

3.2 Recommendations for Effective Oversight

GPCR also includes high-level recommendations for the effective oversight of credit reporting systems and suggests that credit reporting systems should be subject to appropriate and effective regulation and oversight by a central bank, a financial supervisory authority, or another relevant authorities. In cases where the relevant regulations in a jurisdiction relate to more than one authority, one of these authorities should undertake the primary role in the oversight function. The central banks, financial supervisory authority, and other relevant authorities should have the necessary powers and resources to carry out their responsibilities to credit reporting systems effectively. The authorities should have clearly defined and disclosed regulatory and oversight objectives, rules, and policies. GPCR should be adopted in the rules and guidelines, where relevant, and applied consistently throughout credit reporting systems. The authorities should cooperate with each other on both the jurisdictional and the international level to promote the development, safety, and efficiency of credit reporting systems.

Regulatory and supervisory authorities for credit reporting systems can comprise central banks, financial supervisors, data protection agencies, consumer protection agencies, or finance ministries. Supervisory oversight can be exercised over CRSPs, data providers, and data users. Box 7 provides selected examples of jurisdictional approaches related to the oversight recommendations of the GPCR.

BOX 7
Regulatory Examples of GPCR Oversight Recommendations

Most countries with specific credit reporting regulations have on-site supervision and inspection provisions for supervisory authorities. Having assigned central banks as authorities, the supervision processes of CRSPs closely mimic bank supervision in many countries (World Bank 2020a). Like regulated financial institutions, CRSPs are obligated to regularly submit a set of off-site reports to the authority. Also, while not as often as at banks, the supervision teams can conduct on-site supervision at CRSP facilities. It is not uncommon for on-site examinations to be accompanied by IT examinations that assess supervised entities' information security governance.

Effective oversight is only possible with appropriate enforcement mechanisms. As such, most countries established enforcement provisions in their credit reporting regulations. These provisions can include various tools for authorities, such as issuing notices and warnings, requests for corrective actions, and penalties and fines imposed to ensure compliance. Noncompliance cases on specific rules, as opposed to processes, usually cannot be corrected through notice; instead, an appropriate penalty must be imposed.

Most regulations include monetary fines for noncompliance. For example, GDPR has provisions for fines that can be high, depending on the severity of the infringement, and administered by data protection regulators in member countries. In this case, stringent enforcement of detailed regulatory rules can hamper the effective functioning of credit reporting activities.

Some countries follow a closer approach to oversight on credit reporting activities. In Nigeria and Uganda, central banks require regulatory evaluation and approval of credit reporting products before the CRSPs can introduce them to the market. In the case of specific offenses, some countries have credit reporting laws that lead to imprisonment of the responsible officer (Singapore).

4

KEY RISKS IN CREDIT REPORTING

Major types of risks related to credit reporting systems include strategic risk, operational risk, cyber risk, model risk, reputation risk, compliance risk, and legal risk. CRSPs are technology-intensive operations and deal with multiple parties that provide and use large amounts of data. The potential loss from operational errors is therefore significant. Operational risk can be related to failures in information technology and infrastructure, human errors, or attempted fraud. Such risks can also lead to legal risks, stemming from failure to comply with applicable laws and regulations. Reputational risk is particularly relevant to CRSPs due to the extensive amounts of personal data processing. Continuous innovations in technology, new business models, and emerging new players also increase the level of risks in CRSP activities. Cybersecurity risks have been on the rise, as evidenced by the number of CRSPs that have been subject to cyber incidents in the last few years. The incidents have caused severe financial, operational, and reputational loss for the targeted entities and the industry in general. It cannot be ruled out that realized risks in CRSP activities can result in wide-scale failures in lending markets. The risks in credit reporting activities are not necessarily mutually exclusive; they are interrelated and overlap in many ways. Also, a given CRSP activity or function will in most cases be associated with more than a single risk type.

4.1 Strategic Risk

Strategic risk is the risk to current or projected financial resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the business environment (OCC 2019). Strategic risk covers all risks that affect a CRSP's business strategy and strategic objectives and includes any risks that can decrease a CRSP's profitability and viability, such as any unexpected declines in revenues or increases in costs.

Strategic risk is primarily a concern for the CRSP's board of directors and senior management. It is management's responsibility to develop and implement robust strategic and business planning processes. In a fast-changing industry, business models must be reviewed and updated if necessary to satisfy data users' needs. For example, management's failure to follow advances in technology can result in obsolescence of IT systems.

Strategic risk emphasizes the importance of sound governance. Failures in CRSP governance can result from lack of oversight by the board of directors, inefficient administration by senior management, insufficient monitoring and control, and lack of business resilience. Negative consequences may arise if management and staff do not have the necessary knowledge, skills, and qualifications to assess the risks of new technologies and innovative business models. Cyber incidents or noncompliance with data privacy regulations can be attributed to a failure in good governance in most cases.

Adverse business decisions can result in inaccurate credit reports. Errors in credit reports can cause loss of market share, a decrease in profits and enterprise value, a decline in customer confidence, and potential regulatory enforcement actions. Inaccurate credit reports and flawed credit scores can also cause consumers to be excluded from access to credit. Due to the inherent operational and technical details, credit reports can be prone to error even in established markets. A study of the US credit reporting industry found that five percent of consumers had errors on one of their three major credit reports (FTC 2021). While these errors are attributable to the data providers in many cases, the management of CRSPs should have proper governance strategies to ensure the accuracy of credit reports.

Governance strategies should assess, evaluate, and manage the risks of innovative credit reporting products. CRSPs must take into account the potential risks of adopted technologies and

possible regulatory interventions. In the absence of sound new product approval and change management processes, innovative products can implicate risks for credit reporting systems if their reliability, consistency, and integrity are not ensured.

Competition risk is evident as most CRSPs operate in a competitive environment. Management should be able to develop strategies and respond to changing conditions, especially in challenging cases of regulatory arbitrage and unfair competition. For example, alternative credit reporting service providers can emerge in any credit reporting market. Where credit bureaus are licensed and regulated, but new players in the same market operate without a license, a regulatory arbitrage case can arise for the unlicensed players. Unscrupulous, practices such as predatory lending by new players, may also lead to regulatory arbitrage and become sources of potential instability. In addition, credit registries may sell credit reports, in competition with credit bureaus. This is expected in a free market, but operating conditions should be the same for all the competitors. Credit registries with privileges in data collection can create conditions of unfair competition for other CRSPs in the same market. Finally, the credit reporting industry is increasingly internationalized in the sense that globally recognized players compete with local CRSPs in numerous markets. CRSPs that operate in multiple countries can benefit from operational cost efficiencies, an advantage against local competitors that could lead to consolidation of CRSPs.

4.2 Operational Risk

Operational risk is the probability of loss resulting from inadequate or failed internal processes, people, systems, or external events (BCBS 2011). Any event that disrupts the normal flow of business and generates loss or damage to a CRSP can put operations at risk. Operational risk is inherent in all products, activities, processes, and systems of credit reporting.

Above all, deficiencies in the control environment, such as lack of adequate management oversight, can form a basis for many risks. A sound governance framework covers an internal control environment throughout the CRSP organization. Any gaps in internal control points or weaknesses in control practices can give rise to fraud losses, product errors, system outages, or security breaches.

Lack of human capital capacity can affect CRSPs, as to operate they must employ staff with necessary technical qualifications to carry out credit reporting activities. The absence of adequate training and competency policies has implications. Employees' errors or omissions and the misbehavior of employees can be a major source of operational, legal, and reputational risks. For example, social engineering techniques can target the employees allowed access to the credit reporting network. With respect to the commercial value of credit reporting data, rogue staff members who aim to steal data are also a potential source of vulnerability.

Failures in operational resilience can damage the credit reporting systems in the event of unexpected incidents. Given their intermediation role, CRSPs should make every effort to continue their activities in the event of severe incidents. Failure to establish effective business continuity and disaster management plans can disrupt credit reporting services, which can also interrupt access to credit. A recent example of the importance of business continuity is the COVID-19 pandemic, which affected most businesses globally. It was vital during the pandemic for CRSPs to continue credit reporting services even though most employees had to work remotely. Box 8 briefly discusses the implications of COVID-19 for the credit reporting industry.

Security vulnerabilities, also a component of cyber risk, can be a significant threat for CRSPs that lack adequate information security protocols. Increased connectivity to the internet improves operational efficiency significantly. Yet it can give rise to security vulnerabilities to cyberattacks. Failures in adequate cybersecurity investments could cause obsolescence in systems and make CRSPs vulnerable to cyber threats. In particular, CRSPs that operate in developing countries with limited financial resources can be impeded by the high cost of the most recent technologies.

Contagion risk is another concern, as leading CRSPs have global operations in which many functions are managed from a central or regional headquarters. Global operations provide cost-effective management and reduce infrastructure overhead at the country level. It is possible, however, for a service interruption in a globally active CRSP to affect operations in multiple countries across its network. Also, CRSPs with global operations can be victims of fraud schemes tailored to the regions where they operate.

Outsourcing risk is also a major issue. Most CRSPs outsource to third parties at least some of their services, including IT infrastructure, software, and data platforms. Where data centers are commonly outsourced in Africa and Europe, professional services such as websites and call centers are outsourced in the Americas (ICCR 2019b). Third-party vendors provide many benefits to CRSPs, such as improved business focus, cost efficiencies, and greater flexibility, scalability, and connectivity. Despite its certain benefits, the reliance on outsourcing is a source of risk for CRSPs in cases where third-party contractors or fourth-party subcontractors do not comply with cybersecurity, information security, and data privacy standards. That said, a cyber-attack at a contractor or subcontractor can also affect the CRSP's systems. For example, the Equifax breach in 2017 was due to a bug on an outsourced enterprise system.

BOX 8

Implications of COVID-19 for Credit Reporting

The COVID-19 pandemic has significantly impacted credit reporting systems, financial institutions, and countries' economies in general. In many jurisdictions, access to complete, up-to-date public data was severely affected because company/business registries or courts were either closed or had moratoriums imposed. From an operational risk perspective, a severe but plausible scenario had become a reality. The pandemic has the following key implications for CRSPs:

i. The high degree of interconnectedness of the financial sector and interdependencies across firms and markets underlines the importance of ensuring business continuity at the financial system level to avoid systemic impacts resulting from operational incidents at the CRSP level.

ii. Increasing dependence of CRSPs on third-party service providers, especially outsourcing agreements with cloud service providers, raises risks of disruption in credit reporting services if the third-party providers' services are disrupted due to lockdowns in distant locations.

iii. CRSP employees moved to remote working on a mass scale, increasing risks to data protection and from professional conduct and lack of managerial oversight. Also, contingency plans for key staff were needed that could help maintain continuity of services if that staff could not work.

The pandemic has had a potential impact on the integrity of credit reporting systems. In particular, inadequate and untimely data provided by CRSPs undermines the key role of the credit reporting systems. Other potential impacts include possible credit rationing, increased cost of credit, and exclusion of borrowers. ICCR (2020) provides policy recommendations for CRSPs facing the operational implications of the pandemic.

4.3 Cyber Risk

Cyber risk is the risk of financial loss, operational disruption, or damage from the failure of the digital technologies used for operational functions via electronic means due to unauthorized access, use, disclosure, disruption, modification, or destruction of the credit reporting system (NIST 2017). The definition of cyber risk encompasses multiple aspects of risk, and effectively managing cyber risk, as opposed to a technical risk overseen by IT staff, requires organization-wide governance. The general categories of cyber risk can summarized as follows (World Bank 2018a):

i. Continuity risk that the performance and availability of systems and data are impacted and information systems are disrupted.

ii. Data integrity risks that data collected, stored, and processed are incomplete, inaccurate, and inconsistent across different systems.

iii. Change risk as failure in proper management of system changes and updates in a timely and controlled manner.

iv. Outsourcing risk that problems at third-party providers adversely impacts the CRSP.

v. Security risk of unauthorized access to information systems from within or outside the CRSP.

In a digital world, the potential impacts of a cyber incident can be disastrous. In this sense, cybersecurity often goes beyond a business concern and becomes a concern of national security. Credit reporting systems use digital technologies extensively, which expands the potential sources of vulnerabilities. As controllers of valuable data, CRSPs and other participants in the credit reporting ecosystem are potential targets for cybercrime actors. Box 9 provides examples of recent major cybercrime incidents. Common types of cybercrime incidents that can affect credit reporting systems include (ICCR 2019b):

i. Breaches of data belonging to data subjects or the CRSP, in the form of unauthorized access, transmission, reproduction, dissemination, or sale of data.

ii. Deletion or corruption of data by a type of malware.

iii. Unauthorized encryption of data by ransomware that prevents access to data.

iv. Malfunction of the system because of manipulation by a third party.

v. Malfunction of network communication because of an attack such as a distributed denial-of-service.

vi. Disruption at the outsourced systems, such as the cloud servers.

vii. Illegitimate financial transactions as a result of a system intrusion.

Cybercrime incidents can result in severe consequences for the credit reporting systems in the form of economic, financial, legal, and reputational costs. Risk implications for cybercrime incidents include, but are not limited to, the following:

i. Economic costs such as fraudulent loans and credit cards granted in the name of data subjects can ultimately result in defaults and incurred losses for creditors.

ii. Financial costs such as declines in market value, redress payments to data subjects, increased insurance premiums, and additional IT infrastructure costs.

iii. Legal and compliance costs, including fines and penalties imposed by authorities, communication costs from negotiation with authorities and affected parties, and forensic investigation costs.

iv. Reputational costs, including loss of confidence in the CRSP among data subjects, providers, and users and public relations, communication, and other costs to rebuild trust.

v. Disruption in access to credit as a result of failures in services where data users and subjects cannot access credit reports.

vi. Adverse outcomes on the general economy caused by creditors adopting a cautious approach to lending and lacking faith in credit reporting systems.

New technologies can be a source of vulnerability for CRSPs. Innovations in credit reporting such as DLT/blockchain, APIs, cloud computing, and AI/ML have risk implications for the industry. While there are many potential benefits for CRSPs from new technologies, these can also expose the credit reporting system to new sources of cyber risk.

CRSPs' high degree of interconnectedness can affect public data networks, banks, and other financial and nonfinancial institutions within the credit reporting system. New participants, such as alternative data sources, fintechs, alternative lenders, and new data users, join the credit reporting systems daily. The interconnectedness of the credit reporting systems can lead to contagion effects if a CRSP's systems are compromised. Also, a cyber breach in a player of the system can harm the CRSP as well.

BOX 9

Major Cybersecurity Incidents

Solar Winds Cyber Attack in the US

In December 2020, IT products and services company SolarWinds was hacked, and its IT monitoring and management product was corrupted by sophisticated malware. This malware then spread through software updates to several customers, including financial services institutions. NYSDFS in its investigative report on the incident recommended that entities should (i) fully assess and address third party risk; (ii) adopt a "zero trust" approach and implement multiple layers of security; (iii) address vulnerabilities without delay through patch deployment, testing, and validation; and (iv) address supply chain compromise in cybercrime incident response plans (NYSDFS 2021).

Experian South Africa

In May 2020, Experian South Africa experienced a data breach that exposed a suspected fraudster some personal information belonging to roughly 25 million individuals and 800,000 entities. The perpetrator impersonated a director of a known client and proceeded to procure services from Experian as a client. The data was shared with the perpetrator using Experian's secure data transfer protocols. Experian reported the incident to local authorities, after which the fraudster's hardware was impounded and the misappropriated data was secured. The breach incident continued when an unknown individual posted the data files on a restricted file-sharing website; that file too was later deleted (Experian 2021).

Irish Credit Bureau

Between June and August of 2018, a personal data breach occurred at the Irish Credit Bureau (ICB) database when the ICB implemented a code change to its database that contained a technical error. The ICB inaccurately updated the records of 15,120 closed accounts, and before it had fixed the issue the ICB had disclosed these inaccurate account records to financial institutions or data subjects (DPC 2021).

Equifax Data Breach in the US

During the period from May to July in 2017, cybercriminals exploited a US website application vulnerability to access Equifax files. The data breach exposed records containing the Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers of more than 143 million consumers.

4.4 Model Risk

Model risk is the potential for adverse consequences from decisions based on incorrect or misused financial or statistical model outputs (FDIC 2017). Credit scores as analytical credit risk management models are at the very center of the value-added products that CRSPs offer to users. While traditional logistic regression models are still common for credit scores, AI-based models are increasingly used to leverage alternative data. AI facilitates innovative statistical approaches in credit scoring. They are better equipped to process data with nonlinear interrelationships, as is often the case with big data. However, the AI algorithms used for alternative credit scores lack transparency in how data is collected and used and how output is generated. Among other risks, the black box attribute of AI brings a discriminative bias risk for consumers. Therefore, credit scores as an output of AI models bear risks of not being explainable, transparent, and fair.

Explainability implies that an adverse decision regarding a credit application is based on clear reasons. Due to the complex algorithmic decision mechanisms of AI-based scoring models, the ability to understand, explain, and justify the decisions made using such models is challenging. In particular, AI scoring models that use deep neural networks, random forests, and gradient boosting machines are considered black-box models (ICCR 2019a). These models employ complex transformations between the data inputs and the results.

Transparency suggests that the decision-making methods and the scope of data used in an AI-based scoring model must be assessable by an independent party, usually an oversight authority. The model should be traceable and auditable to track all the steps, criteria, and choices throughout the process for enabling the repetition of the process to understand the decisions made by the model (EBA 2020). Due to the lack of transparency in AI algorithms' decision-making methods, authorities can find it difficult to assess (i) how data is collected and used, (ii) which types of data affect scores, and (iii) whether consumers are subject to discriminatory biases.

Fairness requires inclusive scoring models, that is, the absence of any discriminatory or biased practices. AI models can use discriminatory factors in alternative data sources either directly or by approximating them indirectly. The design of an AI algorithm can be applied in a manner that uses information as a proxy for sensitive attributes. Or the input data can be incomplete, unrepresentative, or poorly weighted to reflect bias against protected attributes (World Bank 2021). The risk of unfair practices increases with the extensive use of alternative data, depending on the type of data used in the AI model.

CRSPs may also use AI algorithms developed by third-party providers. Notwithstanding other risks, such as the risks of vendor lock-in and lack of third-party knowledge, these providers can operate outside the scope of any data protection or other relevant regulations. In this case, these AI models can learn discriminatory biases if they are trained using data sources without a legitimate ethical basis. In this case, CRSPs must ensure the explainability, transparency, and fairness of credit products developed by third parties.

4.5 Reputation Risk

Reputation risk arising from negative perceptions by consumers, data providers, data users, shareholders, investors, or regulators can adversely affect a CRSP's ability to maintain existing or establish new business relationships (BCBS 2019). The negative perception regarding a CRSPs' business practices, whether true or not, can have multiple consequences, including (i) damage to business relationships, (ii) loss of confidence of consumers and businesses, (iii) loss of existing and future customers and decline in revenue, (iv) exit of key personnel and management and inability to recruit a qualified workforce, (v) decline in market capitalization, and (vi) fines, penalties, and litigation costs where applicable.

A strong business reputation is key to the success of credit reporting activities. If an incident damages a CRSP's reputation, it can require an extended effort to rebuild and recover. Critical threats to a CRSP's reputation include, but are not limited to, the following:

i. Data security and data privacy breaches.
ii. Enforcement actions or penalties due to noncompliance.
iii. Negative news on traditional or social media.
iv. A high number of customer complaints.
v. Ineffective crisis management of significant events related to the CRSP.

4.6 Legal and Compliance Risk

Compliance risk is the risk of penalties, sanctions, financial loss, or loss to reputation a CRSP can suffer. It can result from a failure to comply with laws, regulations, rules, self-regulatory industry standards, or codes of conduct applicable to their activities (BCBS 2005). Similarly, legal risk is the risk of financial or reputational loss resulting from any type of legal obligation. It includes a lack of awareness, misinterpretation, or misunderstanding of how

laws and regulations apply to credit reporting activities. Legal risk covers, but is not limited to, litigation settlements and fines or penalties resulting from supervisory actions. Legal and compliance risks overlap to some extent, and both also fall under the definition of operational risk. Critical considerations for legal and compliance risk include the following:

i. Financial risks in the form of litigation. In regulations with no caps on class-action lawsuit settlements (for example, in the US), CRSPs can be required to make high payments to data subjects. For example, Equifax has agreed to a settlement that includes up to US$425 million to compensate affected people (Equifax 2021).

ii. Noncompliant innovations. The credit reporting industry evolves rapidly, and innovations may not fit within the applicable regulatory framework. In particular, CRSPs must carefully assess compliance issues regarding the use of alternative data and innovative technologies.

iii. Inappropriate resolution of consumer complaints. CRSPs have regulatory responsibilities to deal with consumer disputes, such as specific deadlines for responding to the filings. Failures to effectively manage consumer complaints can lead to customer distress, reputational loss, and potential fines imposed by the authorities.

5

KEY CONSIDERATIONS FOR A REGULATORY AND SUPERVISORY FRAMEWORK

5.1 Preconditions for Regulation and Supervision

An effective regulatory and supervisory framework should provide the authorities necessary tools to develop, implement, monitor, and enforce policies under both normal and stressed conditions. From a broader perspective, an effective regulatory and supervisory framework should be supported by sound and sustainable macroeconomic policies; a well-formulated financial stability policy framework; an established public infrastructure; a crisis management, recovery, and resolution framework; an appropriate level of systemic protection; and effective market discipline (BCBS 2012).

A sound credit reporting infrastructure is an essential building block for the safety and soundness of credit markets and the financial system in general. The main components of a sound credit reporting infrastructure include, but are not limited to, the following (BIS 2012):

i. A well-founded, clear, transparent, and enforceable legal basis that covers each aspect of credit reporting activities.

ii. An appropriate governance structure to promote the safety and efficiency of the credit reporting infrastructure and support the stability of the broader financial system.

iii. A comprehensive risk management framework that covers the risks and vulnerabilities inherent in credit reporting activities.

iv. Objective, risk-based, publicly disclosed criteria that allow participants fair and open access.

v. Efficient and effective satisfaction of evolving needs of participants and credit markets.

vi. Transparent rules and procedures that enable sufficient disclosure of information to participants on credit reporting activities.

vii. Consistently enforced laws and regulations that include fair dispute resolution mechanisms for participants.

viii. Appropriate and effective regulation, supervision, and oversight by a relevant authority.

5.2 Scope of Application of the Key Principles

The scope of application of the key principles for effective regulation and supervision covers both credit reporting activities and the systems used to carry them out. As facilitated by traditional CRSPs as well as alternative CRSPs, credit reporting activities cover collecting and compiling information on individuals and businesses, processing this information to produce structured data, developing value-added products based on this data, and disclosing or selling this data to users. In addition, credit reporting activity aids in creditworthiness assessment and supports the credit-granting decisions of financial or nonfinancial creditors and prudential oversight. In this sense, *the key principles are applicable to credit bureaus, credit registries, business information providers, and alternative credit reporting service providers. They can be applied on a risk-based approach and a proportionate basis, as necessary*. They are not intended to apply to credit rating agencies that typically provide debt or securities rating services for businesses or to companies that provide proprietary scoring services, including audit firms.

The key principles were developed to be applicable universally; however, they do not aim to provide detailed action plans at the jurisdictional level. Instead, authorities can use the principles as a guide to (i) evaluate the status quo of the credit reporting systems, (ii) identify, review, or update regulatory and supervisory objectives, and (iii) develop regulations, strategies, and policies for achieving these objectives. In addition, international financial institutions (IFIs) such as the World Bank Group, the International Monetary Fund, regional development banks, and others can use these key principles when assessing credit reporting systems and providing technical assistance to countries. Also, the principles may be reviewed in light of significant changes in credit reporting systems due to the evolving nature of credit reporting activities.

Scope of the Responsibilities of Authorities

Credit reporting activities should be subject to appropriate and effective regulation, supervision, and oversight by an authority. Regulatory and supervisory authorities have a vital role in ensuring that CRSPs are able to manage their risks effectively and that their function in the financial system is not disrupted. This role cannot be fulfilled if any of the essential functions of regulation, supervision, or oversight are not working.[4] This report considers an "authority" to be the agency in charge of regulating and supervising credit reporting systems. The supervisory authority[5] varies across countries. Often a banking supervisory authority, either the central bank or an independent agency, is a data protection agency that oversees the activities of CRSPs to the extent they process personal data. If more than one authority is responsible for regulating and supervising CRSPs, one of them should function as the primary overseer (World Bank 2011).

To best ensure the safety and efficiency of credit reporting systems, a regulatory framework should be comprehensive. Regulation of CRSPs should protect data subjects' rights, identify the responsibilities of data providers, and ensure fair access to credit reporting services and unbiased application of specific standards to the participants in the credit reporting system. While regulations define the rules of the playing field, their practical implementation is driven by, among other factors, effective supervision. The success of a regulatory framework is therefore contingent on the supervisory role of a competent authority. In addition to its crucial role in enforcing rules, the supervisor can have a role in interpreting the rules and suggesting changes if necessary. This role is of particular relevance for the challenge of dealing with the inherent complexity, innovations, and continuous change in credit reporting activities. Also, effective supervision can support good business practices in the industry and promote trust in the credit reporting system. The supervisory authority should have the necessary legal powers and financial and human resources to effectively carry out its responsibilities in regulating, supervising, and overseeing CRSPs. The authority should cooperate with other relevant authorities, both domestically and internationally, as appropriate, to promote the safety and soundness of CRSPs.

The authority should adopt the GPCR along with the key principles for effective regulation and supervision of CRSPs and make its best effort to apply them consistently. Consistent application of principles in a jurisdiction and across different jurisdictions is critical as credit reporting systems can depend on each other, compete with each other, or both. The authority should promote consistency and transparency by disclosing the policies applicable to the credit reporting systems it owns or operates. Also, the authority should apply an appropriate level of separation between the oversight and operational functions.

4. Where "regulation" refers to the whole set of laws and rules applicable to credit reporting activities, "supervision" is defined as the monitoring of credit reporting activities and the enforcement of relevant regulations by the authorities. "Oversight" is a function of the authority whereby regulatory and supervisory objectives are promoted by monitoring ongoing activities, assessing them against the objectives, and, where necessary, enforcing change.
5. For simplicity, this document refers to a single "authority" as a supervisory authority, unless stated otherwise, assuming that a single supervisory authority is also responsible for regulation, although this is not the case for all jurisdictions.

6

KEY PRINCIPLES FOR REGULATION AND SUPERVISION OF CRSPs

The objective of the key principles is to ensure the effective functioning of the credit reporting systems. Credit reporting systems should effectively support the sound and fair extension of credit in an economy as the foundation for robust and competitive credit markets. In doing so, credit reporting systems should be safe and efficient and should fully support data subjects' and consumers' rights.

To ensure this objective is met, the key principles framework covers *all credit reporting activities* instead of referring to specific types of CRSPs. This is of particular importance given the evolving nature of credit reporting systems. Credit reporting, as facilitated by credit reporting service providers, is *the credit information sharing mechanism that covers collecting and compiling information on individuals or businesses, processing this information to produce structured data, and disclosing or selling this data to or creating value-added products with this data for third-party users to assess creditworthiness and manage credit risk.*

The framework includes twelve principles for safe and efficient credit reporting activities, along with the roles and responsibilities of the supervisory authority (Box 10). The authority is expected to oversee the credit reporting system as a whole to accomplish the objective of the key principles. This is achieved through a risk-based supervision approach by using supervisory powers, tools, and resources *on a proportionate basis.*

BOX 10

Key Principles for Effective Regulation and Supervision of Credit Reporting Systems

PRINCIPLE 1: *Regulatory Framework*

Credit reporting activities should be subject to regulation and supervision by authorities with clearly defined responsibilities and objectives. An appropriate regulatory framework should be in place for each authority responsible for supervision to provide the necessary legal powers to oversee credit reporting activities.

PRINCIPLE 2: *The Authority*

The authority should be granted, by an appropriate legal framework, operational independence, effective organizational structure, and adequate human capital and financial resources to discharge its duties. The authority should define, disclose, and review its objectives and be accountable for executing its duties and for the use of its resources.

PRINCIPLE 3: *Supervisory Approach*

The authority should adopt a risk-based supervisory approach to identify and assess risks related to credit reporting activities, evaluate these risks by on-site and off-site supervision tools as appropriate, and employ proportionate enforcement actions (with their corresponding dispute resolution mechanisms) to address these risks and ensure compliance.

PRINCIPLE 4: *Cooperation and Collaboration*

The authorities should coordinate and cooperate with each other, at both the jurisdictional and the international level, to promote the development, safety, and efficiency of credit reporting systems, as well as the cross-border exchange of credit information.

BOX 10, *continued*

PRINCIPLE 5: ***Permissible Activities***

The regulatory framework should define and cover permissible activities in credit reporting. Appropriate permission mechanisms, including market entry requirements, should be governed by the authority.

PRINCIPLE 6: ***Access and Transparency***

Credit reporting systems should allow fair and open access to their services, on the basis of reciprocity, by data providers, data users, data subjects, and other relevant stakeholders. Credit reporting systems should be subject to a clearly defined disclosure framework to enable participants to have an accurate understanding of credit reporting activities.

PRINCIPLE 7: ***Governance***

Credit reporting systems should be administered using a governance framework commensurate with the risks and the scope of the activities. The framework should establish policies and procedures, a proper internal control environment, and an appropriate organizational structure with clearly defined duties and responsibilities that ensures system efficiency and effectiveness in serving the markets.

PRINCIPLE 8: ***Risk Management***

Credit reporting systems should be monitored within a comprehensive risk management framework and culture to identify, assess, evaluate, manage, and mitigate all risks related to credit reporting activities on an ongoing basis.

PRINCIPLE 9: ***Data Security***

An appropriate information security framework should govern credit reporting activities to protect the confidentiality, integrity, and availability of information and ensure business continuity and operational resilience.

PRINCIPLE 10: ***Data Collection***

Data providers should provide relevant, accurate, timely, and sufficient information on data subjects, including positive data, to CRSPs to enable a comprehensive credit information sharing mechanism. CRSPs can collect data from all legal, reliable, appropriate, and available sources and retain this information for a sufficient time for credit reporting.

PRINCIPLE 11: ***Personal Data***

Personal data collection, processing, and distribution should be undertaken only for the purposes for which the data was collected, including creditworthiness assessment, credit risk analysis, indebtedness and repayment capacity, ID confirmation, fraud prevention, and prudential supervision.

PRINCIPLE 12: ***Consumer Rights***

Consumers should have clear rights regarding the use of their personal data for credit reporting. These rights should include consent, dispute, notification, and access rights; right to restrict data use; and right to request transfer of data, as appropriate. Effective dispute resolution mechanisms should be established for handling consumer disputes related to credit reporting activities. Credit reporting products should be explainable, transparent, and fair.

PRINCIPLE 1: Regulatory Framework

Credit reporting activities should be subject to regulation and supervision by authorities with clearly defined responsibilities and objectives. An appropriate regulatory framework should be in place for each authority responsible for supervision to provide the necessary legal powers to oversee credit reporting activities.

Credit reporting activities should be subject to oversight by an appropriate regulatory framework to ensure that *a type of credit reporting activity is regulated by the same rules for any type of CRSP that undertakes such activity*. The same set of rules for the same kind of credit reporting activities enables that all CRSPs, whether a credit bureau, credit registry, business information provider, or alternative credit reporting service provider, to be governed by regulations that promote fair competition and block regulatory arbitrage. If the regulatory authority is also the owner or operator of the credit registry, the management and oversight functions of the credit registry should be separated by a clear mandate.

The responsibilities and objectives of the authorities involved in oversight of credit reporting activities should be clearly defined in laws or regulations. The primary objective of oversight is to ensure that the credit reporting systems effectively support the sound and fair extension of credit in the economy as the foundation for robust and competitive credit markets. To this end, credit reporting systems should be safe and efficient and should fully support the rights of data subjects and consumers.

The authority should have the legal power to reasonably and confidentially access the board of directors, senior management, staff, policies and procedures, functions, and any relevant records of CRSPs. In particular, the authority should have access

to the essential sources of information to undertake the following (i) understand the functions, activities, and overall condition of CRSPs; (ii) assess the risks inherent in credit reporting systems, the financial system, and the broader economy; and (iii) evaluate the CRSP's compliance with relevant regulations and policies. The power to access includes gathering information through regular or ad hoc reports, on-site visits, inspections, and dialogues with stakeholders in the credit reporting systems. In addition, the authority should be able to access relevant confidential information from CRSPs and confidentially share it with other relevant authorities to minimize gaps in regulation or oversight. The authority should have the legal power to oversee all the activities within the scope of credit reporting, including the power to supervise foreign-owned credit reporting activities operating in its jurisdiction.

The authority can encourage CRSPs to form industry associations to facilitate communication and collaboration among stakeholders and develop codes of conduct. While codes of conduct constitute a type of self-regulation and can be beneficial in establishing consensus for acceptable practices in the industry, they cannot substitute for a regulatory framework. Codes of conduct for credit reporting activities support the regulatory framework by outlining the norms, rules, responsibilities, and common good practices for the industry.

PRINCIPLE 2: The Authority

The authority should be granted, by an appropriate legal framework, operational independence, effective organizational structure, and adequate human capital and financial resources to discharge its duties. The authority should define, disclose, and review its objectives and be accountable for executing its duties and for the use of its resources.

The authority should be granted, by appropriate provisions, operational independence to ensure no third-party interference occurs that compromises the decision-making processes for discharging the oversight duties of credit reporting activities. Where the authority has broader oversight responsibilities, the independence of the oversight function should not be undermined by the authority's other supervisory functions and objectives.

The authority should have a transparent governing body for the oversight function of credit reporting activities. Its organization should be designed to avoid conflicts of interest and enable effective oversight with timely decisions and enforcement actions when necessary. The staff should have essential credibility in their professional conduct and integrity, appropriate knowledge and skills, and accountability under appropriate legal provisions.

The authority should have adequate financial resources and qualified human resources to perform its regulatory and oversight responsibilities. The organizational structure of the authority should be appropriate for the effective use of these resources. The financial resources of the authority should be sufficient to (i) employ and retain qualified staff with necessary skills, (ii) allocate adequate staff for the sole purpose of oversight, (iii) provide function-focused training programs regularly, (iv) invest in necessary physical and technological infrastructure, and (v) engage with external resources, such as technical experts, when and where needed. The duties for the regulatory oversight functions within the organization should be clearly defined, with proper delegation of tasks. Staff should have the necessary tools to perform their daily operations, monitor credit reporting activities, conduct on-site inspections, and take enforcement actions when necessary.

The authority should clearly define and disclose its regulatory and supervisory objectives, roles, and policies concerning credit reporting activities. A clear framework for oversight objectives creates a basis for policy-making decisions and provides a benchmark by which the effectiveness of achieving the objectives can be evaluated. Public disclosure promotes transparency, accountability, and consistency in policy implementation by the authority. Consistent with the regulatory framework, the objectives should be supported by specific policy documents, guidelines, notices, circulars, standards, and supervisory letters that are regularly reviewed. The authority should support accountability forits responsibilities and objectives by publishing information on its oversight activities in annual or ad hoc activity reports. The disclosure of regulations, rules, objectives, policies, and functions should be in plain-language documents to ensure they are available to and understandable by credit reporting system participants. While public disclosures facilitate compliance with applicable requirements and standards, the primary responsibility for complying with regulatory and oversight principles rests with the CRSPs.

PRINCIPLE 3: Supervisory Approach

The authority should adopt a risk-based supervisory approach to identify and assess risks related to credit reporting activities, evaluate these risks by on-site and off-site supervision tools as appropriate, and employ proportionate enforcement actions (with their corresponding dispute resolution mechanisms) to address these risks and ensure compliance.

The authority should adopt a risk-based approach for determining and assessing the nature, impact, and scope of the risks related to credit reporting activities. The authority should establish *a forward-looking risk assessment framework* with a well-defined methodology to address the risk profile, scope of activities, governance, risk management, and internal control environment of CRSPs against the oversight objectives. The risk assessment should include the following elements:

i. Occurs regularly to determine the priority and scope of supervision of CRSPs.

ii. Identifies the emerging risks, trends, and innovations in the credit reporting system as a whole.

iii. Takes into account the overall environment and developments in related sectors, such as the banking system.

iv. Recognizes the supervisory inputs, feedbacks, and concerns from the other relevant authorities.

v. Complements an assessment of compliance with relevant regulations as necessary.

The authority should employ the appropriate range of tools to supervise credit reporting activities based on the risk assessment outcomes. The scope of activities undertaken by different types of CRSPs can vary greatly. Therefore, *a one-size-fits-all CRSP supervisory treatment may not be appropriate.* This is the fundamental reason why the authority should adopt a risk-based approach. Supervisory tools should include appropriate on-site and off-site supervision, and allocation of supervisory resources should be based on the results of the risk assessment.

The on-site and off-site supervision tools should be used within a coherent supervisory planning process. The authority should ensure that on-site and off-site functions are deployed with clear responsibilities, objectives, and outputs with an effective coordination and information-sharing mechanism between both functions.

The off-site reporting framework should include an appropriate variety of information to regularly assess compliance with relevant regulations, determine the safety and efficiency of credit reporting activities, evaluate the inherent and emerging risks, and identify areas of supervisory concern. Off-site reports should cover all relevant information, submitted ad hoc or regularly, such as audit reports, statistics on data subjects, data inquiries, and consumer complaints.

On a proportionate basis, on-site supervision should be conducted based on the results of the risk assessment, the evaluation of the off-site reports, and the availability of resources. The on-site supervision team should consist of the authority's supervisors; however, the authority can use external auditors for inspections that require technical expertise. The on-site supervision function should include, among others, the following objectives:

i. Evaluate the adequacy of governance structures and control environment.

ii. Develop a better understanding of the strategy, business model, activities, and products of the CRSP.

iii. Validate and confirm the accuracy and reliability of the off-site reports provided by the CRSP.

iv. Inspect areas of supervisory concern and follow up with previous supervisory findings.

The findings of both off-site and on-site supervision functions should be communicated to the CRSPs by appropriate letters, notices, and reports.

The authority should be granted, by an appropriate legal framework, an adequate range of supervisory tools to impose enforcement actions. These actions include written warnings, penalties, fines, corrective actions, restrictive orders, interventions, and other means deemed necessary and proportionate. The authority should have the tools needed for corrective actions when the CRSP is not compliant with the regulations, engages in unsafe credit reporting activities, and fails to establish sound governance and control practices and proper risk management. The relevant regulations should clearly define the supervisory tools for enforcement.

The enforcement tools should be applied, without undue delay, *on a proportionate basis* according to the nature of the supervisory concern at the CRSP. The authority should prioritize the objectives of the safety and efficiency of the CRSP and of the credit reporting system in deciding the appropriate enforcement actions. The enforcement actions should be subject to an appropriate judicial dispute resolution mechanism for solving disputes regarding the enforcement action. The range of enforcement tools can include the following:

i. Supervisory letters that identify areas of concern and require improvement.

ii. Administrative penalties and fines.

iii. Notices that require prompt corrective actions or requests for specific action plans, or

iv. Restrictions and prohibitions on specific type of activities, applying stringent limits and requirements, and requesting changes in organization and management.

v. License revocation or exclusion from the official (state) register, if appropriate.

PRINCIPLE 4: Cooperation and Collaboration

The authorities should coordinate and cooperate with each other, at both the jurisdictional and the international level, to promote the development, safety, and efficiency of credit reporting systems, as well as the cross-border exchange of credit information.

Consistent with the relevant legal powers and regulatory frameworks, cooperation arrangements should be designed to support authorities' mutual objectives of maintaining safe and efficient credit reporting systems. The ideal arrangements will be formal, as appropriate, and will include mechanisms to fulfill oversight roles efficiently and in a manner that minimizes duplication of efforts and inconsistent policy decisions.

Formal arrangements backed by relevant regulations are necessary for cooperation with regulation and supervision of credit reporting systems with significant cross-border linkages or operations in multiple jurisdictions. CRSPs that operate across borders and serve more than one jurisdiction should be subject to oversight by a designated authority with primary responsibility, supplemented by a committee of competent regulators and supervisors of the relevant jurisdictions. The authority primarily responsible should formulate effective cooperation and consultation mechanisms with relevant authorities to develop policies on common issues and stay abreast of developments related to the credit reporting systems.

At the jurisdictional level, if more than one authority exercises the oversight function of credit reporting activities, one of them should be identified as having primary responsibility. Cooperation arrangements should ensure consistent regulatory and supervisory policies and minimize duplication of efforts and the regulatory burden on CRSPs. Also, relevant authorities in a jurisdiction should address any existing gaps in regulation or supervision of CRSPs through changes in rules, where possible, or by other means.

It is the responsibility of the primary authority to carry out comprehensive assessments of the credit reporting ecosystem and related activities and systems as a whole. A comprehensive assessment can only be facilitated by the following:

i. Efficient communication channels among authorities and relevant stakeholders.

ii. Adequate inputs of analysis and information by the relevant authorities, as shared on a regular or ad hoc basis.

iii. Consultation processes to exchange interests and concerns regarding policy decisions.

iv. Consensus on issues of common interest related to risks in credit reporting activities.

The authority should cooperate with relevant regulators of alternative data, such as telecommunications or insurance regulators, to facilitate the lawful sharing of such data with CRSPs.

The authorities should adopt best practices on international cooperative agreements. Cooperation arrangements with non-domestic authorities should be designed to fulfill the oversight responsibility of CRSPs that operate in multiple jurisdictions. For internationally active CRSPs, the primarily responsible authority can be the authority in the location of its headquarters or as determined cooperatively by all authorities in relevant countries. International cooperation arrangements should ideally be contained in a formal agreement to exchange supervisory concerns, insights, and policy discussions. To increase the efficiency of cooperation, authorities can leverage regulatory roundtables, supervisory colleges, joint research initiatives, and mutual consultations in addition to formal exchanges of information.

Cooperation arrangements, either domestic or international, should include crisis management plans as appropriate. Where an authority identifies any activities or functions as unsafe or unsound, the relevant authorities should immediately be notified to ensure corrective actions are carried out without delay.

Authorities of respective countries should coordinate to develop policies to facilitate cross-border credit reporting. Provided that individuals benefit from transferring their credit reports over national borders with their consent, authorities should permit and/or encourage cross-border exchange of data, including fostering regulatory changes to allow for it. Credit reporting industry associations should support the authorities in developing efficient and secure systems to enable cross-border flow of credit reports.

PRINCIPLE 5: Permissible Activities

The regulatory framework should define and cover permissible activities in credit reporting. Appropriate permission mechanisms, including market entry requirements should be governed by the authority.

The authority can impose reasonable market entry requirements for CRSPs to ensure effective oversight of the credit reporting activities. Entry requirements should also provide for the cancellation of licenses and appropriate mechanisms for ongoing custody or disposal of the credit information database. Entry requirements can include one or more of the following frameworks:

i. Licensing regime as a requisite for entry that allows the authority to assess whether a CRSP is suitable and eligible to operate within the jurisdiction before starting activities. Licensing regimes should be accompanied by clear eligibility conditions, such as necessary expertise, technical infrastructure, and management experience. Licensing regimes can be limited to a specific type of CRSP, such as a credit bureau.

ii. Registration regime that requires CRSPs to be recorded on a directory at the authority. While registration does not involve a process for granting approval, it allows the authority to have proper oversight of the entities dealing with credit reporting activities. Registration regimes should be accompanied by an appropriate regulatory framework for operational rules. The list of registered CRSPs can be published by the authority to support the transparency of the industry.

iii. Activity-based licensing that requires a specific type of credit reporting activity subject to a licensing regime. The activity-based approach enables a closer oversight role for the authority for credit reporting activities with more relative importance. Priority assessment of activities uses a risk-based approach, updated regularly and when necessary.

iv. Custom licensing that adopts a sequenced or phased approach. The custom licensing approach allows new CRSPs

to begin operations in a testing environment, like innovation hubs, or a live setting with limited activities. Activity-based and custom licensing regimes are particularly relevant for alternative credit reporting service providers seeking to leverage innovative technologies or alternative data.

In line with the market entry requirements, the regulation should restrict use of "credit bureau" or similar names subject to licensing frameworks. The authority should disclose the list of licensed or registered CRSPs to the public and monitor whether any other entities deal with permissible activities in the market.

The authority should closely monitor credit reporting activities with respect to the applicable permission requirements and should prevent regulatory arbitrage in the credit reporting market and ensure fair competition by enforcing permission rules for all players equitably.

PRINCIPLE 6: Access and Transparency

Credit reporting systems should allow fair and open access to their services, on the basis of reciprocity, by data providers, data users, data subjects, and other relevant stakeholders. Credit reporting systems should be subject to a clearly defined disclosure framework to enable participants to have an accurate understanding of credit reporting activities.

CRSPs should identify, assess, and manage all potential risks arising from a new participant, whether a data provider or a data user, to the credit reporting system. Participation in the credit reporting system should have a well-founded basis to ensure the information-sharing mechanism complies with relevant regulations.

Participants in the credit reporting system should comply with the established principles, such as reciprocity, rules, regulations, and codes of conduct, on an ongoing basis. The authority should monitor data providers' and data users' compliance, as well as that of CRSPs, to the relevant rules. Appropriate enforcement tools should be applied to participants to ensure the safety and integrity of the overall credit reporting system.

Credit reporting systems should establish appropriate precautions to ensure uninterrupted access by the participants. CRSPs should set up necessary procedures for business continuity and operational resilience of their services to avoid disruptions. Such procedures should determine critical business services, assess impact tolerances, and identify key processes for ensuring continuous services in severe conditions. The authority should consider the continuity of access to the credit information sharing mechanism in exceptional circumstances.

Credit reporting systems should facilitate fair and unbiased access to credit reporting products on competitive terms. Individual data subjects should be able to access their data through user-friendly channels. The authority can establish rules that allow consumers to request their credit reports at little or no cost. The authority should promote consumers' financial literacy, enabling them to benefit to the greatest extent from credit reporting systems.

CRSPs should disclose information to the public on the scope of their credit reporting activities, governance policies, and codes of conduct. CRSPs should share financial statements, prepared using internationally accepted standards, that fairly reflect their financial condition, along with a qualified independent external auditor's opinion.

The CRSPs should be subject to external audit annually and to information security audit as deemed necessary by the authority. The annual external audit should cover assessing and assuring the accuracy and reliability of the financial statements following internationally accepted financial reporting standards. The external audit reports should include any identified weaknesses in the governance and control process of the CRSP and any discovered cases of noncompliance. The information security audit provides a technical assessment to evaluate the adequacy of the CRSP's information security framework, identify vulnerabilities, if any, and provide recommendations on mitigation of risks.

PRINCIPLE 7: Governance

Credit reporting systems should be administered using a sound governance framework commensurate with the risks and the scope of the activities. The framework should establish sound policies and procedures, a proper internal control environment, and an appropriate organizational structure with clearly defined duties and responsibilities to ensure system efficiency and effectiveness in serving the markets.

CRSPs should establish sound governance policies, processes, and procedures to undertake safe and efficient activities and manage the inherent and emerging risks of credit reporting. To this end, the regulations can impose appropriate fit-and-proper requirements for the board of directors and senior management.

In line with their fitness and probity criteria, regulatory authorities should ensure that the shareholding and governance structures of CRSPs minimizes potential for conflict of interest and anticompetitive behavior.

The board of directors should be appropriately qualified to exercise its duties of care and loyalty. The board should approve and oversee the CRSP's business strategies; establish sound policies, procedures, and control environment; and create a corporate code of conduct that is communicated throughout the organization. Such policies should be reviewed on a regular basis to confirm they are still fit for purpose. CRSPs are encouraged to

cooperate with each other to develop codes of conduct to establish industry best practices, set operating standards, and promote the safety and efficiency of the overall credit reporting system.

Senior management should have the necessary qualifications to fulfill their administrative duties and assess, control, manage, and mitigate the risks related to credit reporting activities. Management should establish a proper organizational structure with adequate and qualified staff, implement sound business practices in line with established policies and procedures, maintain a control environment with appropriate segregation of duties, and ensure proper oversight of day-to-day activities.

A robust internal control framework should be established within the organization for a sound operating environment covering all credit reporting activities. It should be reviewed on a regular basis to confirm it remains fit for purpose. The internal control framework should address, at a minimum, the following considerations:

i. Clear definitions of duties and responsibilities.

ii. Delegation of authorities and segregation of duties throughout the organization.

iii. Decision-making processes and separation of critical functions.

iv. Access privileges and physical safeguarding ofassets.

CRSPs should have an independent, permanent, and effective internal audit function responsible for assessing the effectiveness, sufficiency, and compliance of policies, processes, and internal controls within the organization. The internal audit function should have sufficient powers, including a direct reporting line to the board, and adequate resources and staff with the necessary qualifications and experience to understand and evaluate the credit reporting activities.

Credit reporting systems should efficiently and effectively meet the needs of their participants and the markets they serve. The authority should encourage CRSP to form industry associations that establish a collaborative environment for reviewing the efficiency and effectiveness of credit reporting activities. Industry associations can also develop and promote good practices for the industry to ensure efficient and effective services.

Competition is an effective tool to promote the efficiency of credit reporting systems. In coordination with the relevant authority, the authority should promote competitiveness in the credit reporting industry. The authority should promote comprehensive information-sharing mechanisms and evaluate the roles of all CRSPs in the market to determine whether unfair access privileges hamper competition. Also, CRSPs should avoid anticompetitive practices, such as price fixing, setting restrictive terms of use, and unfair price differentiation.

PRINCIPLE 5: Risk Management

Credit reporting systems should be monitored within a comprehensive risk management framework and sound risk management culture to identify, assess, evaluate, manage, and mitigate all risks related to credit reporting activities on an ongoing basis.

CRSPs should develop a risk management framework and establish it throughout the organization. The framework should take a forward-looking approach, facilitating in-depth understanding of future risks and their potential impact on credit reporting activities. The framework should be adequately documented, regularly reviewed, and appropriately adjusted to reflect changes in the business environment. Policies and procedures should be consistent with risk management strategies and should cover clearly defined management responsibilities to monitor and control risk. Management should ensure that a sound risk management culture is communicated throughout the organization. A proper risk management function with the necessary resources, independence, and authority should be established to cover all material risks. This function is complemented by a sound internal control environment and an independent internal audit function.

CRSPs should have an adequate operational risk management framework commensurate with the scope of credit reporting activities. Operational risk management relates closely to sound governance policies, processes and procedures, and the internal control environment throughout the organization. The framework should include effective disaster recovery and business continuity plans, including scenario analysis, to ensure continuity of services under severe conditions that could disrupt credit reporting activities.

CRSPs should establish policies and processes to assess, manage, and monitor outsourced activities. Outsourcing arrangements should cover conducting appropriate due diligence for selecting service providers, managing risks associated with the outsourcing agreement, ensuring an effective control environment, and maintaining viable contingency plans.

The authority should require CRSPs *to establish a model governance framework* for credit scoring models to ensure that the credit score is explainable, transparent, and fair. The model governance framework should meet the following standards:

i. The models use lawfully obtained, clear, understandable, and disclosable data.

ii. The methods and techniques employed are independently assessable and auditable.

iii. The score is free of any discriminatory practices.

CRSPs are responsible for ensuring these standards are developed and used by third parties.

CRSPs should have an effective compliance function with an adequate number of staff with the necessary qualifications and with experience managing the legal and compliance risks. The compliance function should ensure ongoing compliance assessments in credit reporting activities. The function should be complemented with a sound evaluation process for all new sources of data, products, activities, and data users to assess legal, compliance, and other potential risks.

PRINCIPLE 9: Data Security

An appropriate information security framework should govern credit reporting activities to protect the confidentiality, integrity, and availability of information and ensure business continuity and operational resilience.

The authority should develop an appropriate information security framework with cybersecurity strategies for credit reporting systems covering all stakeholders such as data providers, data users, and third-party service providers. This framework can either be part of the national cyber strategy framework or the financial sector information security framework or be developed for the credit reporting industry. The information security framework should enable interagency cooperation for monitoring cybersecurity threats and vulnerabilities.

The information security framework should include the following:

i. A cyber governance framework with effective board oversight, clearly defined and documented roles and responsibilities for information security functions, and allocation of adequate staff with necessary qualifications and appropriate budgets to ensure the sound management of information security and cyber risks.

ii. Information security policies and procedures that identify, assess, monitor, and manage all risks related to the use of information and communication technologies.

iii. Information security strategies, as part of overall business strategies, which are reviewed and updated as necessary.

iv. Control and risk mitigation tools, such as minimum access, access recertification, user accountability, activity logs, or authentication measures.

v. Regular cyber audits to assess and assure, with a risk-based approach, the organization's compliance with the information security framework.

vi. Cybercrime incident, disaster recovery, and business continuity plans, to ensure continuity of services under severe conditions, such as cyberattacks.

vii. Cyberattack simulations to assess the effectiveness of cyber incident response plans and update information security policies in line with simulation results.

viii. Outsourcing policies for third-party providers that include appropriate and proportionate information-security policy requirements, such as minimum cybersecurity standards, data retention periods, data encryption requirements, network security processes, and cybercrime incident handling plans.

The authority should develop and enforce information-sharing mechanisms that facilitate cybersecurity-focused collaboration in the credit reporting industry. These mechanisms should promote sharing of timely, actionable, and relevant unclassified information related to cyber threats, vulnerabilities, and emerging risks to collectively protect the integrity of the credit reporting systems. Information-sharing mechanisms can be encouraged through industry associations.

PRINCIPLE 10: Data Collection

Data providers should provide relevant, accurate, timely, and sufficient information on data subjects, including positive data, to CRSPs to enable a comprehensive credit information-sharing mechanism. CRSPs can collect data from all legal, reliable, appropriate, and available sources and retain this information for a sufficient time for credit reporting.

The authority should encourage a comprehensive information-sharing system. Data providers should send CRSPs positive and negative information with the most depth and breadth possible, and as appropriate. To the extent possible, the information submitted should be free of error, truthful, complete, and up to date.

Data providers should include, at a minimum, banks and NBFIs operating within the jurisdiction's borders. To the extent possible, alternative lenders, if any, and nonfinancial creditors such as utilities, rental companies, phone companies, retailers, and e-commerce companies should be recognized as data providers.

Data should be collected systematically by consistently applying appropriate rules and procedures for all data providers. Data should be collected at regular intervals and as frequently as possible and appropriate. The frequency can be predefined or can depend on specific triggers like defaults, arrears, or fraud. Rules and procedures for data submission can be defined by a common code of conduct developed by the relevant stakeholders and approved by the authority.

CRSPs are encouraged to collect nontraditional data from alternative sources. To the extent possible, *the authority should promote access to alternative data.* It is the responsibility of the CRSP to ensure that alternative data is lawfully shared, relevant, accurate, complete, and up to date.

The regulation should also enable CRSPs access to public records, to the extent possible, as appropriate and relevant for credit reporting.

CRSPs should only retain data for a specific period sufficient for the purpose of credit reporting. If deemed appropriate, the regulations can determine different periods for negative and positive information. Data should be deleted or restricted for statistical or modeling purposes after the end of the retention periods as specified in the regulation.

PRINCIPLE 11: Personal Data

Personal data collection, processing, and distribution should be undertaken only for the purposes for which the data was collected, including creditworthiness assessment, credit risk analysis, indebtedness and repayment capacity, ID confirmation, fraud prevention, and prudential supervision.

Data collected and processed for credit reporting purposes can only be disclosed, sold, or distributed to data users for the same purposes, in the form of credit reports, scores, ID verification, fraud prevention, or similar products, by any means of communication.

CRSPs should ensure the following conditions regarding collecting, processing, and disclosing personal data of individual data subjects:

i. Types of personal data collected are relevant to credit reporting purposes and include only as much data as necessary for credit reporting purposes.

ii. As appropriate, individuals are informed of the processing of their personal data and the distribution of their credit reports to data users.

iii. Personal data is kept accurate and up to date and retained for only as long as necessary for the credit reporting purposes.

iv. Credit reports should not include any type of personal data irrelevant to credit reporting or any type of personal data or creditworthiness assessment that can lead to discrimination against the individual.

v. Data users cannot use the credit reports for any purpose other than the purpose specified for the distribution.

CRSPs should ensure that data users can promptly, without delay, access credit reports used to support their credit-granting decisions. Credit reports should cover all the negative and positive information, including relevant nontraditional information, as appropriate for the creditworthiness assessment. Data subjects should be able to access their data at CRSPs under conditions similar to those under which data users access the data.

PRINCIPLE 12: Consumer Rights

Consumers should have clear rights regarding the use of their personal data for credit reporting. These rights should include consent, dispute, notification, and access rights; the right to restrict data use; and the right to request transfer of data, as appropriate. Effective dispute resolution mechanisms should be established for handling consumer disputes related to credit reporting activities. Credit reporting products should be explainable, transparent, and fair.

Individual data subjects, as consumers, should have clear rights regarding the use of their personal data. Depending on the applicable data protection framework, these rights can include provisions on the following topics:

i. Dispute incomplete or inaccurate personal data and request correction within a reasonable time.

ii. Be informed about the purpose of processing and time of retention of personal data and the third parties with whom personal data is shared.

iii. Have access and receive a copy of personal data.

iv. Ask for a consumer credit score.

v. Request the erasure, as appropriate, of personal data.

vi. Request restrictions on the use of personal data.

vii. Request the move, copy, or transfer of personal data.

viii. Suspend access in case of ID theft or fraudulent activity.

ix. File for compensation for violation of rights.

If required by relevant laws and/or regulations, data providers should obtain consent for collecting, storing, and distributing the personal data of data subjects.

Effective dispute resolution mechanisms should include internal complaint handling functions at the CRSPs as well as other extrajudicial mechanisms. CRSPs should establish easily accessible in-house dispute resolution functions to address in a timely manner any disputes raised by data subjects. These functions, including the websites of CRSPs, should include communication of consumer rights in clear, plain language. The CRSP's website should ideally have online tools to file disputes.

CRSPs should establish policies and procedures for the proper handling and resolution of data subjects' complaints. These policies should have the following key considerations:

i. Establishing appropriate channels for submission of complaints.

ii. Convenient, affordable, and prompt resolution of disputes.

iii. Internal procedures covering the steps of the dispute resolution process, including specific communication channels with

data providers.

iv. Adequate training and independence of the staff responsible for handling complaints.

v. Clear communication of the consumers' rights, including the right to apply to the extrajudicial mechanism.

vi. Keeping appropriate dispute records to ensure accountability.

The extrajudicial mechanisms can include appeals to a credit ombudsman as established by the regulation or appeals to an alternative dispute resolution service provider offering tools such as arbitration, mediation, or online dispute resolution. An appropriate regulatory framework should support these mechanisms. This framework should cover the rights, responsibilities, and objectives of the mechanism and provide proper resources to fulfill these objectives. The authority should assess and ensure the effectiveness of the dispute resolution tools in terms of their convenience, diligence, and promptness.

CRSPs should ensure the fairness of the models, techniques, and technologies employed in developing products. In particular, credit reporting products should protect the fundamental rights of individuals and not entail any discriminatory biases. Credit reporting products, including credit scores, should be explainable, transparent, and fair, that is:

i. The types of data that provide the basis of the products are legitimate, clear, understandable, and disclosable to the data subjects.

ii. The methods and techniques employed and the scope of data used in the model are assessable and auditable by an independent third party.

iii. The model is inclusive in the sense that it is free of any discriminatory biases.

7

SUGGESTED APPROACH FOR REGULATORY AND SUPERVISORY AUTHORITIES

An effective regulatory framework for credit reporting systems is possible with a properly functioning supervisory framework. *Holistic oversight of the functioning of the credit reporting system is vital* to ensure that the players in credit reporting activities are able to manage the risks related to credit information sharing. While the primary focus of supervision has traditionally been on credit bureaus, the authority should now make other types of CRSPs, data providers, and data users part of the supervisory framework. Considering the differences in the nature of CRSP credit reporting activities and their varying risk implications for the credit reporting system, the supervisory framework should *adopt a risk-based, proportionately applied approach for effective oversight.*

Supervision of credit reporting activities should be undertaken with a risk-based approach to ensure that (i) supervisory resources are deployed effectively, and (ii) the most relevant risks and areas of concern in credit reporting activities are adequately identified and addressed. The risk-based approach enables the application of key principles on a proportionate basis. A proportionate approach is particularly important as (i) the scope of activities of CRSPs varies to a great extent, (ii) credit reporting systems are evolving, and (iii) innovations facilitate new business models. Therefore, attempting to apply a one-size-fits-all approach is not productive.

In many countries' existing regulatory frameworks, central banks, or financial sector supervisors are responsible for supervising CRSPs. This, in practice, makes the authority's approach to CRSP supervision similar to financial institution supervision. While the primary function of CRSPs is to support the creditworthiness assessments of financial institutions, they are not financial entities that deal with lending activities and should not be treated as such. The core activity of a CRSP is to collect, store, process, produce, distribute, and use data to support lenders' credit-granting decisions. In essence, CRSPs deal with data management. Therefore, the objective of oversight with regard to the applicable regulatory framework should be whether:

i. The types and sources of collected data are permitted.

ii. The data are accurate, adequate, and to the extent possible, updated.

iii. The security of data is ensured by adequate technical, physical, and governance measures.

iv. The data are distributed to and used by data users for permissible purposes.

v. Consumer rights are protected, and consumer complaints are appropriately handled.

vi. Services are provided to data users on an ongoing basis using a sound risk management framework with disaster recovery and business continuity plans.

7.1 Risk-Based Supervision

The risk-based approach differs from compliance-based supervision, which conducts mainly backward-looking oversight of entities' adherence to regulatory requirements. Risk-based supervision focuses on assessing the most significant risks for the entities and how effectively these risks are managed, allowing for better allocation of supervisory resources.

The key characteristics of risk-based supervision for authorities responsible for oversight of credit reporting systems can be summarized as follows:

i. The supervisory focus is on the most important risks, that is, those that have the potential to cause maximum damage for the CRSP, the credit reporting system, and the financial system in general. In determining the importance of a risk, consideration is given to both impact (the extent of losses if the risk were to materialize) and likelihood (the possibility of the risk to materialize). However, the overall risk depends on how the identified risks are controlled and managed by the CRSP (see Figure 1).

FIGURE 1: Risk Assessment

ii. Risks can originate from a broad range of sources, which must be taken into consideration. Risks can be entity-specific, credit reporting industry-related, or arise from external factors on a broader, macroeconomic level. While CRSPs may not be able to control risks from external sources, the potential implications for such risks should be managed.

iii. The risks of CRSPs are assessed and graded, often using a risk matrix, to provide a structured way of thinking about them and to form a basis for comparing, evaluating, and prioritizing the risk types and their effects on CRSPs and the credit reporting sector.

iv. Risk assessment criteria and their evaluations are documented and updated as necessary. The assessments can be entity-specific (focused on individual CRSPs) or thematic (focused on activities, such as credit scores, or risk types, such as cybersecurity risk). Thematic assessment covers the selected theme in all credit reporting industry entities.

BOX 11

Supervisory Approach

NET RISK	SUPERVISORY FOCUS	SUPERVISORY ACTIONS
Low	Normal oversight	
Low to medium	Normal oversight	Address minor deficiencies
Medium to high	Increased oversight	Address deficiencies Corrective action plans
High	Increased oversight	Immediate corrective actions Restrictive orders Changes in management

The risk-based approach is dynamic and forward-looking (Toronto Center 2018). It aims to identify and address emerging areas of risk and to evaluate the effectiveness of the CRSPs' risk management. Risk assessments are performed consistently to form a foundation for annual or biennial supervisory programs. Also, outcomes of previous supervisory actions are evaluated as part of the assessment.

The risk-based approach facilitates, in most cases, allocating scarce supervisory resources to the most effective areas by prioritizing entities, sectors, activities, or risk types. Supervisory actions should focus on identified risks and proportionate in resource allocation (see Box 11).

To develop and maintain effective communication with regulated entities, authorities can share their risk assessments with the CRSPs to express concerns and expectations and get feedback on the assessments. For example, the Financial Conduct Authority (FCA) shares with CRSPs (credit reference agencies) its view of the key risks of harm, as summarized here (FCA 2020):

i. Loss or misuse of personal data, causing identity theft or financial loss.

ii. Consumers excluded from credit products or borrowed inappropriately based on poorly designed credit reporting products, ineffective product governance, and poor data quality.

iii. Disruption in services, with creditors and consumers unable to access credit reporting services or credit data.

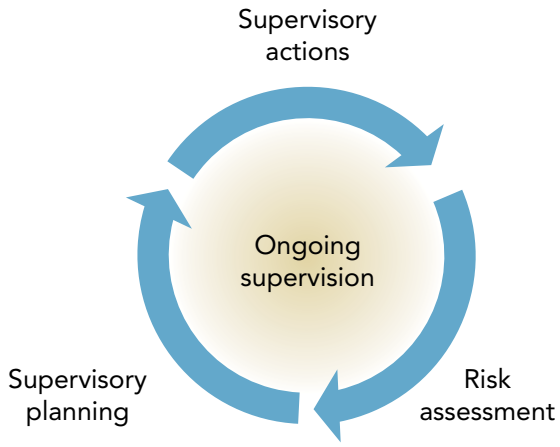
iv. Inappropriate resolution of complaints, causing consumer loss or distress.

7.2 Supervisory Program

The authorities carry out their supervisory activities through annual or biennial supervisory programs, which mandate supervision of entities as part of the authority's responsibility. In line with the key principles, credit reporting systems should also be part of supervisory programs.

Applying a risk-based approach, the authority assesses the potential impacts and probabilities for the key risks in CRSP activities. Following the assessment of key risks, the adequacy and effectiveness of risk governance is evaluated to develop an understanding of the net risks (see Figure 1). Outcomes of risk assessments form the basis for developing the supervisory program. The supervisory program includes risk assessment, supervisory planning, off-site reviews, on-site supervision, and supervisory action components (see Figure 2).

FIGURE 2: Supervisory Program



The authority should assign a dedicated team or department with clearly established roles and responsibilities for the oversight of credit reporting activities. The team responsible for oversight of CRSPs should have the necessary knowledge and qualifications to analyze the nature and scope of credit reporting. An effective oversight function consists of both off-site review and on-site supervision.

7.2.1 Off-Site Review

The main objective of the off-site review is to ensure that CRSPs and data providers operate in compliance with the relevant regulations. Supervisors should establish an off-site reporting framework to fulfill this objective. This framework should be automated to the possible extent and should allow data extraction by supervisors from the CRSPs' information systems and/or a regular reporting mechanism prepared and sent by CRSPs. Supervisors can require CRSPs to submit various types of information, as appropriate, such as:

i. Annual audited financial statements and external audit reports.

ii. Data quality statements, statistics on credit reports, data subjects, data inquiries, and consumer complaints.

iii. Credit market reports on credit growth, quality, borrower segmentation, and arrears.

As part of the off-site review, the team responsible for the CRSP should evaluate the adequacy, accuracy, consistency, and timeliness of its reports to ensure the CSRP is complying with regulations. Regular off-site reports can be supplemented by ad hoc requests for information from the CRSP and other available sources of information. Statistical data from CRSPs can also be compared to data regularly submitted by regulated financial institutions to confirm compliance.

The off-site review process covers (i) general compliance monitoring based on the regular reports, (ii) analysis of credit reporting activities to identify potential risks, (iii) analysis of credit market trends, (iv) assessment of the scope and scale of consumer complaints, and (v) reviews focused on specific themes such as information security. Based on the findings from the off-site review, the team can identify particular areas of focus for on-site supervision; prepare recommendations of policy actions for the CRSP, data providers, or users; or propose enforcement actions in cases of noncompliance.

From the supervisory authority's perspective, it is essential that the information sent by CRSPs is properly reviewed, assessed, and analyzed and any identified vulnerabilities or areas of concern or noncompliance are reported as appropriate. Off-site reviews provide an effective tool for the authorities, especially to assess compliance. However, the effectiveness of such reviews depends on the adequacy of the reports' analyses. Off-site reports provide little value without adequate review by the authority. This is a particular concern for authorities in developing countries, which may have limited staff resources available to dedicate to off-site review of credit reporting systems.

Authorities with limited supervisory resources can leverage supervisory technology (SupTech) tools for off-site reviews. SupTechs use technology to facilitate and enhance authorities' supervisory processes. SupTechs can help authorities process information quickly and in large quantities, automate and streamline processes, identify trends, and analyze key risks for CRSPs (World Bank 2020d). Examples of SupTech tools for specific use cases include the following:

i. Automated reporting: Used with efficient staff allocation, automated reporting requires less manual work and more judgment-based analytical work.

ii. Early warning indicators: Indicators are useful for analyzing the trends of credit exposures, monitoring overindebtedness, and providing systemic oversight.

iii. Validation: Validation ensures integrity and consistency of data through cross-checking algorithms.

iv. Text-mining and natural language processing (NLP): NLP productively evaluates licensing applications and improves processes.

7.2.2. On-Site Supervision

The main objective of on-site supervision is to complement off-site reviews, with a focus on high-risk areas identified during the off-site review process. The team responsible for on-site supervision should understand CRSP operations fully and be able to identify governance, risk management, and internal control weaknesses during the on-site supervision process. To this end, the team should receive the necessary training before being

assigned to a CRSP and should possess the essential background in information technology, credit information and reporting, consumer protection, and risk management. The team should include, where necessary, specialist IT supervisors to perform IT consistency checks focused on fraud prevention and maintaining data integrity.

The on-site supervision task focuses on areas of concern identified in the off-site review process: business strategy, compliance checks, data accuracy and security, cyber resilience, resolution of consumer complaints, governance policies and procedures, internal controls and risk management, and financial performance. The team should have the legal rights and the means to request and access any information from the CRSP, including trade secrets, as long as the information is relevant to the scope of the supervision. The findings of the on-site supervisory team and any areas of concern should be drafted in a report and discussed in a meeting with the senior management and the CRSP board.

The root causes of issues revealed during the on-site supervision should be identified, as they may indicate potential problems with the data providers or users. Examples include inaccurate data submission by providers, improper access or use of the data by users, and handling of consumer disputes or a disproportionate number of disputes. These issues can also indicate increased credit risk to the financial institutions or potential areas of noncompliance. If the findings concern regulated financial institutions or other regulated data providers, the authority should bring the findings to the attention of the bank supervision department or other relevant authority.

The off-site review and on-site supervision can result in enforcement actions, penalties, or fines as defined by the regulation. Such actions include, but are not limited to, (i) official letters to the CRSP regarding identified areas of concern requiring improvement, (ii) noncompliance cases that demand corrective actions, and (iii) administrative penalties and financial fines as defined in the regulation. For cases that necessitate extended action plans, CRSPs should be required submit board- or senior-management-approved plans with specific actions required to be completed within a defined timeline.

7.3 Considerations in Adopting the Principles

The key principles provide regulatory and supervisory guidance to ensure the effective functioning of credit reporting systems. In essence, these principles build on existing guidance such as the GPCR, guidance documents of the ICCR and IFIs, common regulatory rules in jurisdictions, and industry best practices. The key principles also provide a risk-based approach to the authority for proportionate application. In applying the principles to address the evolving risks of credit reporting systems, the authority can benefit from the following considerations.

7.3.1 Scope

Traditionally, credit bureaus are the most regulated and supervised entities among the different types of CRSP. This is because (i) the types of data collected by credit bureaus are treated as confidential under banking laws or personal data protection laws; (ii) CSRPs often operate under a licensing regime to provide, or sometimes force, structured data flows from banks, as historical experience shows voluntary data collection is ineffective; and (iii) credit scores provided by credit bureaus are a key tool for promoting access to finance. IFIs and national authorities therefore promote the incorporation of credit bureaus and regulate and oversee the safety and efficiency of their operations.

On the other hand, the key principles suggest different types of CRSPs should be covered by a regulatory and supervisory framework. In essence, the key principles provide a framework for credit reporting activities rather than pinpointing specific CRSPs in most cases. This is particularly important as the definitions of different types of CRSPs are not as clear as they were in the past. The competitive environment in the credit reporting system is evolving, making the following considerations important for evaluating the status of different types of CRSP against the principles.

7.3.2 Credit Registries

Where public credit registries are known to support prudential supervision as a primary objective, many credit registries collect and process personal data and, in some cases, operate as competitors to the private credit bureaus. Therefore, as the key principles suggest, credit registries should be subject to the same rules to the extent that their credit reporting activities involve serving the market. A key challenge in applying the key principles to a credit registry is that the supervisory authority is also the credit registry operator. In this case, the functions of supervising the CRSPs and operating the registry should be clearly separated under different departments, or, ideally, under different directorships.

The authority should ensure that the credit registry and other CRSPs operate on a level playing field while they are serving the market. For example, credit registries can have access to public records databases that other CRSPs cannot. It is also not uncommon for credit registries to collect data directly from credit bureaus. This is expected, considering the systemic oversight role of credit registries. In this case, the authority should fulfill the objective of promoting comprehensive information-sharing mechanisms but also evaluate the roles of all CRSPs in the market to determine whether unfair access privileges hamper competition.

Credit registries play an essential role in supporting the prudential supervision of the financial system and provide a key tool for systemic oversight. Credit registries play a growing role for policy makers overseeing financial stability. To this end, applying the key principles to the credit registries, as appropriate, can provide certain benefits such as:

i. Improved comprehensiveness of data sources enables the credit registry to provide an accurate overview of credit exposures, emerging risks of overindebtedness, and early warning indicators on credit concentrations.

ii. Enhanced governance, control, and risk management policies ensure the safety of operations.

iii. Oversight of activities provides a line of defense against the risks inherent in credit registry activities.

7.3.3 Business Information Providers

Business information providers play an essential role in extending trade credit by producing business intelligence for credit risk assessment. The business credit reports produced by these entities are generally based on public databases or retrieved directly from businesses (for example, trade receivables information). Historically, activities of business information providers often did not fall under the scope of credit reporting regulations. In general, they did not collect personal data, and they were not granted access privileges by a credit information-sharing mechanism. However, this may not be the case today for a few reasons.

First, business information providers must collect personal data, mainly the personal data of business owners, shareholders, or sole entrepreneurs. This is primarily because regulations such as GDPR do not differentiate between the personal data of an individual and a sole entrepreneur or between private personal data and the publicly available personal data found in public business registers. Second, business information providers can collect personal data because they provide a range of value-added products that deal with personal information and so can compete with credit bureaus for credit reporting services in some markets, and vice versa. Therefore, as the key principles suggest, business information providers should follow the same rules to the extent that they are involved in credit reporting activities and collect and process personal data.

Business information providers have an important role to play in managing the risks of trade credit. To this end, applying the key principles to business information providers, as appropriate, can provide benefits such as:

i. Improved mechanisms for comprehensive information sharing to facilitate services and products.

ii. Enhanced governance, control, and risk management policies to ensure the safety of operations.

iii. A clearly defined and consistently applied set of regulatory rules to improve the competitive environment.

iv. Oversight of activities to support and improve the efficiency of the overall credit reporting sector.

7.3.4 Alternative Credit Reporting Service Providers

The key principles also set forth the regulatory oversight of alternative credit reporting service providers as a type of CRSP. As an emerging type, correctly identifying these entities is important, as no widely accepted definition for alternative credit reporting service providers exists. Broadly speaking, two types of innovative entities are involved with credit reporting activities. The first group focuses on developing innovative solutions by leveraging scores from credit bureaus. The second group focuses on developing credit scores by leveraging alternative data sources, innovative technologies, or both. While the difference between the two groups may not be clear, alternative credit reporting service providers fall into the second category. From an authority's perspective, the key consideration is to identify the nature of the entity's activities and decide whether it is a CRSP.

The authority should determine whether the innovative entity, or fintech, is an alternative credit reporting service provider. This decision requires evaluating whether its business model actually falls under the definition of credit reporting. Credit reporting involves a credit information sharing mechanism that covers collecting and compiling information on individuals or businesses, processing this information to produce structured data, and disclosing or selling this data or creating value-added products on this data to *third-party users* to assess creditworthiness and manage credit risk. The decision process for evaluating the status of an innovative entity can require the following steps for proper consideration:

i. Assessing the entity by its business model and/or its innovation by focusing on the function rather than the entity itself.

ii. Applying relevant regulatory frameworks to the function and determining whether this function falls under the scope of credit reporting regulation and/or other applicable regulations such as alternative lenders, AISPs, or similar entities.

iii. Consulting and collaborating with other relevant authorities, especially if the oversight of fintechs falls under the responsibility of another authority.

iv. Deciding whether the entity is an alternative credit reporting service provider.

v. Applying the relevant regulatory framework, including custom licensing rules if appropriate.

7.3.5 Oversight of Credit Scoring Models

The authority should oversee the credit scoring models of CRSPs to ensure that the credit scores are explainable, transparent, and fair. This is particularly relevant when using AI models, which usually involve complex algorithms. Notwithstanding the technical complexity of these models, the authority must take ethical considerations into account. The mitigation of bias risk in algorithmic models is not only a technical problem: it requires policy con-

siderations at a broad level to define and promote ethical and responsible innovation (CDEI 2020).

The authority should ensure that CRSPs establish and document an appropriate governance and accountability framework to assure the reliability, fairness, accuracy, auditability, and relevance of the AI models, the data used, and the outputs. To guide the CRSPs in establishing effective model governance frameworks, the authority should consider the following (ICCR 2019a):

i. Governance policies to assess unintended consequences, disregard protected types of data, perform regular reviews, and back-test and validate model performance.

ii. A rights-based ethical policy framework that upholds fundamental human rights and ethical principles as part of model governance. This ethical framework can be established with the active involvement of industry associations and CRSPs to support the responsible use of AI.

iii. A data accountability framework that covers policies to ensure data security, privacy of personal data, accuracy of data, and legitimacy of data sources.

iv. Collaborative initiatives with stakeholders to exchange knowledge, support financial literacy, and foster innovative models while mitigating risks.

v. Building capacity and/or engaging with independent qualified experts to develop skills at the authority to understand and oversee innovations in the credit scoring models.

In particular, CRSPs should include the following practices to establish sound model governance frameworks (World Bank 2021).

i. Assess potential limitations of the composition of the training data.

ii. Review the representativeness and reliability of the training data.

iii. Identify groups of most concern for data errors and unequal treatment to test for potential biased use.

iv. Ensure that an appropriate definition of fairness is applied when designing AI systems and that the applied definition of fairness is measured and tested.

v. Identify thresholds for detecting, measuring, and correcting for potentially biased outputs.

The authority can require regular external audits of AI models as appropriate. Audits should assess input data, training data, design and testing processes, decision factors, and outputs for potential negative impacts. Assessments can involve testing AI models using hypothetical scenarios to identify potential negative impacts and recommend appropriate risk mitigation measures.

7.3.6 Promoting Comprehensive Information Sharing

The authority should promote the use of alternative data sources to support comprehensive information-sharing mechanisms and advocate for the inclusion of individuals and MSMEs into the credit markets. Despite its potential benefits, the use of alternative data sources has inherent risks and challenges. The authority can use a range of policy tools to mitigate these risks while promoting alternative data and ensuring the accuracy, quality, and completeness of credit reports.

The authority can introduce regulations, circulars, or guidelines for collecting and processing alternative data while ensuring its lawful collection. Often separate regulators of alternative data, such as telecommunications or insurance regulators, must be consulted to facilitate sharing their data with CRSPs. In this sense, the authority can prioritize regulating and enforcing the collection of data from sources that provide the most benefit. Sources of alternative data with the most potential benefits include financial data that is widely used, structured, accurate, and up to date, such as digital loans, utility payments, rental payments, tax payments, P2P transactions, e-commerce transactions, mobile transactions, and registries of assets. These sources can vary at the jurisdictional level.

Alternative lenders play a growing role in the financial inclusion of unserved or underserved consumers. Activities of alternative lenders do not usually fall within the scope of regulations. In addition to potential benefits in building an inclusive credit system, alternative data is important to avoid the risk of consumer overindebtedness, a significant bottleneck to financial inclusion (AFI 2016). To support a comprehensive information-sharing mechanism, the authority should emphasize that alternative lenders' credit information be included in the credit reporting system.

The authority should consider introducing regulations aimed at improving the availability, quality, and accuracy of alternative data. Depending on the varying needs of jurisdictions, these regulations can include tools such as (ICCR 2018):

i. Standard IDs for individuals and businesses.

ii. Access to public databases for ID validation purposes.

iii. Digitized government services and an open data approach facilitating for CRSP access.

iv. Digital footprints, such as incentivizing the use of digital payments.

v. An expanded list of data providers in the credit reporting system to cover the most creditors possible.

vi. Lowered or, if possible, eliminated minimum thresholds for data collection.

While the authority can introduce regulations to promote collection of alternative data, often technical impediments arise associated with collecting data from new sources. As such, the authority can benefit from collaborating with industry associations and relevant agencies to develop and introduce these regulations. The risks, challenges, costs, and potential benefits of leveraging new data sources should be discussed with the credit reporting industry to develop policies that will benefit stakeholders to the greatest possible extent.

7.3.7 Collaboration with Industry Associations

The credit reporting industry has a long history of self-regulation in many ways. Considering the technical details and associated risks of dealing with massive numbers of individuals, businesses, data, and intelligence, many jurisdictions introduced general legislation for credit reporting systems, while CRSPs developed their own codes of conduct.[6] In this sense, self-regulatory mechanisms developed in credit reporting industry associations in many jurisdictions. Industry associations exist throughout the world at both the national and the regional levels.[7] Considering the highly technical nature of credit reporting activities, the authority can benefit from collaborations with industry associations, which can develop guidelines, under the oversight of the authority, on the following topics:

i. Standards for harmonizing data attributes and improving the depth and breadth of data shared by data providers (for example, Consumer Data Industry Association developed the Metro2 system for data providers).

ii. A code of business ethics covering areas of concern, such as the use of AI-based scoring models.[8]

iii. Principles of responsible innovation to guide handling of potential risks, like predatory lending.

iv. Cyber threat information-sharing mechanisms to protect the overall credit reporting system against cyber risks.

v. Financial literacy programs to increase consumer awareness on topics like data privacy and credit scores.

Codes of conduct have multiple potential benefits for the credit reporting industry. For example, they can promote greater industry transparency, enhance stakeholder or investor confidence, ensure compliance with regulations to minimize breaches, establish quality control and minimum service levels, and help create cost-effective complaint handling mechanisms (ACCC 2011).

6. In jurisdictions such as the Pacific Islands, voluntary codes of conduct, in lieu of formal regulations, have been used to govern behavior.

7. ICCR has industry associations among its members. They include ACCIS, the Association of Credit Information Sharing Africa (ACISA), Asociación Latinoamericana de Crédito (ALACRED), US Consumer Data Industry Association (CDIA), Federation of Business Information Service Europe (FEBIS), and Business Information Industry Association (BIIA).

8. For a broad overview of the existing ethics guidelines on AI, see Hagendorff (2020). A guidance document on responsible use of technology in credit reporting is also forthcoming from the ICCR.

8

ASSESSMENT METHODOLOGY

The key principles outlined in this report are intended to help countries assess the quality of their CRSP regulatory and supervisory frameworks and to provide guidance for identifying areas for improvement. An assessment of a country's current regulatory and supervisory framework against the principles should identify weaknesses in the existing framework and assist government authorities and supervisors to develop a reform agenda. A country's regulatory and supervisory authorities bear primary responsibility for conducting reviews against the key principles.

This section provides a methodology for assessing the regulatory and supervisory frameworks at the national level.[9] The assessment methodology is primarily intended for IFIs, but it is also helpful for national authorities and other internal and external assessors. A complete and accurate assessment requires the cooperation of the relevant regulatory and supervisory authorities. Assessors should have the necessary access to all public information and all relevant parties for their study. Also, relevant nonpublic information, such as internal policies and procedures, supervisory manuals, and statistical data, should be disclosed for the purposes of conducting the assessment. Nonpublic information provided to the assessors should be treated confidentially and not disclosed to or shared with third parties. If assessors cannot access key information or staff, or other challenges impair the assessment's quality, the report should reflect that.

The relevant regulatory and supervisory framework of a country, as documented in the applicable laws, regulations, and circulars, forms the basis of the assessment. In some cases, the actual application of the framework can differ from that called for in the formal framework, so assessors should observe the actual interpretation of the framework in practice. This in-practice assessment requires formal meetings and/or other communication with the stakeholders in the credit reporting system, including regulators, CRSPs, data providers, data users, and bodies representing consumers.

The team of assessors should have the necessary set of skills, relevant experience, and strong ethics to ensure a quality assessment. The set of skills include the expertise to evaluate regulatory and supervisory frameworks, knowledge of the policy issues regarding regulations and oversight, thorough understanding of the credit reporting activities, and knowledge of CRSP products and the underlying technologies.

8.1 Assessment Framework

Assessment of the observance of the key principles and recommendations for improving regulation and supervision should be done at the country or jurisdictional level. Although some principles can require that assessors review regulators or CRSPs at the individual level, conclusions and, if any, ratings to reflect the degree of observance should be drawn at the country level. The scope of the assessment should be clearly determined and agreed with the relevant regulatory and supervisory authorities and communicated in advance to the relevant stakeholders. As part of their conclusions, assessors are also expected to provide insights on ways to improve the framework.

Assessors should gather the facts necessary to develop conclusions on each of the key principles. The existing situation should be analyzed on the basis of the principles and key considerations associated with them, as provided in Section 7. Assessors can use the following questions to gain general understanding of the framework during the assessment:

i. Which laws and regulations apply to the country's credit reporting activities? This can include credit reporting laws,

9. This section follows the methodology for assessment of the GPCR as outlined in ICCR (2013).

data protection laws, consumer protection laws, commercial laws, banking laws, cybersecurity regulations, or any other relevant legislative framework.

ii. What are the national regulatory and supervisory authorities responsible for overseeing the observance of the applicable laws and regulations? The credit reporting activities can be subject to the oversight by more than one authority.

iii. Which types of CRSPs operate in the country, and to what extent are they covered within the applicable laws and regulations? All types of entities that deal with credit reporting activities in the country should be identified, which may include unregulated data providers.

iv. What is the authorities' approach to observing the key principles? Do the relevant authorities conduct self-assessments of their observance of the country's regulatory and supervisory framework against the key principles?

v. Have the relevant authorities developed a roadmap for strengthening the regulatory and supervisory framework in response to the results of any self-assessment? Authorities can identify areas of reform and establish ongoing projects to improve observance of the framework.

vi. Does any other evidence support the assessment of the observance of the key principles? Stakeholders such as CRSP associations can conduct their own assessment studies regarding the framework.

For each of the principles, assessors should summarize the country's current framework and practices. For any areas of concern, assessors should describe the issue, the underlying reasons for it, and its potential implications for the regulatory and supervisory framework and the credit reporting system as a whole. In describing these concerns, assessors should review the materiality and relative importance of the concern and how it interrelates with the other principles. Recommendations should build on the facts as described regarding the concern and be accompanied by one or more potential solutions to guide the responsible authorities.

Assessors can use ratings as part of their conclusions on the observance of the key principles. Country ratings support a better understanding of the assessment result and promote consistent assessments over time. It should be noted, however, that ratings are not country rankings of regulatory and supervisory frameworks. Table1 presents a rating system based on the rating scale used in assessments by the Financial Sector Assessment Program (FSAP) of the IMF and the World Bank. The rating is built on the assessment's conclusions and reflects assessors' judgment regarding the materiality and importance of the associated areas of concerns and the potential risk implications. To guide the authorities in establishing timeframes for action, assessors should establish priorities based on the level of materiality of any areas of concern. If observance of a particular principle could not be assessed adequately, the assessors should explain and document those instances.

TABLE 1: Assessment Rating System

RATING	DESCRIPTION
Observed	The principle is observed. Identified gaps, if any, are not areas of concern and could be considered in the normal course of business.
Broadly Observed	There are one or more areas of concern that the authority is encouraged to address within a defined timeline. Such areas require attention, but that is not critical for the whole credit reporting system.
Partly Observed	There are one or more areas of concern that require the attention of the authorities and should be addressed in a timely manner.
Not Observed	The principle is not observed. There are one or more critical areas of concern that require the immediate attention of the authorities and are addressed accordingly.
Not Applicable	The principle is not applicable due to the particular legal, structural, or institutional characteristics of the country's credit reporting system.

APPENDIX
GENERAL PRINCIPLES ON CREDIT REPORTING

The General Principles are aimed at meeting the following public policy objectives for credit reporting systems: Credit reporting systems should effectively support the sound and fair extension of credit in an economy as the foundation for robust and competitive credit markets. To this end, credit reporting systems should be safe and efficient and fully supportive of data subject and consumer rights.

Data

GENERAL PRINCIPLE 1: Credit reporting systems should have relevant, accurate, timely, and sufficient data, including positive data, collected on a systematic basis from all reliable, appropriate, and available sources and should retain this information for a sufficient amount of time.

Data Processing: Security and Efficiency

GENERAL PRINCIPLE 2: Credit reporting systems should have rigorous standards of security and reliability and should be efficient.

Governance and Risk Management

GENERAL PRINCIPLE 3: The governance arrangements of credit reporting service providers and data providers should ensure accountability, transparency, and effectiveness in managing the risks associated with the business and provide users with fair access to the information.

Legal and Regulatory Environment

GENERAL PRINCIPLE 4: The overall legal and regulatory framework for credit reporting should be clear, predictable, nondiscriminatory, proportionate, and supportive of data subject and consumer rights. The legal and regulatory framework should include effective judicial or extrajudicial dispute resolution mechanisms.

Cross-Border Data Flows

GENERAL PRINCIPLE 5: Cross-border credit data transfers should be facilitated, where appropriate, provided adequate requirements are in place.

Roles of Key Players

ROLE A: Data providers should report accurate, timely and complete data to credit reporting service providers on an equitable basis.

ROLE B: Other data sources, in particular public records agencies, should facilitate access to their databases to credit reporting service providers.

ROLE C: Credit reporting service providers should ensure that data processing is secure and should provide high quality and efficient services. All users having either a lending function or a supervisory role should be able to access these services under equitable conditions.

ROLE D: Users should make proper use of the information available from credit reporting service providers.

ROLE E: Data subjects should provide truthful and accurate information to data providers and other data sources.

ROLE F: Authorities should promote a credit reporting system that is efficient and effective in satisfying the needs of the various participants and supportive of data subject/consumer rights and of the development of a fair and competitive credit market.

Recommendations for Effective Oversight

RECOMMENDATION A: Credit reporting systems should be subject to appropriate and effective regulation and oversight by a central bank, a financial supervisor, or other relevant authorities. It is important that one or more authorities exercise the function as primary overseer.

RECOMMENDATION B: Central banks, financial supervisors, and other relevant authorities should have the powers and resources needed to carry out effectively their responsibilities in regulating and overseeing credit reporting systems.

RECOMMENDATION C: Central banks, financial supervisors, and other relevant authorities should clearly define and disclose their regulatory and oversight objectives, roles, and major regulations and policies with respect to credit reporting systems.

RECOMMENDATION D: Central banks, financial supervisors, and other relevant authorities should adopt, where relevant, the General Principles for credit reporting systems and related roles and apply them consistently.

RECOMMENDATION E: Central banks, financial supervisors, and other relevant authorities, both domestic and international, should cooperate with each other, as appropriate, to promote the safety and efficiency of credit reporting systems.

GLOSSARY

TERM	DEFINITION	SOURCE
Code of conduct	A self-regulatory framework for credit reporting service providers that governs their relationship to data providers, users, borrowers, other bureaus, and the supervisory authority.	World Bank (2018a)
Consumer	See data subject.	
Consumer consent	A data subject's freely informed and specific agreement, written or verbal, to the collection, processing, and disclosure of personal data.	World Bank (2011)
Credit bureau	Model of credit information exchange with the primary objective of improving the quality and availability of data for creditors to make better-informed decisions.	World Bank (2011)
Credit registry	Model of credit information exchange whose main objectives are to assist prudential supervision and enable data access to regulated financial institutions to improve the quality of their credit portfolios.	World Bank (2011)
Credit risk	The risk that a counterparty will not settle the full value of an obligation – neither when it becomes due, nor at any time thereafter.	ECB (2022)
Credit score	Form of statistical analysis that provides an estimate of the probability that a loan applicant, existing borrower, or counterparty will default or become delinquent.	ICCR (2019a)
Creditworthiness	The ability of a borrower to repay current and prospective financial obligations in a timely manner. It is used as an assessment of a borrower's past credit behavior to assist a potential lender to decide whether to extend new credit.	World Bank (2011)
Data provider	Creditors and other entities that proactively and in a structured fashion supply information to the credit reporting service providers.	World Bank (2011)
Data subject	An individual or a business whose data could be collected, processed, and disclosed to third parties in a credit reporting system.	World Bank (2011)
Data user	An individual or business that requests credit reports, files, or other related services from credit reporting service providers, typically under predefined conditions and rules.	World Bank (2011)
Default	Failure to complete a payment obligation under a credit or loan agreement.	World Bank (2011)
Negative information	Statements about defaults or arrears and bankruptcies. It may also include statements about lawsuits, liens, and judgments obtained from courts or other official sources.	World Bank (2011)
Personal data	Information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an ID number or one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity.	ICCR (2021)
Positive information	Information that covers facts of contractually compliant behavior. It includes detailed statements about outstanding credit, amount of loans, repayment patterns, assets, and liabilities, as well as guarantees and/or collateral.	World Bank (2011)
Structured data	Any data that reside in a fixed field within a record or file. Typically, the data reside in the form of relational databases and spreadsheets. The formal structure allows one to easily enter, store, query, and analyze the data.	ICCR (2019b)
Unstructured data	Data that do not have a predefined data model or are not organized in a predefined manner. They exist typically in the form of text files, images, social media data, and sensor data.	ICCR (2019b)

BIBLIOGRAPHY

ACCC (Australian Competition & Consumer Commission). 2011. "Guidelines for Developing Effective Voluntary Industry Codes of Conduct." https://www.accc.gov.au/system/files/Guidelines%20for%20developing%20effective%20voluntary%20industry%20codes%20of%20conduct.pdf.

ACCIS. 2020. "ACCIS Membership Survey 2020." https://accis.eu/facts-and-figures/.

AFI (Alliance for Financial Inclusion). 2016. "The Policy Framework on Responsible Digital Credit." https://www.afi-global.org/sites/default/files/publications/2020-04/EN_Policy_Framework_for_Responsible_Digital_Credit.pdf.

Barci, G., G. Andreeva, and S. Bouyon. 2019. "Data Sharing in Credit Markets: Does Comprehensiveness Matter?" European Credit Research Institute Research Report No. 23. http://www.ecri.eu/sites/default/files/accis_ecri-ceps-ue_data_sharing_in_credit_markets-web_0.pdf.

BCBS (Basel Committee for Banking Supervision). 2005. "Compliance and the Compliance Function in Banks." Bank for International Settlements, Basel. https://www.bis.org/publ/bcbs113.pdf

BCBS (Basel Committee for Banking Supervision). 2011. "Principles for the Sound Management of Operational Risk." Bank for International Settlements, Basel. https://www.bis.org/publ/bcbs195.pdf.

BCBS (Basel Committee for Banking Supervision). 2012. "Core Principles for Effective Banking Supervision." Bank for International Settlements, Basel. https://www.bis.org/publ/bcbs230.htm.

BCBS (Basel Committee for Banking Supervision). 2019. "Supervisory Review Process: Risk Management." Bank for International Settlements, Basel. https://www.bis.org/basel_framework/chapter/SRP/30.htm.

Berg, T., V. Burg, A. Gombović, and M. Puri. 2019. "On the Rise of FinTechs — Credit Scoring Using Digital Footprints." Michael J. Brennan Irish Finance Working Paper Series Research Paper No.18-12. http://dx.doi.org/10.2139/ssrn.3163781.

BIS (Bank for International Settlements). 2012. "Principles for Financial Market Infrastructures." Bank for International Settlements, Basel. https://www.bis.org/cpmi/publ/d101a.pdf.

CDEI (Centre for Data Ethics and Innovation). 2020. "Review into Bias in Algorithmic Decision-making." Centre for Data Ethics and Innovation, London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf.

Consumer Financial Protection Bureau (CFPB). 2020a. "Supervision and Examination Manual." https://files.consumerfinance.gov/f/documents/cfpb_supervision-and-examination-manual.pdf.

Consumer Financial Protection Bureau (CFPB). 2020b. "Supervisory Highlights on Consumer Reporting." https://www.consumerfinance.gov/compliance/supervisory-highlights/.

Credit Information Sharing Association of Kenya (CIS). 2021. "Code of Conduct for Third-Party Credit Information Providers." https://ciskenya.co.ke/wp-content/files/2021/05/Code-of-Conduct-2021-Final-as-Approved.pdf.

Creditinfo. 2020. "Global Lending Industry Trends." Creditinfo, Reykjavík. https://creditinfo.com/wp-content/uploads/2017/08/creditinfo_trends_2020.pdf.

DPC (Data Protection Commission of Ireland). 2021. "Inquiry to the Irish Credit Bureau." Data Protection Commission of Ireland, Dublin. https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Summary%20of%20Decision%20Irish%20Credit%20Bureau.pdf.

EBA (European Banking Authority). 2019. "EBA Guidelines on ICT and Security Risk Management." European Banking Authority, Paris. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.

EBA (European Banking Authority). 2020. "EBA Report on Big Data and Advanced Analytics." European Banking Authority, Paris. https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf.

ECB (European Central Bank). 2018. Anacredit. European Central Bank, Frankfurt Am Main. https://www.ecb.europa.eu/stats/money_credit_banking/anacredit/html/index.en.html.

ECB (European Central Bank). 2022. Glossary. European Central Bank, Frankfurt Am Main.
https://www.ecb.europa.eu/services/glossary/html/glossc.en.html

Equifax. 2021. "Equifax Data Breach Settlement." Equifax, Atlanta.
https://www.equifaxbreachsettlement.com/. Last accessed June 24, 2021.

European Union (EU). 2016. "General Data Protection Regulation." European Union, Brussels. https://gdpr-info.eu/.

European Union (EU). 2021. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." European Union, Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

Experian South Africa Data Incident. 2021. Experian, Dublin. https://www.experian.co.za/fraudulent-data-incident. Last accessed June 24, 2021.

FCA (Financial Conduct Authority). 2020. "Credit Reference Agencies Portfolio Letter." Financial Conduct Authority, London. https://www.fca.org.uk/publication/correspondence/cra-cisp-portfolio-letter.pdf.

Federal Deposit Insurance Corporation (FDIC). 2017. "Supervisory Guidance on Model Risk Management." Federal Deposit Insurance Corporation, Washington, DC. https://www.fdic.gov/news/financial-institution-letters/2017/fil17022a.pdf.

Federal Trade Commission (FTC). 2021. "Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans." Federal Trade Commission, Washington, DC. https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports.

Financial Conduct Authority (FCA). 2021. "Building Operational Resilience."
https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience.

Financial Stability Board (FSB). 2021. "The Compendium of Key Standards." Financial Conduct Authority, Basel. https://www.fsb.org/work-of-the-fsb/about-the-compendium-of-standards/wssb/.

Frost, J., L. Gambacorta, Y. Huang, H. S. Shin, P. Zbinden. 2019. "BigTech and the Changing Structure of Financial Intermediation." BIS Working Papers No. 779. Bank for International Settlements, Basel. https://www.bis.org/publ/work779.pdf.

Gambacorta, L., Y. Huang, and J. Wang. 2019. "How Do ML and Non-Traditional Data Affect Credit Scoring? New Evidence from a Chinese Fintech Firm." BIS Working Papers No: 834. Bank for International Settlements, Basel. https://www.bis.org/publ/work834.pdf.

Ghosh, S. 2019. "Loan Delinquency in Banking Systems: How Effective Are Credit Reporting Systems?" *Research in International Business and Finance*, Elsevier, 47(C): 220–36. https://ideas.repec.org/a/eee/riibaf/v47y2019icp220-236.html.

Girault, M. G., and J. Hwang. 2010. "Public Credit Registries as a Tool for Bank Regulation and Supervision." Policy Research Working Paper No. WPS 5489. World Bank, Washington, DC. http://hdl.handle.net/10986/3972.

Hagendorff, T. 2020. "The Ethics of AI Ethics: An Evaluation of Guidelines." *Minds and Machines* 30: 99–120. https://doi.org/10.1007/s11023-020-09517-8.

Hengel, E. 2010. "Discussion Paper on Credit Information Sharing." Facilitating Access to Finance Discussion Paper Series. OECD, Paris. https://www.oecd.org/global-relations/45370071.pdf.

ICCR (International Committee on Credit Reporting). 2013. "Assessment Methodology for the General Principles for Credit Reporting." World Bank, Washington, DC. http://hdl.handle.net/10986/21813.

ICCR (International Committee on Credit Reporting). 2014. "Facilitating SME Financing through Improved Credit Reporting." World Bank, Washington, DC. http://hdl.handle.net/10986/21810.

ICCR (International Committee on Credit Reporting). 2016. "The Role of Credit Reporting in Supporting Financial Sector Regulation and Supervision." World Bank, Washington, DC. https://consultations.worldbank.org/consultation/role-credit-reporting-supporting-financial-sector-regulation-and-supervision.

ICCR (International Committee on Credit Reporting). 2018. "Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs Operating in the Informal Economy." Global Partnership for Financial Inclusion Guidance Note. World Bank, Washington DC. https://www.gpfi.org/sites/gpfi/files/documents/Use_of_Alternative_Data_to_Enhance_Credit_Reporting_to_Enable_Access_to_Digital_Financial_Services_ICCR.pdf.

ICCR (International Committee on Credit Reporting). 2019a. "Credit Scoring Approaches Guidelines." World Bank, Washington, DC. https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf.

ICCR (International Committee on Credit Reporting). 2019b. "Cybersecurity in Credit Reporting Guidelines." World Bank, Washington, DC. https://thedocs.worldbank.org/en/doc/735641585870130697-0130022020/original/Cybersecurityincreditreportingguidelinefinal.pdf.

ICCR (International Committee on Credit Reporting). 2020. "Treatment of Credit Data in Credit Information Systems in the Context of the COVID-19 Pandemic." World Bank, Washington, DC. https://thedocs.worldbank.org/en/doc/972911586271609158-0130022020/original/COVID19ICCRCreditReportingPolicyRecommendationsfordistribution6346.pdf.

ICCR (International Committee on Credit Reporting). 2021. "Cross-border Credit Reporting." World Bank, Washington, DC. https://www.biia.com/wp-content/uploads/2021/08/ICCR-Cross-Border-Report-final-July-2021.pdf.

International Finance Corporation, Arab Monetary Fund. 2015. "Arab Credit Reporting Guide." International Finance Corporation, Washington, DC. http://hdl.handle.net/10986/25979.

International Monetary Fund (IMF) and World Bank. 2018. "The Bali Fintech Agenda." International Monetary Fund (IMF), Washington, DC; World Bank, Washington, DC. https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda.

International Monetary Fund (IMF) and World Bank. n.d. "Financial Sector Assessment Program (FSAP)." International Monetary Fund (IMF), Washington, DC; World Bank, Washington DC. https://www.worldbank.org/en/programs/financial-sector-assessment-program.

Liu, C., and C. Hou. 2021. "Challenges of Credit Reference Based on Big Data Technology in China." Mobile Networks and Applications 27 (2022): 47–57. https://doi.org/10.1007/s11036-020-01708-y.

Martinez, P., S. Maria, and S. Singh. 2014. "The Impact of Credit Information Sharing Reforms on Firm Financing." Policy Research Working Paper, No. 7013. World Bank Group, Washington, DC. http://hdl.handle.net/10986/20348.

Monetary Authority of Singapore (MAS). 2018. "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector." https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf.

National Credit Bureau of Thailand (NCB). 2016. "Internal Audit Charter." National Credit Bureau of Thailand, Bangkok. https://www.ncb.co.th/about-us/internal-audit-charter-en.

NIST (National Institute of Standards and Technology). 2017. "Cybersecurity Framework." National Institute of Standards and Technology, Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

NYSDFS (New York State Department of Financial Services). 2018. "Cybersecurity Requirements for Financial Services Companies." https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).

NYSDFS (New York State Department of Financial Services). 2021. "Report on the SolarWinds Cyber Espionage Attack and Institutions Response." https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf.

OCC (Office of the Comptroller of the Currency). 2019. "Comptroller's Handbook: Corporate and Risk Governance." Office of the Comptroller of the Currency, Washington, DC. https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/pub-ch-corporate-risk.pdf.

Owens, John, Wilhelm, Lisa. 2017. "Alternative Data Transforming SME Finance." Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/701331497329509915/Alternative-data-transforming-SME-finance.

Steering Committee on Reciprocity (SCOR). 2018. "Information Sharing: Principles of Reciprocity." https://scoronline.co.uk/principles/.

Sutherland, A. 2018. "Does Credit Reporting Lead to a Decline in Relationship Lending? Evidence from Information Sharing Technology." *Journal of Accounting and Economics*, Elsevier, 66 (1): 123–41. https://ideas.repec.org/a/eee/jaecon/v66y2018i1p123-141.html.

Toronto Center. 2018. "Risk-based Supervision." TC Notes.
https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20FINAL.pdf.

Toronto Center. 2020. "Cloud Computing: Issues for Supervisors." TC Notes.
https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20FINAL.pdf.

U.S. Congress. 2019. Algorithmic Accountability Act, H.R. 2231, 116th Congress. https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info. Last accessed September 19, 2021.

World Bank. 2011. "General Principles for Credit Reporting." World Bank, Washington DC.
http://hdl.handle.net/10986/12792.

World Bank. 2017. "How Credit Reporting Systems Contribution to Financial Inclusion." International Committee on Credit Reporting Policy Brief, World Bank, Washington, DC. https://consultations.worldbank.org/consultation/how-credit-reporting-contributes-financial-inclusion.

World Bank Group. 2018a. "Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting." World Bank, Washington, DC. http://hdl.handle.net/10986/31009.

World Bank Group. 2018b. "Financial Sector's Cybersecurity: Regulations and Supervision." Finance, Competitiveness & Innovation Insight Series. World Bank, Washington, DC. https://openknowledge.worldbank.org/handle/10986/29378.

World Bank. 2018c. "Improving Access to Finance for SMEs Through Credit Reporting: Opportunities through Credit Reporting, Secured Lending, and Insolvency Practices." World Bank, Washington, DC. https://documents1.worldbank.org/curated/en/316871533711048308/pdf/129283-WP-PUBLIC-improving-access-to-finance-for-SMEs.pdf.

World Bank Group. 2019a. "Credit Reporting Knowledge Guide 2019." World Bank, Washington, DC. http://hdl.handle.net/10986/31806.

World Bank. 2019b. "Credit Reporting Without Borders: A Regional Credit Reporting Project." Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/482141547662326461/Credit-Reporting-Without-Borders-A-Regional-Credit-Reporting-Project.

World Bank Group. 2019c. "Developing a Strong Credit Reporting System: A Toolkit for Practitioners." International Finance Corporation, Washington, DC. http://hdl.handle.net/10986/31362.

World Bank Group. 2019d. "Disruptive Technologies in the Credit Information Sharing Industry: Developments and Implications." Fintech Note, No.3. World Bank, Washington, DC. http://hdl.handle.net/10986/31714.

World Bank. 2020a. "Credit Bureau Licensing and Supervision: A Primer." World Bank, Washington, DC. http://hdl.handle.net/10986/34760.

World Bank. 2020b. "Doing Business 2020: Comparing Business Regulation in 190 Economies." World Bank, Washington, DC. http://hdl.handle.net/10986/32436.

World Bank. 2020c. "How Regulators Respond to FinTech: Evaluating the Different Approaches — Sandboxes and Beyond." Fintech Note No. 4. World Bank, Washington, DC. http://hdl.handle.net/10986/33698.

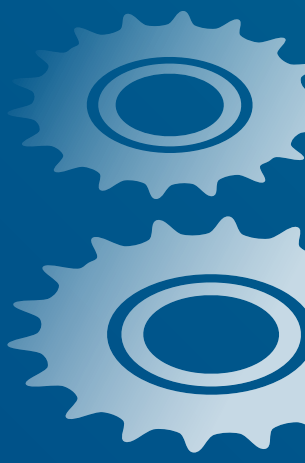
World Bank. 2020d. "A Roadmap to SupTech Solutions for Low Income (IDA) Countries." Fintech Note No. 7. World Bank, Washington, DC. http://hdl.handle.net/10986/34662.

World Bank. 2021. "Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches." World Bank, Washington, DC. http://hdl.handle.net/10986/35699.

World Bank and Cambridge Centre for Alternative Finance (CCAF). 2019. "Regulating Alternative Finance: Results from a Global Regulator Survey." World Bank, Washington, DC; Cambridge Centre for Alternative Finance, Cambridge, UK. http://hdl.handle.net/10986/32592.

World Bank and Consultative Group to Assist the Poor (CGAP). 2018. "Data Protection and Privacy for Alternative Data." Global Partnership for Financial Inclusion Discussion Paper. World Bank, Washington, DC; Consultative Group to Assist the Poor, Washington, DC. https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf.

Yong, J., and J. Prenio. 2021. "Humans Keeping AI in Check: Emerging Regulatory Expectations in the Financial Sector." FSI Insights on Policy Implementation No. 35. Bank for International Settlements, Basel. https://www.bis.org/fsi/publ/insights35.pdf.



WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING