the law will materialize on a 50% basis in 2021 and fully starting in the financial year of 2022.

Furthermore, the aforementioned law decouples the use of tax losses DTAs, resulting from the hedge structure from the institution's future profitability until December 31, 2022, which, according to the principles of international recommendations, allows these DTAs not to be deducted from regulatory capital.

This last provision largely matches Resolution 4,680, of July 31, 2018, which had its term extended by Resolution 4,784, of March 18, 2020, thus allowing, until the end of 2021, the aforementioned DTAs not to be deducted from regulatory capital.

2.3.4 Conclusion

With the enactment of Law 14,031, in July 28, 2020, the tax asymmetry between investment abroad and hedge instruments was eliminated, reducing not only the financial and the liquidity costs and the impact on the hedge instruments market, but, mainly, avoiding that major oscillations arising from the depreciation of the brazilian currency against foreign currencies result in risk to stability, by compromising liquidity from banks more than necessary, result in the weakening of the capital, due to the constitution of DTAs and potentially bring volatility to hedge markets by pro-cyclical divestment decision movements of FIs in the midst of the crisis.

2.4 Information security: cyber incident response and recovery

2.4.1 Introduction

Cyber incidents bring daily concern to a financial institution's technology operation. The effects of these incidents include losses to customers and society, damage to the reputation of an institution, losses due to poorly executed operations, lawsuits for moral and material damages, impacts on other FIs, among other consequences, and may even escalate to a systemic crisis with impacts on financial system stability.

Thus, it is important to answer the question: what is the degree of SFN resilience to cyber incidents that can threaten financial stability? To answer this question,

it is desirable to use a cybersecurity framework that systematizes and enables the assessment of the various activities necessary for organizations to adequately deal with cyber risk.

In this sense, it is worth considering some cyber security frameworks that consolidate the good practices verified in the industry and provide tools for organizations to plan the acquisition of cyber incident management capabilities.

One of the advantages of using a reference framework is to employ an industry standard, facilitating comparison with other organizations, communication with suppliers and the establishment of objective goals in the implementation of best practices. Among the most well-known frameworks are Payment Cards Industry Data Security Standard (PCI DSS),[144] ISO 27001 and supplementary guides (ISO 27017 and ISO 27032),[145] Critical Security Controls (CIS)[146] and Framework for Improving Critical Infrastructure Security (NIST).[147]

No framework is absolute. Each one will have its own specificities (life cycle and evolution, among other aspects) and will be better suited to certain sectors or activities. The PCI framework, for example, establishes security practices for handling credit and debit card information. The most important thing is that companies evaluate the different existing options and adopt procedures and controls in an organized manner, in line with their business models and with their inherent cyber risks.

The comparison between SFN regulation and industry frameworks is an important exercise in identifying possible opportunities for improving the current regulatory framework. At the same time, the verification of the practices effectively implemented by the FIs guides the development of specific actions by the BCB, aimed at improving the controls adopted by the institutions to deal with cyber incidents. These aspects will be explored in the following sections.

144 https://www.pcisecuritystandards.org/
145 https://www.iso.org
146 https://www.cisecurity.org/
147 https://www.nist.gov/

2.4.2 The functions of the NIST cybersecurity framework

The cybersecurity framework developed by NIST[148] has consolidated itself as one of the references regarding cyber incident response and recovery, especially in the financial sector. The practices and objectives established in the NIST framework are divided into five functions.[149]

1. **Identify:** concentrates the practices for organizing and identifying assets, resources and information existing in a business environment, and for mapping risk exposure.

2. **Protect:** addresses corporate access control and the protection and security of data and assets, with the objective of cyber securing the business environment and its surrounding. It can be considered as a preventive phase of the institution's cyber security.

3. **Detect:** concentrates the practices that allow the identification of possible violations, monitoring the logs and taking care of the intrusion detection procedures of the networks and devices.

4. **Respond:** consolidates the response practices to be applied by institutions after an incident is detected, understanding the incident, correcting the vulnerability and proceeding to recovery.

5. **Recover:** gathers recovery procedures, dealing with planning, disaster recovery and backup plans.

Considering that the NIST framework is aimed at acquiring capacities to deal with cyber incidents and has a widespread application in the financial sector, it becomes a good reference to demonstrate the scope of the regulatory framework in force in the SFN on in this matter.

2.4.3 SFN Regulatory Framework and Supervisory Practices

The SFN regulation has a series of provisions that addresses issues present in the functions of NIST, although their references are not organized as established in the cybersecurity framework. As an example, some of these references can be illustrated considering the most

148 https://www.nist.gov/cyberframework
149 https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf

Table 2.4.3.1 – List of regulatory provisions versus functions of the NIST framework

Function	Resolution CMN 4.658 and Circular 3.909 (Cybersecurity Policy)	Resolution CMN 4.557 and Resolution CMN 2.554 (Risk Management and Internal Controls)	GPS
Identifiy	· Sharing relevant incident information. · Establishment of the objectives of the cybersecurity policy and definition of guidelines to be considered in the identification of relevant services of data processing and storage, and cloud computing. · Vulnerability detection tests.	· Definition of risk appetite. · Identification of critical business processes and potential evaluation effects resulting from the interruption of these processes. · Continuous evaluation of the different risks associated with the activities of the institution. · Periodic security testing of information systems.	· Existence of an information governance system. · Alignment between security strategy and business strategy. · Implementation of vulnerability analysis.
Protect	· Implementation of mechanisms for dissemination of cybersecurity culture. · Senior management commitment to continuous improvement of procedures related to cybersecurity. · Dissemination and training. · Implementation of security controls - encryption, information leak prevention, protection against malicious software, among others. · Access control implementation. · Security measures for transmission and data storage. · Segregation of data and access controls to protect customer information. · Development of initiatives for sharing information about relevant incidents.	· Establishment of strategies to ensure continuity of activities and limit losses arising the interruption of critical business processes. · Implementation of information protection and security mechanisms with objective to **preventing**, detecting and reducing vulnerability to digital attacks.	· Implementation of mechanisms for dissemination of risk and security cultures. · Establishment of security system information. · Establishment of policies: data and information classification, cyber, among others. · Segregation of IT environments. · Implementation of audit track. · Implementation of mechanisms of physical and logical security.
Detect	· Controls for intrusion prevention and **detection**. · Handling of information on incidents occurred in service providers.	· Information protection and security mechanisms aiming to prevent, **detect and reduce vulnerability** to digital attacks.	· Monitoring and attack prevention.
Respond	· Establishment of Incident Response Plans. · Reporting to the BCB on occurrence of relevant incidents. · Analysis of the root-cause and impact of incidents. · Mitigation of the effect of relevant incidents.		· Incident handling.
Recover	· In line with actions aimed at continuity business: execution of procedures in case of interruption of contracted relevant services, setting recovery time for restart or normalization of interrupted relevant activities or services.	· Establishment of continuity plans for restart and recover the activities.	· Establishment of business continuity plans.

relevant rules in relation to the topic (Resolution CMN 4,658, of April 26, 2,018, and Circular 3,909, of August 16, 2018; Resolution CMN 4,557, of 23 February 2,017, and Resolution CMN 2,554, of September 24, 1998) and the Supervisory Practices Guide (GPS) – Table 2.4.3.1.[150]

Although the table presented is not exhaustive, it is possible to verify the functions of the NIST framework in the different regulatory or supervisory instruments, either in the risk management structure, in the cybersecurity policy or in the expectations presented in the GPS.

It is worth emphasizing that the digitalization of financial services causes changes in the institutions' risk profile, culminating in increased exposure to technological risks. Thus, institutions must identify and assess risks considering this new context and develop adequate capacities for identification, protection, detection, response and recovery.

2.4.4 Implementation of practices, procedures and controls by the Supervised Entities

At the beginning of this year, the BCB consolidated an information survey (base date April 2020) targeted to FIs and payment institutions in order to establish an overview of the implementation stage of the cyber security policy and other provisions of Resolution CMN 4,658, of 26 April 2018, and Circular 3,909, of September 18, 2018. In addition, institutions were able to declare which typical cyber and information security controls they have already implemented or plan to implement.

Based on the results of the survey, it is possible to have a perspective of the level of preparedness of the institutions of the different groups / prudential segments to deal with cyber incidents. It is worth remembering that the data presented in the survey provide an aggregate perspective on the implementation of security controls; however, the real need for a certain control will depend on the characteristics of the business models of each financial institution and its respective operational profile, which will condition the real exposure to cyber risk and the consequent need for mitigation controls.

150 Guia de Práticas da Supervisão – Gestão do Risco de TI: https://www3.bcb.gov.br/gmn/visualizacao/listarDocumentosManualVinculadoPublico.do?method=pesquisarManualVinculadoPublico&idManualVinculado=2&idManual=1

As can be seen, larger and more complex institutions (institutions in the S1 and S2 prudential segments) have more consolidated security procedures and controls. The percentage of S3 institutions that implement the set of controls is similar to the group of payment institutions. The operational characteristics and the dependence on digital channels indicate the need for significant investments in security controls by these last two groups (Table 2.4.4.1).

A smaller percentage of smaller institutions (segments S4 and S5) has implemented the security controls considered in the survey. However, it is possible to verify some very opportune movements of these institutions, such as the structuring of security operation centers (SOC), secure application development and the execution of vulnerability analyzes.

From the perspective of the functions provided in the NIST framework, it turns out that SFN entities have better proficiency in "protection" and "recovery" functions. Considering the group of smaller and less complex entities (segments S4 and S5), there is a great opportunity for improving the functions to "identify", "detect" and "respond", mainly in the case of institutions that have a relevant dependence on digital channels for the operationalization of their businesses.

Considering specifically the need to improve the functions "identify" and "detect", it is worth highlighting the importance of information sharing on cyber incidents among market participants. This information is decisive for the timely identification of potential weaknesses, as well as for fine-tuning capabilities aimed at detecting threats. Effective information sharing is fundamental for the improvement of these functions in the financial system.

Another finding of the research is the incipient use of tools to deal with advanced threats (anti-APT – Advanced Persistent Threats). The increase in the complexity of the attacks will certainly demand the use of increasingly modern controls and tools for detection and response, always aiming at reducing the time between the moment when an incident is detected and the moment when an effective response is fully implemented. However, considering the survey data, there is an important lag in the use of this type of tool by institutions, notably S2 institutions.

Table 2.4.4.1 – Percentage of institutions that declared to implement IS controls, grouped by NIST functions

Function	Practices / Procedures / Information Security Controls	S1	S2	S3	S4	S5	Credit Union (System)	Payment Institutions
Identify	Vulnerability analysis (IT environment)	100%	100%	89%	53%	57%	67%	85%
	Pentest - Penetration Testing	100%	100%	86%	42%	33%	67%	85%
	Vulnerability analysis (IT systems)	100%	100%	81%	42%	59%	67%	85%
	Evaluation of security controls prior to contracting relevant services	100%	83%	92%	68%	60%	33%	46%
	Red Teaming	83%	50%	38%	10%	2%	0%	62%
Protect	Protection against malicious software (antivirus, antimalware, others)	100%	100%	100%	94%	83%	83%	92%
	Backup of data and information	100%	100%	97%	92%	79%	100%	100%
	Computer network segmentation / segregation of environments	100%	100%	95%	75%	61%	83%	85%
	Management of cryptographic keys and digital certificates	100%	100%	89%	57%	56%	83%	69%
	Logical Access Management	100%	83%	97%	76%	58%	100%	92%
	Cryptography	100%	83%	86%	56%	54%	100%	77%
	MDM - Mobile Device Management	100%	83%	76%	25%	5%	33%	54%
	Patch Management	83%	100%	89%	68%	49%	83%	85%
	Secure systems development	83%	100%	51%	33%	51%	50%	69%
	Password vault	67%	67%	73%	33%	11%	50%	46%
	Network Access Control (NAC)	67%	33%	49%	41%	46%	50%	62%
	Web Application Firewall (WAF)	50%	67%	62%	52%	29%	83%	85%
Protect / Detect	Prevention of DDoS (Distributed Denial of Service) attacks	100%	83%	81%	60%	47%	100%	69%
	Data Loss Prevention - DLP	83%	50%	68%	32%	16%	33%	38%
	Anti-APT (APT - Advanced Persistent Threat)	83%	17%	51%	25%	10%	33%	31%
	Cloud Access Security Broker (CASB)	33%	17%	24%	11%	4%	17%	38%
Detect	Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)	100%	100%	95%	68%	47%	100%	69%
	Traceability mechanisms, including audit trails and log implementation	100%	100%	89%	74%	55%	83%	85%
	Log correlator / Security Information and Event Management (SIEM)	100%	67%	65%	26%	7%	33%	69%
Detect / Respond	Cyber incident management	100%	100%	76%	72%	63%	33%	77%
	Security Operations Center (SOC)	100%	67%	68%	29%	27%	33%	54%
Respond	Mitigation of impact of relevant incidents	100%	67%	73%	63%	54%	50%	77%
Respond / Recover	Establishment of procedures to be followed in case of interruption of relevant services	67%	67%	51%	45%	51%	33%	54%
Recover	Procedures for reporting crisis situations to the BCB	100%	100%	81%	62%	54%	67%	62%
	Definition of RTO (Return to Operation) for relevant activities or services	100%	100%	78%	72%	60%	67%	62%
	Definition of incident scenarios to be considered in business continuity tests	100%	83%	65%	64%	57%	67%	69%

Universe of surveyed institutions: 6 institutions in the S1 segment, 6 institutions in the S2 segment, 37 institutions in the S3 segment, 236 institutions in the S4 segment, 237 institutions in the S5 segment, 6 cooperative systems and 13 payment institutions.

Statistical annex

It is necessary to recognize the increasingly importance of IT service providers in structuring institutions' capacities to deal with incidents, whether providing specialized knowledge or supplying resources for the proper operationalization of services.

In the survey carried out by the BCB, information was also collected on the level of outsourcing of technology and information security activities, from hiring to complement internal teams to the full outsourcing of an activity. Likewise, the information was consolidated by making an association with the functions provided in the NIST framework (Table 2.4.4.2).

The percentage of institutions that have declared some level of outsourcing in information security activities clearly demonstrate an expressive level of outsourcing in this area in all NIST functions, from identification to recovery from cyber incidents. The results show the increasingly intense relationship between regulated (institutions authorized by the BCB), and unregulated (IT and IS service providers) segments, reinforcing the need for the implementation, by financial institutions, of adequate controls for the management of contracted services from third parties.

In this scenario, maintaining an SFN that is operationally resilient and prepared to deal with cyber incidents will require IT service providers to adopt information security standards and procedures equivalent to those that are demanded from regulated institutions.

2.4.5 Final considerations

The importance of the "cybersecurity" theme is expected to increase progressively in the coming years due to factors such as the growth of institution's dependence on IT resources and new technologies in the operationalization of businesses and the increase in the number and complexity of cyber-attacks directed at the financial sector. Considering this scenario, the improvements in financial regulation, as well as in the BCB's supervisory efforts, aimed to ensure the adoption of the best cybersecurity practices by the regulated institutions, focusing on the continuous improvement of security controls of all SFN actors.

Comparing with the NIST framework, it is possible to verify that the SFN regulation has provisions that cover the main functions of that framework, providing a

Table 2.4.4.2 – Percentage of institutions that declared some type of outsourcing of IT and / or IS activities

Função	Technology or information security activities	% of Entities that reported some type of service contracting						
		S1	S2	S3	S4	S5	Credit Unions (System)	Payment Institutions
Identify	Project management, including management of the technology master plan	50%	17%	43%	28%	36%	33%	46%
	Vulnerability analysis (systems)	67%	67%	78%	64%	68%	67%	46%
Protect	Deployment of systems in production environment	67%	67%	65%	54%	67%	33%	62%
	Database administration	67%	83%	59%	69%	76%	67%	46%
	Messaging systems administration	50%	50%	51%	52%	32%	67%	31%
	Server administration	50%	50%	57%	61%	72%	50%	46%
	Computer network administration	33%	67%	62%	57%	70%	50%	46%
	Management of communication channels / links	67%	67%	65%	57%	62%	83%	62%
	User support and service (Help desk / service desk)	100%	100%	86%	60%	58%	83%	62%
	User account administration	67%	50%	51%	40%	58%	67%	46%
	Administration of user accounts with privileged access	50%	33%	38%	38%	38%	67%	46%
	Administration of third-party user accounts	50%	33%	46%	39%	36%	67%	46%
	Administration of digital certificates	50%	17%	35%	31%	32%	17%	38%
	Administration of security tools, such as firewalls, IDS / IPS, WAF, among others	50%	50%	65%	64%	71%	50%	62%
Detect	Monitoring and operation of the production environment	67%	83%	57%	58%	68%	50%	54%
	Batch control and execution	33%	67%	57%	38%	48%	33%	38%
Detect/Respond	Security Operations Center (SOC)	33%	50%	65%	33%	42%	33%	38%
Respond	Incident management - 1st level	67%	100%	73%	46%	55%	50%	46%
	Incident management - 2nd level	83%	67%	76%	49%	56%	67%	46%
	Incident management - 3rd level	100%	50%	73%	56%	57%	67%	38%
Recover	Backup management	50%	67%	57%	58%	71%	50%	38%
	Management of business continuity plans	17%	17%	22%	26%	27%	33%	15%

Statistical annex

regulatory environment compatible with the challenges imposed by the digital evolution of SFN. Thus, institutions are expected to implement controls and continuously improve their cyber defenses to deal with cyber incidents, mitigating their risk exposure.

The data from the survey carried out by the BCB indicates that it is necessary to improve information sharing on cyber incidents among SFN participants in order to improve the functions of identifying and detecting, enabling institutions to better understand the environment in which they operate, to know the most common cyber-attacks and to map their potential weaknesses in technology assets. This information is essential for the establishment of adequate defense systems.

The growing provision of information technology (IT) and cybersecurity services by non-regulated third-party companies stands out as a growing challenge to the governance of FIs and payment institutions. The progressive migration of an institution's IT operations to "cloud computing" solutions represents this phenomenon.

Therefore, the maintenance of SFN's operational and cyber resilience will also depend on the adequacy of security controls of these service providers and the BCB will act permanently with the supervised entities in order to ensure a sound operation.

2.5 Operational risk in Covid-19 pandemic times

The pandemic has impacted and continues to significantly impact financial and payment systems. Entities of these systems, both in Brazil and in other countries, had to adapt to a new reality imposed by measures of social distancing, aiming at preserving the provision of financial services to their clients.

Therefore, it is worth understanding how institutions of the National Financial System (SFN) faced the challenges arising from the health crisis and how they are preparing to operate in an environment that, despite the end of social distancing measures, will be quite different from pre-pandemic times.