APRIL 2019

Financial Sector Cybersecurity Requirements in the Asia-Pacific Region

AUTHORS
William A. Carter
William D. Crumpler

A Report of the CSIS TECHNOLOGY POLICY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2019

Financial Sector Cybersecurity Requirements in the Asia-Pacific Region

AUTHORS
William A. Carter
William D. Crumpler

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by the generous support of Standard Chartered and by general support to the CSIS Technology Policy Program.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Contents

Executive Summary

As the threat of cyberattacks has risen in recent years, financial institutions (FIs) and regulators have taken a range of steps to strengthen the security and resilience of the financial system to cyber threats. In the Asia-Pacific region (APAC), regulators have introduced a raft of new regulations and controls to bolster the resilience of FIs in their jurisdictions. While greater attention to—and engagement on—these issues is important, the development of new regulatory regimes across APAC has created challenges for multinational FIs and regulators, and could hinder the growth of the financial services and fintech industries within the region.

We reviewed the cybersecurity requirements impacting the financial industry in five key jurisdictions, including the largest regional financial centers and consumer markets in APAC: Singapore, Hong Kong, Japan, China, and India. Through a combination of open-source research and on-the-ground interviews—with regulators; local, regional, and global FIs; policymakers; technology experts; and academics—we sought to understand the range of requirements and approaches from different regulators across the APAC region, and the ways in which they impact cyber risks to the regional financial system.

Across the region there is growing focus on cyber risk, with particular emphasis on resilience and business continuity management to protect against systemic risk. Many financial regulators across the region are stressing risk-based regulatory frameworks, penetration testing requirements for vulnerability assessment, and the "people" and "process" elements of cybersecurity. Information sharing is another key priority for many APAC regulators, inspired by the success of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States.

On one hand, we found that many APAC financial regulators have drawn from a common set of international models in establishing their cybersecurity frameworks, including the U.S. National Institute of Standards and Technology (NIST), the Bank of England (CBEST), and the U.S. Federal Financial Examinations Council (FFIEC). Many also utilize common sets of international standards in assessing security and compliance, including ISACA COBIT and the ISO/IEC 27000 series.

On the other hand, some countries and regulators have implemented these requirements very differently, and there is a wide range of sophistication, capacity, and attention to cyber risks among different APAC regulators and FIs. Some jurisdictions, such as Singapore

and Hong Kong, have relatively mature cyber regimes and have developed in-house talent to oversee and manage cybersecurity. Others have comparatively nascent cyber regimes and are still working to develop their capacity to understand and regulate cyber risk for FIs. Some have highly granular and prescriptive controls and requirements, while others utilize more light-touch, risk-based frameworks based on international standards and extensive consultation with industry.

FIs are also facing a growing challenge from evolving data protection regimes in APAC countries, which in some cases threaten to create new obstacles for cross-border data transfer. As new data protection schemes like China's Cyber Security Law and India's proposed Personal Data Protection Bill have proliferated, firms are finding themselves facing stringent new data localization rules and ill-defined restrictions on cross-border data transfers. These requirements greatly complicate the operation of multinational FIs, and could force them to fragment their networks into a patchwork of segregated national systems.

While regional policymakers and regulators are increasingly focused on cyber risks, each is focused narrowly on cyber risks affecting their specific jurisdictions and customers. This makes it hard for them to see and manage the overall threat landscape facing multinational FIs, as well as the regional financial system as a whole. Little coordination is taking place between regulatory regimes in different countries, leading to a growing patchwork of often redundant—and occasionally conflicting—requirements across jurisdictions.

In a region as economically and financially integrated as APAC, inconsistencies and redundancies between regulatory regimes can create challenges for multinational firms and risks to systemic stability. The narrow view of regulators who focus on their own jurisdictions and citizens can create an overlapping and inefficient patchwork of requirements that makes it difficult for multinational firms to prioritize their global crown jewels and allocate resources to their core security needs. Exhaustive and prescriptive control lists and self-assessments, many of which are highly redundant across jurisdictions, can also drain talent, resources, and attention away from operational cybersecurity and toward compliance, hindering the development of a dynamic fintech industry in the region.

At best, this situation leads to costly inefficiencies and prevents regulators from understanding the real threat landscape of the institutions they oversee. At worst, these redundancies can create additional security vulnerabilities. For instance, redundant requirements for penetration tests in production environments may inadvertently disrupt or degrade bank services or expose customer data, which introduces significant risks for FIs.

Harmonizing regulators' approaches to cybersecurity regulation in the region could help reduce systemic risks, improve regulatory efficiency, and make it easier for FIs across APAC to grow. It could also help address the growing workforce shortage of cyber talent. Currently, jurisdictions face a persistent challenge in accessing qualified cyber auditors, examiners, and testers. Reducing redundant compliance requirements would free up cybersecurity professionals to take on more critical operational security and oversight roles at FIs and regulators, and common regulatory frameworks would allow these professionals to more easily support operations across multiple jurisdictions.

This will not be easy and will require sustained engagement on multiple levels. It will necessitate working with a broader swath of agencies than just dedicated financial regulators. Critical infrastructure regulators and data protection authorities must also be part of the conversation, as well as policymakers seeking legislative solutions to address cyber threats. In many cases, these requirements can be more disruptive than sector-specific regulations. For example, restrictions on data flows or data localization requirements can make it difficult to implement certain security measures like network monitoring or move operations to the cloud.

A combination of bilateral and multilateral negotiations; cooperation in regional fora; and global efforts coordinated with U.S., UK, and EU financial regulators will be necessary to achieve lasting and meaningful progress. At the regional level, regulators and FIs should utilize existing mechanisms through organizations like the Asia-Pacific Economic Cooperation (APEC) to push for greater integration and harmonization. Globally, countries should continue to engage through venues like the G20 and the Bank of International Settlements (BIS).

Cyber threats are a transnational issue and will require a transnational response, particularly in highly integrated regions like APAC. Strengthening the security and resiliency of financial networks across the region will require looking at FIs from an enterprise perspective and understanding the cyber risks they face from the perspective of defenders, not the narrow lens of national borders. This will require principles-based approaches that allow for the wide range of business models and capacities of FIs and regulators across the region, and consolidated auditing, examination, and testing procedures to ensure that regulators have an accurate picture of the risks and controls at institutions under their care. Ultimately, regulators' goals must be to ensure that strong security and resilience, not redundant compliance, is the focus for FIs.

> *Cyber threats are a transnational issue and will require a transnational response.*

1 | Introduction

The growing prevalence and cost of cyberattacks is a key challenge for financial institutions, and the Asia Pacific region is an increasingly prominent target of malicious cyber activity and cybercrime. Companies in Asia lost more than $80 billion to cybercrime in 2015, significantly more than organizations in the United States or Europe.[1] The financial sector remains a leading target of cyberattacks, both for profit-seeking criminals and for nation-states seeking political leverage. The financial industry suffered more data breaches than any other sector in 2016,[2] with almost twice the cost per stolen record compared to other businesses.[3]

In recent years, a series of high-profile cyberattacks on financial institutions has highlighted the risk of cyber incidents for the financial sector, and spurred financial regulators to do more to promote cybersecurity and cyber resilience in the institutions they oversee. Across APAC, regulatory agencies have issued new regulations and controls to manage cyber risks to FIs and protect consumer data. FIs in the region have made significant cybersecurity investments, and the security posture of APAC banks has improved significantly.

However, obstacles have arisen due to the proliferation of regulations, standards frameworks, and inspection regimes in different APAC countries. As regulators in different countries work independently to address these challenges, there is a risk that divergent approaches by different regulators could raise challenges for multinational FIs and undermine the security of the region's deeply interconnected financial sector. Conflicting or redundant regulations and requirements across jurisdictions can raise compliance costs, as well as creating vulnerabilities and friction for multinational FIs in the region.

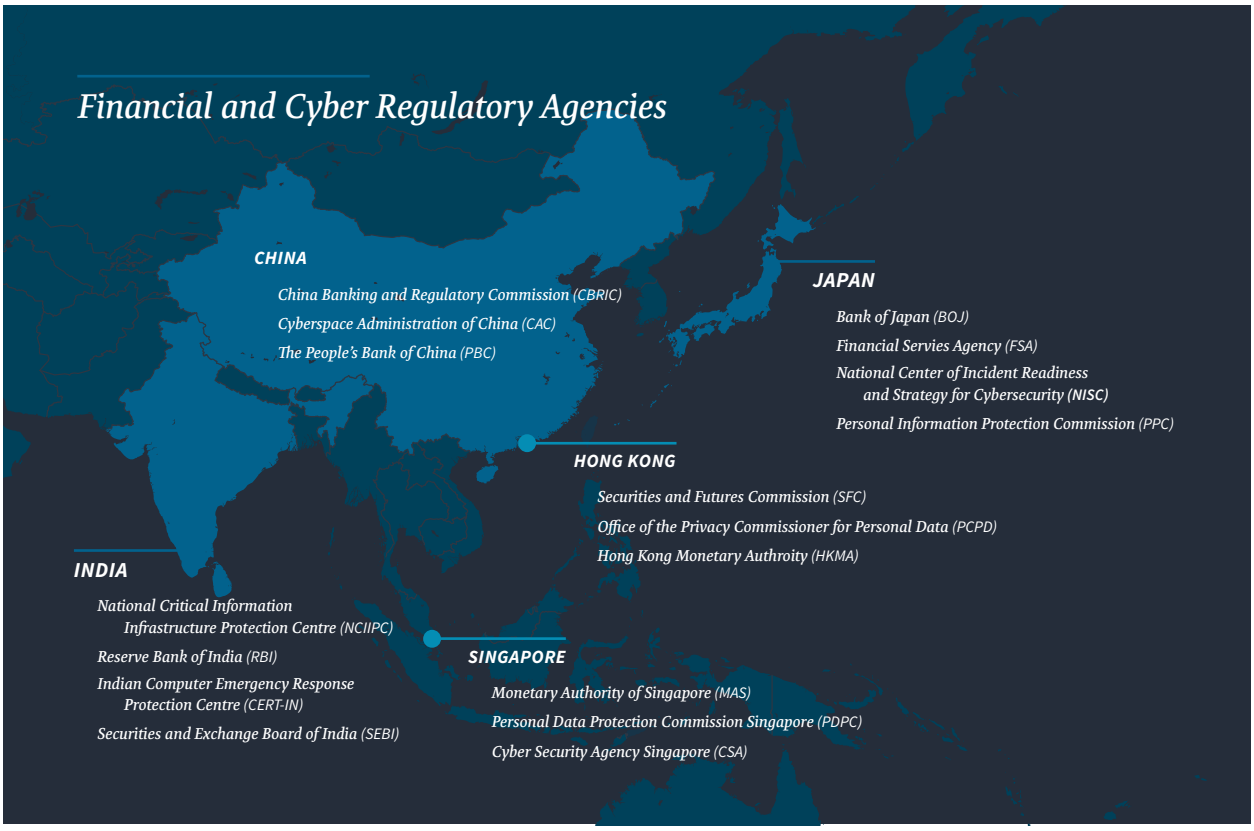
Harmonizing regulations and ensuring interoperability across the region would both reduce costs for multinational FIs and strengthen the security and resiliency of the regional financial system. The APAC economy and financial system are highly integrated, and a major cyberattack on a FI in one jurisdiction could lead to contagion across the

1. "Cyber attacks cost global businesses $300bn+," Grant Thornton, September 22, 2015, https://www.grant-thornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/.
2. "2017 Data Breach Investigations Report: 10th Edition," Verizon, July 26, 2017, http://www.verizonenterprise.com/verizoninsights-lab/dbir/2017/.
3. "2017 Cost of Data Breach Study," Ponemon Institute LLC, June 2017, https://www01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

region and around the world. Regulatory harmonization could also support innovation in the APAC financial services industry. Improving access to data and regional markets could boost the growth of the dynamic fintech sector in APAC financial centers, providing a significant boost to the regional economy.

> *Harmonizing regulations and ensuring interoperability across the region would both reduce costs for multinational FIs and strengthen the security and resiliency of the regional financial system.*

In this paper, we begin by reviewing the cybersecurity and data protection requirements for financial institutions in the leading financial centers and largest consumer markets in the APAC region: Singapore, Hong Kong, Japan, India, and China. This review was supported by a series of interviews with leading experts on the ground in each country, including regulators; representatives of leading national, regional and global financial institutions; auditors; legal and regulatory experts; and academics. We then discuss potential avenues for strengthening the security posture of FIs across the region, improving regional resiliency, and supporting global financial stability. Finally, we provide recommendations for how to strengthen the security and resilience of the APAC financial system against cyber threats.



2 | The Cybersecurity Regulatory Landscape for Financial Institutions in the APAC Region

Cyber regulations for FIs in the APAC region have evolved significantly in recent years. The growing drumbeat of cyberattacks on Asian FIs, as well as the results of simulations and exercises across the region, have demonstrated gaps in the security of the regional financial sector. This has put pressure on regulators to strengthen the security and resiliency of the regional financial system against cyberattacks.

Key Regional Trends and Themes

The overall trend in the APAC region is towards risk-based regulatory frameworks utilizing a combination of self-assessment and robust penetration testing to evaluate the effectiveness of controls. Many of the local experts we interviewed noted that regional regulators have relied heavily on Western regulatory and governance models in developing their own requirements.

The Bank of England's CBEST framework, in particular, serves as a key model for regulators in the region, as does the U.S. Federal Financial Institutions Examination Council's (FFIEC) cybersecurity examination program and the National Institute of Standards and Technology (NIST) Framework. While few regulators officially direct entities in their jurisdictions to comply with specific international standards, ISACA COBIT, the ISO/IEC 27000 series, and the Information Security Forum Standard of Good Practice for Information Security, among others, inform regulators' views and are used to guide compliance oversight.

There are a number of themes emphasized by regulators across the region. In particular, cyber resilience and business continuity management remain prime areas of focus for APAC regulators, and there is a growing emphasis on the importance of the people and process elements of cybersecurity preparedness and incident response. Governance and accountability are also key points for regulators. First and foremost, boards and senior management must be held accountable for the security posture of their institutions. Additionally, clear lines of responsibility and reporting must not only be outlined in strategic plans, but also demonstrated in simulations and red-teaming exercises.

Establishing scalable oversight and accountability models to cover small and medium enterprises (SMEs) and non-bank FIs as well as large multinational banks is also a recurring theme for Asian regulators, expanding the scope of new regulatory and oversight regimes to a broader cross-section of FIs in their jurisdictions. In Japan, for example, the three megabanks (Mitsubishi UFJ, Sumitomo Mitsui, and Mizuho) account for 18 percent of financial assets, but the Japanese financial sector is also comprised of hundreds of smaller Shinkin banks and credit unions that form an important part of the national financial system.[4] Regular self-assessments, independent audits, and certified penetration tests—combined with a risk-based schedule of periodic oversight inspections—are the primary means of expanding regulatory coverage to these smaller institutions with limited internal capacity.

Another regional priority is information sharing and incident reporting. The success of the Financial Sector Information Sharing and Analysis Center (FS-ISAC) in the United States has spurred regulators to establish information sharing mechanisms for FIs across APAC, and driven multinational FIs in the region to advocate for more robust threat intelligence sharing. All five countries we reviewed have created, or are creating information sharing organizations for regional financial institutions, from Financials ISAC Japan to CERT-Fin in India. Some interviewees did note that incentivizing robust sharing from sometimes-reluctant FIs, as well as ensuring the relevance and interoperability of shared information, posed continuing challenges. However, in APAC, as in other parts of the world, FIs are seen as generally ahead of other industries in implementing information sharing initiatives.

> *Cyber resilience and business continuity management remain prime areas of focus for APAC regulators.*

Finally, evolving data protection regimes in many APAC countries are creating new requirements and risks for financial institutions, particularly around their cross-border operations. New data protection schemes based on Europe's General Data Protection Regulation (GDPR) are proliferating, including stricter security requirements for customer data protection, data localization requirements, and controls on cross-border data flows. China's Cyber Security Law (CSL) imposes strict restrictions on cross-border data flows, and India's Draft Personal Data Protection Bill would enforce stringent new data localization rules. Singapore and Hong Kong have laws on the books that would allow data regulators to restrict cross-border data flows to countries not on "whitelists" of countries with adequate data protection regimes, but these rules are not currently in force. In Japan, the updated Act on Protection of Personal Information (APPI) has created a system of national adequacy assessments and a whitelist for cross-border data transfers, but also retains a number of other methods by which data may be transferred across borders.

In this section we outline the key cybersecurity regulations, laws, requirements, and oversight approaches for financial institutions in each of the five jurisdictions under consideration.

---

4. International Monetary Fund, *Japan: Financial System Stability Assessment* (Washington, DC: International Monetary Fund, 2017), https://www.imf.org/~/media/Files/Publications/CR/2017/cr17244.ashx.

Singapore

The cybersecurity posture of financial institutions in Singapore is primarily regulated by three entities: the Monetary Authority of Singapore (MAS), the Personal Data Protection Commission (PDPC), and the Cyber Security Agency of Singapore (CSA). As Singapore's central bank, the MAS serves as the primary regulatory authority for FIs and conducts reviews of cybersecurity controls and policies as a part of their wider mission of supervising the country's banks. Under the 2018 Cybersecurity Bill, the CSA has the responsibility to protect the country's critical information infrastructure—including financial institutions—by developing policies, codes of practice, and standards for infrastructure operators. Finally, the PDPC is responsible for enforcing the data protection regime established through the 2012 Personal Data Protection Act. These regulations include consent requirements for data collection and processing, standards for breach notification, and restrictions on the transmission of data out of the country.

MAS Regulatory Approach

The primary set of cybersecurity regulations covering financial institutions in Singapore is the MAS's Technology Risk Management Guidelines (TRMG) and associated circulars and notices. These lay out the cybersecurity controls and processes that FIs must implement to remain in compliance with the MAS.[5] The TRMG includes guidance on IT audits, risk management for outsourcing, encryption use, system reliability, user access controls, and more. Compliance is overseen by the MAS' Technology Risk Supervision (TRS) team, a 14-person group under the MAS Chief Cyber Security Officer, charged with overseeing the cybersecurity controls of over one thousand financial institutions.

In order to adequately cover all the FIs under their purview, the team relies on a risk-based supervisory approach that allows low-risk FIs to self-report TRMG compliance by answering a set of questions and submitting the results of external IT audits. For high-risk FIs, the team conducts annual visits, as well as quarterly interviews of information security leaders. Risk assessment is based on the use of the MAS' Comprehensive Risk Assessment Framework and Techniques (CRAFT), which measures four areas of control factors: risk management systems, operational management, internal audits, and compliance.[6] The MAS' IT inspectors assess FIs' cybersecurity controls based on an established list of cyber-related components for each of the four areas.

Although the MAS has the authority to levy penalties on FIs for non-compliance, they rarely do so except in the case of major data breaches. More commonly, enforcement takes the form of comments to the FIs on areas of improvement, or letters of warning. The MAS does not officially use any international standards to guide their compliance regime, though interviews indicate that members of the TRS team coordinate with fellow

---

5. Monetary Authority of Singapore, *Technology Risk Management Guidelines* (Singapore: Monetary Authority of Singapore, 2013), http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf.
6. Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices* (Basel, Switzerland: Financial Stability Board, 2017), http://www.fsb.org/wp-content/uploads/P131017-2.pdf.; Monetary Authority of Singapore, *MAS' Framework for Impact and Risk Assessment of Financial Institutions* (Singapore: Monetary Authority of Singapore, 2015), http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/MAS%20Framework%20for%20Impact%20and%20Risk%20Assessment%20of%20Financial%20Institutions.pdf.

regulators in international fora like the Information Technology Supervisors' Group (ITSG), the Committee on Payments and Market Infrastructures (CPMI), the Financial Stability Board (FSB), and the Basel Committee on Banking Supervision (BCBS).

In general, the MAS is seen as consulting more closely with industry than regulators in other jurisdictions. According to interviews with stakeholders in the financial sector, the MAS has been considering deferring to industry groups on guidelines and standards, with the Authority taking responsibility for setting strategic objectives and industry leading the development of standards.

Cybersecurity Audits and Penetration Testing

The TRMG require FIs to establish auditing procedures for all critical IT operations. Since audit guidelines focus on issues like access control and user privilege management, many other cyber risks are left unaddressed during external audits. This can create an expectations gap between the MAS and bank auditors, undermining the impact of the TRMG at reducing cyber risks.

The Guidelines do, however, contain a requirement for FIs to conduct regular vulnerability assessments, as well as annual penetration tests, on internet-facing systems. According to the TRMG, vulnerability assessments are to be undertaken using a combination of automated tools and manual techniques, and should consider common web vulnerabilities such as SQL injection and cross-site scripting for web-facing systems. Rather than mandating the frequency of vulnerability assessments, the MAS states that the schedule should be determined by the results of each FI's risk assessment.

Expectations for penetration tests are not specified within the TRMG itself, but in 2015 the Association of Banks of Singapore (ABS) released a set of Penetration Testing Guidelines to provide guidance on testing requirements, including test scope, methodology, scoring, and reporting.[7] These guidelines advise that tests should cover the critical risks identified in the Open Web Application Security Project (OWASP) Top Ten lists for web application and mobile security, as well as for the Common Weakness Enumeration and SANS Institute (CWE/SANS) Top 25 Most Dangerous Software Errors. The NIST technical guide to information security testing and assessment is listed as a reference within the Guidelines, along with several other testing frameworks and guidelines from entities like the Payment Card Industry (PCI) Security Standards Council, the Institute for Security and Open Methodologies (ISECOM), and the MITRE Corporation. Interviews indicate that penetration testers also utilize the CBEST framework during assessments. FIs are strongly encouraged by MAS to use penetration testers accredited by the ABS and the Council of Registered Ethical Security Testers (CREST), with Offensive Security, CREST, and the SANS Institute certifications recommended for assessors.

The Future of MAS Cybersecurity Regulations

At the 2016 Hong Kong Cybersecurity Summit, the MAS acknowledged that their current approach to penetration testing was inadequate and did not accurately reflect the true threats faced by financial institutions.[8] In an attempt to improve the quality of penetration

7. Association of Banks in Singapore, *Penetration Testing Guidelines for the Financial Industry in Singapore* (Singapore: Association of Banks in Singapore, July 31, 2015), https://abs.org.sg/docs/library/abs-pen-test-guidelines.pdf.
8. American Bankers Association, et al., *Regulatory-Mandated Third-Party Penetration Testing* (Washington, DC:

testing for Singapore's FIs, the MAS announced in November 2017 that it was partnering with the ABS to update the TRMG to include guidelines for red-teaming to better assess FIs' ability to respond to infiltration attempts.[9] This update to the TRMG is also slated to introduce basic cyber hygiene requirements for FIs, and establish principles for new technologies like open APIs, cloud services, and virtualization.[10]

The most recent update on this initiative was released in September 2018, when the MAS proposed turning six of the TRMG's security measures into legally-binding requirements for banks.[11] These measures—which include installing anti-virus software, strengthening user authentication, and installing security devices—are intended to form a baseline hygiene standard for bank cybersecurity.[12]

These reforms have been motivated in part by the feedback received by the MAS' international Cyber Security Advisory Panel (CSAP), which was convened to provide strategic guidance to the MAS on managing cybersecurity risks for Singapore's FIs.[13] The members of the CSAP, including executives from major FIs and experts in the field of cybersecurity, will likely play a large role in providing direction for these reforms, as will cybersecurity experts in nations like Israel, the United States, and Estonia, where Singapore has recently been conducting "study trips" to better understand how to organize and manage cybersecurity.

Cybersecurity Bill of 2018

On February 5, 2018, Singapore's Cybersecurity Bill was passed into law.[14] The Bill created the post of Commissioner of Cybersecurity, a position held by the chief of the Cyber Security Agency of Singapore (CSA) to oversee and ensure cybersecurity for critical information infrastructure (CII). The Commissioner has the authority to designate which information infrastructure is considered CII and regulate owners through the establishment of cybersecurity codes of practice and standards of performance. Under the Bill, owners of CII—including financial institutions—must conduct cybersecurity risk assessments annually, conduct cybersecurity audits every two years, report all significant cybersecurity incidents to the Commissioner, and comply with all other directives and codes of practice issued by the office.

American Bankers Association et al., July 7, 2016), http://www.gfma.org/WorkArea/DownloadAsset.aspx?id=827.

9. Ravi Menon, "Singapore FinTech Journey 2.0" (remarks presented at the Singapore FinTech Festival, Singapore, November 14, 2017), http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2017/Singapore-FinTech-Journey-2.aspx.
10. Lim Cheng Khai, "Opening Address" (remarks presented at the Investment Management Association of Singapore's 5th Regulatory / Legal Roundup Forum, Singapore, February 9, 2018), http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/Investment-Management-Association-of-Singapore-5th-Regulatory-Legal-Roundup-Forum.aspx.
11. Claudia Chong, "MAS Proposes Legally Binding Cyber-Security Measures for All Singapore Financial Institutions," *Straits Times*, September 6, 2018, https://www.straitstimes.com/business/banking/mas-proposes-6-cyber-security-measures-all-singapore-financial-institutions-must.
12. Monetary Authority of Singapore, *MAS Consults on Measures to Strengthen Cyber Resilience of Financial Institutions* (Singapore: Monetary Authority of Singapore, September 6, 2018), http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-consults-on-measures-to-strengthen-cyber-resilience-of-financial-institutions.aspx.
13. Monetary Authority of Singapore, *MAS Sets Up International Advisory Panel for Cyber Security* (Singapore: Monetary Authority of Singapore, September 20, 2017), http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-Sets-Up-International-Advisory-Panel-for-Cyber-Security.aspx.
14. Parliament of Singapore, *Cybersecurity Act 2018*, No. 9 of 2018, February 5, 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/.

Responding to a public consultation of the draft version of the Cybersecurity Bill, the CSA clarified that the Commissioner and sector-specific Assistant Commissioners (including a senior officer appointed from the MAS for the finance sector[15]) would work closely with regulators to streamline and harmonize their sectoral regulations, codes of practice, and standards.[16] The CSA also committed to referencing internationally-recognized policies and standards where applicable when developing codes of practice and standards of performance. To prepare CII owners for the Bill's implementation, the CSA has developed a Cybersecurity Legislation Initialization Programme for Sector Leads (CLIPS) to clarify the roles and responsibilities of sector regulators and CII owners, including harmonizing policies and streamlining audits and incident reporting.[17]

During his closing speech for the Second Reading on Cybersecurity Bill 2018, Dr. Yaacob Ibrahim, Minister for Communications and Information, clarified that the CSA would not create a national framework for CII cybersecurity audits out of fear of creating "audit fatigue."[18] Instead, the CSA would rely on existing sector-specific audit regimes to ensure the cybersecurity measures were in place, though the CSA would still provide audit guidance and track outcomes. The result of this approach will likely be a reliance on existing MAS audit processes, albeit with greater oversight by the CSA.

Data Protection Regime

The data protection regime in Singapore is based on the Personal Data Protection Act (PDPA) of 2012, which governs the collection and use of personal data by private organizations and their data intermediaries.[19] Personal data is defined by the PDPA as information which would allow for a natural person (non-corporation) to be identified by the data holder. All organizations collecting, using, or disclosing personal data in Singapore are covered by the PDPA, regardless of whether the organization in question is located or formed in Singapore.[20]

Under the PDPA, data users are required to obtain consent from individuals before collecting or using their data, to only use data for the purposes for which it was collected, to make reasonable security arrangements to protect personal data, and to allow individuals the right to access and correct data held on them. The PDPA also limits the transfer of personal data outside of Singapore, except in cases where the data holder can guarantee an equivalent level of protection. The PDPA is enforced by the Personal Data Protection Commission (PDPC), which is empowered to conduct

15. Yaacob Ibrahim, *Closing Speech for Second Reading on Cybersecurity Bill 2018* (remarks presented to the Ministry of Communications and Information, Singapore, February 5, 2018), https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/2/closing-speech-for-second-reading-on-cybersecurity-bill-2018-by-dr-yaacob-ibrahim-on-5-feb-2018.
16. Ministry of Communications and Information and the Cyber Security Agency of Singapore, *Report on Public Consultation on the Draft Cybersecurity Bill* (Singapore: Ministry of Communications and Information and the Cyber Security Agency of Singapore, November 13, 2017), https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/public_consultation_report.ashx?la=en.
17. Open Gov, "Singapore's Cybersecurity Bill Passed into Law, Minister Addresses Concerns," Open Gov, February 6, 2018, https://www.opengovasia.com/singapores-cybersecurity-bill-passed-into-law-minister-addresses-concerns/.
18. Ibrahim, *Closing Speech*.
19. Parliament of Singapore, *Personal Data Protection Act 2012*, No. 26 of 2012, October 15, 2012, https://sso.agc.gov.sg/Act/PDPA2012.
20. Aequitas Law LLP, "Data protection in Singapore: overview," Thomson Reuters, October 1, 2018, https://uk.practicallaw.thomsonreuters.com/6-579-6345.

investigations and levy penalties against businesses that fail to comply with the provisions of the PDPA.

According to the PDPC, the PDPA was developed based on principles drawn from the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, and was benchmarked against data protection regimes in jurisdictions like the European Union, the United Kingdom, Hong Kong, Canada, Australia, and New Zealand.[21] In its enforcement decisions, the PDPC has also revealed its international influences, referring to guidelines of the United Kingdom's Information Commissioner's Office, the Office of the Information & Privacy Commissioner for British Columbia (Canada), and the Code of Practice of the Hong Kong Office of the Privacy Commissioner for Personal Data.[22]

Since 2017, there have been a number of proposed changes to the PDPA. Most prominently, a draft of updates being considered by the PDPC would broaden exceptions for firms to obtain consent from individuals for the collection, use, and disclosure of their personal information, and impose a mandatory data breach notification requirement.[23]

Data Breach Notification

The PDPA does not impose any reporting or disclosure requirements on firms that suffer data breaches. However, the PDPC has made it clear that they are prepared to conduct investigations and enforce penalties against firms that suffer data breaches if the organization is found to have failed to implement effective security measures. Voluntary disclosure of a breach to the PDPC is seen as a mitigating factor for affected organizations in the event of a PDPC investigation.[24] The PDPC has also authored a voluntary Data Breach Guide for organizations, which recommends that breach victims notify data holders and the PDPC as soon as possible.[25]

In July 2017, the PDPC initiated a public consultation on proposed updates to the PDPA, which included a requirement that organizations notify affected individuals as well as the PDPC in situations where the breach is "likely to result in significant harm or impact to the individuals," or where the breach is of a "significant" scale.[26] Notably, this threshold for notification was raised compared to the language in the initial draft, which required notification whenever a breach posed any risk of impact or harm, or affected more than 500 individuals. The language was changed following a public consultation in

---

21. Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (Singapore: Personal Data Protection Commission, July 27, 2017), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthe-digitaleconomy270717f95e65c8844062038829ff000.pdf.
22. Rizwi Wun, "Data Protection and Cybersecurity in Singapore: 2017 So Far," Lexology, July 17, 2017, https://www.lexology.com/library/detail.aspx?g=639f90c8-71a2-4216-b2d3-018e289d1fd3.
23. Personal Data Protection Commission, *Public Consultation*.
24. "Personal Data Protection Breaches," Personal Data Protection Commission, February 18, 2018, https://www.pdpc.gov.sg/Organisations/Enforcement-Matters/Personal-Data-Protection-Breaches.
25. Personal Data Protection Commission, *Guide to Managing Data Breaches* (Singapore: Personal Data Protection Commission, May 8, 2015), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-managing-data-breaches-v1-0-(080515).pdf.
26. Personal Data Protection Commission, *Response to Feedback on The Public Consultation on Approaches to Managing Personal Data in the Digital Economy*, February 1, 2018, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf.

which respondents urged the PDPC to instead adopt a risk-based approach with a higher threshold for notification.

The proposed mandatory data breach notification seeks to bring Singapore's existing voluntary approach to data breach notification in line with international best practices, with the PDPC citing the examples of Australia, Canada, New Zealand, the European Union, the United Kingdom, and the United States in their public consultation.[27] In the event of a breach, firms would be allowed a 30-day assessment period to determine if the breach is eligible for reporting.[28] Following the conclusion of the assessment, companies would be required to notify the PDPC within 72 hours, and contact affected individuals as soon as practicable. Notification requirements would also expand to cover data intermediaries. The PDPC has made clear that the PDPA is meant to apply concurrently with breach notification requirements by sectoral regulators, but allowed that organizations may submit a notification to the PDPC in the same form as is used by their sectoral regulator.

The MAS has its own requirements for breach notification, requiring FIs to notify MAS no later than one hour after discovery of a data breach[29] (defined as a determination that the nature and magnitude of an IT incident meets the criteria set out in the Notice on Technology Risk Management[30]). A root-cause and analysis report is required within 14 days. No requirement exists for notifying data subjects.

Data Localization

One of the nine principal obligations under the PDPA is a limit on transferring personal data to any organization outside of Singapore unless they can ensure a standard of protection comparable to the protections outlined in the PDPA. If the data is to remain under the control of a Singaporean organization while being transferred out of the country, the PDPA simply requires that the organization ensure the protections of the PDPA do not lapse. If it is transferred to a third party, the recipient must be bound by legally enforceable obligations to provide a similar standard of protection.[31] Legally enforceable obligations include obligations imposed on the data recipient under any law, contract, or binding corporate rules in accordance with Regulation 10 of the Personal Data Protection Regulations 2014,[32] or any other legally binding instrument.[33]

To date, the PDPC has produced no whitelist of countries pre-approved for data transfer. However, in March 2018, Singapore signed on to APEC's Cross-Border Privacy Rules

---

27. Personal Data Protection Commission, *Public Consultation*.
28. Personal Data Protection Commission, *Response to Feedback*.
29. Monetary Authority of Singapore, *Instructions on Incident Notification and Reporting to MAS*, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Instructions%20on%20Incident%20Notification%20and%20Reporting%20to%20MAS.pdf.
30. Monetary Authority of Singapore, *Frequently Asked Questions: Notice on Technology Risk Management*, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/FAQs_Notice%20on%20TRM.pdf.
31. Lee Soo Chye, Jacqueline Teo, and Sheam Zenglin, "Data protection in Singapore," Thomson Reuters Practical Law, October 1, 2018, https://uk.practicallaw.thomsonreuters.com/6-579-6345?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1.
32. "Personal Data Protection Regulations 2014," Ministry of Communications and Information, July 2, 2014, https://sso.agc.gov.sg/SL/PDPA2012-S362-2014?DocDate=20140519.
33. Chye et al., "Data protection in Singapore."

(CBPR) and Privacy Recognition for Processors (PRP) frameworks.[34] By the end of the year, the PDPC is expected to launch a certification scheme that would allow the transfer of data between certified organizations in participating APEC economies.

Hong Kong

Cybersecurity requirements for the financial sector in Hong Kong are primarily overseen by the Hong Kong Monetary Authority (HKMA) and the Hong Kong Securities and Futures Commission (SFC). All financial institutions in Hong Kong are regulated by the HKMA, which is responsible for monitoring FIs for compliance with Hong Kong's Banking Ordinance. As part of its supervisory regime, the HKMA is empowered to issue non-statutory guidelines setting out its expectations for FIs.

The current cybersecurity regime in Hong Kong largely dates back to the 2015 Whole Industry Simulation Exercise (WISE), organized by the Hong Kong Financial Services Business Continuity Management Forum (HKFSBCM). The exercise, which simulated a systemic cyber incident in the Hong Kong banking sector, revealed some significant shortcomings in the cyber readiness of FIs relying on the HKMA's long-standing General Principles for Technology Risk Management, originally drafted in 2003.[35]

In response, the HKMA released a circular in September 2015 on Cyber Security Risk Management, highlighting the importance of cybersecurity for licensed FIs in Hong Kong.[36] The circular noted that FI boards and senior leadership are "expected to strengthen their oversight in those areas," including evaluating their cybersecurity controls against a "credible benchmark." Although the circular did not prescribe which benchmark should be used, it suggested that banks consider ISACA COBIT, the SANS Top 20 Critical Security Controls, the ISF Standard of Good Practice for Information Security, or the ISO/IEC 27000 series as possible benchmark standards.

HKMA Cybersecurity Fortification Initiative

In May 2016, the HKMA launched its Cybersecurity Fortification Initiative (CFI) to address the shortcomings identified in the 2015 WISE exercise and improve the resilience of Hong Kong FIs to cyber threats. The CFI has three parts: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Program (PDP), and the Cyber Intelligence Sharing Platform (CISP).[37]

The C-RAF is heavily based on the CBEST framework, featuring a two-part self-assessment and an intelligence-led cyberattack simulation test (iCAST). The self-assessment, based heavily on the FFIEC Cybersecurity Assessment Tool (CAT), as well as the NIST Framework and the BIS/IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, asks banks to evaluate the security of systems impacting Hong

34. Maki DePalo, "Singapore Joins the APEC CBPR and PRP," Alston & Bird, March 7, 2018, https://www.alston-privacy.com/singapore-joins-apec-cbpr-prp/.
35. Hong Kong Monetary Authority, *General Principles for Technology Risk Management*, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf.
36. Hong Kong Monetary Authority, *Cyber Security Risk Management*, September 15, 2015, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf.
37. Hong Kong Monetary Authority, *Cybersecurity Fortification Initiative*, December 21, 2016, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf.

Kong customers against a set of 366 controls, an approach that some interviewees considered overly granular and prescriptive. The C-RAF's iCAST component is based on the CBEST Cyber Resilience Testing Framework, and requires banks to undergo comprehensive penetration tests based on realistic threats. These tests must be conducted by certified examiners in production environments and are required to extend to the people and process elements of the FI's controls.

One of the biggest challenges of the C-RAF program is the cyber talent shortage. Due to a lack of qualified assessors, the HKMA announced it would adopt a phased approach to implementation of the C-RAF, with the first 30 institutions (all major retail banks, selected global banks, and a few other small institutions) completing the inherent risk and maturity assessments by the end of September 2017 and the iCAST by the end of June 2018. Incorporating feedback from the first phase, the second phase would cover all other institutions, who would be expected to complete the inherent risk and maturity assessments by the end of 2018.[38]

The CFI also created a professional development program (PDP) to address the talent gap. The PDP is a training and certification program intended to increase the supply of cybersecurity talent for Hong Kong financial institutions and regulators. At the end of 2016, the HKMA rolled out a new local certification scheme for cybersecurity professionals called the Certified Cyber Attack Simulation Professional (CCASP), which is supported by the Hong Kong Applied Science and Technology Research Institute (ASTRI), the Hong Kong Institute of Bankers (HKIB), and the Council of Registered Ethical Security Testers (CREST) International.[39] The certifications under CCASP were specifically designed to meet the HKMA's expectations for C-RAF and iCAST assessments, though the HKMA also provided a list of other professional certifications it considers equivalent, including ISACA certification for C-RAF assessors, and CREST, Global Information Assurance Certification (GIAC), or Offensive Security certifications for the iCAST.[40]

The third part of the CFI is the CISP, a mechanism for sharing threat intelligence between banks and enhancing collaboration on cyber resilience. The HKMA worked with the Hong Kong Association of Banks (HKAB) and ASTRI to stand up the platform, which was launched at the end of 2016. By September 2017, reports indicated that the platform was beginning to spur progress in the information sharing landscape within Hong Kong. However, trust concerns and lingering delays in getting banks to interface their own intelligence databases to the platform have left the CISP a work in progress. Nonetheless, the results so far have been positive enough for ASTRI to begin creating similar networks for Hong Kong's insurance and brokerage industries.[41]

---

38. Hong Kong Monetary Authority, *Implementation of Cyber Resilience Assessment Framework*, June 12, 2018, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180612e1.pdf.
39. "Certified Cyber Attack Simulation Professional (CCASP)," The Hong Kong Institute of Bankers, https://www.hkib.org/en/training-examinations/ccasp; "Cybersecurity Training," Hong Kong Applied Science and Technology Research Institute, https://www.astri.org/cybersecurity-training/.
40. Hong Kong Monetary Authority, "Cybersecurity Fortification Initiative."
41. Enoch Yiu, "Cybersecurity Platform to Expand to Hong Kong's Brokers and Insurers," *South China Morning Post*, June 5, 2017, https://www.scmp.com/business/companies/article/2096975/cybersecurity-platform-expand-hong-kongs-brokers-and-insurers.

HKMA Supervisory Regime

The HKMA exercises supervision over FIs' information systems through regular on-site examinations, off-site reviews, and prudential meetings.[42] Examinations are overseen by the HKMA's own team of specialists, who have expertise in cybersecurity and technology risk.[43] The HKMA takes a risk-based approach to compliance, requiring different benchmarks and review cycles for institutions with different risk profiles.[44] Off-site reviews represent the core of the HKMA's supervisory regime, and are based on the review of monthly assessments submitted by FIs, as well as the reports of external and internal auditors.[45] On-site examinations occur at least once every year for major locally incorporated institutions and once every four to five years for institutions incorporated overseas.[46]

On-site reviews generally focus on priority areas identified through the off-site review.[47] During the examination, the HKMA team will review policies and procedures and evaluate how they are being applied.[48] The team will also interview staff at various levels and conduct tests on information systems to follow up on cybersecurity audits and C-RAF vulnerability assessments. The HKMA also involves an external IT security consulting firm to assess the cybersecurity controls of financial market infrastructures based on the requirements of C-RAF.[49]

The HKMA's supervisory regime follows international practices as recommended by the Basel Committee on Banking Supervision[50] and the Financial Stability Board.[51] The HKMA has also committed[52] to complying with international regulatory standards on Financial Management Information Systems (FMIs), including the CPMI and International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructures.[53] Interviews with stakeholders in the financial sector indicate that the HKMA does not issue enforcement actions, but rather offers "observations" about improvements that banks should make.

Hong Kong Securities and Futures Commission

The SFC is responsible for regulating all financial trading services in Hong Kong, and includes requirements for electronic trading security controls in its code of conduct

---

42. "Regulatory & Supervisory Framework," Hong Kong Monetary Authority, June 12, 2018, https://www.hkma.gov.hk/eng/key-functions/banking-stability/banking-policy-and-supervision/regulatory-supervisory-framework.shtml.
43. Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices* (Basel, Switzerland: Financial Stability Board, 2017), http://www.fsb.org/wp-content/uploads/P131017-2.pdf.
44. Ibid., 77; Hong Kong Monetary Authority, *Cyber Security Risk Management*, September 15, 2015, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf.
45. "Oversight of Financial Market Infrastructures," Hong Kong Monetary Authority, https://www.hkma.gov.hk/eng/key-functions/banking-stability/oversight.shtml.
46. Hong Kong Monetary Authority, *Guide to Authorization, Chapter 3: The Legal and Supervisory Framework*, (Hong Kong, China: Hong Kong Monetary Authority, June 8, 2018), https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/guide-authorization/Chapter-3.pdf.
47. Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations*.
48. Hong Kong Monetary Authority, *Banking Supervision in Hong Kong* (Hong Kong, China: Hong Kong Monetary Authority, 2003), https://www.hkma.gov.hk/media/eng/publication-and-research/background-briefs/bank_sup/full_version_2003.pdf.
49. Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations*.
50. "Basel Committee on Banking Supervision (Basel Committee)," Hong Kong Monetary Authority, https://www.hkma.gov.hk/gdbook/eng/b/basel_com_bank_sv.shtml.
51. Hong Kong Monetary Authority, "Regulatory & Supervisory Framework."
52. Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations*.
53. Bank for International Settlements and OICU-IOSCO, *Principles for Financial Market Infrastructures* (Basel, Switzerland: Bank for International Settlements, 2012), https://www.bis.org/cpmi/publ/d101a.pdf.

for licensed brokers.[54] These requirements include controls on user authentication, mechanisms for intrusion detection, and regular reviews of risk management systems. The SFC has conducted cybersecurity reviews of internet trading platforms since 2014. It has also released circulars to licensed operators, warning of major risks and suggesting controls and procedures for improving security. In 2015, this process led the SFC to issue a circular requiring internet trading services to perform regular self-assessments of their internet trading systems, network infrastructure, and related policies.[55] These assessments are based on a checklist prepared and distributed by the SFC.

In October 2016, the SFC launched a review to assess the cybersecurity preparedness and compliance of brokers in Hong Kong.[56] The review included questionnaires for small and medium-sized brokers to assess cybersecurity controls, as well as on-site inspections of selected institutions to evaluate their cybersecurity controls. As part of the review, the SFC committed to benchmarking Hong Kong's regulatory requirements and market practices against other international financial services regulators and market practices.

In October 2017, the SFC issued a circular and associated Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, requiring all those engaged in internet trading to implement 20 baseline requirements to improve cybersecurity resilience and mitigate hacking risks.[57] The most significant of the new controls is the requirement that clients use two-factor authentication to access internet trading accounts. In addition, the Guidelines call for prompt client notification of account activity, the use of monitoring systems to detect unauthorized access, the use of strong encryption, and password protection. They further implement requirements for network management practices, incident reporting, and the management and supervision of personnel. Though the Guidelines do not have the force of law, both the SFC and HKMA have stated that the Guidelines would be incorporated into their ongoing compliance process, making them effectively mandatory for entities wishing to remain licensed within Hong Kong.[58]

Personal Data Protection

Hong Kong's data protection regulations are based on the 1995 Personal Data (Privacy) Ordinance, most recently amended in 2012.[59] The Ordinance contains six data protection

---

54. Securities and Futures Commission, *Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission*, 2017, https://www.sfc.hk/web/EN/assets/components/codes/files-current/web/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission.pdf.
55. "Circular to all Licensed Corporations on Internet Trading Internet Trading Self-Assessment Checklist," Securities and Futures Commission, June 11, 2015, https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=15EC34.
56. "SFC commences cybersecurity review on brokers' internet and mobile trading systems," Securities and Futures Commission, October 13, 2016, https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=16PR103.
57. Securities and Futures Commission, *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*, https://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf; "Implementation of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading," Securities and Futures Commission, October 27, 2017, https://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=17EC72.
58. Hong Kong Monetary Authority, *Security Controls for Internet Trading Services*, October 27, 2017, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20171027e1.pdf.
59. Legislative Council of the Hong Kong Special Administrative Region of the People's Republic of China, *Personal Data (Privacy) Ordinance*, Cap. 486, L.N. 343 of 1996, August 1, 1996, https://www.elegislation.gov.hk/hk/cap486.

principles (DPPs) governing entities responsible for handling personal data. These DPPs stipulate that data must be accurate, collected for a lawful purpose, used for the purpose for which it was collected, not kept for longer than necessary, safeguarded from misuse, and made accessible for data subjects to access.[60]

The enforcement of the Ordinance is overseen by the Office of the Privacy Commissioner for Personal Data, who has the power to issue codes of practice and guidelines in relation to the Ordinance, as well as undertake the investigation of breaches. The DPPs are not legally binding, but a failure to adhere to the principles is viewed highly unfavorably in cases where the Commissioner has to investigate a firm for a possible breach of the Ordinance. Hong Kong's Privacy Commissioner has observed a smaller than expected deterrent effect of the Ordinance in dealing with violations.[61]

The most recent modification to the Ordinance was its amendment in 2012, which greatly tightened restrictions on the use of personal data for direct marketing, requiring notification and consent for any related use of personal information.[62] No further major modifications are planned, although the Commissioner has stated that he is highly focused on the impact of the GDPR and other emerging data protection frameworks around the world.[63] Additionally, though no official movements have been made, a 2017 survey by APEC indicated that Hong Kong was actively considering joining the APEC CBPR.[64]

Breach Notification

Breach notification, while not required by the Ordinance, is required by the HKMA Circular on Customer Data Protection, issued on October 14, 2014.[65] According to the Circular, for serious privacy incidents with a large number of affected customers and a loss of sensitive customer data, institutions are expected to report the incident to the HKMA and affected customers as soon as practicable. Institutions are also strongly encouraged to report incidents to the Privacy Commissioner and furnish reasoning to the HKMA if they choose not to.

Cross-Border Data Transfers

Notably absent from the Personal Data (Privacy) Ordinance are any additional restrictions concerning sensitive data or the transfer of personal data outside of Hong Kong. The ordinance has always included a provision (section 33) regulating the export of personal

---

60. "The Ordinance at a Glance," Privacy Commissioner for Personal Data, https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.
61. Jeffie Lam, "Personal information more at risk than ever in age of big data, Hong Kong privacy watchdog head says," *South China Morning Post*, December 23, 2017, https://www.scmp.com/news/hong-kong/community/article/2125533/personal-information-more-risk-ever-age-big-data-hong-kong.
62. Nicholas Blackmore, "Data protection in Hong Kong: Overview," Thomas Reuters Practical Law, June 1, 2018, https://uk.practicallaw.thomsonreuters.com/9-505-7567?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1&comp=pluk.
63. Gabriela Kennedy and Karen H. F. Lee, "Data Security and Cybercrime in Hong Kong," Lexology, https://www.lexology.com/library/detail.aspx?g=686e9ff6-f89f-49ba-8829-710a73d2a0ab.
64. Bui Hang, Viet Nam E-Commerce and Information Technology Agency, Ministry of Industry and Trade, *Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs* (Asia-Pacific Economic Cooperation, 2017), https://www.apec.org/Publications/2017/01/Survey-on-the-Readiness-for-Joining-Cross-Border-Privacy-Rules-System---CBPRs.
65. Hong Kong Monetary Authority, "Consumer Data Protection," October 14, 2014, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf.

data from Hong Kong, but this provision has never been brought into force, and the Commissioner has indicated that this is unlikely to occur any time soon.[66] However, in a guidance document published in 2015, institutions are urged to voluntarily comply with the terms of section 33, in anticipation of their eventual implementation.[67]

If enacted, section 33 would outlaw all transfer of data out of Hong Kong except in the case of voluntary consent from the data subject, when the transfer was occurring to whitelisted jurisdictions as decided by the Privacy Commissioner, or if the data user has "reasonable grounds for believing that there is in force in that place any law which is substantially similar to… the Ordinance." [68] Currently, no jurisdictions have been officially whitelisted. However, in 2013, the Privacy Commissioner reported that he had carried out a survey of 50 jurisdictions to assess their suitability, though this list and the Commissioner's conclusions have not been made public.[69] The "substantially similar" provision only applies to jurisdictions that have not yet been assessed by the Commissioner, making it uncertain what standing a company would have to rely on this provision as the basis for a transfer given that no information has been publicly released about the Commissioner's assessments.[70]

In addition, entities may transfer data if they have taken "all reasonable precautions and exercised all due diligence to ensure that the personal data concerned is given equivalent protection to that provided for by the Ordinance." To meet this criteria, companies must either use one of the model data transfer clauses prepared by the Commissioner to form a legally-binding contract with the overseas entity, or use non-contractual oversight and auditing mechanisms to monitor for compliance.

According to the 2015 guidance, section 33 would apply not only in instances when data was deliberately transferred overseas, but also where an MNC stored personal data within Hong Kong while allowing access to employees outside of Hong Kong, as well as in instances where personal data would be stored in the cloud in a way that is accessible outside of Hong Kong.

Japan

Introduction/Overview

In Japan, the primary source of cybersecurity regulations for banks comes from the Japanese Financial Services Agency (JFSA), as set out in their guidelines for the

66. Kennedy and Lee, "Data Security and Cybercrime in Hong Kong."
67. Office of the Privacy Commissioner for Personal Data, "Guidance on Personal Data Protection in Cross-border Data Transfer," 2015, https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_cross-border_e.pdf.
68. "Data Protection Laws of The World," DLA Piper, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwjJx8qKp-raAhUPMd8KHdzBDp0QFghUMAU&url=https%3A%2F%2Fwww.dlapiperdataprotection.com%2Fsystem%2Fmodules%2Fza.co.heliosdesign.dla.lotw.data_protection%2Ffunctions%2Fhandbook.pdf%3Fcountry-1%3DHK&usg=AOvVaw39wdE9HaGyXf-H0gP24Tbea.
69. Office of the Privacy Commissioner for Personal Data, Hong Kong, *Report on the Work of the Office of the Privacy Commissioner for Personal Data (PCPD) in 2013*, LC Paper No.CB(2)790/13-14(01), January 28, 2014, http://www.legco.gov.hk/yr13-14/english/panels/ca/papers/cacb2-790-1-e.pdf.
70. Mark Parsons and Peter Colegate, "Hong Kong Privacy Commissioner Issues Guidance on Cross-Border Data Transfers," Hogan Lovells, January 2015, http://ehoganlovells.com/rv/ff001ca08e5b031041a96129654abb678a4b-b1e4.

supervision of major banks. These guidelines take a principles-based approach to cybersecurity controls, laying out expectations on areas ranging from network monitoring to vulnerability assessments. Banks are also required to submit to supervision by the Bank of Japan as part of their agreement as account holders, and work with the government's National Center of Incident Readiness and Strategy for Cybersecurity to comply with emerging controls on critical information infrastructure. Finally, Japanese FIs must comply with data protection provisions as set out in the Act on the Protection of Personal Information (APPI), which sets out restrictions on data collection, use, and international transfer as enforced by the Personal Information Protection Commission.

Japan Financial Services Agency

The JFSA serves as the principal regulator of banks in Japan, and has the authority to supervise banks as delegated by the Prime Minister. The JFSA is responsible for developing cybersecurity regulations for the institutions under its jurisdiction, and has established a separate division for cybersecurity staffed by 25 experts in IT risk monitoring in order to manage the review of institutions' security posture. According to the JFSA's most recent guidelines for the supervision of major banks, FIs are required to monitor information systems to detect intrusions, operate an intra-organization Computer Security Incident Response Team (CSIRT) for emergency response, participate in information gathering and sharing platforms, maintain a multi-layered defense to protect against attacks, evaluate security controls through vulnerability assessments and intrusion tests, create secure authentication systems for users, and take measures to mitigate damage in the case of a major incident.[71] The JFSA does not, however, have the authority to conduct audits or penetration tests. According to interviews with stakeholders with JFSA officers, the JFSA does not have specific technical requirements for FIs, but instead utilizes a principles-based approach based off the NIST Framework, ISO standards, and Center for Financial Industry Information Systems (FISC) security guidelines.

FISC is a nonprofit organization established in 1984 by the Ministry of Finance to conduct research on the technology, utilization, control, and security of information systems in the financial sector. FISC security guidelines detail recommended controls for FI computer systems, and include measures to detect and prevent unauthorized access to information systems, ensure proper management of hardware and software, and establish mechanisms to mitigate and recover from system failures.[72]

In 2018, FISC updated their guidelines for the first time since 2012. Though the new text has yet to be released, the updates will likely take into account the recommendations included in recent FISC reports, such as the June 2017 Report of the Council of Experts on FinTech in Financial Institutions,[73] and the February 2014 Report of the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions.[74] These reports

---

71. "主要行等監督上の評価項目," Japanese Financial Services Agency, June 2017, https://www.fsa.go.jp/common/law/guide/city/03c2.html.
72. FISC, "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions," June 2012, https://d0.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824.pdf.
73. The Center for Financial Industry Information Systems, *Report of the Council of Experts on FinTech in Financial Institutions* (Japan: The Center for Financial Industry Information Systems, 2017), https://www.fisc.or.jp/data/english/pdf/FISC_FinTech_Report_2017.pdf.
74. The Center for Financial Industry Information Systems, *Report of the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions* (Japan: The Center for Financial Industry Information Systems,

recommend adopting a risk-based approach to the application of the security guidelines, and expanding measures covering risks from outsourced services, DDoS attack defenses, vulnerability assessments, network monitoring, and major incident response procedures.

In their Strategic Directions and Priorities for 2018, the JFSA indicated that they would work to improve the capabilities of small and medium financial institutions through more inclusive industry-wide exercises (Delta Wall II) and encourage large financial institutions to utilize more sophisticated evaluation methods to further improve their resilience to cyber risks.[75]

Bank of Japan

Though it has no regulatory power to supervise banks,[76] the Bank of Japan (BoJ) is empowered to conduct on-site examinations and off-site monitoring to assess the conditions of financial institutions holding BoJ accounts, as set forth in the Bank of Japan Act.[77] As a part of this supervision regime, the BoJ assesses the operational risk management systems used by banks, including frameworks for IT and cybersecurity risk. In its latest examination policy, for instance, the BoJ announced its intention to review banks' cybersecurity management frameworks, determine the appropriateness of information collection and sharing, examine the effectiveness of measures to prevent cyber attacks, and assess the contingency plans and damage mitigation procedures in the event of a major incident.[78]

Regulation as Critical Information Infrastructure

FIs in Japan are also affected by recent developments in the regulation of critical information infrastructure (CII). In 2014, Japan passed the Basic Act on Cybersecurity, which strengthened the organization and authority of the government institutions responsible for overseeing cybersecurity for the nation.[79] As a result of the Act, the Information Security Policy Council was reorganized into a cabinet-level Cybersecurity Strategic Headquarters charged with coordinating cyber strategy, policy, and procedures. The Act strengthened the authorities of the HQ, allowing it to demand mandatory reports from other government bodies and issue formal recommendations to support Japan's Cybersecurity Strategy, which was issued soon afterwards in 2015.[80]

The HQ is led by a Chief Cabinet Secretary and also includes the foreign minister, the defense minister, the trade and economy minister, the internal affairs minister, the chairman of the National Public Safety commission, and others as appointed by the Prime Minister.

2014), https://www.fisc.or.jp/data/english/pdf/FISC_Report_February26_2014.pdf.
75. Financial Services Agency, *Strategic Directions and Priorities 2017-2018*, November 2017, https://www.fsa.go.jp/en/news/2018/2017StrategicDirectionsSummary-English.pdf.
76. Tatsu Katayama et al., "Banking regulation in Japan: Overview," Thomson Reuters, August 1, 2018, https://uk.practicallaw.thomsonreuters.com/w-007-5339?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.
77. National Diet of Japan, *Bank of Japan Act*, Act No. 89, June 17, 1997, http://www.japaneselawtranslation.go.jp/law/detail/?id=92&vm=02&re=01.
78. Bank of Japan, *On-Site Examination Policy for Fiscal 2018*, March 13, 2018, http://www.boj.or.jp/en/finsys/exam_monit/exampolicy/kpolicy18.pdf.
79. National Diet of Japan, *The Basic Act on Cybersecurity*, Act No. 104, November 12, 2014, http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760.
80. Tomoo Yamauchi, "Cybersecurity Strategy in Japan," (presented at the Third French Japanese Meeting on Cybersecurity, Tokyo, Japan, April 24, 2017), https://project.inria.fr/FranceJapanICST/files/2017/05/TYamauchi_presentation_2017.pdf.

Situated under the Cybersecurity Strategic Headquarters is the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which serves as the secretariat for the HQ. NISC is responsible for coordinating and planning new cybersecurity policies, monitoring government organizations, interfacing with international partners, and serving as the organizing agency in times of crisis.

NISC is also responsible for developing standards for information security in government agencies. Under the Cybersecurity Basic Act, it was given the authority to monitor compliance through third-party management audits and penetration testing.[81] However, NISC's authorities only extend to government agencies and government-affiliated entities, though they cooperate closely with ministries like the JFSA, which is responsible for regulating CII operators.

NISC has also been responsible for formulating new policies like the 2016 General Framework for Secured IoT Systems[82] and the 2017 Cybersecurity Policy for Critical Infrastructure Protection (4th Ed.).[83] The NISC Cybersecurity Policy for Critical Infrastructure Protection establishes a framework for cooperation between government and CII operators to improve cybersecurity protection. The Policy lays out voluntary measures to be undertaken by government agencies and CII operators to improve information sharing, risk management, and incident response. Much of the Policy centers around the application of the 2015 Guidelines for Establishing Safety Standards of CIIP, which encourages the adoption of a number of cybersecurity policies, including risk assessments, business continuity plans for information system failure, information handling policies, outsourcing risk management practices, and network monitoring.[84] Under the Policy, NISC commits to conducting a questionnaire survey and visiting CII operators every year to examine their cybersecurity measures and ascertain how the safety principles have been adopted among operators. NISC does not have enforcement powers, but instead uses these reviews as an opportunity to update its guidelines and advise CII operators on implementation.

The Policy also highlights NISC's responsibility to disseminate their Risk Assessment Guidelines for Mission Assurance to CII operators involved in preparations for the Olympic games in 2020.[85] Ahead of Tokyo 2020, NISC has been identifying essential service providers—about one hundred entities in both the public and private sector, representing domains ranging from telecoms to electricity, finance, weather forecasting, transit, and others—and requesting they perform security assessments.[86] Six assessments are planed prior to the games, covering security providers in Tokyo and nearby cities.

---

81. Cybersecurity Strategic Headquarters, "Common Standards for Information Security Measures for Government Agencies (FY2016)," August 31, 2016, https://www.nisc.go.jp/eng/pdf/Common%20Standards(FY2016).pdf.
82. National Center of Incident Readiness and Strategy for Cybersecurity, *General Framework for Secure IoT Systems*, August 26, 2016, https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.
83. Cybersecurity Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection* (April 18, 2017), https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf.
84. Cybersecurity Strategic Headquarters, *Guidelines for the Establishment of Safety Standards of CIIP*, May 25, 2015, https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v4.pdf.
85. National Center of Incident Readiness and Strategy for Cybersecurity, 2020 *年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況*, https://www.nisc.go.jp/conference/cs/dai11/pdf/11shiryou03.pdf.
86. Ko Ikai, "Cybersecurity for Tokyo 2020," June 2017, *National Center of Incident Readiness and Strategy for Cybersecurity*, https://www.oasis-open.org/events/sites/oasis-open.org.events/files/1-Speaker-Ko.pdf.

The risk assessments will form the basis of cybersecurity measures released by NISC to boost security prior to the games. The first assessment was completed in Spring 2017, and involved about 70 the essential service providers.

NISC is also reported to be working on setting up a national center to facilitate the sharing of threat data between government and CII operators.[87] Currently, information sharing for cyber threats is facilitated by the Financials Information Sharing and Analysis Center (ISAC) of Japan, the financial sector Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR), and the Cyber Security Information Sharing Partnership of Japan (J-CSIP), a public-private partnership overseen by the Information-Technology Promotion Agency (IPA).[88]

In June 2018, the Japanese government finalized an outline of its next cybersecurity strategy.[89] The strategy includes a strong emphasis on information sharing, commitments to expand special protections for critical infrastructure, and updates on the management of personal information.

Data Protection Regime

The management and protection of personal data in Japan is governed by the 2003 Act on the Protection of Personal Information (APPI).[90] Under the Act, entities undertaking the collection and processing of personal information must notify customers of the purpose of this data use. Data users are further prohibited from using that information beyond its initial purpose without obtaining the subject's consent, except in the case of certain limited exceptions. The Act also includes a broadly-stated obligation for companies to "take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data."

In July 2018, Japan and the European Union agreed to recognize each other's data protection regimes as adequate for the handling of personal data, allowing data to flow freely between companies in the two jurisdictions without additional checks.[91] In September, Japan's Personal Information Protection Commission (PPC) announced supplementary rules for data transferred from the European Union, tightening regulations in several areas to bring Japan's protections up to the level of the GDPR. The PPC is also involved in discussions to harmonize its regulations with the APEC CBPR and the UK government.

---

87. Aaron Tan, "How Japan is gearing up to secure the Tokyo Olympics," *ComputerWeekly*, July 31, 2017, https://www.computerweekly.com/news/450423606/How-Japan-is-gearing-up-to-secure-the-Tokyo-Olympics.
88. Melissa Hathaway, "Japan Cyber Readiness at A Glance," Potomac Institute, September, 2016, http://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS1.pdf; Mihoko Matsubara and Danielle Kriz, "Putting the METI Cyberthreat Information Sharing Recommendation Into Action in Japan," July 25, 2016, https://research-center.paloaltonetworks.com/2016/07/cso-putting-the-meti-cyberthreat-information-sharing-recommendation-into-action-in-japan/.
89. National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, June 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.
90. National Diet of Japan, *Act on the Protection of Personal Information*, Act No. 57, 2003, http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.
91. Michihiro Nishi, "Data Protection in Japan to Align With GDPR," Skadden, September 24, 2018, https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

Breach Notification

Breach notification is not mandated under the APPI, but PPC guidelines urge firms to alert both victims as well as the PPC as soon as possible as a matter of good practice. Interviews indicate that the guidelines are interpreted as mandatory by FIs, though institutions largely decide how they will comply. However, in the financial sector, breach notification is mandated by the Guidelines Targeting Financial Sectors Pertaining to the Protection of Personal Information, established by the PPC and JFSA.[92] These guidelines require FIs to immediately report any leakages of personal information to the supervisory authority and affected individuals, and promptly make a public announcement addressing the facts of the breach.[93] In addition, the Guidelines mandate that financial institutions implement procedures to protect personal data, including organizational, technical, and human safety control measures.

Cross-Border Data Transfer

In May 2017, an amendment to the APPI came into force, which among other updates introduced constraints on the transfer of personal data out of Japan. The amendment prohibits the transfer of personal data to third parties in a foreign country without the subject's prior consent, except in cases where the PPC has deemed the recipient country to have acceptable controls on data transfer, or where the data user has taken steps to ensure the same level of data protection as exists in Japan. To date, no country has been announced as covered by the PPC whitelist exemption. However, in April 2018 the PPC published draft guidelines relating to the adequacy findings for data transfers between Japan and Europe. If they come into force in their current form, subject to the European Union's adequacy decision, they will allow for the transfer of personal data between Japan and the European Economic Area.[94]

In the meantime, institutions within Japan are required to take reasonable safeguards to ensure that any data transferred out of the country is subject to an equivalent level of protection as exists in Japan. According to remarks by the Director of the PPC Secretariat, institutions with existing reasonable safeguards—like privacy policies or data protection terms in contracts—would likely be found compliant with the terms under the amended APPI.[95] In addition, the director noted that certification of compliance with the APEC CBPR, of which Japan is a part, would be taken as evidence of appropriate safeguards for the purpose of the APPI.

India

Introduction

In India, the cybersecurity of financial institutions is principally regulated by the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI). Banks are also

---

92. Japanese Financial Services Agency, *金融分野における個人情報保護に関するガイドライン*, February 2017, https://www.fsa.go.jp/common/law/kj-hogo-2/01.pdf.
93. Hitomi Iwase, Hiroko Shibata, and Mitsukuni Terada, "Data security and breach notification in Japan," Lexology, October 15, 2018, https://www.lexology.com/library/detail.aspx?g=dcfead6c-c9ef-4b59-8be9-8fd199926741.
94. Daisuke Tatsuno and Kensaku Takase, "Data Protection - Significant Developments on Adequacy Findings Between Japan And Europe," *Baker McKenzie*, May 2, 2018, http://www.bakerinform.com/home/2018/5/2/data-protection-significant-developments-on-adequacy-findings-between-japan-and-europe.
95. Harriet Pearson, Julie Brill, Mark Parsons, and Hiroto Imai, "Changes in Japan Privacy Law to Take Effect in Mid-2017; Key Regulator Provides Compliance Insights," Lexology, February 1, 2017, https://www.lexology.com/library/detail.aspx?g=efa0a2b0-b73e-456c-b4fa-26a268e9e751.

covered by critical infrastructure regulations as set by the National Critical Information Infrastructure Protection Centre (NCIIPC) and data protection regulations as set out in the country's 2000 IT Act. Guidance issued by RBI, SEBI, and NCIIPC require banks to adhere to certain standards of security, primarily based on ISO 27000, and to commit to regular vulnerability assessments, penetration tests, and information security audits. Compliance and enforcement of these regulations is inconsistent, however. Under the country's data protection framework, institutions are required to meet certain basic levels of security for their customers' data, and are restricted from transferring data out of the country absent equivalent protections for entities overseas. The government's proposed Protection of Personal Data Bill would enhance these protections, creating a GDPR-like regime which protects the individual rights of data subjects and imposes strict localization requirements on many types of personal data.

Reserve Bank of India

The Reserve Bank of India (RBI) is the principal entity responsible for formulating and enforcing cybersecurity regulations for Indian banks. Historically, the RBI has been responsible for developing guidelines on internet banking and digital records management, as well as frameworks for reporting internet banking fraud and managing outsourcing risks. Since 2015, the development and supervision of cybersecurity guidelines for banks has been the responsibility of the RBI's Cyber Security & IT Examination Cell (CSITE). The work of CSITE is supported by two entities: the RBI's Institute for Development and Research in Banking Technology (IDRBT) and the RBI's IT subsidiary, Reserve Bank Information Technology (ReBIT) Pvt. Ltd. The IDRBT is a research institute responsible for the development of best practices, such as the Cyber Security Checklist of July 2016[96] and the Cloud Security Framework of August 2013.[97] ReBIT is responsible for assisting the RBI in carrying out IT and IS audits, vulnerability assessments, and penetration tests.[98]

The current foundation of the RBI's regulatory scheme is their 2016 Cyber Security Framework in Banks, which details the necessary components of a comprehensive internal cybersecurity framework for banks and updates the RBI's 2011 Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds.[99] The Framework requires banks to put into place a board-approved cybersecurity policy covering, among other areas, the establishment of a security operations center (SOC), the completion of a risk assessment for critical systems, and the implementation of baseline cybersecurity and resilience requirements.

The baseline requirements laid out in the Framework include a wide range of security controls, from network monitoring to incident reporting, and require "professionally

---

96. Institute for Development and Research in Banking Technology, *Cyber Security Checklist* (Hyderabad, India: IDRBT,2016), http://www.idrbt.ac.in/assets/publications/Best%20Practices/CSCL_Final.pdf.
97. Institute for Development and Research in Banking Technology, *Cloud Cybersecurity Framework for Indian Banking Sector* (Hyderabad: IDRBT,2013), http://www.idrbt.ac.in/assets/publications/Best%20Practices/Cloud%20Security%20Framework%20(2013).pdf.
98. Ministry of Finance, "Press Release on the Report of the Working Group for Setting Up Computer Emergency Response Team in the Financial Sector," Press Release, https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.
99. Reserve Bank of India, *Cyber Security Framework in Banks*, June 2, 2016, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF.

qualified teams" to conduct "periodic" vulnerability assessment and penetration testing exercises. This requirement is not new, however, as banks have been expected to conduct regular vulnerability assessments and penetration tests, and report their findings on a quarterly basis to the RBI, since 2013.[100] The Framework also encourages banks to use red teams to identify vulnerabilities and business risks, but does not mandate their use. CSITE is responsible for monitoring compliance with the Framework.

In late 2017, ReBIT released their Cyber Security Maturity Model (CMM) to help guide Indian banks in the implementation of the RBI framework, and to help promote uniformity in standards adoption.[101] The CMM provides a tool for banks to conduct self-assessment of risks and evaluate the maturity of their security controls. The CMM is heavily based on the NIST Cybersecurity Framework, and is explicitly designed to be consistent with other international standards frameworks like COBIT 5.0 and ISO 27000.

In general, interviews with stakeholders indicate that the RBI is a highly prescriptive regulator, promulgating a large number of circulars containing very specific requirements. However, implementation is inconsistent and ad-hoc, and resource constraints have hampered the RBI's efforts to be more proactive in inspections and oversight. The RBI apparently looks to U.S. regulators and UK frameworks like CBEST for inspiration, as well as international standards like ISO 27000, and has been engaging major banks for feedback on international best practices. The RBI has established an Inter-disciplinary Standing Committee on Cyber Security to review threats from emerging technologies and suggest policies and security standards to mitigate risks.[102]

Information Security Audit Regime

Requirements for information security (IS) audits are laid out in the RBI's 2011 Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds.[103] The Guidelines cover a wide range of controls for addressing information security, IT governance, and cyber frauds, among other concerns. Banks are required to establish an audit committee to oversee their IS audit performance as well as their compliance with regulatory requirements under RBI circulars and the IT Act of 2000. Under the Guidelines, IS audits must be independent and conducted by professionally competent auditors.

The Guidelines specify that it is "desirable" for auditors to possess Certified Information Systems Auditor (CISA), Diploma in Information System Audit (DISA), or Certified Information Systems Security Professional (CISSP) certifications, along with two or more years of IS audit experience. Other releases by the RBI—such as their 2010 circular to payment system operators—require annual audits by CISA or DISA-certified auditors.[104]

---

100. "Business Continuity Planning (BCP), Vulnerability Assessment and Penetration Tests (VAPT) and Information Security," Reserve Bank of India, June 26, 2013, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=8061&Mode=0.
101. ReBIT, *Cybersecurity Maturity Model Implementation Guide*, October 28, 2017, https://rebitorgin.s3.ap-south-1.amazonaws.com/2018-09/CMM_Implementation_Guide.pdf.
102. Reserve Bank of India, *Reserve Bank Establishes an Inter-disciplinary Standing Committee on Cyber Security*, February 28, 2017, https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR230352D612E69EC045D5A86C-FA85D10094C4.PDF.
103. Reserve Bank of India, *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds* (2011), https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.
104. "Directions for submission of system audit reports from CISA qualified Auditor," Reserve Bank of India,

Under the 2011 Guidelines, banks are allowed to outsource their audits so long as the external auditors possess the same level of qualifications required of internal auditors, and so long as the bank itself remains responsible for the audit planning process, risk assessment, and follow-up compliance. The Guidelines also lay out the steps banks should take when planning a risk-based audit and detail documentation requirements for the audit process.

Though India's 2013 National Cyber Security Policy calls for the creation of a cybersecurity assurance framework to allow for conformity assessment and compliance certification with cybersecurity standards, reports indicate that little progress has been made in operationalizing this provision.[105] In theory, the framework would be based on "international best practices," though only ISO 27001 is explicitly listed as a model. Auditors empaneled by the Indian Computer Emergency Response Team (CERT-In) would be responsible for verifying compliance.[106] The Ministry of Communications and IT released a security assurance framework for government entities in 2010, but this has gained little traction within agencies, and no indication exists that the government is considering expanding it to cover critical infrastructure.[107]

Regulatory Compliance

Compliance with the 2011 RBI Guidelines is monitored at the board level of individual banks, and assessed as part of RBIs' inspection regime.[108] When the Guidelines were released, the RBI stated that it would review implementation progress during its quarterly discussions with banks, and examine implementation as part of future annual financial inspections.[109] Since 2015, CSITE has been responsible for conducting IT examinations for the RBI, and it has been assessing banks' IT infrastructure and cybersecurity preparedness through a process independent from the RBI's risk-based supervision. These examinations adhere to the most recent 2016 Framework and are performed along the lines of "some of the best international standards on cybersecurity assessment."[110] CSITE also conducts off-site monitoring of cyber risks based on banks' reports of cyber incidents, technology implementations, self-assessed gaps in preparedness, and details of remedial actions.[111] According to reports, more than 30 major banks were to be covered in CSITE's detailed 2016/17 IT examinations, and all banks were to be covered in 2017/18.[112]

December 27, 2010, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6177&Mode=0.

105. Ministry of Communication and Information Technology, *Notification on National Cyber Security Policy-2013*, July 2, 2013, https://www.cert-in.org.in/ISAC-Power/National_Cyber_Security_Policy_2013.pdf; Jigar Saraiya, "India Badly in Need of Cyber Security Assurance Framework," Transcend Consultants, December 5, 2017, http://transcons.net/2017/12/05/india-badly-need-cyber-security-assurance-framework/.
106. Ministry of Finance, "Press Release."
107. Ministry of Communication and Information Technology, *E Security Assurance Framework: Catalog of Security Controls eSAFE–GD 200* (2010), http://egovstandards.gov.in/sites/default/files/eSAFE%20GD200%20Catalog%20Of%20Security%20Controls%20Ver1.0.pdf.
108. Ministry of Finance, "Press Release."
109. "Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations," Reserve Bank of India, April 29, 2011, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6366&Mode=0.
110. Ministry of Finance, "Press Release."
111. Ibid.
112. Special Correspondent, "RBI to set up computer emergency response unit," *Hindu*, April 17, 2017, https://www.thehindu.com/business/Economy/rbi-to-set-up-computer-emergency-response-unit/article18080388.ece.

Stakeholders in India, however, have noted that enforcement of these cybersecurity regulations has been rare.[113] Policymaking authority for the financial sector is dispersed over numerous agencies, creating a complex regulatory and compliance environment that has driven up compliance costs and been generally ineffective in driving the adoption of new security controls. To date, no financial regulator has announced enforcement action in relation to cybersecurity obligations, and the appellate body for causes of action under the IT Act has not adjudicated a single case since 2011.[114] Compliance has suffered in this environment, with some reporting that banks have taken no steps to implement the RBI's Cyber Security Framework despite a strict deadline given by the regulator.[115]

Securities and Exchange Board of India

Cybersecurity regulations have also been developed by the Securities and Exchange Board of India (SEBI), covering all authorized market infrastructure institutions (MIIs). The primary set of regulations promulgated by SEBI is the 2015 circular on cybersecurity and cyber resilience.[116] This circular requires MIIs to develop a cybersecurity policy, appoint a chief information security officer (CISO), implement continuous security monitoring, establish intrusion detection and prevention systems, and develop response and recovery plans. The circular also requires institutions to "regularly conduct" vulnerability assessments and carry out penetration tests at least once per year. The circular advises that MIIs should work to incorporate best practices from international standards like ISO 27000 and COBIT 5. SEBI requires that all MIIs include the controls listed in the circular in their mandatory annual independent system audits, with results to be communicated to SEBI to ensure compliance. In May 2017, SEBI established a High-Powered Steering Committee on Cybersecurity to provide guidance on cyber initiatives and advise SEBI in developing new security controls in alignment with global best practices.[117]

Regulations for Critical Infrastructure

Banks in India are also covered by regulations pertaining to critical information infrastructure, with the financial sector having been designated a critical sector in the 2000 IT Act. Cybersecurity controls for CII operators are primarily developed by the National Critical Information Infrastructure Protection Centre (NCIIPC), formed in 2014 under the National Technical Research Organization (NTRO), one of India's intelligence agencies. NCIIPC works to develop standards, best practices, and protection strategies for CII, and issue guidelines and advisories in coordination with CERT-In. NCIIPC is also responsible for producing vulnerability assessment and auditing methodologies for operators. The preeminent set of regulations for CII operators are the 2015 Guidelines for

---

113. Tarun Krishnakumar, "Cyber Insecurity: Regulating the Indian Financial Sector," Oxford Business Law Blog, August 21, 2017, https://www.law.ox.ac.uk/business-law-blog/blog/2017/08/cyber-insecurity-regulating-indian-financial-sector.
114. Soibam Rocky Singh, "India's only cyber appellate tribunal defunct since 2011," *Hindustan Times*, December 21, 2018, https://www.hindustantimes.com/india/india-s-only-cyber-appellate-tribunal-defunct-since-2011/story-208HGrEN7hXrABg7lAb69N.html.
115. Praveen Dalal, "Cyber Security Trends In India 2017 By Perry4Law Organisation (P4LO)," P4LO, December 31, 2016, http://feedreader.com/observe/perry4law.org/%3Fp%3D123+itemId=4954814261.
116. Securities and Exchange Board of India, *Subject: Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories*, July 6, 2015, https://www.sebi.gov.in/sebi_data/attachdocs/1436179654531.pdf.
117. Press Trust of India, "Sebi sets up panel on strengthening cyber security," *Economic Times*, May 2, 2017, https://economictimes.indiatimes.com/markets/stocks/news/sebi-sets-up-panel-on-strengthening-cyber-security/articleshow/58474769.cms.

Critical Information Infrastructure Protection, a set of 35 controls and guiding principles for strengthening cybersecurity in critical sectors.[118]

The Guidelines are divided into five families of controls, covering planning, implementation, operation, disaster recovery, and reporting requirements for CII operators. Included among these controls are requirements for an organizational information security policy, expectations for security certification of information security personnel, the incorporation of risk assessments into corporate strategy, the implementation of intrusion detection and monitoring systems, the establishment of contingency plans for disaster recovery, the conduct of penetration testing at all levels of security, and the periodic auditing and vulnerability assessment of critical systems.

Little detail is given on the particular expectations for security controls under the Guidelines, but NCIIPC has clarified some of their requirements through the release of additional documents like the Framework for Evaluating Cyber Security in Critical Information Infrastructure[119]—covering risk assessments for CII operators—and the Standard Operation Procedure (SOP) for Auditing of CIIs[120]—detailing expectations for information security audits. The SOP for auditing CIIs establishes that CII operators should form internal audit teams to conduct internal assessments twice a year. CIIs are also required to carry out annual external audits by either CERT-In empaneled auditors or private auditors with at least six years of experience and recognition by international standards organizations. Audit reports and remedial actions must be reported to NCIIPC within two months.

Though NCIIPC is empowered to act as a regulator, it has so far seemed more interested in taking example from the U.S. Critical Information Infrastructure Act 2002, emphasizing voluntary cooperation rather than enforcement to build a more collaborative relationship between the Centre and the private sector.[121] Furthermore, while NCIIPC's guidelines so far remain generalized to all CII operators, it has approached the banking sector to try to develop sector-specific plans and SOPs, which could lead to more tailored regulations in the future.[122]

The other major regulator of critical infrastructure operators is the Indian Computer Emergency Response Team, formed in 2004 under the IT Act of 2000. Though CERT-In's primary duty is incident response, it also serves a regulatory function insofar as it is authorized to issue guidelines, advisories, and policies to CII operators to improve information security. The most notable of these guidelines is the 2006 Information

118. National Critical Information Infrastructure Protection Centre, *Guidelines for Protection of Critical Information Infrastructure* (New Delhi: NCIIPC, 2015), http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.
119. National Critical Information Infrastructure Protection Centre, *NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure* (New Delhi: NCIIPC), http://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf.
120. National Critical Information Infrastructure Protection Centre, *Standard Operating Procedure: Auditing of CIIs/Protected Systems by Private/Government Organisation*, June 2017, http://nciipc.gov.in/documents/SOP-CII_Audit.pdf.
121. Saikat Datta, "The NCIIPC & Its Evolving Framework," Digital Policy Portal, October 27, 2016, http://www.digitalpolicy.org/nciipc-evolving-framework/.
122. Saikat Datta, "Defending India's Critical Information Infrastructure," *International Democracy Project*, March 2016, https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf.

Security Policy for Protection of Critical Information Infrastructure, which requires critical sector organizations to appoint a CISO, carry out periodic risk assessments, test security control measures, and assign an independent IT security auditing organization to carry out an annual audit of IT infrastructure.[123]

Specific to the financial sector, CERT-In has also issued advisories on topics ranging from online banking to cloud security, e-wallets, and Aadhaar payment systems. CERT-In has also requested that the RBI carry out audits through empaneled auditors for all digital wallets, advised banks to conduct periodic vulnerability assessment and penetration testing, and established continuous monitoring to detect cybersecurity incidents.[124]

India has also been considering the establishment of CERT-Fin, a sectoral CERT for the financial sector. Though approved by a working group within the Ministry of Finance and included in a 2017 cybersecurity proposal by India's Finance Minister,[125] CERT-Fin has not been included in the most recent 2018 budget,[126] and has been criticized as unnecessary and redundant.[127]

Data Protection

The collection, storage, and use of personal data in India is primarily regulated according to the IT Act of 2000 and subsequent guidelines. Security procedures and privacy rules under the IT Act are laid out in the 2011 Information Technology Rules, which require data collectors to obtain consent from data subjects, use collected information only for relevant and lawful purposes, and retain the data no longer than is required.[128] The Rules clarify the level of protection entities are expected to provide for sensitive personal information, citing ISO 27001/2 as one example of an acceptable standard. Entities desiring to regulate themselves by standards other than the ISO are required to have their codes of practice approved by the Central Government. To date, no alternate codes have been approved.[129] Importantly, the 2011 rules only apply to people or corporations located within India, and not to just any corporation handling the personal information of Indian customers.[130]

According to the Act, data holders may face criminal punishment for disclosing personal information without the subject's consent, or in cases of breach of contract. The Act also holds service providers liable to provide compensation for a failure to observe reasonable security practices and procedures. However, as-written, data holders cannot be punished just for failing to maintain these security practices, but instead are only liable when those

123. Department of Information Technology, *Information Security Policy Protection of Critical Information Infrastructure*, May 2006, https://web.archive.org/web/20180107170230/http://mapit.gov.in/securityaudit/downloads/CERT-In%20Info_Sec_Policy.pdf.
124. Ministry of Finance, "Press Release."
125. Varun Haran, "Separate Financial CERT Proposed: Will It Prove Effective?," InfoRiskToday, February 3, 2017, https://www.inforisktoday.in/separate-financial-cert-proposed-will-prove-effective-a-9667.
126. Suparna Goswarni, "New Indian Budget Doesn't Mention CERT-Fin," Bank Info Security, February 2, 2018, https://www.bankinfosecurity.asia/new-indian-budget-doesnt-mention-cert-fin-a-10626.
127. Krishnakumar, "Cyber Insecurity."
128. Ministry of Communication and Information Technology, *Notification*, April 11, 2011, https://meity.gov.in/writereaddata/files/GSR3_10511%281%29.pdf.
129. Stephen Mathias and Naqeeb Ahmed Kazia, "Data Security and Cybercrime in India," Lexology, https://www.lexology.com/library/detail.aspx?g=e7b6cb3b-f534-45ba-b1fb-86d7ed39e558.
130. "India IT Act of 2000 (Information Technology Act)," Parliament of India, https://termsfeed.com/blog/india-it-act-of-2000-information-technology-act/.

failures lead to wrongful loss. As such, the law simply codifies the law of negligence.[131] Additionally, the IT Act waives the requirement to adhere to these security practices when parties agree privately to their own set of security procedures, limiting the reach of the 2011 rules' protections. The IT Act established a Cyber Regulations Appellate Tribunal to handle complaints arising from the provisions in the Act, but this tribunal has been defunct since 2011.[132]

Recent findings by the European Union that India's data protections do not provide adequate protection have helped drive interest within the Indian government in passing a comprehensive data protection law. In July 2018, the Government of India's Committee of Experts released a draft Protection of Personal Data Bill.[133] This legislation comes in response to a 2017 finding by the Supreme Court of India that privacy is a fundamental right under India's Constitution, and that the government should formulate a data protection regime for Indian citizens.[134] The Bill is modeled on the GDPR, granting individual rights to data subjects, strengthening consent requirements, and empowering a proposed Data Protection Authority (DPA) with the power to investigate companies for compliance with the Bill's provisions. The Bill has been criticized, however, for the lack of independence granted to the DPA, as well as for its broad application of criminal liabilities for violations.[135]

Data Breach Notification

In February 2017, the RBI announced that all banks were mandated to report cyber incidents to RBI within two to six hours.[136] Banks are also required to share root cause analysis and forensic audit findings as soon as possible. Banks also face an uncertain legal requirement to report breaches to the Indian CERT, though CERT-In has taken the stand that notifications are mandatory.[137] There is currently no requirement under the IT Act, Privacy Rules, or RBI policies to notify affected customers.[138]

The draft Protection of Personal Data Bill greatly increases firms' obligations with respect to breach notification, requiring data controllers to notify the DPA of any breach of personal data "likely to cause harm to any data principal."[139] The Bill allows the DPA to specify a time period for breach notification and lays out the information that must be included in companies' reports. The Bill also states that the DPA shall determine whether the breach should be reported to the data subjects, taking into account the severity of the breach and the need for mitigation.

---

131. Mathias and Kazia, "Data Security and Cybercrime in India."
132. Soibam Rocky Singh, "India's only cyber appellate tribunal defunct since 2011," *Hindustan Times*, December 21, 2018, https://www.hindustantimes.com/india/india-s-only-cyber-appellate-tribunal-defunct-since-2011/story-208HGrEN7hXrABg7lAb69N.html.
133. Ministry of Electronics and Information Technology, *The Personal Data Protection Bill*, 2018, http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.
134. "Indian Supreme Court in landmark ruling on privacy," BBC, August 24, 2017, https://www.bbc.com/news/world-asia-india-41033954.
135. Ananya Bhattacharya, "India's first data protection bill is riddled with problems," Quartz India, July 30, 2018, https://qz.com/india/1343154/justice-srikrishnas-data-protection-bill-for-india-is-full-of-holes/.
136. Geetha Nandikotkur, "RBI: Banks Must Report Breach Incidents Within 6 Hours," Bank Info Security, February 28, 2017, https://www.bankinfosecurity.asia/rbi-banks-must-report-breach-incidents-within-6-hours-a-9743.
137. Stephen Mathias and Naqeeb Ahmed Kazia, "Data Protection & Privacy," Getting the Deal Through, September 2018, https://gettingthedealthrough.com/area/52/jurisdiction/13/data-protection-privacy-2018-india/.
138. Stephen Mathias and Naqeeb Ahmed Kazia, "Data security and breach notification in India," Lexology, October 29, 2018, https://www.lexology.com/library/detail.aspx?g=ea085538-f5c7-4d9f-b267-dd8d930ff1d0.
139. Ministry of Electronics and Information Technology, *The Personal Data Protection Bill, 2018*.

Cross-Border Transfer of Data

The 2011 IT Rules allow entities to transfer sensitive personal information to other entities within or outside India, including to third parties, so long as the recipients provide an equivalent level of protection.[140] These regulations have not been consistently enforced, however.[141]

RBI regulations on outsourcing permit FIs to transfer data outside of India, provided that the RBI is not prevented from undertaking audits or inspections, the liquidation of the offshore provider does not affect the availability of records to RBI, the offshore regulator does not have access to the data simply because it is being processed overseas, and the jurisdiction of the overseas courts does not extend to the operations of the bank in India. Further, the regulations require customer data be isolated and clearly identified, and not be comingled with other data.

Recent guidelines from the Ministry of Electronics and Information Technology (MEITY) require government agencies contracting with cloud vendors to ensure that all relevant data is stored within India, but no such requirements yet exist for the financial sector.[142] There exists a little-known law that requires Indian companies to maintain backups of company accounts on servers physically located in India, though this rule has not been enforced by regulators.[143] And while India has expressed its interest in joining APEC for a number of years, it is currently an observer, meaning that APEC rules do not apply in the Indian jurisdiction.[144]

The recently-released draft Protection of Personal Data Bill would update the requirements for companies transferring personal data across borders, most significantly by requiring that companies maintain copies of all personal data within India, and by requiring that all critical personal data—a category to be defined by the Central Government—only be processed in a server or data center within India.[145] Other categories of data may be transferred outside of India only if consent has been given by the data subject, the transfer is to a country approved by the Central Government and DPA, or if the transfer is made under contractual clauses or schemes approved by the DPA. The DPA and Central Government may only approve data transfers if satisfied that the data will be subject to "an adequate level of protection" in the destination jurisdiction. The Bill is currently under deliberation and is expected to be introduced in Parliament in June 2019.[146]

A great deal of uncertainty surrounds the data localization regime of India, however, due to sudden, rapid changes in regulation, inconsistent enforcement, and unclear provisions.

---

140. Mathias & Kazia, "Data Security and Cybercrime in India."
141. N.S. Nappinai, "India's data protection law: Strengthen rules but also follow through to the last mile," *Hindustan Times*, December 31, 2018, https://www.hindustantimes.com/analysis/india-s-data-protection-law-strengthen-rules-but-also-follow-through-to-the-last-mile/story-OL3UbLd78dyN4psWa5S0nL.html.
142. Ministry of Electronics and Information Technology, "Guidelines for Government Departments on Contractual Terms Related to Cloud Services," March 31, 2017, http://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms_0.pdf.
143. Mathias and Kazia, "Data Security."
144. Aditi Subramaniam, "India," *The Privacy, Data Protection and Cybersecurity Law Review*, 4th ed., December 2017, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151286/india.
145. Ministry of Electronics and Information Technology, *The Personal Data Protection Bill, 2018*.
146. Martin F.R., "India's Data Protection Bill Will Now Be Tabled in June," *Analytics India Magazine*, January 2019, https://www.analyticsindiamag.com/indias-data-protection-bill-in-june/.

For instance, the RBI's April 2018 circular on the storage of digital payment system data created a sudden, highly-disruptive requirement that all payment system providers keep full transaction details for all Indian customers within the country.[147] The RBI refused requests to extend the deadline for major providers like Visa and Google, but has taken no enforcement action against those who failed to comply.[148]

In the case of the proposed Personal Data Protection Bill, the draft has been criticized for leaving many critical provisions unclear. Concerns such as defining critical personal data, clarifying data processor obligations through codes of practice, and deciding the scope of exemptions for data protection requirements and international transfer restrictions are all left to future actions by the Central Government.[149]

China

Introduction

Chinese financial institutions have two primary sources of cybersecurity regulations: the China Banking and Insurance Regulatory Commission (CBIRC), which is China's banking regulator, and the critical information infrastructure protection regime, which was established by the 2016 Cybersecurity Law (CSL) and is administered by the Cybersecurity Administration of China (CAC). Under the CBIRC, banks are required to adhere to a detailed set of security controls and risk management practices as laid out in an array of guidances and standards that have been released continuously over the past decade. As critical information infrastructure, banks are also required to participate in the emerging regime of information security measures begun by the CSL. These involve not only the implementation of standard security controls, but also an adherence to the Ministry of Public Security's (MPS) and CAC's evolving system of security reviews for critical products and services. Banks are also obligated to adhere to the CSL's data protection provisions, which grant GDPR-like rights to data subjects and strictly limit cross-border data transfers.

People's Bank of China

The People's Bank of China (PBoC) is the central bank of the People's Republic of China (PRC), responsible for overseeing monetary policy and FI regulation on the mainland. The PBoC's regulatory authority, laid out in Chapter 5 of the Law of the People's Republic of China on the People's Bank of China, primarily concerns the inspection and supervision of banks' deposit reserves, inter-bank lending and bond markets, foreign exchanges, AML provisions, the state treasury, and other largely monetary concerns.[150] The PBoC is not explicitly responsible for developing and implementing regulations pertaining to risk management for FIs. However, the PBoC has a mandate to establish a system for internal auditing and inspection for the central bank system, and its 2016 annual report indicates

147. "Storage of Payment System Data," Reserve Bank of India, April 6, 2018, https://rbi.org.in/scripts/FS_Notification.aspx?Id=11244&fn=9&Mode=0.
148. Nappinai, "India's data protection law."
149. "Consultation on the Personal Data Protection Bill 2018," Ministry of Electronics and Information Technology, September 29, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.
150. "Law of the People's Republic of China on The People's Bank of China," National People's Congress, December 27, 2003, http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383712.htm.

that it regularly undertakes internal audits and risk assessments of IT systems at its head office and affiliated institutions.[151]

China Banking and Insurance Regulatory Commission

The China Banking and Insurance Regulatory Commission (CBIRC), which prior to April 2018 existed as separate banking (CBRC) and insurance (CIRC) entities, is the foremost financial regulator for commercial banks in China. Prior to its reorganization, the CBRC issued several major regulatory policies concerning cybersecurity controls for Chinese FIs. Principal among these are the Commercial Bank Information Technology Risk Management Guidelines, released in March 2009.[152] These guidelines lay out expectations for a wide range of information security policies, strategies, and controls, covering everything from information system development and testing to business continuity planning and risk management for IT outsourcing. The Guidelines are based heavily on international standards and best practices, drawing from ISO 27000 standards for information security controls, COBIT and Information Technology Infrastructure Library (ITIL) best practices for its IT management provisions, and the Basel Core Principles for business continuity management.[153]

CBIRC expectations on internal controls have been clarified through the release of three other documents. In 2010, the Enterprise Internal Control Application Guide for Information Systems laid out expectations for banks' information security processes, including the installation of security software; the establishment of a user management and access rights system; and the use of firewalls, vulnerability scanning, and intrusion detection to guard against attacks.[154] The CBIRC's 2015 guidance on Dynamic Monitoring Indicators for IT Risk of Commercial Banks identified eight indicators banks are advised to monitor to improve their information security posture, including system availability, system update success rate, phishing website blocking rate, and number of security events.[155] Finally, the On-site Examination Manual on IT Risk Management enumerates 300 key risk factors for information systems and provides guidance on the methods and procedures for ensuring compliance with CBIRC rules.[156] Specific guidance also exists on the expectations for data center security practices.[157]

In addition to these controls, banks are required to develop and implement risk management strategies and policies at the system level to improve their ability to identify, manage, and mitigate against institutional risks like information security threats. These expectations are laid out in CBIRC notices, including the 2016 Comprehensive Risk

---

151. "Annual Report 2016," The People's Bank of China, http://www.pbc.gov.cn/english/130739/3398661/3398676/index.html.
152. "商业银行信息科技风险管理指引," China Banking Regulatory Commission, March 2009, http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/20090601FC296F80D3957B65FFFA9EDA836D7300.html.
153. Shanghai Anyan Information Technology Company, "Comparison Map Between ISO27001 and Bank Information Technology Risk Management Guidelines," http://www.aryasec.com/0e2d3e35-afec-6a3d-f1ed-a9e9a8ade7ff/e3d03b79-1fa5-1144-c809-793c23bdf4df.shtml.
154. "企业内部控制应用指引第 18号——信息系统," Ministry of Finance of the People's Republic of China, 2010, http://www.law-lib.com/law/law_view.asp?id=315992.
155. "银监办发[2015]121号," China Banking Regulatory Commission, http://www.cbrc.gov.cn/govView_810A47B1E9F04531A1DB90EEBCC93D55.html.
156. "商业银行信息科技风险现场检查指南," The People's Bank of China, https://www.banklaw.com/laws/bffa-2f4699ee11e89b644ccc6a5a6fc1.html.
157. "商业银行数据中心监管指引," China Banking Regulatory Commission, 2010, https://baike.baidu.com/item/商业银行数据中心监管指引/2192141.

Management Guidelines for Banking Financial Institutions, the 2014 Guidelines for Consolidated Management and Supervision of Commercial Banks and Guidelines on Internal Control of Commercial Banks, the 2010 Guidelines for the Supervision of Data Centers of Commercial Banks, and the 2007 Guidelines for Operational Risk Management of Commercial Banks.[158] These regulations require FIs to establish IT risk monitoring mechanisms to protect information systems and customer data, develop disaster recovery plans in the event of system disruptions, and undertake annual internal audits of their risk management efforts. The CBIRC has noted that these policies are heavily based on the Basel Banking Committee's Core Principles for Effective Banking Supervision,[159] and the International Monetary Fund (IMF) has found that the CBIRC's regulatory regime is broadly compliant with the Basel Principles.[160]

Business continuity management is another major focus of the CBIRC's regulations. On a general level, the 2007 Operational Risk Management Guidelines and 2011 Business Continuity Supervision Guidelines require banks to establish response and recovery plans in the event that critical systems are disrupted.[161] Specific to information security, the CBIRC's Management Standards on Emergency Response of Banks' Important IT Systems and Notice on Strengthening the Safety of Significant Information Systems specifically require banks to strengthen protections for key information system risks like communications facilities and power support.[162] Under the Business Continuity Guidelines, banks are required to submit annual audit and assessment reports for their business continuity management, and the CBIRC is required by both the Operational Risk Guidelines and Business Continuity Supervision Guidelines to incorporate the supervision of business continuity risks into their examination regime.

CBIRC Supervisory Regime

Risk management efforts and information security controls are assessed by the CBIRC, both as a component of the Commission's broader supervisory regime for operational risk, as well as more specifically under the requirements of the 2009 IT Risk Management Guidelines. The CBIRC's supervision of operational risks is carried out under the authority of China's 1995 Commercial Bank Law and 2004 Banking Supervision Law,[163] which

158. "银行业金融机构全面风险管理指引的通知," China Banking Regulatory Commission, 2016, http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/A0D2DC141DDF4781AF9EB218A883F3AC.html; "并表管理与监管指引的通知," China Banking Regulatory Commission, 2014, http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/27E97E0235134CBDBD5AD4F5AD0A4D42.html; "Notice on Issuing the Guidelines on Internal Control of Commercial Banks," China Banking Regulatory Commission, September 12, 2014, http://www.cbrc.gov.cn/EngdocView.do?docID=231AD998D90B4AE585383BF38089E194; CBRC, "商业银行数据中心监管指引"; "中国银行保险监督管理委员会," China Banking Regulatory Commission, 2007, http://www.cbrc.gov.cn/govView_6C25993381CA4293A804FC5DBB4B76B1.html.

159. "银行业金融机构全面风险管理指引," China Banking Regulatory Commission, September 30, 2016, http://www.cbrc.gov.cn/chinese/home/docView/89ABDA2B659D4A178F1CCF146B7529F0.html.

160. "People's Republic of China: Financial Sector Assessment Program- Detailed Assessment of Observance of Basel Core Principles for Effective Banking Supervision," International Monetary Fund, December 26, 2017, https://www.imf.org/en/Publications/CR/Issues/2017/12/26/Peoples-Republic-of-China-Financial-Sector-Assessment-Program-Detailed-Assessment-of-45516.

161. CBRC, "中国银行保险监督管理委员会"; "商业银行业务连续性监管指引," China Banking Regulatory Commission, December 29, 2011, http://www.chinastor.com/dp/bcm/0124361012017.html.

162. IMF, "Assessment of Observance of Basel Core Principles."

163. "Law of the People's Republic of China on Commercial Banks," The National People's Congress of the People's Republic of China, http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383716.htm; "The Law of the People's Republic of China on Banking Regulation and Supervision," China Banking Regulatory Commission, www.cbrc.gov.cn/EngdocView.do?docID=2916.

empower the CBIRC to carry out inspections and audits of bank operations at any time to assess compliance with legal and regulatory requirements. Comprehensive on-site inspections of banks for operational risk management are mandated at least every five years, with the actual frequency determined by the FI's risk profile and systemic importance.[164] Operational risks are also evaluated by the CBIRC during special thematic inspections of the industry as well as through their ongoing off-site monitoring of banks.[165]

Under the IT Risk Management Guidelines, banks are required to conduct internal audits of information security controls at least every three years, but each FI is advised to develop their own schedule based on the risk profile of their institution as well as the nature of their business. The Guidelines contain no explicit requirements for auditor qualifications, and allow organizations to use an external audit institution providing the auditors have "corresponding qualifications." There is no explicit requirement for the audit results to be submitted to the CBIRC for review. However, the board members of each FI are directed to confirm the audit report and implement rectification, all of which would be captured in the annual report that the board is required to submit each year to the CBIRC.

Additional oversight is provided through the CBIRC's ongoing supervision of regulatory compliance, which is overseen by the CBIRC's dedicated IT risk supervision division.[166] In addition to conducting off-site supervision and on-site inspections of banks' IT controls, the CBIRC's IT division is also responsible for formulating new banking industry policies, handling IT emergencies, and carrying out standardization work.[167] Since the establishment of the IT division, IT risks have become a central aspect of the CBIRC's on-site examinations, and today these examinations cover everything from IT risk governance, information security, and business continuity to IT outsourcing, system development, and IT operation and maintenance.[168] As of the end of 2017, the CBIRC had undertaken 38 on-site examination programs involving 36 banking institutions, which the IMF notes has helped drive banking institutions to be proactive in their development of risk prevention strategies.[169]

However, in discussing the challenges of IT risk management for small, medium, and rural FIs, some commentators have noted that IT auditors face a number of challenges in China, including the lack of any uniform standard for IT auditing programs and procedures.[170] Accordingly, some auditors struggle to effectively translate the IT Risk Management Guidelines into practice, and often ignore the requirements of other national regulatory authorities like the People's Bank of China.[171] The CBIRC has been active in enforcing

---

164. "中国银监会现场检查暂行办法," China Banking Regulatory Commission, 2015, http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/E5DE45C66AD34380AFC8F3A713D9BEA3.html.
165. "中国银监会非现场监管暂行办法," China Banking Regulatory Commission, 2015, http://www.cbrc.gov.cn/govView_77141551F9C54B21A02BA36D4EF30FEF.html.
166. IMF, "Assessment of Observance of Basel Core Principles for Effective Banking Supervision."
167. Editorial Department, "商业银行怎解合规难——信息科技合规：地位凸显," *中国信息化*, No. 23, xzbu.com, 2012, https://www.xzbu.com/8/view-4080346.htm.
168. IMF, "Assessment of Observance of Basel Core Principles for Effective Banking Supervision."
169. Ibid.
170. 苏宝华, "农村金融机构信息科技审计的问题及对策," *金融电子化*, August 18, 2016, http://www.cfc365.com/management/risk/2016-08-18/13991.shtml.
171. 胡昂, "信息科技风险管理流程优化," NS Focus, June 14, 2017, http://blog.nsfocus.net/information-technology-risk-management-process-optimization/.

its regulations, however, with violators being fined upwards of 720 million RMB ($100 million) for a failure to implement IT security procedures as mandated in the IT Risk Management Guidelines and elsewhere.[172]

Critical Information Infrastructure

In addition to their obligations under the CBIRC, banks operating in China are also considered critical information infrastructure (CII) by the national government, and as a result must adhere to strict requirements on security testing, data protection, and risk management as set out in the 2016 Cybersecurity Law[173] (CSL) and associated guidance.[174] The CSL represents the foundation of a new cybersecurity supervision regime by the Chinese government, and while the exact scope and details of this regime are still in the process of being clarified through the periodic release of new standards and guidelines, the Law has already had a significant impact due to its promised restrictions on cross-border data transfers and its mandate of intrusive security reviews for critical network equipment and cybersecurity services.

The CSL requires that all CII operators implement security controls according to the Ministry of Public Security (MPS) Multi-Level Protection System (MLPS), which requires different levels of security controls depending on a network's importance for national security, economic development, and Chinese society.[175] Though the relationship between the MLPS' five-tier rating system and the CSL's CII designation has yet to be clarified, at minimum FIs can expect certain baseline requirements, such as establishing internal cybersecurity management systems, adopting technical measures for network monitoring and defense, and adopting data classification, backup, and encryption policies for their information systems.[176]

FIs will likely also continue to be subject to enhanced scrutiny by the MPS, as the latest MLPS update requires operators to connect network monitoring systems with MPS networks, implement redundancy and recovery measures for important equipment, and engage MPS-accredited agencies to conduct testing on critical systems both before network launch and annually post-launch.[177] Operators are also required to use only those network products and cybersecurity services that have been approved by the MPS for use in "important parts of networks."

---

172. "中国经济网, "银监会史上最大罚单(全文):广发银行遭罚没超7亿元," China Economic Net, December 8, 2017, http://finance.ce.cn/rolling/201712/08/t20171208_27180171.shtml.
173. Rogier Creemers, "Cybersecurity Law of the People's Republic of China," New America, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
174. Cyberspace Administration of China, "Critical Information Infrastructure Security Protection Regulations," trans. Graham Webster, Paul Triolo, and Rogier Creemers, China Copyright and Media, July 11, 2017, https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/.
175. "网络安全等级保护条例," The Ministry of Public Security, June 27, 2018, http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html.
176. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," CSIS, August 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF.
177. Covington and Burling LLC, "China Seeks Public Comments for Draft Regulations on Cybersecurity Multi-level Protection Scheme to Implement the Cybersecurity Law," July 5, 2018, https://www.cov.com/-/media/files/corporate/publications/2018/07/china-seeks-public-comments-for-draft-regulations-on-cybersecurity-multilevel-protection-scheme-to-implement-the-cybersecurity-law.pdf.

These sourcing restrictions under the MLPS are further compounded by provisions in the CLS requiring that all products and services affecting national security undergo a review by the Cyberspace Administration of China (CAC) prior to their sale. The CAC has released draft measures[178] for this certification regime and a draft catalog of affected products and services subject to review, but the exact standards and procedures for these reviews have yet to be finalized.[179] Currently, there is still considerable uncertainty over the interplay between the CSL and MLPS certification regimes, but it is clear at least that FIs in China will be expected to adapt their equipment sourcing according to the eventual consensus of China's security and standards bodies.[180]

Under the CSL, network operators are also required to formulate emergency response plans for cybersecurity incidents, provide technical support and assistance to Chinese security services, and implement real identity verification for users. CII operators, including FIs, are further required to comply with CAC policies on cybersecurity certification, testing, and risk assessment; implement systems to monitor, detect, and report cybersecurity events; and set up specialized bodies to manage security risks. At least once a year, CII operators are required to conduct an inspection and assessment of their network security and submit a report on the findings to regulators. Overall, analysts have noted that the majority of the security controls mandated by the CSL are closely aligned with the NIST Cybersecurity Framework and the ISO 27000 family of standards, with the exception of the CAC's regime for equipment certification and review.[181]

The CSL was only the first step towards China's larger goal of building a robust cybersecurity protection regime for critical information infrastructure. As such, various authorities in China including the CAC, the National Information Security Standardization Technical Committee (TC260), the Ministry of Industry and Information Technology (MIIT), and others are actively continuing to develop new guidelines and standards to refine and deepen the regime sketched out in the CSL. Prominent among these are draft guidelines for CII operators circulated by the TC260 on the procedures for security inspections, draft indicators for security evaluation and monitoring, and draft cybersecurity protection requirements and security controls.[182]

Though none of these standards have entered into force and all are technically voluntary, the government has already begun to approach companies to check if they are in compliance. Enforcement has already begun for aspects of the CSL already in place, with

178. Cyberspace Administration of China, "Interim Security Review Measures for Network Products and Services," trans. Rogier Creemers, China Copyright and Media, May 2, 2017, https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/.
179. "网络关键设备和网络安全专用产品目录," Central Cybersecurity Affairs Commission, June 9, 2017, http://www.cac.gov.cn/2017-06/09/c_1121113591.htm; Sacks and Li, "Chinese Cybersecurity Standards."
180. Ibid.
181. "China's Cybersecurity Law and its Impacts - Key Requirements Businesses Need to Understand to Ensure Compliance," Protiviti, https://www.protiviti.com/CN-en/insights/china-cybersecurity-law-and-impacts.
182. "Public Comments on 24 Information Security Standard Drafts," Seconded European Standardization Expert in China, June 26, 2018, http://www.sesec.eu/26-06-2018national-information-security-standardization-technical-committee-sac-tc260-called-for-public-comments-on-24-information-security-standard-drafts/; "China Releases Four Draft Guidelines in Relation to Cybersecurity Law," Hunton Andrews Kurth LLP, September 5, 2017, https://www.huntonprivacyblog.com/2017/09/05/china-releases-four-draft-guidelines-relation-cybersecurity-law/.

local authorities having investigated a number of network operators for violations of the Law's security protection obligations.[183]

Data Protection

In addition to risk management requirements and cybersecurity controls, the CSL also contains a number of provisions addressing the obligations of CII operators towards the collection and handling of customer and business data. Under the CSL, operators are obligated to obtain consent before collecting user data; explicitly state the purpose, means, and scope of the collected data's use; allow users to correct and amend their personal data; and alert customers in the event of a data breach. Some analysts have noted that the privacy protections included in the CSL are very similar to existing data privacy regimes in other jurisdictions, including Hong Kong's Personal Data (Privacy) Ordinance.[184]

The Chinese government has further refined its approach to data protection through the release of the Personal Information Security Specification by TC260, which entered into effect in May 2018.[185] The Specification is voluntary, but regulators are able to use it as a reference in their administration and enforcement activities, making it a de-facto requirement for all network operators handling personal or important data. The Specification establishes a set of best practices for data collection, use, and transfer, as well as expectations for security controls and post-breach incident response.

The definition of personal data under the standard is closely aligned with the strict interpretation given in the GDPR, and many of the provisions in the Specification are highly similar to the GDPR's approach to data protection. This includes the establishment of rights for individual data subjects and the requirement of explicit consent prior to the collection and use of sensitive personal information (though this category is more broadly defined under the Chinese regime).[186] Though the Specification is more lenient in its provision of exceptions for consent requirements, on the whole, it represents an even more onerous privacy regime than the GDPR for CII operators handling personal data.[187]

Enforcement of the CSL regulations has so far been uneven, but regulators have already used it and its associated Personal Information Specifications in audits of companies like the Alibaba-linked Ant Financial.[188] A separate law focused on the protection of personal information is in its early legislative stages, but is at least one to three years away from completion. When this law is released, it will lead to a new round of regulation and standards that may invalidate those currently on the books.

---

183. "China's New Cybersecurity Law Brings Enforcement Crackdown," Jones Day, October 2017, https://www.jonesday.com/files/Publication/8085e76c-cec0-400c-a564-cc26ab4aef71/Presentation/PublicationAttachment/dcbf387e-d23d-4487-9a36-427f28733cbc/Enforcement%20of%20China's%20Cyber%20Law%20Commentary.pdf; Karen Ip, Mark Robinson, Nanda Lau and James Gong, "China Cyber Security Law: Update on Enforcement," Lexology, January 18, 2018, https://www.lexology.com/library/detail.aspx?g=0b3d049d-0edb-41ff-b144-ddf71a8bd7dc.
184. Protiviti, "China's Cybersecurity Law and its Impacts."
185. TC 260, *Information security technology — Personal information security specification*, GB/T 35273-2017 (TC260, 2017), https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf.
186. Yan Luo and Phil Bradley-Schmieg, "China Issues New Personal Information Protection Standard," Covington and Burling LLC, January 25, 2018, https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/.
187. Samm Sacks, "New China Data Privacy Standard Looks More Far-Reaching than GDPR," CSIS, January 29, 2018, https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.
188. Sacks, "Chinese Cybersecurity Standards."

The CBIRC has also issued its own draft guidance on personal data protection, requiring FIs to establish data governance policies and a data management architecture to protect data throughout its lifecycle.[189] The Guidelines require banks to establish self-assessment mechanisms for their data governance processes and implement systems to ensure data quality throughout their organization. The Guidelines mark the first sector-specific rules around data security to come out since the TC260 Personal Information Security Specification was released in December 2017. Government enforcement of the specification is likely to be uneven and ad hoc, but the fact that the banking industry has issued its own version indicates that this is a sector where the risk of regulatory audit may be higher.

Data Breach Notification

The Cybersecurity Law requires network operators to immediately report any cybersecurity flaws, vulnerabilities, or events to affected users and to the relevant government departments. This requirement is reiterated in the Personal Information Security Specification, though no severity threshold or reporting time requirement is specified. MPS regulations issued in June 2018 require network operators to report cyber incidents to the local MPS branch within 24 hours.[190] Finally, under the 2011 Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information, banks are required to report breaches of personal financial data to the PBoC within seven working days.[191]

Data Localization

The CSL was also significant in introducing a data localization regime to CII operators, requiring that they store personal information and "important data" within mainland China. If operators want to move data out of China, they are required to conduct a security assessment according to the provisions laid out by the CAC. China has clarified this process through the release of a draft regulation and accompanying standard,[192] intended to be finalized by the end of 2018.[193] The regulations lay out the criteria operators must use to conduct self-assessments to determine eligibility for cross-border transfer; require operators to report the results of self-assessments to regulators; and introduce obligations to seek explicit regulatory authority for certain types of transfers, including those involving large amounts of sensitive data or data affecting national security and social public interests. Though the regulations help to clarify the CSL's localization provisions, much remains vaguely-worded and left to the discretion of regulators. Until enforcement actions or further interpretations provide greater clarity, FIs are under pressure to adopt the most conservative readings of terms like "important data" and "social public interest" in order to avoid the threat of sanction.

---

189. "银行业金融机构数据治理指引," China Banking Regulatory Commission, May 21, 2018, http://www.cbrc.gov.cn/chinese/newShouDoc/0DD5F9E320AE41488849F82466FE0B22.html.
190. Richard Bird, "Where are we now with data protection law in China?," Lexology, September 13, 2018, https://www.lexology.com/library/detail.aspx?g=dbe04c03-7990-4e0d-8368-e0170637de08.
191. "做好个人金融信息保护工作的通知," People's Bank of China, 2011, http://www.gov.cn/gongbao/content/2011/content_1918924.htm.
192. "个人信息和重要数据出境安全评估办法," Cyberspace Administration of China, April 11, 2017, http://www.cac.gov.cn/2017-04/11/c_1120785691.htm; National Standards of the People's Republic of China, *信息安全技术 数据出境安全评估指南*, https://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf.
193. Sacks, "Chinese Cybersecurity Standards."

In addition, a 2011 notice by the PBoC requires financial personal data relating to Chinese citizens to be stored, processed, and analyzed within China, except when FIs have obtained permission from the PBoC or are otherwise allowed under separate rules or regulations.[194] The Shanghai branch later clarified that PRC branches of foreign banks can transfer client information to overseas branches if certain criteria are satisfied.

194. Richard Bird, "Where are we now."

3 | Common Challenges to Security, Stability, and Harmonization

A number of challenges complicate the regulatory environment in the APAC region, increasing costs for FIs and undermining regulators' efforts to increase the stability and resilience of the regional financial industry. The first is the wide range of capacity levels among regulators and FIs across the region, which makes crafting a common and scalable set of expectations for cybersecurity controls and oversight processes a constant challenge. Regulatory regimes demanding high levels of technological sophistication from FIs and regulators can overwhelm smaller institutions, while more accessible regimes may not adequately address security vulnerabilities in the largest banks.

In the APAC region, interviewees highlighted the MAS and HKMA were highlighted as regulators with a relatively mature cyber risk framework and a fair amount of in-house capacity, while others like the JFSA and RBI had comparatively nascent cyber regulatory regimes (although they have developed significantly in the last few years). Some interviewees at regional and global banks noted that the challenges can be far greater in smaller developing countries, with oversight efforts being hampered by gaps in talent, infrastructure, and understanding among regulators.

Additionally, national regulators tend to focus on risks from the perspective of their own jurisdictions and customers. Multinational FIs, however, generally have integrated systems, and the overall institution's risk profile may not map well to a country-specific risk assessment. As one bank executive put it, "Our global crown jewels do not always correspond to the crown jewels in [a specific jurisdiction]. It's not feasible for us to do risk-based security on a country-by-country basis."

> *The challenges can be far greater in smaller developing countries, with oversight efforts being hampered by gaps in talent, infrastructure, and understanding.*

The highly integrated nature of the regional economy and financial sector means that a cyber incident in one jurisdiction can quickly lead to contagion across national borders.

Effectively managing systemic risk requires allowing FIs to evaluate their overall threat landscape and prioritize resources irrespective of their location or the number of customers in any particular jurisdiction that use them.

As one bank executive pointed out, for many large multinational banks, as much as 80 percent of their systems are global, including many of the most sensitive parts of their networks like online banking portals. Instead of focusing their resources on implementing robust security for those systems, many multinational banks are forced to conduct redundant security reviews and tests of these global systems under dozens of separate national testing regimes and evaluate potential risks and vulnerabilities with respect to each jurisdiction's individual pool of users. This is not only inefficient, but also provides a poor basis for regulators to understand the real threat landscape at the institutional level and the effectiveness of controls from the perspective of network operators and security teams.

This challenge can be most clearly seen in the growing patchwork of redundant—and in many cases highly granular—controls and self-assessments required of banks in the region. For example, while the FFIEC CAT serves as a model for self-assessments used in Singapore, Hong Kong, India and Japan, each regulator has its own list of hundreds of unique assessment questions and controls which are not always readily mapped to each other or back to the FFIEC CAT. As a result, multinational FIs must regularly fill out self-assessments mapping the same security protocols to thousands of different assessment questions and controls.

In some cases, controls are highly prescriptive, and it can be a challenge for FIs to comply with and track so many detailed requirements across multiple jurisdictions. The degree to which this is an issue varies greatly by regulator. In particular, FIs interviewed pointed to the highly prescriptive regimes from the RBI, HKMA, and CBIRC as particularly onerous, while the principles-based, collaborative approach favored by the MAS was viewed as more effective and practical. Some regulators, including the JFSA and HKSFC, rely on a largely principles-based regulatory framework, but are also viewed as relatively new to the game and reliant on checklist-based examination and compliance approaches.

Perhaps the most significant challenge for regional cybersecurity is the massive cyber talent shortage in APAC countries. Asia is facing a dramatic shortage of more than 2 million cybersecurity professionals, nearly three quarters of the global cyber workforce shortage, and those cyber professionals who are available often spend their days on administrative and compliance tasks whose security value is not commensurate with the time they take up.[195] Nearly every interviewee cited the talent gap as a key challenge for both financial regulators and FIs.

One of the biggest complaints among both regulators and FIs was the challenge of getting consistent and qualified cyber auditors, examiners and testers. Some regulators have been forced to rely on outside auditors and examiners, primarily from the "Big Four" accounting and auditing firms[196] for oversight and enforcement (e.g. HKSFC), while others rely on

195. *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens*, ((ISC)², 2018), https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D-0FB51698D9BA6BF13EEABFA48BD17DB0.
196. EY, KPMG, Deloitte, and PwC

detailees or rotations to fill positions within their cyber teams (e.g. JFSA). A number of interviewees expressed frustration at the lack of first-hand experience working in FIs among regulators, and noted that a key weakness of third-party audit and testing regimes is the lack of understanding of the unique circumstances and business of the organization under review. The result, according to both FIs and regulators we spoke to, can be a shallow level of expertise and inconsistent standards, methodologies, and priorities among examiners. This makes it difficult for regulators to advance long-term strategic oversight priorities and can lead to conflicting and inconsistent feedback to FIs, further complicating their security and compliance efforts.

> *Perhaps the most significant challenge for regional cybersecurity is the massive cyber talent shortage in APAC countries.*

FIs themselves also vary widely in their cyber capacity and the maturity of their cybersecurity teams. Many Japanese and Indian FIs, for example—including some of the largest banks—have only recently appointed CISOs and risk officers responsible for cybersecurity, and many of these are general risk officers with little to no technical knowledge or cyber experience. They often lack the staff, budget, and seniority within the organization compared to CISOs at major Western FIs. Cybersecurity strategies at many of these companies are new and only partially implemented, and some interviewees complained that they depend heavily on outside consultants whose expertise is more in regulatory compliance than operational cybersecurity.

Some requirements create more immediate risks to security and stability in the regional financial sector. Perhaps the most worrisome is penetration testing in production environments. As the CBEST regulatory model continues to gain traction in the region, financial institutions potentially face redundant requirements for realistic, intelligence-based penetration tests on critical assets. Conducting frequent penetration tests in production environments can raise significant risks to FIs, as testers can inadvertently disrupt or degrade bank services or expose customer data.

Finally, some policy trends are making it difficult for FIs to operate across borders and threaten to impose requirements on multinational FIs that would force them to fragment their networks into a patchwork of segregated national systems. The first is data localization requirements and restrictions on data flows. Currently, of the five jurisdictions in this study, only China has broad restrictions on cross-border data flows in force, though India, Singapore, and Hong Kong all have potentially restrictive laws that may be implemented in the future.

Some countries have also implemented policies requiring data to be stored in-country, which can greatly complicate the operations of multinational FIs, even if they do not explicitly restrict data flows. For example, India requires that certain communications data be stored domestically by FIs and insists that systems and facilities be available for on-site inspections by regulators in the country. Restrictions on cross-border data flows and data

localization requirements can be hugely damaging to FIs, whose business depends on the free flow of information between branches, counterparties, partners, and customers. They can also restrict FIs' ability to leverage security technologies, for example making it difficult to implement network monitoring or move operations to the cloud.

The other fragmentation challenge comes from domestic content requirements and third-party risk management rules that could be used to force FIs to work with domestic vendors and service providers. China, in particular, imposes onerous restrictions on third-party vendors, requiring FIs to use only government-approved products and services in "important parts of networks."[197] These requirements are not only costly to implement, but they cause significant security challenges, increasing the complexity of the network, making it difficult to maintain interoperability and visibility across the whole enterprise, and complicating efforts to implement security solutions on a wide variety of systems from a range of vendors.

The Case for Regulatory Harmonization

While financial regulators in APAC have drawn from a common set of international models in establishing their cyber regulatory regimes, regulations across the region are not coordinated, often leading to redundancy and friction for multinational banks and businesses. Harmonizing regulatory approaches across the region offers significant potential benefits for regulators, FIs, customers, and businesses across the region.

Most interviewees agreed that true conflicts of laws and regulations are rare. Regional regulators have largely developed their cybersecurity regulatory frameworks based on the same international models, primarily CBEST and the FFIEC, and are heavily influenced by a common set of international standards in conducting examinations and evaluating compliance. Interviewees from the banks largely agreed that the challenges of overlapping regulatory obligations are generally more burdensome from a compliance perspective than they are operationally challenging.

That said, each jurisdiction has significantly adapted these models to their own circumstances, creating a patchwork of similar but not necessarily complementary regulatory and oversight regimes for multinational FIs. Establishing common standards and harmonizing requirements across the region offers an opportunity to better manage systemic risk, increase regulatory efficiency, and raise the baseline level of security and protection across the regional financial system, particularly in smaller countries with limited cybersecurity capacity.

Regulatory harmonization also offers a powerful solution to the workforce challenge. Eliminating redundant security assessments, audits, and penetration tests can make more cybersecurity professionals available for other tasks, such as operational security roles at FIs and critical oversight and examination roles in regulatory agencies. Establishing common standards, certification requirements, and reporting regimes can simplify the regional talent pipeline, making it easier for new workers to gain the skills, expertise, and certifications they need, as well as allowing available workers to support security operations and regulatory compliance across multiple jurisdictions.

197. Covington and Burling LLC, *China Seeks Public Comments*.

Harmonization also promises to reduce regulatory overhead and barriers to competition, both for major banks and small, innovative fintech companies. The regional fintech sector is one of the fastest-growing industries in Asia, and spurring the growth of this dynamic sector was identified as a strategic priority by all of the regulators interviewed. In smaller jurisdictions, primarily Singapore and Hong Kong, fintech development requires easy access to larger regional markets, and the ability to compete for the attention and investment of major multinational banks depends on providing seamless access to large markets across APAC from a base with comparatively strong institutions and robust infrastructure.

> *Establishing common standards and harmonizing requirements across the region offers an opportunity to better manage systemic risk, increase regulatory efficiency, and raise the baseline level of security and protection.*

For regulators in large markets like China and Japan, growing the international presence of national FIs is also a priority. For some, a broader international portfolio can help diversify assets and increase profitability for large national banks. For others, expanding the international reach of major national banks offers an opportunity to extend their influence overseas, and to provide seamless financial support to other business sectors as they expand their global footprint. In Japan, for example, many interviewees noted that Japanese banks focus primarily on catering to Japanese businesses, and that their international branches and operations serve as financial links between their domestic and overseas operations.

4 | Recommendations

In a perfect world for multinational FIs, regulators would consolidate all of their requirements, audit specifications, inspection manuals, and testing regimes into a single set of rules, but this is unlikely to happen. Regulators are responsible for the protection of consumers and citizens and will not cede their authority over the entities that operate within their jurisdictions. That said, as mentioned above, regulatory fragmentation and inconsistency create real risks and challenges for the regional financial sector, undermining the goals of security, resiliency, efficiency, and innovation for all regulators.

The first step for APAC regulators to improve the security and resilience of the regional financial system against cyber threats is to establish a shared lexicon for cybersecurity. While regulators will likely never use a single set of requirements across jurisdictions, most regional regulators draw from the same sources to control for similar risks. However, because of small differences and ambiguities in regulatory language, it can be difficult and time-consuming for FIs to map their internal controls to the thousands of specific controls and examination questions used by different regulators. The goal of this effort should be to establish a common vocabulary for cybersecurity control principles that can be utilized by regulators across the region, and allow FIs to seamlessly map requirements from a variety of regulators to their internal security controls.

Regulators should also adopt flexible, principles-based approaches based on this common lexicon, avoiding highly granular requirements. This would allow more room for regional FIs to adapt their security controls to the wide range of business models, sizes, and threat landscapes across the region. It would also reduce the likelihood of conflicts of laws and regulations between jurisdictions. Some regulators, for example MAS, are already adopting this type of approach, but there is inconsistency across the region.

Perhaps the most important step that regulators can take to strengthen regional and global resiliency is to view FIs through a global lens, understanding their risks from the perspective of the enterprise as a whole rather than its operations in a specific country. Regulators have traditionally taken a local view of cyber risks, evaluating threats to FIs from the narrow perspective of direct threats to customers within their jurisdictions. On the one hand this makes sense, as regulators' authority is generally based on laws with territorial scope designed to protect citizens within their own country. Malicious actors do not recognize borders, however, and the interconnected nature of the global financial

system means that any attack on a major FI, whether it directly targets customers within a specific jurisdiction or not, can have significant consequences for all.

> *The most important step that regulators can take to strengthen regional and global resiliency is to view FIs through a global lens.*

Instead of requiring dozens of separate vulnerability assessments, penetration tests, and audits tailored to each specific jurisdiction, regulators should work with industry to establish a common testing and evaluation framework that will allow banks to conduct one set of highly rigorous security assessments on their global systems that could be submitted to a range of regulators. By moving to a common testing and evaluation framework for FIs' global systems, regulators could remove the duplication of efforts required under current regulations, allowing FIs to conduct more rigorous and in-depth assessments of their global risks and allocate greater resources to operational cybersecurity rather than compliance.

This does not mean that regulators cannot test local systems independently. Many FIs use a combination of local and global systems to serve their customers, and local audits and assessments are appropriate to local systems.

This common framework should have two elements. The first is shared audit guidelines for cybersecurity and IT audits of global systems. Instead of having separate audit standards and certifying or empaneling auditors within each jurisdiction, regional regulators should establish a common set of guidelines and certifications for cybersecurity audits so that different regulators can accept the results of a standard global IT audit of FIs. These guidelines should be based on the international standards already used by most regulators in the region, including the NIST Framework, ISO 27000, and ISACA COBIT.

The second element is establishing a single, rigorous penetration testing framework, including agreed upon testing standards, assessor certifications, and reporting formats that can be accepted by regulators across the region. Conducting multiple realistic threat-based penetration tests in production environments is costly and risky for firms, and these tests often look for similar vulnerabilities in the same systems. A shared framework can help regulators establish a better picture of risks at a systemic level, compare threats and security measures across the region and between institutions, reduce the cost and inefficiency of redundant testing regimes, and make it easier for small and medium-size institutions to conduct rigorous and effective security testing. The testing framework should be developed in close consultation with industry efforts like the Global Financial Markets Association's (GFMA) Key Principles for a Commonly Accepted Penetration Testing Framework or the Association of Banks in Singapore's Penetration Testing Guidelines for the Financial Industry in Singapore. [198]

198. "GFMA Publishes Cybersecurity Penetration Testing Framework," Global Financial Markets Association, April 3, 2018, http://www.gfma.org/news/press-releases/2018/gfma-publishes-cybersecurity-penetration-testing-framework/; Association of Banks in Singapore, *Penetration Testing Guidelines*.

Regulators should also work to facilitate robust information sharing between jurisdictions. While regulators have recognized the importance of cyber threat information sharing between FIs in many jurisdictions, cross-border sharing remains a challenge, as well as automated sharing of indicators of compromise (IOCs) and signatures.

Harmonization should not be limited to financial regulators. For many FIs, the mostly costly and disruptive requirements being considered are data localization laws and data flow restrictions, which are often developed by non-sector-specific data protection authorities. Ensuring the interoperability of privacy and data protection schemes among Asian economies is essential given the importance of data transfers to cross-border financial flows. Currently, Japan and Singapore are members of APEC CBPR, and Hong Kong is reportedly considering joining as well, which would provide a baseline set of privacy protections among major regional financial centers.[199] These countries should work with their regional partners, including non-APEC members like India, to establish interoperable data privacy regimes across the region.

The Complicated Multilateral Landscape in APAC

Harmonizing cybersecurity requirements for FIs across APAC is complicated by the size and diversity of the region, the wide range of fora in which multilateral and multi-stakeholder discussions on cyber issues are held, and the inconsistent membership of various regional organizations.

Different regulators and countries had different views on which international organizations would be effective venues to discuss harmonization. APEC, for example, was cited by many regulators and experts, particularly in Hong Kong and Singapore, as a key forum for regulatory harmonization, but it does not include India (yet). Japanese experts pointed to the G7, despite the fact that Japan is the only Asian member country. Others felt that the G20 or BIS would be the appropriate venue, as effective harmonization should include major financial hubs like New York and London. Regardless, harmonization will require coordinated efforts at multiple levels to be effective, including bilateral and multilateral negotiations, cooperation in regional fora, and global efforts coordinated with U.S., UK, and EU financial regulators.

At the regional level, regulators and FIs should utilize existing mechanisms under APEC to push for greater integration and harmonization across the region. The mission of APEC is to "synchronize regulatory systems" across the Asia-Pacific region to accelerate regional economic integration and trade. It is a voluntary, consensus-based organization that includes the major Asian economies, as well as key Pacific partners like the U.S. and Australia that have significant links to the Asian financial system.[200]

In addition to CBPR, the APEC Finance Ministers' Process (FMP) provides a venue to bring together senior financial ministry and central bank officials from APEC member countries. The FMP works closely with the Asia-Pacific Financial Forum (APFF), a private

199. Bui Hang, "Survey on the Readiness for Joining Cross Border Privacy Rules System."
200. APEC's member economies are: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Vietnam.

sector working group within APEC, on questions of cyber and data regulation. In 2018, APFF produced two guiding documents: An APEC Roadmap for a New Financial Services Data Ecosystem and A Roadmap for the Development of APEC's Financial Market Infrastructure.[201] The FMP should work with the APFF to translate these roadmaps into concrete proposals for consistent, consolidated regional regulatory frameworks that can be adopted by regulators in APEC member states.

> *Harmonization will require coordinated efforts at multiple levels to be effective, including bilateral and multilateral negotiations, cooperation in regional fora, and global efforts coordinated with U.S., UK, and EU financial regulators.*

Interestingly, while many regulators and experts called for Asian countries to lead their own efforts toward harmonization, cooperation among regulators within the APAC region is limited. Most looked to the United States and European countries for guidance, not to their more immediate neighbors. One regulator argued this is because of a perception that there are relatively few mature cyber regulatory frameworks for FIs within the Asia Pacific, while other interviewees suggested it has to do with competitive political dynamics between East Asian countries. Integrating regulatory harmonization efforts between regional and global institutions will be essential, not only to create a strong global cyber resiliency framework, but also to get real buy-in from APAC nations.

Most of the experts we spoke to identified the G20 and the BIS as key venues for global regulatory harmonization efforts. The BIS hosts a number of existing working groups, programs and organizations including the Committee on Payments and Market Infrastructures, the Financial Stability Board, and the Basel Committee on Banking Supervision.

The BIS and G20 processes have produced some significant progress in establishing norms and best practices for global cyber risk management and governance in recent years, but their processes are slow, bureaucratic, and difficult to implement. The Third Basel Accord, for example, was agreed to in 2010, but still has not been brought into force. While these institutions can be useful to facilitate long-term global coordination—and APAC countries should work with them and leverage best practices and guidance, like the CPMI-IOSCO Guidance on Resilience for Financial Market Infrastructures, in establishing regional regimes—APAC countries should also work with regional partners to establish voluntary, non-binding consensus mechanisms for regional cooperation.[202]

---

201. Asia-Pacific Financial Forum (APFF), *An APEC Roadmap for a New Financial Services Data Ecosystem* (APFF, 2018), https://www2.abaconline.org/assets/2018/APFF/Data_Ecosystem_Roadmap_2018-08-03.pdf; Asia-Pacific Financial Forum (APFF), *A Roadmap for the Development of APEC'S Financial Market Infrastructure*, https://www2.abaconline.org/assets/2018/APFF/Roadmap_for_the_Development_for_APEC_s_Financial_Market_Infra_20180515.pdf.
202. Bank for International Settlements, *Guidance on cyber resilience for financial market infrastructure* (BIS, 2016), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf.

5 | Conclusion

As cyber threats to financial institutions continue to grow, it will be incumbent on the regulators responsible for the security and resiliency of the global financial system to ensure that they have the mechanisms in place to effectively manage cyber risks. The financial system is global, and so are malicious actors, launching attacks across borders that target thousands, if not millions of customers at once across multiple jurisdictions. In this environment, APAC countries face threats not only from the vulnerability of individual institutions within their own borders but also from broader vulnerabilities across the region and throughout the operations of multinational firms.

While regional regulators are increasingly focused on cyber risks, each is focused narrowly on cyber risks affecting their specific jurisdictions and customers, making it hard to see and manage the overall threat landscape facing multinational FIs and the regional financial system as a whole. Little coordination is taking place between regulatory regimes in different countries, leading to a growing patchwork of often redundant and occasionally conflicting requirements across jurisdictions.

Improving this situation will require working with a broader swath of agencies than just dedicated financial regulators. As financial institutions are increasingly being classified as critical infrastructure, and as more countries develop cybersecurity rules and requirements for critical infrastructure operators, it will become increasingly important to ensure that regulators are able to cooperate not only between countries, but also within them. Data protection authorities will also play an increasingly important part as countries around the world revisit the concept of digital privacy and its implications for institutions like FIs that hold large amounts of sensitive consumer data.

For the deeply integrated Asia-Pacific region, taking on the transnational cyber threat will require a transnational response. Strengthening the security and resiliency of financial networks across the region will require looking at FIs from an enterprise perspective and understanding the cyber risks they face from the perspective of defenders, not the narrow lens of national borders. It will require principles-based approaches that allow for the wide range of business models and capacities of FIs across the region, and consolidated auditing, examination, and testing procedures to ensure that regulators have an accurate picture of the risks and controls at institutions under their care. Ultimately, regulators' goals must be to ensure that strong security and resilience, not redundant compliance, is the focus for FIs.

About the Authors

William A. Carter is deputy director of the Technology Policy Program at CSIS. His research focuses on international cyber and technology policy issues, including artificial intelligence, surveillance and privacy, data localization, cyber conflict and deterrence, financial sector cybersecurity, and law enforcement and technology, including encryption. He has spoken at events and conferences around the world and participated in Track 2 dialogues on cyber and technology policy issues with China, Russia, and Australia. Before joining CSIS, he worked in the Goldman Sachs Investment Strategy Group, where he performed research and analysis on geopolitics and the macro economy and produced reports and presentations on international affairs and current events and their impact on markets. He previously worked at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University with a BA in economics.

William D. Crumpler is a research assistant with the Technology Policy Program at CSIS, where he works on issues related to the governance of emerging technologies, the development of national and international cybersecurity policy, and innovation in the digital economy. His recent work has focused on topics including the regulation of AI technologies in the U.S. and China, security and innovation in 5G mobile networks, and the harmonization of global cybersecurity and data governance regulations. He holds a B.S. in materials science and engineering from North Carolina State University.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**