****

**CYBERSECURITY IN CREDIT REPORTING GUIDELINE**

**CONTENTS**

[**ACKNOWLEDGEMENTS** 4](#_Toc13641159)

[**EXECUTIVE SUMMARY** 5](#_Toc13641160)

[**ACRONYMS AND ABBREVIATIONS** 8](#_Toc13641161)

[**GLOSSARY OF TERMS** 9](#_Toc13641162)

[**1.** **INTRODUCTION AND BACKGROUND** 10](#_Toc13641163)

[**2.** **THE EVOLVING CREDIT REPORTING CYBER LANDSCAPE** 13](#_Toc13641164)

[**2.1** **Evolution of the credit reporting cyber ecosystem** 13](#_Toc13641165)

[**2.2** **Evolving cyber incidents in credit reporting industry** 14](#_Toc13641166)

[**2.3** **Potential sources of risks** 17](#_Toc13641167)

[**3** **GLOBAL CREDIT REPORTING CYBER SECURITY LANDSCAPE** 23](#_Toc13641168)

[**3.1** **Introduction** 23](#_Toc13641169)

[**3.2** **Demographics of Respondents** 23](#_Toc13641170)

[**3.3** **Survey Findings** 24](#_Toc13641171)

[**3.3.1** **Local cyber environment** 24](#_Toc13641172)

[**3.3.2** **Legal and regulatory environment** 25](#_Toc13641173)

[**3.3.3** **Board, management cyber and information security strategy** 26](#_Toc13641174)

[**3.3.4** **Outsourcing critical IT services** 28](#_Toc13641175)

[**3.3.5** **Information sharing cyber incidents** 28](#_Toc13641176)

[**3.3.6** **Training and awareness** 29](#_Toc13641177)

[**3.3.7** **Resources** 30](#_Toc13641178)

[**3.3.8** **Risk management and compliance** 30](#_Toc13641179)

[**3.3.9** **Audit** 31](#_Toc13641180)

[**3.3.10** **Incident Response** 31](#_Toc13641181)

[**3.3.11** **Data loss prevention (DLP)** 32](#_Toc13641182)

[**3.3.12** **Preventative controls** 33](#_Toc13641183)

[**4** **CYBERSECURITY GUIDELINES** 35](#_Toc13641184)

[**4.1** **Existing Credit Reporting Guidelines on Cybersecurity** 35](#_Toc13641185)

[**4.2** **Detailed Cybersecurity Guidance** 35](#_Toc13641186)

[**4.2.1** **Cybersecurity and Data Privacy strategy** 36](#_Toc13641187)

[**4.2.2** **Governance** 39](#_Toc13641188)

[**4.2.3** **Risk Management** 40](#_Toc13641189)

[**4.2.4** **Compliance** 42](#_Toc13641190)

[**4.2.5** **Data Privacy** 43](#_Toc13641191)

[**4.2.6** **Awareness and Education** 46](#_Toc13641192)

[**4.2.7** **Information Sharing and Communications** 47](#_Toc13641193)

[**4.2.8** **Resilience** 48](#_Toc13641194)

[**4.2.9** **Technology Operations** 49](#_Toc13641195)

[**4.2.10** **Security Operations** 54](#_Toc13641196)

[**5** **POLICY CONSIDERATIONS** 60](#_Toc13641197)

[**5.1** **Enhancing Cyber Legal and Regulatory Environment** 60](#_Toc13641198)

[**5.2** **Development of Cybersecurity Strategy and Framework** 60](#_Toc13641199)

[**5.3** **Enhancing Cyber Governance** 61](#_Toc13641200)

[**5.4** **Cyber Training for Board Directors** 61](#_Toc13641201)

[**5.5** **Cyber breach disclosure frameworks** 62](#_Toc13641202)

[**5.6** **Outsourcing of Critical IT Services** 62](#_Toc13641203)

[**5.7** **Periodic Cyber Risk Assessments** 63](#_Toc13641204)

[**5.8** **Periodic Cyber Audits** 63](#_Toc13641205)

[**5.9** **Establishment of Cyber Information Sharing and Collaboration Mechanisms** 64](#_Toc13641206)

[**5.10** **Incident Response, Disaster Recovery and Business Continuity** 64](#_Toc13641207)

[**6** **REFERENCES** 66](#_Toc13641208)

[**7** **SURVEY QUESTIONAIRE** 84](#_Toc13641209)

[**i.** **Contact Information** 85](#_Toc13641210)

[**ii.** **Local Cyber Security Environment** 85](#_Toc13641211)

[**iii.** **Local Legal and Regulatory Environment** 86](#_Toc13641212)

[**iv.** **Board, Management and Cybersecurity and Information Security Strategies** 87](#_Toc13641213)

[**v.** **Outsourcing Critical IT Services** 89](#_Toc13641214)

[**vi.** **Information Sharing** 89](#_Toc13641215)

[**vii.** **Training and Awareness** 89](#_Toc13641216)

[**viii.** **Resources** 90](#_Toc13641217)

[**ix.** **Risk Management & Compliance** 90](#_Toc13641218)

[**x.** **Audit** 91](#_Toc13641219)

[**xi.** **Incident Response** 91](#_Toc13641220)

[**xii.** **Data Loss Prevention (DLP)** 92](#_Toc13641221)

[**xiii.** **Preventive Controls** 93](#_Toc13641222)

[**8** **REFERENCES** 95](#_Toc13641223)

**ACKNOWLEDGEMENTS**

This guideline is a product of the International Committee on Credit Reporting (ICCR) and the World Bank Group (WBG) as an input to the Financial Inclusion Global Initiative (FIGI) guidance on cybersecurity for the financial infrastructure. This report builds on previous work conducted by the ICCR namely “The General Principles for Credit Reporting”(2011) and existing work of the FSB, the IMF, ENISA, the CPMI, IOSCO and G7 on cybersecurity in financial sector.

The guideline was prepared by Marcelo Roldan (Senior IT Officer, Security, Risk and Compliance), Aquiles Almansi (Lead Financial Sector Specialist), Collen Masunda (Financial Sector Consultant) and Luz Maria Salamina (Lead Financial Sector Specialist). The document benefited from a consultation process with ICCR Cybersecurity Working Party, Plenary members and representative organisations, and external peer reviewers.

The ICCR would also like to thank the Chairman of the ICCR, Sebastian Molineus; the Secretariat: Luz Maria Salamina and Collen Masunda; Neil Munroe, Chair of the ICCR Cybersecurity Working Party and the other members of the Working Party. Special thanks to colleagues from the World Bank Group who provided useful insights: Fredesvinda Montes, and Dorothee Delort. The Committee also acknowledges the managerial oversight by Mahesh Uttamchandani, the incoming ICCR Chair.

**EXECUTIVE SUMMARY**

The importance of credit reporting systems to the global financial system has been increasing over time. Robust credit reporting systems can promote access to affordable and sustainable credit for individuals and companies and promote financial stability and economic growth. Credit reporting service providers (CRSPs) have been at the frontier of technology adoption to enhance their efficiencies as well as data acquisition, processing and storage capabilities.

The credit reporting industry landscape has changed over the past decade with the adoption of new technologies, new business models and the emergence of new players helping improve the speed of service provided and the quality and completeness of credit data. These positive changes in the credit reporting ecosystem, however, also present a source of risk for the CRSPs. Several CRSPs have been subject to data breaches, denial of service attacks and phishing attacks, among other cyber incidents in the last couple of years.

The incidents have resulted in severe financial, economic, operational and reputational loss for the targeted organization and the industry at large. The implications can also be far reaching due to increasing interconnectedness of the financial sector. Against this background, there is need for enhanced cybersecurity and data standards at the CRSP and jurisdiction level.

This guideline provides findings of a landscaping survey conduct on CRSPs across the globe on best practice. The survey found that CRSPs across the globe were in general implementing cybersecurity practice. The survey also identified the following key issues:

* CRSPs were subjected to less attacks than data providers and other prominent institutions.
* The most common incident among CRSPs was denial of services.
* The majority of jurisdictions have enacted legislation or regulations to deal with cybersecurity and information security. The Central Bank emerged as the regulatory authority for most of the respondents. All, except one, jurisdiction place an obligation on the CRSPs to notify the affected parties.
* CRSPs have broadly embedded cyber and information security in their governance processes.CRSPs are also building capacity for staff and board members. A growing number of CRSPs’ have created a function of Chief Information Security Officer (CISO) or its equivalent that is responsible for cyber and information security.
* Cyber insurance is gaining prominence as one of the risk mitigant options**.**
* CRSPS are increasingly considering outsourcing critical services.
* The sharing of information on cyber incidents is gaining momentum, with the majority of CRSPs participating in industry programs designed to promote information sharing. Third parties are also significantly contributing to information sharing.
* CRSPs are increasingly committing specific resources to improve their cybersecurity capabilities.
* The majority of CRSPs have a formal risk management framework that includes cyber risk as one of the risk areas. Institutions are also recognizing the importance of internal audit as a central pillar in cybersecurity.
* Most CRSPS have documented incident response plans, though, notable gaps were observed with respect to partnering with the Computer Emergency Response Team (CERT), external communications and simulation exercises.
* CRSPs had implemented programs to monitor and prevent breaches, and certain rules to control printing of sensitive information.
* CRSPs are successfully implementing controls against cyber risks.

Based on the survey results, these guidelines provide detailedguidance to CRSPs onmanaging cybersecurity and data privacy risk. The guidelines focus on the areas of strategy, governance, risk management, compliance, functional operations, technology operations, data privacy, awareness & education, information sharing & communication and incident response and business continuity and emphasize the need to ensure risk-based approach and proportionality in the application of the guidelines.

The guidelines conclude by providing policy consideration that address some of the weaknesses identified in the survey. These recommendations are designed at enhancing the security of national cyber space in respect of credit reporting. The policy considerations are:

1. Policy makers should consider implementing and/or enhancing cyber laws and regulations that provides incentives for better protection of data and systems.
2. Regulatory authorities should consider developing national and/or sector-wide cybersecurity strategies and frameworks.
3. To the extent possible, regulatory bodies should consider implementing practices or standards that promote the strengthening of cyber governance by CRSPs.
4. Where applicable, regulatory bodies should ensure that CRSPs develop detailed programs for training their boards of directors.
5. Regulatory authorities should issue guidance on the level and extent of disclosures of security and data breaches.
6. Regulatory authorities should ensure that CRSPs implement sound outsourcing procedures that detail the controls and processes to be followed when evaluating and managing relationships with third parties.
7. Regulatory authorities should also consider subjecting third parties that service CRSPs with the same level of risk management practices expected of the entities themselves.
8. Supervisory authorities should consider conducting annual cybersecurity risk assessments of critical infrastructure players.
9. In carrying out this responsibility, where possible, the supervisory authorities should consider collaborative methods, such as including information sharing and joint assessments, to reduce regulatory burden on the CRSPs.
10. Authorities should consider promoting CRSPs to conduct their own internal assessments on a periodic basis.
11. Regulatory authorities should consider promoting regular cyber audits of cyber functions.
12. Regulatory and/or industry bodies should consider developing mechanisms that foster and enforce cyber information sharing and collaboration among parties.
13. Regulatory bodies should also publish or promote publication of redacted reports on cybersecurity issues on a semi-annually (half yearly) basis.
14. Regulatory authorities should ensure that CRSPs actively participate and collaborate with national cybersecurity actors such as CERTs.

**ACRONYMS AND ABBREVIATIONS**

|  |  |
| --- | --- |
| APEC | Asia-Pacific Economic Cooperation |
| BYOD | Bring Your Own Device |
| CERT | Computer Emergency Response Team |
| CFO | Chief Finance Officer |
| CRO | Chief Risk Officer |
| CISO | Chief Information Security Officer |
| CPMI | Committee on Payments and Market Infrastructure |
| CRSP | Credit Reporting Service Providers |
| CSIRT | Computer Security Incident Response Team |
| DFS | Department of Financial Services |
| DPO | Data Protection Officer |
| DDoS | Distributed Denial of Service |
| GDPR | General Data Protection Regulation |
| IEC | International Electrotechnical Commission  |
| IMF | International Monetary Fund |
| ENISA | European Agency for Network and Information Security |
| FIGI | Financial Inclusion Global Initiative  |
| FINRA | Financial Industry Regulatory Authority |
| IOSCO | International Organization of Securities Commissions |
| IDS/IPS | Intrusion Detection System / Intrusion Prevention System |
| ISO | International Organization for Standardization |
| NIST | National Institute of Standards and Technology |
| NPL | Non-performing loans |
| OECD | Organization for Economic Cooperation and Development |
| PCI DSS | Payment Card Industry Data Security Standard |
| RCSA | Risk and Control Self-Assessments |
| SIEM | Security Information and Event Management |
| SOC | Security Operation Centers |
| SOC Report | Service Organization Controls Report |

**GLOSSARY OF TERM[[1]](#footnote-1)S**

Credit Reporting Service Provider An entity that administers a mechanism enabling credit information collection, processing and further disclosure to users of data as well as value added services based on such data. The main types of CRSPs are credit registries, credit bureaus and commercial credit reporting companies.

Cyber Attack An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Incident An occurrence that results in actual or potential violation of an explicit or implied security.

Cyber Risk The risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction.

Cyber Threat An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

Cyber Vulnerabilities Refers to a flaw/ weakness in a system that can leave it open to attack.

# **INTRODUCTION AND BACKGROUND**

**Credit reporting systems are seen as a crucial part of the financial infrastructure, whose function can have a significant impact on the stability of the global financial system[[2]](#footnote-2)**. Robust credit reporting systems can promote access to affordable and sustainable credit for individuals and companies and promote financial stability and economic growth.

**Failure of the credit reporting infrastructure can impact the effective functioning of credit markets**. Widespread cyber incidents can trigger lenders to curtail credit granting in response to fears of widespread frauds that could emanate from such data incidents. The resultant credit rationing can then impact on aggregate demand by individuals and firms profitability. Cyber incidents can also lead to an increase in the granting of fraudulent credit facilities which can translate into an increase in NPLs..

**The credit reporting industry has evolved over the past decade through the adoption of new technologies, new business models and emergence of new players.** The adoption of new technologies and the entrance of new players to the credit-reporting ecosystem[[3]](#endnote-1) has been seen as a way of improving the speed of service and the quality and completeness of credit data. New technologies are enhancing the ability of CRSPs to collect and share credit data in a faster, more efficient and more cost-effective way thus promoting financial inclusion. New players are tapping into new data sources to assist with creditworthiness assessment helping with the offering of credit to clients with thin or no credit files.

**Notwithstanding the benefits, the evolution of credit reporting can become a threat and source of vulnerability for the credit reporting system and financial infrastructure in general.** As cyber ecosystems grow, the potential sources of vulnerabilities increase. Vulnerabilities at individual entities are more likely to have an impact on the whole ecosystem.

**The interconnectedness of the financial infrastructure exposes the global financial systems to systemic risk[[4]](#endnote-2).** A localized incident in one of the players, can impact entities interfaced to it, thus triggering a widespread disruption across the entire system. This might end up affecting the whole financial ecosystem and ultimately impact global financial stability.

IBM (2017)[[5]](#endnote-3) noted a surge in financial services sector cyber-attacks in 2017. The financial sector experienced 65 percent more attacks than the average client organization across all industries in 2016. This observation could be partly attributed to the fact that most of the new financial service providers and/or fintech startups may not have sufficient resources to invest in robust system security standards and data protection. As such these institutions might find themselves at risk and eventually become a source of vulnerability of the whole ecosystem.

**A cyber incident can have serious financial ramifications on credit providers.** Cyber incidents can result in consumers experiencing financial harm, loss of privacy and loss of trust in the financial system. Credit providers can also be affected by a cyber incident through decline in their enterprise value, loss of reputation, significant costs in breach remediation, regulatory and compliance costs, and higher insurance premiums[[6]](#endnote-4). A cyberattack on Equifax[[7]](#endnote-5) in 2017 impacted more than 143 million customers revealing their personal information and identification numbers and resulted in significant financial costs to the CRSP.

**As a result of some cyber incidents experienced over the past years, CRSPs and their regulatory authorities are under increased scrutiny[[8]](#footnote-3)**. Some regulators have been challenged on how they have handled cyberattacks, particularly, the lack of timely disclosure of breaches to the public.

**Against this background, there is** **renewed focus by members of the public and supervisory and regulatory authorities on cybersecurity of the credit reporting ecosystem.** Regulatory agencies, international financial institutions and standard setting bodies have developed various guidance on cybersecurity for financial institutions. For example, the US Financial Industry Regulatory Authority (FINRA) have developed basic checklists for alternative lenders, especially new financial players and third-party providers who support alternative lending approaches. The New York Department of Financial Services (DFS), also implemented cyber regulations for credit reporting agencies in June 2018. The regulations require CRSPs to register with the DFS, comply with the state’s strict cyber security standard, including a requirement to appoint a Chief Information Security Officer and to report known cyber breaches within 72 hours[[9]](#endnote-6).

**The International Committee on Credit Reporting (ICCR) through the General Principles on Credit Reporting (GPCR) provides high level guidelines on security, data protection and risk management.** In terms of the GPCR[[10]](#endnote-7), participants in a credit reporting ecosystem should undertake best efforts to implement commercially reasonable data security safeguards to protect data against cyber and other potential threats.

**The objective of this guideline is to provide detailed guidance on cybersecurity for credit reporting service providers.** The guideline is produced as an input to the FIGI guidance on cybersecurity for the financial infrastructure and will build on existing work by the FSB, the IMF, ENISA, the CPMI, IOSCO, G7 and others in the financial sector. In addition, the Committee will leverage on earlier work of the GPCR on cybersecurity and the findings of the global credit reporting survey that was conducted on cyber and data security.

# **THE EVOLVING CREDIT REPORTING CYBER LANDSCAPE**

# **Evolution of the credit reporting cyber ecosystem**

The credit reporting cyber ecosystem[[11]](#footnote-4) is undergoing a significant change as a result of the evolving credit reporting ecosystem, typified by the entrance of new players, emergence of new data providers, availability of new technologies and proliferation of new data sets.

* + 1. ***Emergence of new data providers/ sources***

The credit reporting industry has witnessed the expansion of the types of data providers from the traditional financial institutions to now include other entities such as non-bank financial institutions, municipal authorities, telecommunication firms, payment firms and governments. The sector has also seen the emergence of alternative lenders who are providing data and/ or subscribing to credit reporting systems. The proliferation of big data has also resulted in the emergence of new data providers and sources including social media networks. The changes in the number and nature of data providers and subscribers brings new sources of cyber risks.

* + 1. ***Emergence of new data subscribers***

The emergence of new types of data subscribers is also increasing the complexity of information sharing. The Facebook-Cambridge Analytica incident is an example of how CRSPs must take extra precaution as to what data users will do with the data that they get, even under contractual agreements. More importantly, the incident highlights the importance of trust within the ecosystem. In the Cambridge Analytica case, Facebook was punished for the commissions and omissions of its customer. Facebook suffered reputational risk, regulatory scrutiny and an estimated loss of up to $134 billion in its stock market valuation[[12]](#endnote-8).

* + 1. ***Proliferation of new data sets***

Credit reporting has traditionally been based on the use of credit data focusing on specific subsets of available structured data such as actual loan repayment behavior linked to certain demographic and official data, such as address, date of birth and government identity number. In some jurisdictions the nature of credit data has expanded to include other non-conventional credit such as post-paid utilities and court records. Some of these new data sets, particularly alternative data sets, are sourced in ways that may make credit reporting systems more susceptible to cyber risks.

* + 1. ***Entrance of new players***

The industry has also experienced the emergence of new CRSPs in the form of alternative credit scoring providers, who are competing or complimenting the traditional players. The new players also bring new sets of innovative products and services leveraging on advances in information technology which is providing increased computing, data mining and analytic capabilities. These capabilities are also enabling CRSPs to leverage non-traditional data. While these players are promoting access to credit for marginalized groups, some of these players are also a possible source of vulnerability to the industry.

# **Evolving cyber incidents in credit reporting industry**

The cyber incidents that can affect CRSPs continue to evolve with increasing sophistication of cyber actors. The CRO Forum as cited in OECD (2017) identified four main broad categories:

1. data breaches;
2. system malfunction;
3. data integrity/availability; and
4. malicious activity.

The diagram below lists the different types of incidents

****

**Figure 1: Common type of cyber incidents that affect Credit Reporting Services Providers**

Several CRSPs have been subject to some of the incidents shown above. Some examples of recent cyber incidents/ attacks are given in the box below:

**Box 1: Recent cyber incidents/attacks of Credit Reporting Service Providers**

**Equifax Data Breach**

Criminals exploited a U.S. website application development vulnerability to gain access to certain files. Based on the company’s investigation, the unauthorized access occurred from mid-May through July 2017. The breach exposed records containing Social Security Numbers, birth dates, addresses, and in some cases driver's license numbers of more than 143 million consumers.

**Experian Breaches**

***Experian US***

In March 2012, Experian purchased the assets of Court Ventures, a company that focuses on collecting court records that contain limited personally identifiable information (PII). As a side to its primary business, Court Ventures, at the time of acquisition, had a contract with US Info Search. That contract allowed customers of Court Ventures to access US Info Search’s data to find the address of a person in order to determine which court records to review.

After Experian’s acquisition of Court Ventures, the U.S. Secret Service notified Experian that Court Ventures had been and was continuing to resell data from a U.S. Info Search database to a third party, possibly engaged in illegal activity. The suspect in this case posed as a legitimate business owner and obtained access to U.S. Info Search data through Court Ventures prior to the time Experian acquired the company.

Following notice by the U.S. Secret Service, Experian discontinued reselling U.S. Info Search data and worked closely and in full cooperation with law enforcement to bring Vietnamese national Hieu Minh Ngo, the perpetrator, to justice. Ngo pleaded guilty to his crimes and was sentenced. This breach did not compromise Experian’s credit database.

***Experian US***

One of Experian’s business units, not its consumer credit bureau, experienced an unauthorized acquisition of information from a server that contained data on behalf of one of its clients, T-Mobile, USA, Inc. The data included some personally identifiable information for approximately 15 million consumers in the US, including those who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015, based on Experian's investigation. This incident did not impact Experian's consumer credit database.

Upon discovery of the incident, Experian took immediate action, including securing the server, initiating a comprehensive investigation, and notifying U.S. and international law enforcement. The data acquired included names, dates of birth, addresses, and Social Security numbers and/or an alternative form of ID like a drivers' license number, as well as additional information used in T-Mobile's own credit assessment. No payment card or banking information was acquired.

Experian notified consumers that may be affected, and safeguarded their identity and personal information by offering two years of credit monitoring and identity resolution services.

**Korea Credit Bureau (KCB)**

A consultant of Korea Credit Bureau (KCB) stole credit card data over the course of several years to January 2014. The employee stole data by copying the data to an external hard drive. The data was then resoldcredit traders and telemarketing companies.

# **Potential sources of risks**

As the credit reporting industry grows, cybercrime actors are developing new infiltration techniques to target the credit reporting ecosystem. These techniques include targeting the CRSPs directly and/or the other participants of the credit reporting ecosystem. Some of the potential sources of vulnerabilities are discussed below.

* + 1. ***Innovative technologies***

There are several new technologies that have emerged that enable better identification, transacting, networking, sharing and hosting of data, all of which have implications for the credit reporting industry. Some of the key technologies include distributed ledger technologies, biometrics, advanced computing, artificial intelligence and machine learning[[13]](#endnote-9).

Notwithstanding their benefits, these technologies can possibly expose the credit reporting system to new sources of cyber risks. The adoption of technology and its widespread usage within the credit reporting ecosystem increases the potential entry points and targets through which the CRSPs can be attacked.

|  |
| --- |
| **Box 2: Innovative technologies are also susceptible to cyber attacks****Biometrics**Biometric technology has been hailed as a solution to enable the identification of data subjects. As a result, there has been an increase in the adoption of biometric systems for user identification and authentication particularly by financial institutions. Several major leaks of biometric data and instances of attempted usage of leaked biometric data have already occurred[[14]](#endnote-10).**Distributed Ledger Technology (DLT)**One of the major use cases of DLT is lockchain. While blockchain has been praised for its security, the recent experience of numerous cyber-attacks on crypto exchanges has highlighted the vulnerability of the technology. More than 10 online exchanges have been subject of cyber fraud amounting to an aggregated figure of at least USD 1.45 billion since 2013 (IMF, 2018). **Cloud Computing**Most CRSPs have embraced various cloud computing services models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software-as-a-Service (SaaS). As a result, data, services and applications are being moved to the cloud. In instances of migration to public cloud, the CRSPs may outsource the security function of certain infrastructure to third parties, some of which are small and are not regulated. An attack on the service provider can impact the CRSPs. Equifax breach happened through a web application that the company outsourced.[[15]](#endnote-11)**Mobile applications**Some credit bureaus have developed consumer-driven data sharing platforms driven primarily by the need to provide portability of credit data. These innovations, while customer centric, can be another source of risk for the specific CRSPs and the whole ecosystem as they expand the surface of attack. |

* + 1. ***Interconnectedness***

Credit reporting systems are a crucial part of the financial infrastructure and are in many cases highly interconnected to networks and institutions within the financial markets. The participants in the credit ecosystem are increasing due to the emergence of new entities such as FinTechs start-ups, some of which could be seen as relatively high risk due to their small cyber security budgets and limited visibility of their cybersecurity practices. Data transfer protocols, including web applications and Application Program Interfaces (APIs), between entities in the infrastructure can also be a source of risks. The interconnectedness of the financial institutions and credit ecosystem infrastructure represent a Single Point of Failure (SPF) through which an attack can be propagated. The high degree of interconnectedness across firms can lead to rapid contagion effects. A disruption at one of the institutions might have implications on the whole financial market infrastructure or a large number of large financial institutions[[16]](#endnote-12).

* + 1. ***Outsourcing*, Third Parties and Fourth Parties**

CRPSs are increasing outsourcing some of their services to third parties. The outsourced services include infrastructure, software and platforms. This practice is resulting in a growing reliance on third parties or even fourth parties for the management of outsourced services and ultimately the security of such services. The outsourced services can be nodes through which a credit reporting system can be attacked. Equifax breach happened through a bug on an unpatched outsourced enterprise system[[17]](#endnote-13).

While CRSPs have increased their scrutiny and monitoring on third parties, less attention has been devoted to fourth parties. Fourth parties are companies that are connected to the CRSP through another party, usually a third party. These include such entities as sub-contractors. An attack/ incident at the fourth party can affect a third party which might have access to the CRSP’s database or system.

* + 1. ***Global* *operations***

Most CRSPs have global operations which are run from a central point. While centralization of similar functions improves efficiencies and reduces costs, this can also be a single point of entry to propagate an attack across the network. In addition, centralization might expose the network as system upgrades might not be implemented on time due to the capital outlay required. CRSPs with global operations must also be wary of the cyber threats prevalent in the regions that they operate in.

* + 1. ***Internal threats***

Cyber criminals are employing advanced social engineering techniques, targeting key staff of CRSPs to get access into the company network and in turn access data. Staff are being targeted using readily available data (for example executives email addresses) and non-confidential data. Rogue staff are also a source of vulnerability as they can steal data belonging to data subjects or can hold CRSPs at ransom. This is especially typical with contractors or ex-staff.

* + 1. ***Business* *Operations***

Connectivity to the internet dramatically improves operational tasks, but the increased connectivity can also lead to new security vulnerabilities. Poorly secured internet connections can heighten the risk of attacks.

* + 1. **Advanced threat actors**

The credit reporting industry is not immune to attacks by threat actors. Both nation state and e-Crime adversaries have increased their capabilities as they seek both geopolitical influence and financial gain. Average threats and break-out time for 2018 was estimated at 240 billion per day and 4hours 37 minutes, respectively. E-Crime adversaries tracked by CrowdStrike Intelligence in 2018 were found to have conducted banking trojans, ransomware and point of sale compromises, all of which increase cyber risk for CRSPs.[[18]](#endnote-14)

* 1. **Potential impact of Cyber incidents**

Cyber incidents can have serious ramifications on CRSPs, consumers and other parties including credit providers. The implications can be reputational, financial and economic. These are discussed below.

* + 1. **Implications on customers**

**Cyber incidents can result in consumers experiencing financial harm, loss of privacy and loss of trust in the financial system.** Consumer data can be exposed to risk of theft, alteration or destruction, accidental disclosure and/or loss of data, among others. The Equifax breach[[19]](#endnote-15) in 2017 impacted more than 143 million customers revealing their personal information and identification numbers thus exposing them to the risk of identity fraud.

* + 1. **Economic Cost**

**Incidents can also have serious ramifications on the availability of credit and ultimately economic growth.** Data breaches can result in fraudulent loans and credit cards opened which can causes organizations to incur increased losses. This can lead to lenders adopting a more cautious approach to lending and in instances where lenders proceed to lend in the face of breaches, they expose themselves to increased losses and reputational risk.

* + 1. **Financial Cost**

**The financial cost of a breach includes a decline in enterprise value, breach remediation costs, regulatory and compliance costs, fines and penalties, and higher insurance premiums.** Following the disclosure of the data breach in September 2017, Equifax incurred costs of $175 million (including professional and customer support) and is forecasted to have litigation of between $56 and $110 million[[20]](#endnote-16). In other instances, companies such as shipping company Maersk for instance, had to reinstall 4,000 new servers, 45,000 new PCs, and 2,500 applications because of the NotPetya infection at a cost of approximately $300 million dollar. And the UK’s National Health Service has estimated the total damages of the WannaCry infection to be around 92 million British Pounds[[21]](#endnote-17).

**Several jurisdictions have laws and regulations that impose fines and penalties as a result of a data confidentiality breach involving personally identifiable information**. The magnitude of these fines varies by jurisdiction and sector but are usually either a fixed amount or a percentage of turnover. In Europe, the GDPR, for example, imposes fines of up to EUR 20 million or 4% of worldwide annual turnover (whichever is greater).

**Another significant cost associated with a breach is the cost of public relations and communications.** Post breach, a CRSP can incur notification costs associated with advising the authorities and in certain instances the data subjects. In addition, massive budgets can be spent in media campaigns during the crisis and after the crisis. Significant public relations costs can also include the implementation of credit/ identity theft monitoring mechanisms. Another significant cost is the forensic investigation of the breach[[22]](#endnote-18).

* + 1. **Reputational costs**

Breaches may also cause a loss of reputation for CRSPs, in turn affecting their profitability and market value. In the five trading days following the disclosure, Equifax lost $3.5 billion in market value (Reuters, 2017) and its third quarter profits decreased by 27%. The stock price remained 30% down at the end of September (Petterson, 2017). In addition, reputational loss can result in loss of customers and business relations, though this has seldom been seen as most companies embark on a dedicated public relations drive to ensure this doesn’t happen.[[23]](#endnote-19)

# **GLOBAL CREDIT REPORTING CYBER SECURITY LANDSCAPE**

# **Introduction**

This chapter presents the findings of the Credit Reporting Cybersecurity Survey undertaken in February 2019. The survey sought to understand the cybersecurity practices of credit reporting institutions using a questionnaire with **74 questions covering 12 assessment factors**. The assessment factors included the cybersecurity environment, legal and regulatory environment, governance and strategy, outsourcing, information sharing, training and awareness, resources, risk management & compliance, audit, incidence response, data loss prevention and preventative controls. A copy of the survey is included in section 7 of these guidelines.

In total 43 respondents completed the survey. A total of 8 responses were excluded on account of incomplete responses and duplications. As a result, **35 responses** were analyzed.

# **Demographics of Respondents**

The survey respondents were drawn from both public and private sector credit reporting services providers. Figure 3 below provides a breakdown of respondents by organization type and region.

***Figure 3: Distribution of Respondents***

# **Survey Findings**

# **Local cyber environment**

**The increasing interconnectedness of the financial system requires that CRSPs pay particular attention to the broader cyber environment.** The survey revealed data providers and prominent institutions in jurisdictions had been subjected to more attacks (43% and 26% respectively) than CRSPs (23%) during the past two years. The survey findings reveal increasing susceptibility arising from parties other than the CRPSs themselves.

***Figure 4: Cyberattacks/ incidents by institution category***

**The survey revealed that the most common incident amongst the CRSPs that responded to the survey was denial of services.** Data breaches were most noticeable among data providers and other prominent institutions. All three types of organizations experienced ransomware and unauthorized network penetration.

**Indicative of the distribution of respondents, data breaches were more prevalent in Europe and Africa as shown in Figure 5**. Europe recorded the highest level of denial of services and unauthorized network penetration incidents. Conversely, the Americas experienced other cyber incidents in the form of for example compromised banking systems.. Asia had the least number of cyber incidents.

***Figure 5: Cyber incidents across regions***

# **Legal and regulatory environment**

**The majority of the jurisdictions (83%) in which the respondents operate have enacted legislation or regulations to deal with cybersecurity and information security.** Most countries have enacted legislation on cybersecurity that sets acceptable standards, establishes financial and socio-legal sanctions, safeguards individual and national interest, mitigates against risk and facilitates cooperation between countries. African countries were lower in terms of legislation compared to other regions. The Central Bank emerged as the regulatory authority for most of the respondents. The other major regulator was the equivalent of the supervisory authorities (such as GDPR supervisory authority). Figure 6 below provides more detail on the legal and regulatory environment

**Figure 6: Legal and regulatory frameworks**

**Cyber security regulations place responsibility on CRSPs by requiring them to notify affected parties on cyber security issues, report cyber security issues to regulators or supervisory authorities and compensate affected parties.** All the legal and regulatory frameworks require the regulated entities to report cyber security incidents to regulatory authorities. Of these frameworks, only one does not place an obligation on the CRSPs to notify the affected parties. Most of the laws (80%) provides for both financial and non-financial penalties. Non-financial penalties include civil and criminal penalties. Notwithstanding the penalty requirement, more than 21% of these laws do not however provide for compensation of data subjects affected by cyber incidents.

# **Board, management cyber and information security strategy**

**Credit reporting service providers have broadly embedded cyber and information security in their governance processes.** All but one of the surveyed CRPSs have developed cyber security strategies, and policies and procedure manuals to enhance their security and resilience levels in view of evolving threats. It was however noted that some (11%) of the strategies are not board approved and 20% are not reviewed by the board on a regular basis. Failure by boards to ensure regular reviews of cyber security strategies can expose the institutions. Although most (54%) of strategies contain a provision for cyber insurance, less than half (45%) include a provision on outsourcing.

**Boards are working on improving their cyber security knowledge.** The majority (77%) of the respondents’ boards have at least one director with cyber security knowledge and experience. 48% of the respondents stated their board has an understanding of cyber security controls which is reflected in the fact that 75% of the boards retain the services of cyber experts to enhance their understanding of cyber security.

**Figure 7: Board and Senior Management**

**A growing number of CRPS’ have created a function of Chief Information Security Officer (CISO) or its equivalent who is responsible for cyber and information security.** The emergence of a CISO is founded on the need to separate ICT security from ICT risk taking functions.The survey revealed that the most senior officer responsible for cyber security were Chief Information Officers (49%) and Chief Information Security Officer (40%). The rest of respondents had cyber security functions reporting to legal, risk or the CEO or its equivalent. The survey revealed that 51% of senior cyber security officers were independent from areas using or administering the institution’s information technology assets.

**Cyber insurance is gaining prominence as one of the risk management options.** Of the respondents, 51% are insured for cyber security events. This finding is consistent with the earlier finding that revealed that 54% of the respondents had embedded cyber security insurance as part of their strategy.

# **Outsourcing critical IT services**

**In view of the evolving technological innovations and the need to enhance efficiency, some CRSPs (37%) are outsourcing critical IT services such as security operations centre, data centres and applications.** Data centers are commonly outsourced in Africa and Europe, while in the Americas CRSPs mostly outsource services including web and professional services. The prevalence of outsourcing data centers can be seen as reflective of the benefits associated with this type of activity such as guaranteed uptime, higher scalability, better flexibility and speed, improved latency and connectivity and improved business focus. Notwithstanding the benefits of outsourcing, this can be a source of risks for CRSPs in instances where the contractors do not comply with cybersecurity, information security and data privacy standards.

**More organizations (54%) are increasingly considering outsourcing critical services.** Although only 37% of the respondents were outsourcing critical IT services, the survey revealed that more than half of the respondents had implemented cybersecurity policies that provide guidance on relationships with third parties.

# **Information sharing cyber incidents**

**Sharing of cyber incidents is gaining momentum.** The survey revealed that while overall 66% of the CRSPs boards of directors encourage their cyber teams to engage in information sharing arrangements with other institutions, the practice was less matured in Europe and Africa. The exchange of information can help CRSPs to identify and adapt more quickly to evolving attacks.

**Third parties are also significantly contributing to information sharing.** Of the surveyed CRSPs, 77% receives timely notifications of cyber security incidents from service providers with whom they have material outsourcing arrangements. This is particularly important in the context of increasing levels of outsourcing and the potential for outsourced services to become a source of vulnerability.

**A majority (63%) of respondents are participating in industry programs designed to promote information sharing**. The survey revealed that most of the CRSPs also monitor the cyber security incidents within and outside of the financial services industry and participate in industry programs. This can help the CRSPs achieve an understanding of all the potential vulnerabilities given the increased levels of interconnectedness. Ultimately such practices can improve the level of resilience of the financial industry and nations.

# **Training and awareness**

**Training and awareness are an important step in creating a cyber security culture within a CRSP.** As much as 85% of CRSPs have implemented ongoing training and awareness programs. The training programs which include incidence responses and new trends target managers, employees with privileged access permissions and board members. The survey, however revealed that training for board members is lagging the training of other staff with only 25 CRSPs having trained their board members within the last 12 months. In terms of regional activity, Africa is lowest in terms of implementing cyber awareness programs.

***Figure 9: Training and Awareness***

# **Resources**

**CRSPs are increasingly committing specific resources to improve their cybersecurity capabilities.** Four-fifths of respondents recognize the importance of cyber security and have put in place specific cyber security budgets. Allocating resources for cyber security allows the institutions to invest in hardware, software and human capital. A majority (88%) of respondents noted that their cyber budgets were commensurate with the risk levels.

# **Risk management and compliance**

**CRSPs have embedded risk management into cyber security.** Most (94%) of the CRSPs have a formal risk management framework that includes cyber risk as one of the risk areas. Embedding risk management in cyber security processes enables security to be an organization-wide responsibility. The risk management frameworks were considered commensurate to the level of cyber risk.

***Figure 10: Risk Management and Compliance***

**All CRSPs comply with data protection and privacy regulations.** Consistent with the increasing regulatory environment on data protection and privacy across jurisdictions, CRSPs are putting in place mechanisms to ensure compliance.

# **Audit**

**CRSPs are recognizing the importance of internal audit as a central pillar in cybersecurity.** More than three-quarters (77%) of the respondents have enhanced their internal audit functions with resources and expertise to enable them to conduct cyber security assessments.

**The audit (internal and external) functions are validating cyber security controls and processes.** Most of the respondents have ensured that their audit function assesses the effectiveness of cyber security controls, incidence response and threat information. The survey however, revealed that 49% of the CRSPs’ audit functions did not validate the effectiveness of third-party relationship management reflecting an inherent risk area in view of the increased outsourcing of critical ICT services.

# **Incident Response**

**Awareness of the importance of a cybersecurity incident response plan is growing across CRSPs.** More than 90% of the CRSPS have documented incident response plans. Notable gaps were however noted with respect to partnering with their national Computer Emergency Response Team (CERT), external communications and simulation exercises. Only 51% of the respondents have a partnership relationship with their national CERT potentially depriving the CRSPs of access to advice and support that come with such platforms. 35% of the CRSPs do not perform simulation exercises to assess the effectiveness of their incident response plans. Simulation exercises play an important role of assisting CRSPs identify potential gaps and areas of enhancement.

**Figure 11: Incident Response**

# **Data loss prevention (DLP)**

**In view of the importance of data and the emerging laws on data protection and privacy, most CRSPs have stringent**[**data protection**](https://searchdatabackup.techtarget.com/definition/data-protection)**or**[**access**](https://whatis.techtarget.com/definition/access)**components programs.** 80% of the CRSPs had implemented programs to monitor and prevent breaches, and some rules to control printing of sensitive information. This finding is consistent with an earlier finding which revealed that less than 5% of CRSPs had been subject to a data breach. The survey revealed that 40% of the CRSPs have not implemented user verification mechanisms before emails are sent.

**Figure 12: Data Loss Prevention**

# **Preventative controls**

**CRSPs are successfully implementing controls against cyber security risks.** All respondents have implemented physical controls, user rights and conducted an inventory of IT assets. CRSPs have not matured in terms of implementing detective controls, as reflected by 43% of entities which do not have automated processes to detect and block unauthorized changes to software and hardware. As a result, these CRSPs are susceptible to system attacks as there is no mechanism to provide adequate warnings.

**Figure 12: Preventative Controls**

# **CYBERSECURITY GUIDELINES**

# **Existing Credit Reporting Guidelines on Cybersecurity**

**The ICCR, in the General Principles for Credit Reporting, published in 2011 provided high level guidance on cybersecurity**.General Principles 2 and 3, and Recommendation E outline the need for rigorous standards of security to ensure that data is protected.

**Box 3: Credit Reporting Guidance on Cybersecurity**

**General Principle 2: Data Processing – Security and Efficiency**

Credit reporting systems should have rigorous standards of security and reliability, and be efficient…….All participants in a credit reporting ecosystem should undertake best efforts to implement commercially reasonable data security safeguards to protect data against these and other potential threats…. Credit reporting service providers should protect data against any loss, corruption, destruction, misuse or undue access.

**General Principle 3: Governance and Risk Management**

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 fair access to the information by users.

**Recommendation E**

Central Banks, Financial supervisors, and other relevant authorities, both domestic and international should cooperate with each other, as appropriate in promoting the safety and efficiency on credit reporting systems.

Against the background of growing importance of credit reporting systems as crucial part of the financial infrastructure and the changing credit ecosystem, it is important to provide more detailed guidance as outlined below. This guidance builds on the survey findings described in section 3.

# **Detailed Cybersecurity Guidance**

Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and satisfy a set of defined security requirements.[[24]](#footnote-5)

The diagram below depicts the key areas of focus for cybersecurity:



**Figure 2: Cybersecurity Focus Areas**

The principle of proportionality should be taken into consideration when applying these guidelines. Proportionality responds to three main characteristics: adequacy, necessity, and non-excessiveness. Hence, when applying these guidelines, organizations should take into consideration security requirements according to their business nature, scale and complexity, and adhere to regulatory standards applicable to their jurisdiction. A risk-based approach should be followed to ensure that security controls are commensurate with the risk to critical infrastructure and organizational objectives. The focus areas are discussed in the following sections.

# **Cybersecurity and Data Privacy strategy**

**A cybersecurity and data privacy strategy are a key element for transforming the cybersecurity function into a business enabler, allowing the organization to take a proactive approach to managing cyber and data privacy risks**. The strategy should aim to provide cohesion and strategic direction to the organization’s cyber security and data privacy activities, organizing them with a purpose under a comprehensive program, and facilitating its alignment with the organization’s strategic goals. For this reason, the strategy should be tailored to the culture and complexity of the organization’s environment, taking into consideration the regulatory framework, the organization’s risk appetite and the relevant cyber security and data privacy exposures.

**The cyber security and data privacy strategy must focus on delivering strategic value to the organization**. Hence, it should be aligned with the business strategy to deliver strategic value by achieving increased stakeholder confidence, minimizing business impact in case of an incident, and improving market adoption. For example, if the organization intends to gain competitive advantage by leveraging technologies such as Cloud, Mobile or Big Data, the strategy should be geared toward managing risks associated with those technologies.

**Developing a cyber and data privacy strategy requires a significant amount of effort, but a multi-pronged approach can be followed to break it down into manageable phases.** The development of a cyber security and data privacy strategy can be seen initially as an overwhelming task, but it can be accomplished by breaking down the process into a few simpler steps as proposed in Box 4.

**Box 4: Steps to Develop a Strategy**

1. **Prioritize critical information assets**. Create an inventory of information assets (data, physical devices, information systems, software) that support the organization’s critical business processes. Identify the potential impact (financial, operations, reputation) to the organization if the integrity, confidentiality or availability of those assets get compromised, and assign a criticality rating to each asset. Prioritize the inventory of assets by criticality and focus on the most critical information assets.
2. **Understand the threats.** Identify the threat actors (e.g. state-sponsored entity, organized crime, hacktivist, malicious insider) that are relevant to your organization and rank them by capability and motivation to compromise the organization’s critical assets.
3. **Assess current state.** Conduct a candid assessment of current cyber capabilities and performance using an industry-recognized cyber framework (e.g. NIST Cyber Security Framework). Understand the weaknesses and shortcomings to meet the business and IT strategic goals.
4. **Define the future state.** Set the vision and long-terms goals for the cybersecurity function taking into consideration the organization’s strategic goals. These should be aspirational shifts that set the direction for the future of the cybersecurity function in the organization.
5. **Create an implementation plan.** Conduct a gap analysis between the current cyber capabilities and the desired future-state and identify initiatives that would help bridging the gap. Estimate the cost and level of effort for each initiative and determine the security benefit they will provide. Create a roadmap by arranging the list of initiatives in a multi-year timeline, giving high priority to those that provide high benefit with low cost or level of effort to implement.
6. **Implement and track progress**. Assign necessary resources to implement the roadmap. Track key performance indicators and frequently report progress to senior management.

**Appropriate resources must be allocated for the successful implementation of the strategy.** The cyber security and data privacy strategy should be explicitly approved by the Board of Directors or similar governing authority, and have adequate senior management involvement in the definition, implementation and periodic review of the strategy and implementation plan.

**Organizations also need to understand how they compare against peers and comparable organisations.** To support continuous improvement and adjust the strategy as needed**,** organizations in the credit-reporting industry should regularly conduct benchmark exercises to compare their cyber security and data privacy readiness against comparable industry organisations and peers. For this purpose, a leading cybersecurity assessment framework (e.g. NIST Cybersecurity Framework) could be leveraged.

**Innovation and cybersecurity have been traditionally seen at different ends of the business strategy, but there is an opportunity to change this through the cyber security and data privacy strategy.** Innovation is considered a driver for efficiency, growth and revenue generation, whereas cyber security can be seen as an obstacle for agility in service delivery. However, this is changing, and the Board of Directors and business executive teams understand that cyber security is no longer a compliance exercise. The ability to deliver secure services leveraging disruptive technology like Robotic Process Automation (RPA), Artificial Intelligence (AI) or Blockchain is a competitive differentiator that can help build long lasting customer relationships. Having a mature cyber security and data privacy program can instill confidence amongst stakeholders and pave the way for seamless adoption of disruptive technologies.

Please refer to the [*Strategy*](#Strategy) section in the References annex for specific security controls.

# **Governance**

**Implementation of the strategy must be monitored to ensure that the program delivers expected strategic value to the organization.** Therefore, a cyber security and data privacy governance framework should be established to define roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the strategy. Policies, standards, and guidelines should be documented, approved, published, regularly reviewed and communicated to all relevant stakeholders. These documents should set the direction in line with business strategic goals and demonstrate support for cyber security and data privacy across the organization. Dependencies and critical functions for the delivery of critical services should be identified, along with the resilience requirements to support the delivery of those services.

**The roles and responsibilities of individuals carrying the cyber security and data privacy program must be formalized.** Mature organizations usually have a qualified individual appointed as Chief Information Security Officer (CISO), who is responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policies. Appropriate lines of reporting should be established for the CISO to communicate to the Board of Directors or equivalent authority, the effectiveness of the cybersecurity program and, material cybersecurity risks and events. The same should apply to the role of Data Protection Officer (DPO) recognizing the importance of data privacy.

**Sponsorship from the Board of Directors is crucial to sustain the execution of the cyber security and data privacy program outlined in the strategy.** Accordingly, the Board of Directors or similar governing authority should ensure that adequate resources are allocated, appropriate authority is assigned, and access to the Board of Directors or similar governing authority is established. The Board of Directors should also take a proactive role and frequently asked questions to the CISO/DPO to understand the current state of cyber security and data privacy in the organization, what the top risks are that may be affecting the organization and how they are being addressed. Some examples of these questions are included in Box 5 below.

**Box 5: Questions that the Board Should be Asking**

1. What are the top cyber and data privacy risks that our organization faces?
2. What are the measures by which we mitigate these risks?
3. What is the recommended method for the Board to measure and monitor these risks?
4. Have we seen threats directed against our organization from capable adversaries, and how were those threats detected?
5. How will we respond to a cyber incident that could negatively affect our customers, our operations or our reputation?
6. Has our program been audited, and how are we doing in such audits?
7. What technical solutions and risk reduction measures should be implemented in the next 3 years?
8. How do we compare with our competitors in the industry?
9. Do we have the right cybersecurity and data privacy teams with the required skills?
10. How do we keep our employees and customers prepared to play their role in cybersecurity?

Please refer to the [*Governance*](#Governance) section in the References annex for specific security controls.

# **Risk Management**

**Implementation of the cyber security strategy and execution of the program will inevitably uncover risks that need to be appropriately managed.** Cyber security should be considered a dimension of the overall IT risk management, which in turn should be integrated with the organization’s enterprise risk management. Cyber security risks (including third-party and external dependencies risks) should be managed in a manner that is consistent with the organization’s mission and business objectives outlined in the strategy to enable cyber security activities prioritization and resource allocation.

**A cyber security risk management framework provides guidance for the consistent identification, assessment, and response to cyber risks.** The framework should include the risk taxonomy used to reduce risks identified from different sources and activities like internal audits, incident reports, new technology risk assessments, etc. Similarly, the framework should provide guidance on how to assess risks in a consistent manner by defining likelihood and impact scales and thresholds. The framework should also provide guidance on risk treatments (avoid, mitigate, transfer or accept) including a decision framework that outlines what level of authority can accept risks depending on different residual risk thresholds.

**The cyber security risk management framework also describes the strategy to monitor and communicate risks.** As risks are dynamic, a reporting and monitoring mechanism should be established to allow cyber security risks to be timely communicated to the Board of Directors or similar governing authority. This in turn allows the Board of Directors to monitor the effectiveness of the organization’s mitigation plan and assess whether it is consistent with the approved risk appetite and tolerance thresholds. A risk register that includes the identified risks and associated attributes should be maintained to facilitate this process. The register may include attributes like risk identification number, description, category (from the taxonomy), owner, residual likelihood and impact, risk triggers, mitigation and contingency plan, etc.

**Leading organizations frequently conduct risk and control self-assessments to assess the effectiveness of the cyber security risk management and identify corrective actions.** For these assessments to be successful, key process owners and stakeholders should participate in these exercises to identify risk and assess risks identified against key business objectives. Controls should then be identified for each of those risks and the effectiveness of the controls assessed to determine whether the controls are working as intended. Control weaknesses or gaps should be documented along with proposed corrective actions. Finally, a high-level summary of the results of the risk and control self-assessment should be sent to the Board of Directors or similar governing authority.

Please refer to the [*Risk Management*](#Risk) section in the References annex for specific security controls.

# **Compliance**

**Compliance risk is still a top concern for Board of Directors**. On the one hand, non-compliance penalties can be very high as the scope of regulatory focus continues to increase. On the other, the traditional bottom-up compliance approach that focuses on the repetitive testing of controls contributes very little to reducing the residual operational risk of the organization. For this reason, organizations should review their security compliance program to find opportunities for better alignment with the overall risk management framework and focus on residual risks that matter to the enterprise.

**Compliance does not equal security, but there are synergies that should be maximized.** The design, operation, use and management of information systems in the credit reporting industry are subject to legal, regulatory, and contractual security requirements. Accordingly, organizations should have a compliance program in place to avoid breaches of any applicable law, regulations, contractual obligations or requirements established in the security policies. To the extent possible, compliance and cyber security efforts should be aligned to minimize duplicative efforts (e.g. control testing, risk assessments, risk reporting) and facilitate a risk-based allocation of resources to address risks relevant to the organization.

**Compliance with data privacy regulations is a key requirement for organizations in the credit reporting industry.** CRSPs manage customers’ personal data by nature of the business. Accordingly, they should ensure compliance with data privacy requirements in alignment with relevant legislation, regulations, and contractual agreements. To achieve compliance, organizations should obtain a comprehensive understanding of the data collected and the security controls implemented to meet those privacy requirements. The *Data Privacy* section below provides more guidance on privacy requirements and best practices.

Please refer to the [*Compliance*](#Compliance) section in the References annex for specific security controls.

# **Data Privacy**

**Recent high-profile data breaches and new privacy regulations around the world emphasize the importance of data privacy.** Organizations in the credit reporting industry have recently observed high-profile data breaches that led to the compromise of the privacy of personal information held about individuals. Even though the direct costs associated with these incidents are already high, most of the time it only accounts for the known costs (e.g. technical investigation and cyber improvements, customer breach notification and post-breach protection) but fails to take into consideration other less visible costs (e.g. reputational damage and loss of customer confidence, increase cost to raise capital, increases in insurance premium and , disruption of operations). Privacy regulations in Europe and Asia are further tightening the compliance requirements and will very likely be followed by similar strict requirements in other geographical regions, making it even more clear to organizations processing personal data that protecting the privacy of their personnel and customers’ data is a business requirement.

**A data privacy policy is the first step towards addressing the increased pressure on protecting the privacy of personal data.** A data privacy policy should be documented, approved, published, regularly reviewed and communicated to all relevant stakeholders, setting direction in line with business objectives and demonstrating support for data privacy across the organization. The policy should define what is personal data, provides guidance on security controls for protecting the privacy of personal data, and establishes roles and responsibilities for protecting the privacy of personal data (e.g. data owner, data custodian). The policy must consider legal, regulatory and contractual data privacy requirements. Organisations should consider the appointment of a Data Protection Officer (DPO) to provide guidance to internal and external users and service providers on their data protection responsibilities and established procedures related to data privacy protection.

**The effectiveness of data privacy protection efforts hinges on the organization’s comprehensive understanding of the type of personal data collected or processed**. In addition to completing a data inventory on a regular basis, organizations should consider conducting a data flow mapping exercise to be able to trace the movement of personal data from its source to its point of use, providing visibility into all the ways it has changed throughout the data lifecycle. This would also help organizations to effectively identify and manage risks associated with personal data shared with third parties.

**The risks arising from activities conducted by third parties require ongoing oversight.** The Board of Directors is ultimately responsible for managing activities conducted through third-party relationships to the same extent as if the activity were handled within the organization.Before entrusting customer or staff personal data to a third-party, the CRSP should make appropriate contractual arrangements and obtain verified proof (e.g. attestation from independent auditor) that the third-party has implemented appropriate technical and organizational controls that meet applicable legal requirements to protect the personal data. Compliance with those requirements should be monitored on an ongoing basis.

**Organizations should implement both, technical and process controls to ensure confidentiality and integrity of personal data.** Organizations must deploy technical controls such as data masking, encryption, strong authentication, data loss prevention and logging to ensure access to personal data is restricted to business objectives. Similarly, process controls like periodic impact assessments, incident response and breach notification readiness can help reduce potential exposure to this risk.

**An established breach notification process is not only a key requirement in most privacy regulations but is also seen as best practice for organizations taking data privacy seriously**. The data breach notification process should describe the criteria, format, timeline requirements and procedures for notifying appropriate supervisory authorities and data subjects of a data breach in a timely manner. The data breach communication should describe the nature of the incident, what data was involved, and recommendations to mitigate potential adverse effects.

**Beyond compliance, consideration should be given to leading data privacy principles, standards and frameworks.** There are multiple relevant data privacy frameworks (e.g. APEC[[25]](#footnote-6) Privacy Framework, OECD[[26]](#footnote-7) Guidelines) and jurisdiction-specific data privacy regulations (e.g. the European Union GDPR). There is some variation in the definitions, issues and principles used in the frameworks. However, there are some important concepts that are similar across the frameworks and regulations and should be considered by all organizations trying to improve their data privacy efforts. Box 6 provides some examples of those key concepts.

**Box 6 - Some Key Privacy Considerations**

1. **Choice and Consent**: Organizations should provide information to data subject of the available choices for accessing, updating and restricting access to their personal data. Explicit consent should be obtained from the data subject before using their data for specific purposes.
2. **Purpose and Collection Limitation**: Organizations should specify at the time of collection the purpose for which the personal data is collected. These personal data should be obtained by lawful and fair means.
3. **Data Minimization**: Organizations should ensure that data collected on a subject are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Storage Limitation**: Organizations should not keep personal data for longer than necessary to support the purposes for which they were collected.
5. **Openness, Transparency and Notice**: Organizations should communicate to data subjects their rights, details about the personal data that are being collected and for what purpose. Organizations should answer questions in a manner that is clear and easy to understand.
6. **Privacy by Design and by Default**: Organizations should build appropriate safeguards into the full lifecycle of personal data processing and implement appropriate technical and organizational controls for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.
7. **Accuracy and Quality**: Organizations should ensure that the collected personal data are relevant, necessary, accurate, complete and up to date.
8. **Individual Participation**: Organizations should provide easy-to-use processes to allow data subjects to access their personal data and have the data erased, rectified, completed or amended, and to withdraw consent to use their personal data.
9. **Security Safeguards**: Organizations should establish technical and administrative security controls that address confidentiality, integrity and availability of data, and mitigate the risks of unauthorized or unlawful processing, loss, damage or destruction of personal data.
10. **Accountability**: Organizations should be accountable for the governance and risk management of personal data and for ensuring compliance with all applicable legal requirements.

Please refer to the [*Data Privacy*](#Privacy) section in the References annex for specific security controls.

# **Awareness and Education**

**Employee awareness is as important as the technology or processes in place at the organization to manage cyber security risks.** Cyber security attacks frequently target uninformed employees or contractors with a view to accessing an organization’s systems. For example, phishing email attacks are conducted by perpetrators pretending to be someone (e.g. one of the organization’s senior executives) or an internal operation (e.g. the Help Desk) with the intention of tricking the user to provide sensitive information such as usernames and passwords. Phishing e-mails may also be used by the perpetrator to deliver malware (e.g. ransomware) when the user opens an attachment or clicks on a link. Earlier on, phishing e-mails attacks were massively deployed through spams campaigns but now the phishing attacks are more targeted (e.g. “whaling” or phishing attacks targeting the organization’s executives). To counter these types of attacks, organizations should implement cyber security awareness and education programs to equip the workforce with the appropriate knowledge to conduct their duties in a secure way and prevent becoming victims of cyber security attacks that could lead to the compromise of the organization’s systems. Programs should periodically gauge the effectiveness of their awareness campaigns by conducting tests.

**People in an organization can often be considered the weakest link, but with appropriate understanding of their role in protecting the organization against cyber-attacks, they can also be the first line of defense.** Cyber security awareness and education initiatives should be undertaken to keep personnel informed on common cyber security attack patterns and how to protect the organization’s assets from existing and evolving cyber security threats. These awareness efforts should ensure that all personnel understand their roles and responsibilities with regards to protecting the organization’s information assets. For that purpose, the content of the awareness and education campaigns should be tailored to target different types of users, from IT administrators and developers, all Operation centers and administration staff to senior management and members of the Board of Directors.

**It is also imperative to provide timely and relevant cyber security awareness and education training to customers**. As financial institutions rely more and more on digital channels to communicate with the customers, it has become crucial to educate these customers against common attack patterns, so they can distinguish between a legitimate request from the institution and a dangerous attempt through a phishing e-mail to compromise their user credentials or other sensitive information. Organizations are using all available channels, from the corporate website, mobile applications to social media postings, to educate their customers on how to prevent identity theft, fraud and scams.

Please refer to the [*Awareness and Education*](#Awareness) section in the References annex for specific security controls.

# **Information Sharing and Communications**

**Information sharing helps improve awareness among CRSPs.** The interconnectedness of the financial infrastructure may expose the credit-reporting industry to systemic risk. A localized breach in one of the CRSPs could be propagated to others who are interfaced to it, triggering a widespread disruption across the entire credit ecosystem. Similarly, CRSPs may be unaware that a coordinated attack against several other CRSPs in the region is underway, hindering the ability to timely react and prevent the widespread disruption of services.

**Sharing threat intelligence and recent attack patterns would help strengthen cyber security and enhance resilience in the** **credit reporting industry.** Sharing tactical and technical information, such as threat intelligence and details on how vulnerabilities were exploited in recent cyber security attacks, allows organizations to learn about emerging attack patterns and improve its detecting and response capabilities. Collaboration among private and public entities and authorities allows for a deeper understanding of the vulnerabilities in the credit reporting ecosystem and how they could be potentially exploited by an attacker, leading to the disruption of operations. To enhance the cyber security resiliency of the credit-reporting industry, CRSPs and public authorities should identify and address impediments to information sharing.

Please refer to the [*Information Sharing and Communications*](#InfoSharing) section in the References annex for specific security controls.

# **Resilience**

**When it comes to responding to a cybersecurity incident, it is important to have a formalized incident response plan.** Reacting without a plan once the network has been infiltrated or data has been breached, will result in confusion and slower overall response times. Plans, procedures, and technologies should be established and maintained by organizations to analyze and respond to cybersecurity events and to sustain operations throughout a cyber security incident, commensurate with the risk to critical infrastructure and organizational objectives. The incident response plan should define criteria for categorizing and prioritizing incidents and provide guideline on the actions to be followed such as preparation, identification, containment, eradication, recovery and lessons learned.

**Establishing a dedicated Computer Security Incident Response Team (CSIRT) will boost the organization’s capabilities to timely respond to cyber security incidents.** Clear roles and responsibilities should be established for carrying out response activities enabling a rapid response in the case of cyber security events. Many leading organizations also rely on specialized Security Operation Centers (SOCs), internal or outsourced, as the first line of defense and focal point for coordination of efforts with local specialized teams such as a national Computer Emergency Response Team (CERT).

**Business continuity and disaster recovery plans are key elements of cyber security preparedness, with the focus on the necessary activities to recover in case of a cyber incident.** As modern organizations continue to rely on IT to conduct its business activities, the IT disaster recovery plan should be developed in conjunction with the business continuity plan. While the business continuity plan focuses on the procedures to allow restoration of business operations, the IT disaster recovery plan must detail the procedures to be executed to ensure timely restoration of systems and information assets. A business impact analysis should be frequently conducted to determine the information assets (including outsourced systems and services) that support critical business processes and establish and adjust the required recovery objectives. Restoration activities should be coordinated with relevant internal and external parties (e.g. Internet Service Providers, vendors, local CERTs).

**Incident response, business continuity and disaster recovery plans may become obsolete if they are not frequently tested and updated.** These plans should be frequently tested against a variety of realistic scenarios, involving relevant internal and external stakeholders. Scenarios like extended power outages or distributed denial-of-service (DDoS) attacks should be tested through tabletop and functional exercises to evaluate the effectiveness of the plans and the readiness of the personnel to respond to an incident. Lessons learned from tests and forensic analysis conducted on real events should be incorporated into the plans to improve the organization’s ability to effectively and timely respond to cyber events.

Please refer to the [*Resilienc*](#IRandBC)*e* section in the References annex for specific security controls.

# **Technology Operations**

The key components of the cybersecurity program described in this section are *Identity and Access Management, Asset Management, Change and Configuration Management, Secure Software Development* and *Third-Party Management.*

***Identity and Access Management***

**Access to critical information assets must be limited to only the necessary individuals at the necessary times based on business needs.** Effective *Identity and Access Management* is key to manage the risk of unauthorized access to organization’s information assets and to maintain the confidentiality and integrity of information assets. Processes, procedures and technologies should be established to appropriately manage the entire life cycle of digital identities and profiles for entities that may be granted logical or physical access to the organization’s information assets.

**Greater control of user access can help organizations reduce the risks of internal and external data breaches.** Access to an organization’s information assets should be managed, following the principles of least privilege and separation of duties. Access permissions should be duly authorized, assigned, monitored, periodically reconciled and timely revoked. Remote access to the organization’s network and information systems should be authorized and monitored, and only granted after appropriate configuration requirements are met. Such requirements for example may include the use of encrypted communication channels or multi-factor authentication.

**Special attention should be given to the allocation of privileged access rights.** This may require conducting a more thorough and frequent review of the need to have those access rights, and evaluation of the measures in place to manage risks associated with the concentration of privileged access on some individuals. Additionally, guidelines should be in place to determine when additional protection would be required for those privileged accounts, like the use of strong authentication.

Please refer to the [*Identity and Access Management*](#IAM) section in the References annex for specific security controls

***Asset Management***

**To manage cyber security risks effectively, organizations need to identify and prioritize the critical information assets that must be protected from the most relevant threat actors.** Without a comprehensive understanding of the information assets (data, physical devices, information systems, software) that enable the organization to achieve business purposes, it would not be possible to effectively prioritize activities and efficiently allocate resources to address cyber risks. Processes, procedures and technologies should be established for managing the organization’s information assets throughout all stages of their life cycle.

**An inventory of all internal and external information assets should be maintained**. The inventory should record important information such as a unique asset identifier, asset owner, data classification, software version, physical location, etc. Similarly, external assets like information systems operated by third parties or data entrusted to third parties for processing should be catalogued. Internal and external assets should be prioritized based on their classification, criticality, and business value.

Please refer to the [*Asset Management*](#Asset) section in the References annex for specific security controls.

***Change and Configuration Management***

**Changes should be appropriately managed to avoid the introduction of vulnerabilities into information systems that enable the organization to achieve business purposes.** The increase in complexity of information systems supporting business operations also increases the likelihood of accidental errors when changes are made to the configuration of related information assets. This may expose them to cyber security attacks that could compromise the confidentiality, availability and integrity of those assets. For example, cloud service providers offer powerful administration consoles to simplify the management of organization’s assets in the cloud. Recently, several cybersecurity events have been published where cloud repositories containing corporate sensitive information were accidentally made available to external users. *Change and Configuration Management* covers the continuous process of controlling and approving changes to information assets that enable the organization to achieve its business purposes.

**Information asset configuration should be managed throughout their entire life cycle.** Organizations following best practices usually establish and maintain processes, procedures and technologies for managing the information asset configuration throughout the entire life cycle. This includes the definition of an approved configuration baseline and the verification that assets are configured according to the baseline.

Please refer to the [*Change and Configuration Management*](#Change) section in the References annex for specific security controls.

**Software Security**

**Security vulnerabilities in enterprise applications could be exploited by attackers to access the organization’s infrastructure and compromise critical information assets.** A well-defined process for developing and acquiring software provides the foundation for the successful development, implementation, and operation of organizational information systems. Information security activities should be built-in to the process to ensure that security requirements are identified in early phases of the project and security controls to ensure those requirements are included in the design of the solution.

**Applications should be inspected for security vulnerabilities through the development phase.** Application security testing should be conducted throughout the different phases of the software development and acquisition life cycle to verify that the security controls are working as expected and the software is free from significant vulnerabilities. Any residual risks stemming from control gaps or vulnerabilities that cannot be fully mitigated should be assessed and accepted as per the organizational risk framework. Security activities such as risk assessment, architecture analysis, threat modelling, source code review, vulnerability and penetration testing, security configuration review should be embedded in the different phases of the software development effort.

**Software developed by third parties should be carefully tested to verify that is free from significant security vulnerabilities.** Appropriate processes, procedures and technologies should be in place to evaluate, assess and test the security of externally developed software before it is commissioned into production.

**Developers’ access to the production environment should be appropriately controlled to prevent potential unauthorized changes to enterprise applications.** Segregation of duties for deployment of code into production should be enforced through technical controls to ensure that changes are appropriately tested before they are promoted to production. Access to code repositories, development and testing environments should be restricted to only authorized individuals, keeping the development and testing environments separate from the production environment.

Please refer to the [*Software Security*](#SSDLC) section in the References annex for specific security controls.

***Third-Party Management***

**IT services can be outsourced, but accountability for managing their associated cyber security risks should remain with the organization.** Organizations across all industries are leveraging outsourcing capabilities such as cloud computing, to more efficiently run their business and better serve their customers. Cost savings, increased scalability, flexibility and resiliency are among the benefits that makes this technology appealing to different enterprises. However, the accountability for managing the risks arising from the relationship with third parties remains with the organization. Hence, maintaining a comprehensive understanding of key relationships and managing their associated cyber security risks are essential for the secure, reliable, and resilient delivery of services. In this regard, organizations should establish an appropriate set of controls to manage these risks and ensure that third parties are aware of the expectations.

**Contractual agreements should incorporate security and data privacy requirements for third parties.** Contracts with third parties should contain appropriate terms and conditions to comply with applicable legal and regulatory requirements and include appropriate service level requirements. Also, contractual agreements should ensure that the organization retains the ability to frequently review the service provider’s security posture and adherence to international standards and compliance with industry recognized security certifications. Finally, appropriate arrangements should be established to ensure business continuity in the event of an unforeseen interruption of the outsourced services.

Please refer to the [*Third-Party Management*](#ThirdParty) section in the References annex for specific security controls.

# **Security Operations**

The components of the cybersecurity program described in this section are *Physical and Environmental Security, Network Security, End-Point Security, Data Protection, Threat and Vulnerability Management,* and *Event Detection, Logging and Monitoring*.

***Physical Security and Environmental Controls***

**Physical security is one of the basic layers of an in-depth approach to defense.** Unauthorized access, potential damage to critical assets or interference with the operations should be prevented by physical and environmental controls commensurate with the risk to critical infrastructure and organizational objectives. Among other things, security perimeters should be considered to protect areas that contain information and information processing facilities. Access to those secure areas should be protected by entry controls to ensure that only authorized personnel are allowed. Similarly, environmental protection should be in place against potential damage from different forms of natural or man-made disaster.

**Vendor security certifications should be frequently reviewed when data center services are outsourced.** The data center service provider should produce evidence of compliance with security certifications and standards relevant to the organization’s environment (e.g. ISO 27001, PCI DSS[[27]](#footnote-8), SOC reports[[28]](#footnote-9)). The CRSP should establish procedures to frequently review these certifications and identify and manage any residual risks associated with the outsourcing of data center operations.

Please refer to the [*Physical and Environmental Security*](#Physical) section in the References annex for specific security controls.

***Network Security***

**The network perimeter of organizations is extending with blurred boundaries between work and home networks, personal and business-issued devices, on-premises and cloud infrastructure, but the security of the network still needs to be managed.** Appropriate procedures should be implemented to manage security at the network level, including access management, vulnerability management, incident identification and notification, device configuration and patch management, and network architecture, including wireless networks.

**Among other things, network segmentation should be considered for enhanced security.** Organizations should consider segmenting networks in multiple, separate trust/security zones with defense-in- depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate the impact of potential cyber-attacks, leveraging protective and detective technologies (i.e. firewalls, intrusion detection systems, intrusion prevention systems).

**The corporate network should be protected against attacks from the internet that may impact service availability.** Data breach investigation reports indicate that entities in the financial industry have increasingly been targeted in distributed denial of service (DDoS) attacks. The purpose of these attacks is to disrupt the organization’s processes by overwhelming their systems and telecommunications networks with massive amounts of data requests. Sometimes the purpose of these attacks is to distract the attention of the incident response team while other more sophisticated attacks are conducted against the organization. In any case, organizations should ensure that appropriate DDoS mitigation measures are in place commensurate to the organization’s tolerance to availability loss.

Please refer to the [*Network Security*](#Network) section in the References annex for specific security controls.

***End-Point Security***

**Increase in teleworking and Bring Your Own Device (BYOD) practices are good examples of why organizations need to protect endpoints.** Appropriate protection mechanisms and controls should be implemented and maintained at the end-points (i.e. workstations, servers, network components, mobile devices), including but not limited to antivirus protection, full disk encryption, malware protection, hardware access control and patch management, commensurate with the risk to critical infrastructure and organizational objectives.

**Organizations need to develop, document and maintain under configuration control a current baseline configuration of the endpoints.** Baseline configurations should be documented, formally reviewed and agreed-upon for the endpoints. Automated mechanisms should be used to maintain an up-to-date, accurate and readily available baseline configuration of the endpoints.

Please refer to the [*End-Point Security*](#EndPoint) section in the References annex for specific security controls.

***Data Protection***

**A data breach can be a costly matter.** It can lead to direct financial losses, such as lost sales or fines, but loss or theft of essential financial information can also severely damage the organization’s reputation, lose the trust of customers and lead to a significant reduction in productivity. Data governance processes should be established along with appropriate mechanisms to prevent the compromise of sensitive data. These mechanisms include but are not limited to data loss prevention tools, cryptographic controls, etc.

**A data classification policy is a key aspect of data protection.** The data classification policy and procedures should specify the criteria for classifying the data (e.g. public, confidential, strictly confidential) and provide guidance on required security controls for each type of data (e.g. encryption at rest and in transit, data loss prevention). The data classification policy should also establish roles and responsibilities for protecting the data (e.g. data owner, data custodian). In the same vein, organizations should consider appointing a data protection officer, responsible for providing guidance to internal and external users and service providers on their responsibilities and established procedures related to data protection.

**Encryption is a popular and effective data protection control**. Especially when sensitive data is stored outside the organization, like in a cloud service provider. Formal policies and procedures should be in place addressing the need to use cryptographic controls to protect sensitive data where it is stored and when it is in transit. Requirements for managing and protecting the encryption keys should also be addressed in the policy.

**Critical data must be appropriately protected when it leaves the production environment.** Organizations should consider preventing the use of production data in development and testing environments unless appropriate controls (e.g. data masking) are applied to protect the confidentiality of data. Policies and procedures should be established to restrict the use of removable media and apply appropriate controls to prevent the loss or leakage of critical information. Finally, physical assets should be formally managed throughout removal, transfers, and disposition to prevent the loss or leakage of critical information stored in those assets, and data should be destroyed according to the established data disposition policy.

Please refer to the [*Data Protection*](#DataProtection) section in the References annex for specific security controls.

***Threat and Vulnerability Management***

**The evolving cyber security threat landscape demands near-real-time knowledge of emerging threats and how they could impact the operations of the organization.** Threat and vulnerability management is a critical component of a cybersecurity program and deals with the activities related to learning and understanding new cyber threats and detecting and managing existing vulnerabilities to prevent cyber-attacks. Following leading practices, organizations should establish and maintain processes, procedures and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities. Box 7 provides a distinction between threat and vulnerability.

**Up-to-date threat and vulnerability information should be obtained from reputable sources and necessary actions taken based on criticality.** Organizations should subscribe to and constantly monitor industry channels that provide updated information about threats and vulnerabilities, recommended patches and remediation actions to be taken. Threats should be analyzed and prioritized considering the characteristics of the threat such as likely intent, capability, and applicability to the organization’s technological environment. Vulnerabilities detected through automatic scans, penetration tests, cybersecurity exercises and audits should be analyzed and prioritized based on the potential impact of the vulnerability on the exposed asset and the criticality of the asset.

**Many cyber security attacks could be prevented by following a basic cyber security hygiene.** Among other cyber security hygiene practices like following documented security standards, securing administrative accounts, implementing firewalls or anti-virus solutions, organizations should deploy in a timely fashion relevant security patches to address known critical vulnerabilities.A process should be in place to obtain, test and automatically deploy security patches and updates in a timely manner based on criticality. For example, a patch was available in March 2017 to address the vulnerability later exploited by the WannaCry ransomware attack in May 2017. This attack that affected several hundred thousand machines world-wide could have been prevented in most organizations by simply applying the patch in a timely fashion as part of the basic cybersecurity hygiene routine. In addition, organizations should also consider and mitigate any risks arising from the use of unsupported software for which security patches are not available anymore.

Please refer to the [*Threat and Vulnerability Management*](#TVM) section in the References annex for specific security controls.

***Event Detection, Logging and Monitoring***

**Anomalous activity should be detected promptly, and its potential impact understood for an effective response.** To be able to effectively respond to potential cyber security events, organizations should develop and maintain a near-real-time knowledge of the dynamic environment they operate in. Awareness of current relevant cybersecurity events external to the organization should be complemented by the appropriate detection, logging and monitoring of events internal to the organization. For this purpose, processes, procedures and technologies should be implemented and maintained to collect, protect and analyze audit logs recording user and administrator activities, exceptions, information security events, etc.

**Event logs from different sources should be normalized, aggregated, and correlated to facilitate the analysis of suspicious activities**. Ideally, logs from applications, infrastructure and network components (e.g. firewalls, IDS/IPS) should be sent to a centralized Security Information and Event Management (SIEM) system, where they can be aggregated and correlated for a better analysis of those suspicious activities. Access to the SIEM should be appropriately restricted to ensure that logs are not tampered with or destroyed.

**Automated analysis of security events should be conducted to identify potential cyber security attacks.** Normal behavior and thresholds should be defined so alerts can be triggered when suspicious activities are detected. For example, an attempt to connect to a server in headquarters by a user that works in a remote branch may be considered anomalous activity, and an alert triggered. The automated analysis of security events should be supplemented by expert analysis on security events to identify potential cyber-attacks.

**Roles and responsibilities for monitoring events should be clearly established.** Organizations should establish clear roles and responsibilities for the personnel responsible for the monitoring of events, and a framework for the timely analysis, categorization and response to the alerts. Detection processes and technologies should be frequently tested, and processes improved based on testing results.

Please refer to the [*Event Detection, Logging and Monitoring*](#LoggingMonitoring) section in the References annex for specific security controls.

# **POLICY CONSIDERATIONS**

In addition to the guidance to Credit Reporting Service Providers outlined in Chapter 4, the survey indicated certain regulatory gaps that require policy intervention. This section outlines a set of policy considerations that policy makers and regulatory authorities should consider to enhance cybersecurity within their jurisdictions.

The recommendations are designed to enhance regulatory oversight and ensure a systematic approach to cyber security across markets. The recommendations are also aimed to promote industry wide mechanisms that support CRSPs specific practices, as a way of mitigating system wide cyber security incidents.

# **Enhancing Cyber Legal and Regulatory Environment**

**Policy makers should consider implementing and/or enhancing cyber laws and regulations that provide incentives for better protection of data and systems.** Policy makers should consider implementing cyber laws and regulations, in instances where such legislation is nonexistent, or enhancing existing frameworks. The frameworks should provide the following:

1. mechanisms for regulatory authorities to have oversight to ensure that key public and private infrastructures including the financial infrastructure services providers meet essential security standards;
2. enforcement mechanisms including penalties and breach compensation for data leaks;
3. cyber security information sharing; and
4. notification and reporting practices.

# **Development of Cybersecurity Strategy and Framework**

**Regulatory authorities should consider developing national and/or sector-wide cyber security strategies and frameworks[[29]](#endnote-20).** While in some countries the focus of cyber security has been on CRSPs, countries should also consider developing national or sectoral cyber security strategies and frameworks that are informed by the cyber security threat and vulnerability landscape. The sector-wide cyber security strategies and frameworks should also outline interagency cooperation among their various state actors responsible for credit reporting ecosystem.

# **Enhancing Cyber Governance**

**To the extent possible, regulatory bodies should consider implementing practices or standards that promote the strengthening of cyber governance by CRSPs.** In jurisdictions where CRSPs are subject to registration/ licensing requirements regulators should consider ensuring that CRSPs cyber security reporting structures are commensurate with their size and complexities and promote independence of the ICT assets administration and ICT Security. Authorities should consider evaluating the need for a Chief Information Security Officers or their variant, as one of the key principal officers/ functions within CRSPs with this position having direct access to the board of directors.

# **Cyber Training for Board Directors**

**Where applicable, regulatory bodies should ensure that CRSPs have in place detailed programs for training their boards of directors or other supervisory body.** The survival and prosperity of companies are now more than ever tied to the robustness and resilience of the IT assets making it important to place cyber security issues firmly within the remit of the board. As such, CRSPs should ensure that their annual training programs incorporate cyber training for staff and importantly the board of directors. Regulatory authorities should work with CRSPs to ensure that boards or other supervisory bodies are adequately trained.

|  |
| --- |
| **Box 7: Cases of Board Training on Cyber Security****UK National Cyber Security Centre (NCSC) Cyber Security Toolkit for Boards** The toolkit is designed to make board member conversant of cyber security and equips them with the knowledge to know and understand the right questions to ask. The toolkit covers general, risk management, measures, information security, cyber resilience, response to cyber incidents, collaborations and partners. The toolkit assesses each of the sections on three levels: the specific actions, the oversight role and the best practice that the board can consider benchmarking the organization’s performance. |

# **Cyber breach disclosure frameworks**

**Regulatory authorities should issue guidance on the level and extent of disclosures in times of breaches.** The framework should consider timeliness, detail of breaches and stakeholders that should be notified of the breach. Regulatory authorities should work with CRSPs to ensure that CRSPs develop and implement breach communication frameworks which clearly spell out the communication strategy, sample statements for media (print, electronic and social media) and breach communication governance.

**Box 8: Case of a breach reporting framework**

**Office of The Privacy Commissioner Canada Guidance Framework**

The OTPCC issued a guidance framework on the obligations of institutions with respect to the mandatory reporting of breaches of security safeguards following the enactment of The *Personal Information Protection and Electronic Documents Act* (PIPEDA) in November 2018. The framework covers:

* [Part 1 – Your obligations for reporting breaches](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1)
* [Part 2 – Submitting a breach report to the OPC](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_2)
* [Part 3 – You need to keep records of all breaches](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_3)
* [Part 4 – When and how to notify individuals](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_4)
* [Part 5 – Notification to Organizations](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_5)
* [Part 6 – Assessing real risk of significant harm](https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_6)
* [PIPEDA breach report form](https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-business/)

# **Outsourcing of keys IT Services**

**Regulatory authorities should work with CRSPs to ensure that they implement sound outsourcing procedures that detail the controls and processes to be followed when evaluating and managing relationships with third parties.** The procedures should also outline the mechanisms for ensuring that the security of outsourced services remain visible to the CRSP and detail how to manage fourth parties. Entities should also ensure that their risk management frameworks incorporate risks inherent in outsourcing.

**Regulatory authorities should also consider ensuring that third parties that provide services to CRSPs operate under risk management practices similar to those expected of the CRSPs themselves.** In most cases the third-party vendors are not under regulatory purview and do not need to comply with any regulatory requirements. This might impact on the investments they make to upgrade their security. As a result, vendors dealing with critical infrastructure institutions should be subject of rigorous standards where applicable (e.g. GDPR in Europe) and the right to audit should be incorporated in the contracts with third parties.

# **Periodic Cyber Risk Assessments**

**Supervisory authorities should consider conducting annual cybersecurity risk assessments of crucial infrastructure players.** Authorities should consider conducting annual risk assessments to identify, estimate, and prioritize risk resulting from the operation and use of information systems. Where there are limitations, the assessments should target critical infrastructure such as credit reporting, payment and settlement systems.

In carrying out this responsibility, where possible, the supervisory authorities should consider collaborative methods, such as including information sharing and joint assessments, so as to reduce regulatory burden on the CRSPs. This is relevant in cases where the supervisory functions are distributed across regulatory agencies.

**Authorities should consider working with CRSPs to ensure they conduct their own internal assessments on a periodic basis.** CRSPs should conduct internal assessments or hire professionals to conduct assessments. Results of such assessments should be shared with regulatory bodies.

# **Periodic Cyber Audits**

**Regulatory authorities should consider working with CRSPs to ensure they undertake regular audits of cyber security functions.** The audit functions should develop audit plans that subject cyber assets and outsourced services to audits, in line with risk-based approach to audit. Where possible, regulatory authorities should promote the use of external auditors to conduct review of cybersecurity functions of CRSPs

# **Establishment of Cyber Information Sharing and Collaboration Mechanisms**

**Regulatory and/or industry bodies should consider developing mechanisms that foster and enforce cyber security information sharing and collaboration among parties.** The mechanism should be public-private partnerships that encompasses the critical infrastructures and actors. Information sharing and collaboration frameworks should promote sharing of timely, actionable and relevant unclassified information. The frameworks should consider the type of information to be shared, detail, frequency of meetings and consequences of failure to share. CRSPs should share threats and vulnerability information, emerging risks and way of collectively dealing with cyber. The framework should also include the penalties for failure or inadequate disclosures.

**Regulatory bodies should also publish or promote publication of redacted reports on cyber security issues on a semi-annually (half yearly) basis.**The industry reports should promote disclosure of timely unclassified information and should be widely circulated within the countries.

# **Incident Response, Disaster Recovery and Business Continuity**

**Regulatory authorities should work with CRSPs to ensure they actively participate and collaborate with national cybersecurity actors such as CERTs.** CRSPs should actively participate with the CERTs in their country to contribute to research, enhancements of the system, and develop best practices and training in cybersecurity.

**Regulatory authorities should work with CRSPs to ensure they develop comprehensive incident response plans that are subject to audit and simulation tests**. The incident response plan should define the criteria for categorizing and prioritizing incidents and provide guideline on the stages to be followed including the preparation, identification, containment, eradication, recovery and lessons learned. The incident response plan should be formalized and reviewed, at least, annually.

**Regulatory authorities should work with CRSPs to ensure they conduct fully simulated attack tests to test the effectiveness of their incident response plan.** The plan should be frequently tested against a variety of realistic scenarios, involving relevant internal and external stakeholders. A typical test involves:

* possible scenarios;
* simulating the deployment of a known threat;
* running the associated incident response plan; and
* documenting the results.

Scenarios like malware infections, extended power outages or DDoS attacks should be tested through tabletop and functional exercises to evaluate the effectiveness of the plans and the readiness of the personnel to respond to an incident. Lessons learned from tests and forensic analysis conducted on real events should be incorporated into the plans to improve the organization’s ability to effectively and timely respond to cyber events.

**Regulatory authorities should work with CRSPs to ensure they establish dedicated Computer Security Incident Response Team (CSIRT).** Establishing a dedicated Computer Security Incident Response Team (CSIRT) will boost the organization’s capabilities to timely respond to cyber incidents. Clear roles and responsibilities should be established for carrying out response activities enabling a rapid response in case of cybersecurity events.

# **REFERENCES**

The table below provides the mapping of the different focus areas discussed in this guideline to industry-recognized security standards and frameworks that illustrate a method to achieve the outcomes associated with each focus area. These references are illustrative and not exhaustive.

|  |  |  |  |
| --- | --- | --- | --- |
| Focus Area  | NIST Cyber Security Framework | ISO/IEC 27001:2013 | NIST SP 800-53 Rev. 4 |
| Strategy | ID.BE-1: The organization’s role in the supply chain is identified and communicatedID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicatedID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicatedID.BE-4: Dependencies and critical functions for delivery of critical services are establishedID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2Clause 4.1A.11.2.2, A.11.2.3, A.12.1.3A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 | CP-2, SA-12PM-8PM-11, SA-14CP-8, PE-9, PE-11, PM-8, SA-14CP-2, CP-11, SA-13, SA-14 |
| Governance | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are establishedID.GV-1: Organizational information security policy is established and communicatedID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partnersID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managedID.GV-4: Governance and risk management processes address cybersecurity risksPR.AT-4: Senior executives understand their roles and responsibilities | A.6.1.1A.5.1.1A.6.1.1, A.7.2.1, A.15.1.1A.6.1.1, A.7.2.2 | CP-2, PS-7, PM-11Controls from all security control familiesPM-1, PM-2, PS-7Controls from all security control familiesSA-2, PM-3, PM-7, PM-9, PM-10, PM-11AT-3, IR-2, PM-13 |
| Risk Management | ID.GV-4: Governance and risk management processes address cybersecurity risksID.RA-1: Asset vulnerabilities are identified and documentedID.RA-2: Cyber threat intelligence is received from information sharing forums and sourcesID.RA-3: Threats, both internal and external, are identified and documentedID.RA-4: Potential business impacts and likelihoods are identifiedID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine riskID.RA-6: Risk responses are identified and prioritizedID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholdersID.RM-2: Organizational risk tolerance is determined and clearly expressedID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | A.12.6.1, A.18.2.3A.6.1.4Clause 6.1.2A.16.1.6, Clause 6.1.2A.12.6.1Clause 6.1.3Clause 6.1.3, Clause 8.3, Clause 9.3Clause 6.1.3, Clause 8.3Clause 6.1.3, Clause 8.3 | SA-2, PM-3, PM-7, PM-9, PM-10, PM-11CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5SI-5, PM-15, PM-16RA-3, SI-5, PM-12, PM-16RA-2, RA-3, PM-9, PM-11, SA-14RA-2, RA-3, PM-16PM-4, PM-9PM-9PM-9PM-8, PM-9, PM-11, SA-14 |
| Compliance | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managedID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.DE.DP-2: Detection activities comply with all applicable requirements | A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5A.15.2.1, A.15.2.2A.18.1.4, A.18.2.2, A.18.2.3 | Controls from all security control familiesAU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12AC-25, CA-2, CA-7, SA-18, SI-4, PM-14 |
| Data Privacy | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managedPR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks) | A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 | Controls from all security control familiesAC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 |
| Awareness and Education | PR.AT-1: All users are informed and trainedPR.AT-2: Privileged users understand roles and responsibilitiesPR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities PR.AT-4: Senior executives understand roles & responsibilities PR.AT-5: Physical and information security personnel understand roles & responsibilities PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | A.7.2.2, A.12.2.1 A.6.1.1, A.7.2.2A.6.1.1, A.7.2.1, A.7.2.2 A.6.1.1, A.7.2.2A.6.1.1, A.7.2.2A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 | AT-2, PM-13AT-3, PM-13PS-7, SA-9, SA-16 AT-3, IR-2, PM-13 AT-3, PM-13PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 |
| Information Sharing and Communications | PR.IP-8: Effectiveness of protection technologies is sharedRS.CO-3: Information is shared consistent with response plansRS.CO-4: Coordination with stakeholders occurs consistent with response plansRS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | A.16.1.6A.16.1.2, Clause 7.4, Clause 16.1.2Clause 7.4A.6.1.4 | AC-21, CA-7, SI-4CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4CP-2, IR-4, IR-8PM-15, SI-5 |
| Resiliency | PR.IP-4: Backups of information are conducted, maintained, and testedPR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managedPR.IP-10: Response and recovery plans are testedRS.RP-1: Response plan is executed during or after an eventRS.CO-1: Personnel know their roles and order of operations when a response is neededRS.CO-2: Events are reported consistent with established criteriaRS.CO-3: Information is shared consistent with response plansRS.CO-4: Coordination with stakeholders occurs consistent with response plansRS.AN-2: The impact of the incident is understoodRS.AN-3: Forensics are performedRS.AN-4: Incidents are categorized consistent with response plansRS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)RS.MI-1: Incidents are containedRS.MI-2: Incidents are mitigatedRS.IM-1: Response plans incorporate lessons learnedRS.IM-2: Response strategies are updatedRC.RP-1: Recovery plan is executed during or after a cybersecurity incidentRC.IM-1: Recovery plans incorporate lessons learnedRC.IM-2: Recovery strategies are updatedRC.CO-1: Public relations are managedRC.CO-2: Reputation after an event is repairedRC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teamsID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers | A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3A.17.1.3A.16.1.1, A.16.1.4A.6.1.1, A.7.2.2, A.16.1.1A.6.1.3, A.16.1.2A.16.1.2, Clause 7.4, Clause 16.1.2Clause 7.4A.16.1.4, A.16.1.6A.16.1.7A.16.1.4A.16.1.5, A.12.2.1, A.16.1.5A.12.2.1, A.16.1.5A.16.1.6, Clause 10A.16.1.6, Clause 10A.16.1.6, Clause 10A.16.1.6, Clause 10A.16.1.6, Clause 10A.6.1.4, Clause 7.4Clause 7.4Clause 7.4A.17.1.3 | CP-4, CP-6, CP-9CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17CP-4, IR-3, PM-14AU-6, CA-7, IR-4, SI-4CP-2, CP-10, IR-4, IR-8 AU-6, IR-6, IR-8CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4CP-2, IR-4, IR-8CP-2, IR-4AU-7, IR-4CP-2, IR-4, IR-5, IR-8SI-5, PM-15IR-4IR-4CP-2, IR-4, IR-8CP-2, IR-4, IR-8CP-10, IR-4, IR-8CP-2, IR-4, IR-8CP-2, IR-4, IR-8CP-2, IR-4CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 |
| Identity and Access Management | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processesPR.AC-2: Physical access to assets is managed and protectedPR.AC-3: Remote access is managedPR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of dutiesPR.AC-6: Identities are proofed and bound to credentials and asserted in interactionsPR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5A.7.1.1, A.9.2.1A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4A.9.1.2 | AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8AC-1, AC-17, AC-19, AC-20, SC-15AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11AC-3, CM-7 |
| Asset Management | ID.AM-1: Physical devices and systems within the organization are inventoriedID.AM-2: Software platforms and applications within the organization are inventoriedID.AM-3: Organizational communication and data flows are mappedID.AM-4: External information systems are cataloguedID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | A.8.1.1, A.8.1.2A.8.1.1, A.8.1.2, A.12.5.1A.13.2.1, A.13.2.2A.11.2.6A.8.2.1 | CM-8, PM-5CM-8, PM-5AC-4, CA-3, CA-9, PL-8AC-20, SA-9CP-2, RA-2, SA-14, SC-6 |
| Change and Configuration Management | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) PR.IP-2: A System Development Life Cycle to manage systems is implementedPR.IP-3: Configuration change control processes are in placePR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled toolsPR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6A.11.2.4, A.15.1.1, A.15.2.1 | CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17CM-3, CM-4, SA-10MA-2, MA-3, MA-5, MA-6MA-4 |
| Software Security | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrityPR.DS-7: The development and testing environment(s) are separate from the production environmentPR.IP-2: A System Development Life Cycle to manage systems is implemented | A.12.1.4A.12.1.4A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 | SC-16, SI-7CM-2PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 |
| Third-Party Management | ID.AM-4: External information systems are cataloguedID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are establishedID.BE-1: The organization’s role in the supply chain is identified and communicatedID.BE-4: Dependencies and critical functions for delivery of critical services are establishedID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholdersID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment processID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management PlanID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providersDE.CM-6: External service provider activity is monitored to detect potential cybersecurity events RS.CO-4: Coordination with stakeholders occurs consistent with response plansRC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams | A.11.2.6A.6.1.1A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2A.11.2.2, A.11.2.3, A.12.1.3A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2A.15.2.1, A.15.2.2A.15.1.1, A.15.1.2, A.15.1.3A.15.2.1, A.15.2.2A.17.1.3A.14.2.7, A.15.2.1 Clause 7.4Clause 7.4 | AC-20, SA-9CP-2, PS-7, PM-11CP-2, SA-12CP-8, PE-9, PE-11, PM-8, SA-14CP-2, CP-11, SA-13, SA-14SA-9, SA-12, PM-9RA-2, RA-3, SA-12, SA-14, SA-15, PM-9SA-9, SA-11, SA-12, PM-9AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9CA-7, PS-7, SA-4, SA-9, SI-4CP-2, IR-4, IR-8CP-2, IR-4 |
| Physical and Environmental Security  | ID.AM-1: Physical devices and systems within the organization are inventoriedPR.AC-2: Physical access to assets is managed and protectedPR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilitiesPR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are metPR.IP-7: Protection processes are improvedDE.CM-2: The physical environment is monitored to detect potential cybersecurity events | A.8.1.1, A.8.1.2A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8A.6.1.1, A.7.2.2A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3A.16.1.6, Clause 9, Clause 10A.11.1.1, A.11.1.2 | CM-8, PM-5PE-2, PE-3, PE-4, PE-5, PE-6, PE-8AT-3, IR-2, PM-13PE-10, PE-12, PE-13, PE-14, PE-15, PE-18CA-2, CA-7, CP-2, IR-8, PL-2, PM-6CA-7, PE-3, PE-6, PE-20 |
| Network Security  | PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)PR.DS-4: Adequate capacity to ensure availability is maintainedPR.PT-4: Communications and control networks are protectedPR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situationsDE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managedDE.CM-1: The network is monitored to detect potential cybersecurity eventsDE.CM-4: Malicious code is detectedDE.CM-8: Vulnerability scans are performedPR.IP-7: Protection processes are continuously improved | A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3A.12.1.3, A.17.2.1A.13.1.1, A.13.2.1, A.14.1.3A.17.1.2, A.17.2.1 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2A.12.6.1A.12.6.1A.16.1.6, Clause 9, Clause 10 | AC-4, AC-10, SC-7AU-4, CP-2, SC-5AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6AC-4, CA-3, CM-2, SI-4AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4SI-3, SI-8RA-5CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 |
| End-point Security  | ID.AM-1: Physical devices and systems within the organization are inventoriedID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business valueID.RA-1: Asset vulnerabilities are identified and documentedPR.DS-3: Assets are formally managed throughout removal, transfers, and dispositionPR.IP-3: Configuration change control processes are in placeDE.CM-4: Malicious code is detectedDE.CM-5: Unauthorized mobile code is detectedDE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performedDE.CM-8: Vulnerability scans are performed | A.8.1.1, A.8.1.2A.8.2.1A.12.6.1, A.18.2.3A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4A.12.2.1A.12.5.1, A.12.6.2A.12.4.1, A.14.2.7, A.15.2.1 | CM-8, PM-5CP-2, RA-2, SA-14, SC-6CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5CM-8, MP-6, PE-16CM-3, CM-4, SA-10SI-3, SI-8SC-18, SI-4, SC-44AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4RA-5 |
| Data Protection | PR.DS-1: Data-at-rest is protectedPR.DS-2: Data-in-transit is protectedPR.DS-3: Assets are formally managed throughout removal, transfers, and dispositionPR.DS-5: Protections against data leaks are implementedPR.IP-4: Backups of information are conducted, maintained, and tested PR.IP-6: Data is destroyed according to policyPR.PT-2: Removable media is protected, and its use restricted according to policy | A.8.2.3A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 | MP-8, SC-12, SC-28SC-8, SC-11, SC-12CM-8, MP-6, PE-16AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4CP-4, CP-6, CP-9MP-6MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 |
| Threat and Vulnerability Management | ID.RA-1: Asset vulnerabilities are identified and documentedID.RA-2: Cyber threat intelligence is received from information sharing forums and sourcesID.RA-3: Threats, both internal and external, are identified and documentedID.RA-4: Potential business impacts and likelihoods are identifiedID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine riskID.RA-6: Risk responses are identified and prioritizedPR.IP-12: A vulnerability management plan is developed and implementedDE.CM-8: Vulnerability scans are performedRS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | A.12.6.1, A.18.2.3A.6.1.4Clause 6.1.2A.16.1.6, Clause 6.1.2A.12.6.1Clause 6.1.3A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 A.12.6.1 | CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5SI-5, PM-15, PM-16RA-3, SI-5, PM-12, PM-16RA-2, RA-3, SA-14, PM-9, PM-11RA-2, RA-3, PM-16PM-4, PM-9RA-3, RA-5, SI-2RA-5CA-7, RA-3, RA-5 |
| Event Detection, Logging and Monitoring  | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policyDE.AE-2: Detected events are analyzed to understand attack targets and methodsDE.AE-3: Event data are aggregated and correlated from multiple sources and sensorsDE.AE-4: Impact of events is determinedDE.AE-5: Incident alert thresholds are establishedDE.CM-1: The network is monitored to detect potential cybersecurity eventsDE.CM-2: The physical environment is monitored to detect potential cybersecurity eventsDE.CM-3: Personnel activity is monitored to detect potential cybersecurity eventsDE.CM-4: Malicious code is detectedDE.CM-5: Unauthorized mobile code is detectedDE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performedDE.DP-1: Roles and responsibilities for detection are well defined to ensure accountabilityDE.DP-2: Detection activities comply with all applicable requirementsDE.DP-3: Detection processes are testedDE.DP-4: Event detection information is communicated to appropriate partiesDE.DP-5: Detection processes are continuously improvedRS.AN-1: Notifications from detection systems are investigated | A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1A.12.4.1, A.16.1.1, A.16.1.4A.12.4.1, A.16.1.7A.16.1.4A.16.1.4A.11.1.1, A.11.1.2A.12.4.1, A.12.4.3A.12.2.1 A.12.5.1, A.12.6.2A.14.2.7, A.15.2.1A.12.4.1, A.14.2.7, A.15.2.1A.6.1.1, A.7.2.2A.18.1.4, A.18.2.2, A.18.2.3A.14.2.8A.16.1.2, A.16.1.3A.16.1.6A.12.4.1, A.12.4.3, A.16.1.5 | AU FamilyAU-6, CA-7, IR-4, SI-4AU-6, CA-7, IR-4, IR-5, IR-8, SI-4CP-2, IR-4, RA-3, SI -4IR-4, IR-5, IR-8AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4CA-7, PE-3, PE-6, PE-20AC-2, AU-12, AU-13, CA-7, CM-10, CM-11SI-3, SI-8SC-18, SI-4. SC-44CA-7, PS-7, SA-4, SA-9, SI-4AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4CA-2, CA-7, PM-14AC-25, CA-2, CA-7, SA-18, SI-4, PM-14CA-2, CA-7, PE-3, SI-3, SI-4, PM-14AU-6, CA-2, CA-7, RA-5, SI-4CA-2, CA-7, PL-2, RA-5, SI-4, PM-14AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 |

# **SURVEY QUESTIONAIRE**



**International Committee on Credit Reporting**

**CYBERSECURITY SURVEY**

**Purpose of survey**

This survey is being conducted by the ICCR to better understand the cybersecurity practices of credit reporting institutions and as an input to the guideline on cybersecurity in credit reporting that is being produced by the Committee. The purpose of this survey is to establish the status of oversight and strategy, resourcing, governance, information sharing, incident management and training and awareness practices of credit reporting system providers. The survey also assesses the preventive controls, risk management & compliance and audit practices.

Please note that all information supplied as part of the survey will be treated as strictly confidential and will only be made available for the purposes of the study to selected staff at the World Bank and to the independent consultant who has been engaged to analyze the results. Any information from the survey published in the study will be aggregated at a country level.

The survey should take less than 15 minutes to complete and we would ask that it is returned to (**lsalamina@ifc.org** ) by **02/21/19**. We would like to thank you in advance for taking the time to complete this survey. Your input is greatly appreciated.

**Structure of the survey**

This survey is divided in thirteen sections:

[i. Contact Information 2](#_Toc536864724)

[ii. Local Cyber Security Environment 2](#_Toc536864725)

[iii. Local Legal and Regulatory Environment 3](#_Toc536864726)

[iv. Board, Management and Cybersecurity and Information Security Strategies 4](#_Toc536864727)

[v. Outsourcing Critical IT Services 6](#_Toc536864728)

[vi. Information Sharing 6](#_Toc536864729)

[vii. Training and Awareness 6](#_Toc536864730)

[viii. Resources 7](#_Toc536864731)

[ix. Risk Management & Compliance 7](#_Toc536864732)

[x. Audit 8](#_Toc536864733)

[xi. Incident Response 8](#_Toc536864734)

[xii. Data Loss Prevention (DLP) 9](#_Toc536864735)

[xiii. Preventive Controls 10](#_Toc536864736)

Thank you once again for your collaboration. If you have any questions, **please contact** **lsalamina@ifc.org**

# **Contact Information**

Country: \*

Name of organization: \*

Your name: \*

Your e-mail: \*

# **Local Cyber Security Environment**

1. Has your institution suffered a cyber security incident in the last two years?

 [ ]  Yes | [ ]  No. If yes:

* Please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Has it been possible to identify the responsible, external or internal actors?

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

1. Has any organization supplying data to, or getting data from, your institution suffered a cyber security incident in the last two years?

[ ]  Yes | [ ]  No If yes:

* please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Has it been possible to identify the responsible, external or internal actors, and who carried out the attack?

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

1. Has any prominent organization in your country, public or private, not in direct electronic contact with your institution suffered a cyber security incident in the last two years?

[ ]  Yes | [ ]  No If yes:

* Please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Has it been possible to identify the responsible, external or internal actors, and who did it?

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

# **Local Legal and Regulatory Environment**

1. Are there laws or regulations establishing minimum cybersecurity security or information security standards for credit reporting institutions in your country?

[ ]  Yes | [ ]  No

1. If your answer to question 4 above is yes:
* List the regulatory and supervisory agencies responsible:

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Is there a legal or regulatory obligation to report cyber security or information security incidents to the supervisory agency?

[ ]  Yes | [ ]  No

* Is there a legal obligation to notify all parties affected by the loss of confidential data derived from a cyber security incident?

[ ]  Yes | [ ]  No

* Is there a legal obligation to compensate the affected parties?

[ ]  Yes | [ ]  No

* Are there any penalties that are levied for the breach? If the answer is yes, please specify the levels (ranges) of penalty (financial and non-financial)?

[ ]  Yes | [ ]  No Level of penalty……………………….

# **Board, Management and Cybersecurity and Information Security Strategies**

1. Does your institution have a documented cybersecurity and/ or information security strategy integrating technology, policies, procedures, and training?

[ ]  Yes | [ ]  No

1. Does the board approve the cybersecurity and/or information security strategy?

[ ]  Yes | [ ]  No

1. Does the board review the cybersecurity and or information security strategies whenever there is a change in the institution’s information technology or when new threats appear?

[ ]  Yes | [ ]  No

1. Do members of the board understand the key cybersecurity controls in place?

[ ]  Yes | [ ]  No

1. Does the board include at least one director with a good understanding of information security in general and cybersecurity in particular?

[ ]  Yes | [ ]  No

1. Does the board engage cybersecurity experts to assist in carrying out its oversight responsibilities?

[ ]  Yes | [ ]  No

1. Do approved information security policies and procedures define key roles and responsibilities and have they have been communicated to all relevant stakeholders?

[ ]  Yes | [ ]  No

1. The most senior officer in charge of cybersecurity or information security is a:

[ ]  Chief Information Security Officer | [ ]  Chief Information Officer | [ ]  Other (please specify) ………………….

1. Does the most senior officer in charge of cybersecurity or information security report to the chief executive officer, or to the board or to a board committee?

[ ]  Yes | [ ]  No

1. Is the most senior officer in charge of cybersecurity or information security independent from areas using or administering the institution’s information technology assets?

[ ]  Yes | [ ]  No

1. Does management hold employees accountable for complying with information security policies?

[ ]  Yes | [ ]  No

1. Does the institution’s strategy include outsourcing critical information technology services (e.g. cloud services)?

[ ]  Yes | [ ]  No

1. Does the institution’s strategy include purchasing insurance against cyber incidents?

[ ]  Yes | [ ]  No

1. If the answer to question 18 above is yes, Is the institution insured?

[ ]  Yes | [ ]  No

1. Does the institution’s strategy include a process to notify authorities and other stakeholders of a breach of confidential data?

[ ]  Yes | [ ]  No

# **Outsourcing Critical IT Services**

1. Does the institution currently outsource critical information technology services?

[ ]  Yes | [ ]  No If the answer is yes,

* Which services are currently outsourced by the institution?

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

* Do the cybersecurity policies of the institution detail the controls and processes to be followed when evaluating and maintain relationships with these third parties?

[ ]  Yes | [ ]  No

# **Information Sharing**

1. Does the board encourage the cybersecurity team to engage in information sharing arrangements with other institutions?

[ ]  Yes | [ ]  No

1. Does the institution monitor cybersecurity incidents in the financial services industry and beyond by participating in industry programs (e.g. Financial Sector Information Sharing and Analysis Center (FS-ISAC))?

[ ]  Yes | [ ]  No

1. Does the institution receive timely notifications of cyber incidents from service providers with whom the institution has material outsourcing arrangements?

[ ]  Yes | [ ]  No

# **Training and Awareness**

1. Has the institution implemented an ongoing cyber awareness training program for all staff?

[ ]  Yes | [ ]  No

1. Has the board undertaken any form of cybersecurity training in the last 12 months?

[ ]  Yes | [ ]  No

1. Does management receive cybersecurity training relevant to their job responsibilities?

[ ]  Yes | [ ]  No

1. Do employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility?

[ ]  Yes | [ ]  No

1. Does annual cyber security or information security training include incident response, and current and emerging cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security)?

[ ]  Yes | [ ]  No

# **Resources**

1. Has the institution a specific cybersecurity budget?

[ ]  Yes | [ ]  No

1. Is there is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process?

[ ]  Yes | [ ]  No

1. Given the risks that the institution faces, is the investment it makes on cyber defenses appropriate?

[ ]  Yes | [ ]  No

# **Risk Management & Compliance**

1. Has the institution implemented a formal risk management framework that includes cyber risks?

[ ]  Yes | [ ]  No

1. Does the risk management function assess that the risk management framework is commensurate with the organization's risk and complexity?

[ ]  Yes | [ ]  No

1. Does the institution comply with data privacy and protection regulation?

[ ]  Yes | [ ]  No

# **Audit**

1. Does Internal Audit have sufficient resources and expertise to audit the cybersecurity or information security strategy implementation?

[ ]  Yes | [ ]  No

1. Does an internal or external independent audit validate that the institution's threat **information sharing** is commensurate with the organization's risk and complexity?

[ ]  Yes | [ ]  No

1. Does the internal or external independent audit validate that the **institution's cybersecurity controls** are commensurate with the organization's risk and complexity?

[ ]  Yes | [ ]  No

1. Does an internal or external independent audit validate that the institution's third-party relationship management is commensurate with the organization's risk and complexity?

[ ]  Yes | [ ]  No | [ ]  N/A

1. Does an internal or external independent audit validate that the institution's incident response program and resilience are commensurate with the institution's risk and complexity?

[ ]  Yes | [ ]  No

# **Incident Response**

1. Does the institution have documented procedures for monitoring, analyzing and responding to cybersecurity incidents?

[ ]  Yes | [ ]  No

1. Does the institution have a dedicated security incident team to respond to and mitigate suspected and/or known security incidents?

[ ]  Yes | [ ]  No

1. Does the institution have a process to escalate breaches of limits and thresholds to Senior Management for significant or critical cybersecurity incidents?

[ ]  Yes | [ ]  No

1. Does the institution have an internal communication plan to address cybersecurity incidents that includes communication protocols for key internal stakeholders (e.g. relevant business units, senior management, risk management, board of directors, etc.)?

[ ]  Yes | [ ]  No

1. Does the institution have an external communication plan to address cybersecurity incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, media, critical service providers, etc.)?

[ ]  Yes | [ ]  No

1. Does the institution have a partnership relationship with a national Computer Emergency Response Team (CERT)?

[ ]  Yes | [ ]  No | [ ]  N/A

1. Does the institution conduct incident-response simulation exercises on a regular basis?

[ ]  Yes | [ ]  No

# **Data Loss Prevention (DLP)**

1. Does the institution have a DLP program and Written Supervisory Procedures WSPs to monitor and prevent data breaches that help to detect and mitigate insider (and other) threats?

[ ]  Yes | [ ]  No

1. Does the institution require user verification prior to permitting the sending of outbound emails?

[ ]  Yes | [ ]  No

1. Does the institution have established consistent structures and processes for capturing DLP events—such as outbound emails and attachments or file transfers containing sensitive information?

[ ]  Yes | [ ]  No

1. Does the institution have established robust DLP rules to identify and block or encrypt the transfer of data, such as customer account numbers, Social Security numbers, etc.

[ ]  Yes | [ ]  No

1. Does the institution have established rules to control printing of sensitive data and documents?

[ ]  Yes | [ ]  No

# **Preventive Controls**

1. Is the institution’s network segmented into multiple, separate trust zones?

[ ]  Yes | [ ]  No

1. Is unauthorized network access (e.g. including wired, wireless and remote access) automatically detected and blocked?

[ ]  Yes | [ ]  No

1. Are there remote access policies and procedures (e.g. usage restrictions and configuration requirements) for accessing internal resources over a public network?

[ ]  Yes | [ ]  No

1. Does the institution tightly control and manage the use of administrative privileges?

[ ]  Yes | [ ]  No

1. Does the institution apply strong authentication mechanisms (e.g. two-factor authentication) to manage user identification and access?

[ ]  Yes | [ ]  No

1. Does the institution maintain an inventory of information technology assets (e.g., hardware, software, data, and systems hosted externally)?

[ ]  Yes | [ ]  No

1. Does the institution document, implement and enforce security configuration standards to all hardware and software assets on the network?

[ ]  Yes | [ ]  No

1. Is a change management process in place to request and approve changes to systems’ configurations, hardware, software, applications, and security tools?

[ ]  Yes | [ ]  No

1. Are there automated processes in place to detect and block unauthorized changes to software and hardware?

[ ]  Yes | [ ]  No

1. Does the institution conduct regular hardware and software vulnerability scans and testing to identify security control gaps in client, server, and network infrastructure?

[ ]  Yes | [ ]  No

1. Is the Data center access restricted by physical controls?

[ ]  Yes | [ ]  No

**Thank you for completing the survey.**

# **REFERENCES**

1. Definitions are adapted from international organizations such as ICCR and NIST [↑](#footnote-ref-1)
2. The World Bank General Principles on Credit Reporting (2011) acknowledges the importance of credit reporting systems as the foundation for robust and competitive credit markets. CRS can also assist prudential regulation hence minimizing risk. [↑](#footnote-ref-2)
3. (E&Y, 2017). EY Insights on GRC cyber ecosystem. [http://www.ey.com/Publication/vwLUAssets/cyber\_ecosystem/$FILE/EY-Insights\_on\_GRC\_Cyber\_ecosystem.pdf](http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/%24FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf) [↑](#endnote-ref-1)
4. Almansi, A. and Ferrari, A. (2017). Financial Sector’s cybersecurity: Regulations and Supervision. World Bank (September, 2017) [↑](#endnote-ref-2)
5. IBM (2017). *Security trends in the financial services sector*. IBM X-Force Research. IOSCO (2016). *Cyber Security in Securities Markets 􀈂 An International Perspective*. International Organization of Securities Commissions. [↑](#endnote-ref-3)
6. <https://www.newnettechnologies.com/equifax-profits-drop-27-percent-following-data-breach.html> [↑](#endnote-ref-4)
7. Equifax experienced a data breach between May and July 2017, as a result of a website application vulnerability. The breach which was disclosed in September 2017, exposed sensitive customer information for up to 143 million customers. [↑](#endnote-ref-5)
8. Following the Equifax breach which exposed personal data of more than 147 million people, there was a number of interventions by US Congress, the Consumer Financial Protection Bureau and Federal Trade Commission. [↑](#footnote-ref-3)
9. <https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2017/09/18/ny-proposes-regulating-credit-reporting-agencies/?slreturn=20180417120511>

<https://www.acainternational.org/news/new-york-issues-cybersecurity-regulation-for-credit-reporting-agencies> [↑](#endnote-ref-6)
10. World Bank (2011) General Principles on Credit Reporting [↑](#endnote-ref-7)
11. E&Y (2017) defines a cyber ecosystem as a complex community of interacting devices, networks, people and organizations, and the environment of processes and technologies supporting these interactions. [↑](#footnote-ref-4)
12. <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-in-2018-and-2019-looking-back-and-moving-forward.html> [↑](#endnote-ref-8)
13. World Bank (2019). Disruptive Technologies in the Credit Information Sharing Industry:Developments and Implications [↑](#endnote-ref-9)
14. Kaspersky (2019) CYBERTHREATS TO FINANCIAL INSTITUTIONS 2019: OVERVIEW AND PREDICTIONS, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27083106/Financial-cyber-threat-predictions-for-2019.pdf> [↑](#endnote-ref-10)
15. <https://www.wired.com/story/equifax-breach-no-excuse/> [↑](#endnote-ref-11)
16. Haksar V (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, WP/18/143, July 2018 [↑](#endnote-ref-12)
17. <https://www.wired.com/story/equifax-breach-no-excuse/> [↑](#endnote-ref-13)
18. Crowd strike Global Threat Report 2019 Adversary tradecraft and importance of speed [↑](#endnote-ref-14)
19. Equifax experienced a data breach between May and July 2017, as a result of a website application vulnerability. The breach which was disclosed in September 2017, exposed sensitive customer information for up to 143 million customers. [↑](#endnote-ref-15)
20. <https://www.newnettechnologies.com/equifax-profits-drop-27-percent-following-data-breach.html> [↑](#endnote-ref-16)
21. <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-in-2018-and-2019-looking-back-and-moving-forward.html> [↑](#endnote-ref-17)
22. OECD (2017), “Types of cyber incidents and losses”, in Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. [↑](#endnote-ref-18)
23. ibid. [↑](#endnote-ref-19)
24. NIST Special Publication 800-53 [↑](#footnote-ref-5)
25. Asia-Pacific Economic Cooperation Privacy Framework [↑](#footnote-ref-6)
26. Organization for Economic Cooperation and Development - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [↑](#footnote-ref-7)
27. Payment Card Industry Data Security Standard [↑](#footnote-ref-8)
28. Service Organization Controls Report [↑](#footnote-ref-9)
29. G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR. <https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf> [↑](#endnote-ref-20)