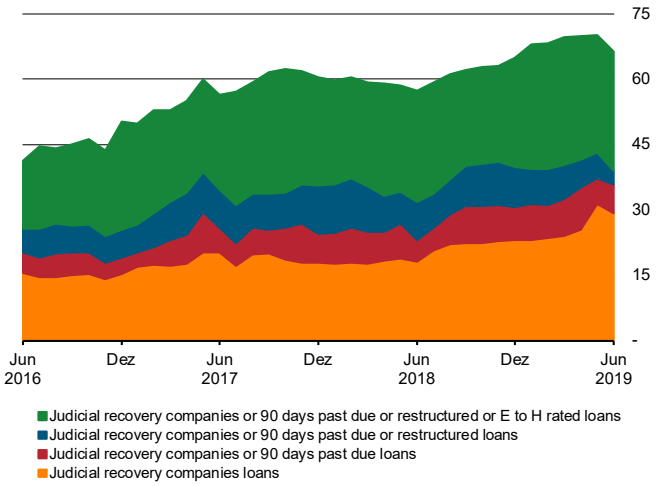
Chart 2.4.6 – Problem assets
Large companies



Statistical annex

2.5 Cyber and operational resilience

2.5.1 National Financial System digital transformation

One of the main features of the National Financial System (SFN) is the intense use of information technology (IT) in the provision of financial products and services, optimization of operational processes and improvement of financial institutions' distribution channels. In recent years, investments in information and communication technologies (ICT) have remained at a high level, fostering an accelerated process of digital transformation, including the development of new IT-enabled business models.

In this context, it is important to highlight the increasingly relevant role of ICT service providers,[104] especially in providing data processing and storage services, including cloud computing services. The contracting of these providers allowed cost reductions to financial institutions and promoted the establishment of a beneficial environment for technological innovation.

Digital transformation is not limited to the context of the SFN, but it is a phenomenon verified in many jurisdictions. Topics such as fintechs[105] and cyber risks are constantly on the agenda of international bodies focused on discussions on financial system regulation and supervision, resulting in studies and publications[106] on the potential impact of digital transformation and technological innovation on the stability of financial systems.

Considering the SFN and the Brazilian Payments System (SPB), regulatory improvements are constantly being made, balancing the promotion of innovation and development of new products and services, and the establishment of rules and safeguards to ensure the safe and soundness of the financial system. Good examples are the legislation and resulting regulation on Payment Schemes and Payment Institutions, which defined the roles and responsibilities of the different types of participants (e.g., payment services providers, payment

104 Based on the current regulatory framework, services provided by cross-border establishments of international groups should be considered as outsourced services.

105 Fintechs: in this context, firms that provide IT-enabled innovative financial products and services.

106 For example, "Sound Practices: implications of fintech developments for banks and bank supervisors" (https://www.bis.org/bcbs/publ/d431.htm), published by the Basel Committee of Banking Supervision.

scheme settlors and payment institutions) and provided new dynamics to the payment system.

Moreover, the Banco Central do Brasil (BCB) recognizes the relevance of technological innovations for the establishment of a more competitive, efficient and inclusive financial system, presenting a set of initiatives for the safe development of technological innovations in the SFN in its work agenda – Agenda BC#. These initiatives include the implementation of Open Banking[107] and the development of an Instant Payments Ecosystem,[108] which are clear stimuli for the development of new financial products and services.

Technological innovation is also in the work agenda of other financial system regulators, such as Securities and Exchange Commission of Brazil (CVM), as well as agencies of other sectors of the Brazilian economy. For instance, the Ministry of Industry, Foreign Trade and Services is leading the Industry 4.0[109] Agenda and initiatives have been developed to improve the regulations in the fields of Internet of Things – IoT.[110]

However, the digital transformation of the Brazilian economy is followed by growing concerns related to the associated risks. Regarding the SFN, the establishment of more distributed processes contributes to increase the interconnectivity between institutions. In these processes, institutions with different roles and responsibilities interact with each other to provide services and share information and data, thus requiring supervisors' scrutiny, given that:

i) a financial institution will hardly be able to operationalize a business process from end to end, i.e., it will certainly depend on other institutions and companies (providers) to support the delivery of value to its clients. Given the increasing interconnectivity, operational disruptions will have a potentially greater impact. In other words, failures in one institution are likely to affect the operations of others;

ii) the digitalization of business and increasingly information flow between institutions will pose challenges in terms information security and cyber risk;

107 Communiqué 33,455, of April 24, 2019.
108 Communiqué 32,927, of December 21, 2018, and Communiqué 34,085, of August 28, 2019.
109 Available at: http://www.industria40.gov.br/.
110 Decree 9,854, of June 25, 2019, established the National Internet of Things Plan.

iii) the focus on developing innovative business models is not always accompanied by the adoption of effective internal controls and risk management measures.

2.5.2 The pursuit of a resilient financial system

Accelerated digital transformation, greater dependence on ICT service providers and greater interconnectivity between entities result in increased exposure of financial institutions and the financial system to operational risk, cyber risk and discontinuity risk. As mentioned in the October 2018 Financial Stability Report (FSR), supervisors have growing concerns about cyber incidents and operational failures that, depending on their complexity and coverage, have the potential to trigger an operational disruption of the financial system, potentially impacting the financial stability.

Recognizing these risks, the National Monetary Council (CMN) and the BCB published regulations[111] aiming at increasing the resilience of financial and payment markets. These regulations require supervised entities[112] to implement a cyber-security policy, provide for contracting of relevant services provided by ICT providers, such as cloud computing services, by supervised entities and require supervised entities' business continuity plans (BCP) covers scenarios considering cyber incidents and major operational failures.

Regarding the establishment of business continuity scenarios, it is worth highlighting the efforts made by financial institutions in the development of scenarios. Based on a recent survey,[113] financial institutions reported considering the following scenarios in their BCP.

The survey shows that almost all institutions consider scenarios of unavailability of IT resources in their

Table 2.5.2.1 – Percentage of institutions by segment that consider the different types of incident scenarios in their continuity tests

	Segmentation – Groups	
Scenario	S1 + S2	S3 + S4 + S5
Unavailability of IT resources	100%	66%
Information leakage	73%	29%
Data integrity issues	45%	26%
Electronic fraud	27%	23%
Other scenarios	64%	24%

Statistical annex

111 Regulations that provides for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing: Resolution 4,658, of April 26, 2018, to be observed by financial institutions and Circular 3,909, of August 16, 2018, to be observed by payment institutions. Regulation that provides for business continuity management: Resolution 4,557, of February 23, 2017.

112 Supervised entities includes banks, financial institutions, payment institutions and other institutions licensed by the BCB.

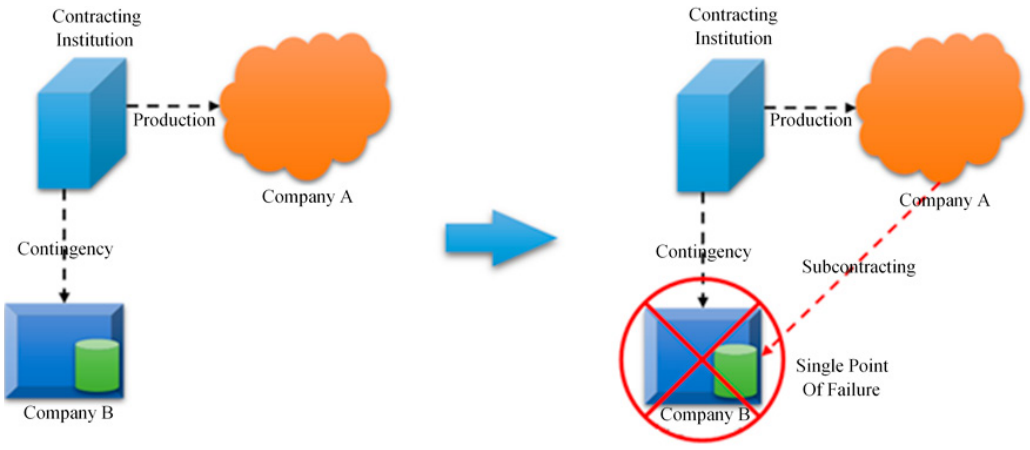
113 Until September 25, 2019, the survey consolidated information submitted by: 6 institutions from segment S1, 5 institutions from segment S2, 37 institutions from segment S3, 128 institutions from segment S4 and 171 institutions from segment S5, considering information on segmentation of prudential conglomerates and independent institutions retrieved from IF.Data (database: June 2019).

testing. In addition, the coverage of other scenarios is also significant, especially for more complex institutions (segment 1 and segment 2), indicating that financial institutions are constantly improving their BCP.

Regarding concerns about the increasing dependence of supervised entities on ICT service providers, two regulatory instruments have been defined aiming at the SFN resilience: i) supervised entities should communicate the BCB on the contracting of relevant ICT services, allowing the supervisor to preventively act on the occurrence of incidents with these relevant ICT providers; ii) the establishment of minimum contractual requirements, including the contractual provision for the supervised entity to be notified when the provider outsources relevant services, allowing the supervised entity do assess if the subcontracting has impact on its cyber risk exposure or its BCP.

For example, consider a financial institution that contracted Company A to provide its ICT production infrastructure and Company B to provide its ICT contingency infrastructure. If Company A outsources its operations to Company B, the financial institution should review its BCP, as illustrated in the figure below.

Figure 2.5.2.1 - Example of the risk arising from subcontracting by the service provider



In addition, the established regulatory framework provides for the establishment of procedures and controls to prevent and to respond to cyber incidents. The preventive approach includes the implementation of controls and information sharing on cyber incidents. The table below shows a perspective on the current stage of implementation of security procedures and controls by financial institutions, based on a recent survey.

Table 2.5.2.2 – Percentage of institutions by segment that reported implementing some of the different types of cyber security control or procedures

Security practices/ Procedures/Controls	Segmentation – Groups S1 + S2	S3 + S4 + S5
Vulnerability assessment – IT systems	100%	61%
Malware protection	100%	89%
Pentest	100%	51%
Logical access management	91%	73%
Anti-DDoS	91%	61%
Secure software development	91%	47%
Security operations center	82%	39%
Data loss prevention	73%	31%

Statistical annex

Although the assessment of the adequacy of security controls depends on different variables, such as the level of utilization of digital channels and the level of outsourcing of IT solutions, the provided information shows that the institutions' investments on implementing security controls are relevant.

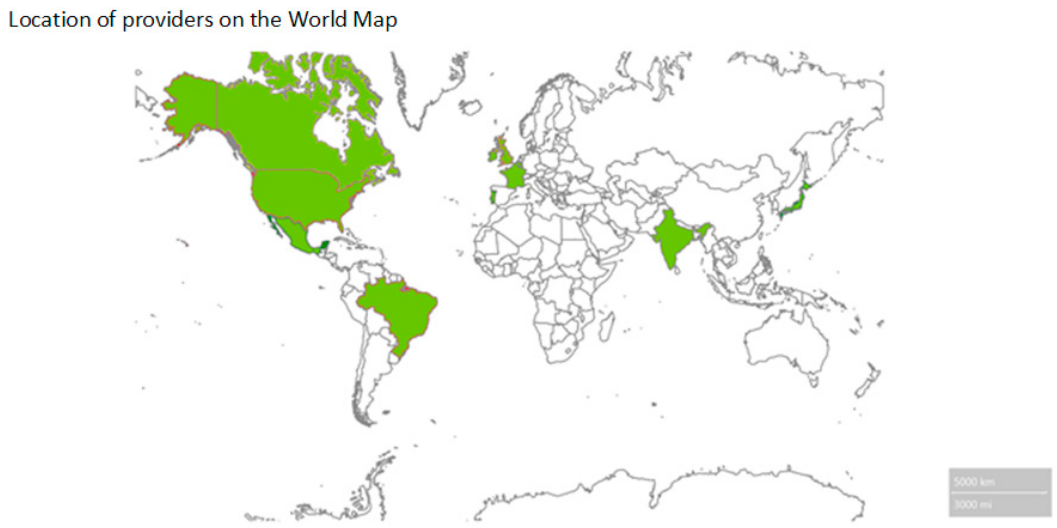
From the responsive approach perspective, it is worth noting the implementation of routines, procedures and controls to respond to incidents and the procedures to mitigate their effects, and the timely communication to the BCB on the occurrence of incidents that lead to crises.

2.5.3 Challenges for regulators/supervisors

As previously mentioned a more digital and interconnected financial system poses challenges not only to supervised entities but also to regulators/supervisors. The provision of services in other jurisdictions highlights the challenges regarding the remediation of operational and cyber incidents that may impact cross-border establishments.

The figure below shows the location of relevant ICT services contracted by financial institutions to support their operations, based on communications to the BCB. Although the majority of these services are provided in Brazil, some services are already provided in other countries (coloured in green). The increased utilization of cloud computing services will probably contribute to greater dependence on services provided abroad.

Figure 2.5.3.1 – Illustration of countries where ICT contracted services are provided, as reported by financial institutions to the BCB



Considering the soundness of the SFN, another existent challenge is the adequate identification of critical services. As stated in documents[114] published by international groups, services classified as relevant by financial institutions could be different from the services classified as relevant from a financial stability perspective.

These challenges will require the establishment of actions for the effective SFN resilience, as follows:

i) the identification and mapping of the SFN critical functions and the interconnectivity between the different entities of the financial system;

ii) the impact assessment of operational disruptions caused by operational and cyber incidents;

iii) the coordination of SFN entities aiming at the establishment of integrated and coordinated BCP that are effective to ensure the continuity of SFN critical functions;

iv) the establishment of operational and cyber resilience actions coordinated with other national agencies and regulators; and

v) the cooperation with regulators/supervisors from other jurisdictions to establish crisis management measures to mitigate the operational and cyber crises that may impact cross-border establishments.

2.5.4 BCB work agenda for SFN's operational resilience

Aware of the digitization process of financial systems and associated challenges, the BCB strengthened its actions for improving operational and cyber resilience of the SFN in recent years. As of 2012, when Brazil was preparing to host international sporting events (Soccer World Cup and Olympic Games), which typically increase the cyber risk exposure of sponsoring financial institutions, the BCB started developing information security assessment of the largest and more complex banks. As of 2017 and 2018, an important milestone was achieved with the issuance of regulations that established the basis for the implementation of policies and management of operation risk and cyber security.

114 FSB: Guidance on Identification of Critical Functions and Critical Shared Services, July 16, 2013, page 6.

Despite these relevant achievements, structuring an operationally resilient financial system requires a continuous work agenda. In line with this mindset, the BCB work agenda – Agenda BC#, presents the strategic initiative "Cyber risk supervision", which includes in its main deliverables: constant dissemination of risk culture to supervised entities; the mapping of relevant ICT providers; the consolidation of BCB supervisory procedures to monitor the response and recovery of relevant operational incidents that occur in supervised entities; and, from a macro prudential perspective, the improvements in BCB procedures to remedy operational crises that may pose a risk to SFN stability.

This initiative also includes development of studies focused on identifying indicators to map the SFN cyber risk, based on the diagnostics of the main critical systems and the interconnectivity between entities. These ongoing actions will potentially improve the BCB's situational awareness as well as support the implementation of response mechanisms to mitigate the escalation of incidents to systemic crises.

From a structural perspective, BCB is continuously working to improve its organizational structure to respond to the challenges posed by the increasing cyber and operational risks. For instance, the BCB Supervision Area incorporated the oversight of financial market infrastructures (FMI) and a new unit – Technological Information and Cyber Security Office (ITSEC), was created to coordinate the discussions on technology and information security within the agency.

It is also important to mention the coordination between the BCB and other agencies in establishing measures to mitigate cyber risk. For example, the participation with other SFN representatives in the "*Exercício Guardião Cibernético*",[115] organized annually by the Ministry of Defense. In this cyber exercise, BCB coordinates SFN-related actions, collaborating in the definition of table top simulation scenarios and discussions of sectorial actions focused for crisis management, thus contributing to the management of systemic cyber risk.

Finally, it is important to highlight BCB's work in implementing the National Information Security Policy in line with Institutional Security Office's directives, participating in international groups focused on cyber and operational resilience and improving information sharing with supervisors from other jurisdictions.

115 The October 2018 Financial Stability Report contains additional information on the "*Exercício Guardião Cibernético*".

2.5.5 Conclusions

Financial stability depends on the establishment of a resilient financial system that can absorb shocks caused by operational and cyber incidents that have potential to disruption critical functions.

Digital transformation provides relevant benefits to society by democratizing access to financial services and increasing competition, enabling the reduction of operations costs. On the other hand, the increased complexity of business models and increased exposure to cybersecurity and discontinuity risks are challenging factors that should be addressed through the coordination of SFN institutions.

All stakeholders, especially systemic institutions, should acquire the necessary crisis management capabilities in an ongoing effort to preserve the customer confidence on financial products and services, which is the foundation for SFN and SPB stability.

The Agenda BC#'s initiative "Cyber risk supervision" highlights the relevance of the topic and the extent of BCB's actions.

2.6 Savings deposits in the context of SBPE – Reserve requirement as an instrument to manage assets and liabilities mismatch in the housing credit market

Funds raised from savings deposits by entities that integrate the Brazilian System of Savings and Loans (SBPE) represent an important funding source for housing credit operations. According to Resolution CMN 4,676 of 2018, 65% of that savings deposits modality should be applied in housing credit operations, while, according to Circular BCB 3,093 of 2002, 20% should be deposited in BCB to meet reserve requirements. Remaining funds are available for treasury management by financial institutions.

The remuneration of savings deposits follows a rule that depends on the level of the Selic rate. When this rate is above 8.5% *p.a.*, savings deposits are remunerated at