KPMG

Regulatory Scrutiny of Technology and Data

Financial Services Regulatory Insights

Contacts

To discuss the issues raised in this report, **please contact:**

Amy Matsuo
Principal and Leader
Regulatory and ESG Insights
amatsuo@kpmg.com

Anand Desai
Principal
Risk Services, Financial Services Leader
ananddesai@kpmg.com

Matt Miller
Principal
Cybersecurity Services
matthewpmiller@kpmg.com

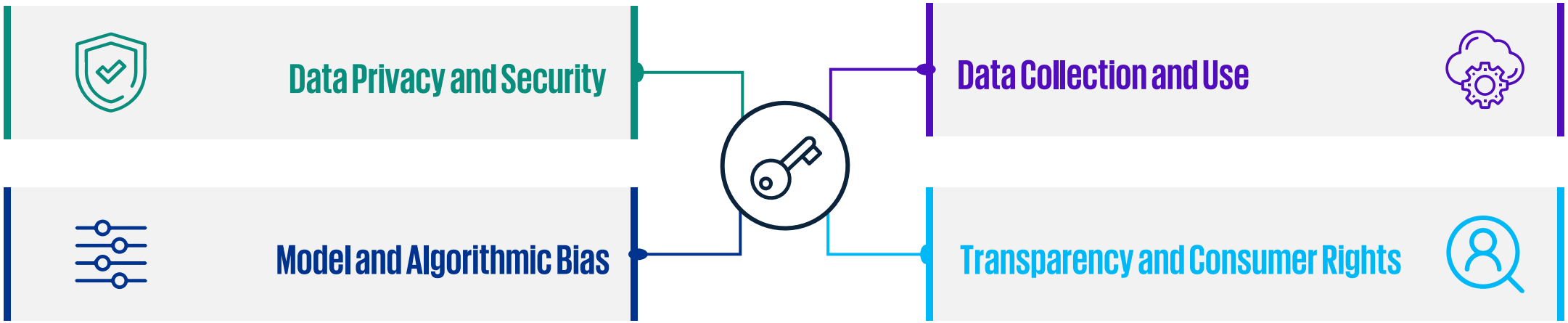
Alexander Smith
Managing Director
Modeling and Valuation Advisory
alexandercsmith@kpmg.com

Nilotpal Roy
Managing Director
C&O Financial Services Advisory
nilotpalroy@kpmg.com

Table of contents

Managing technology and data: Key regulatory themes

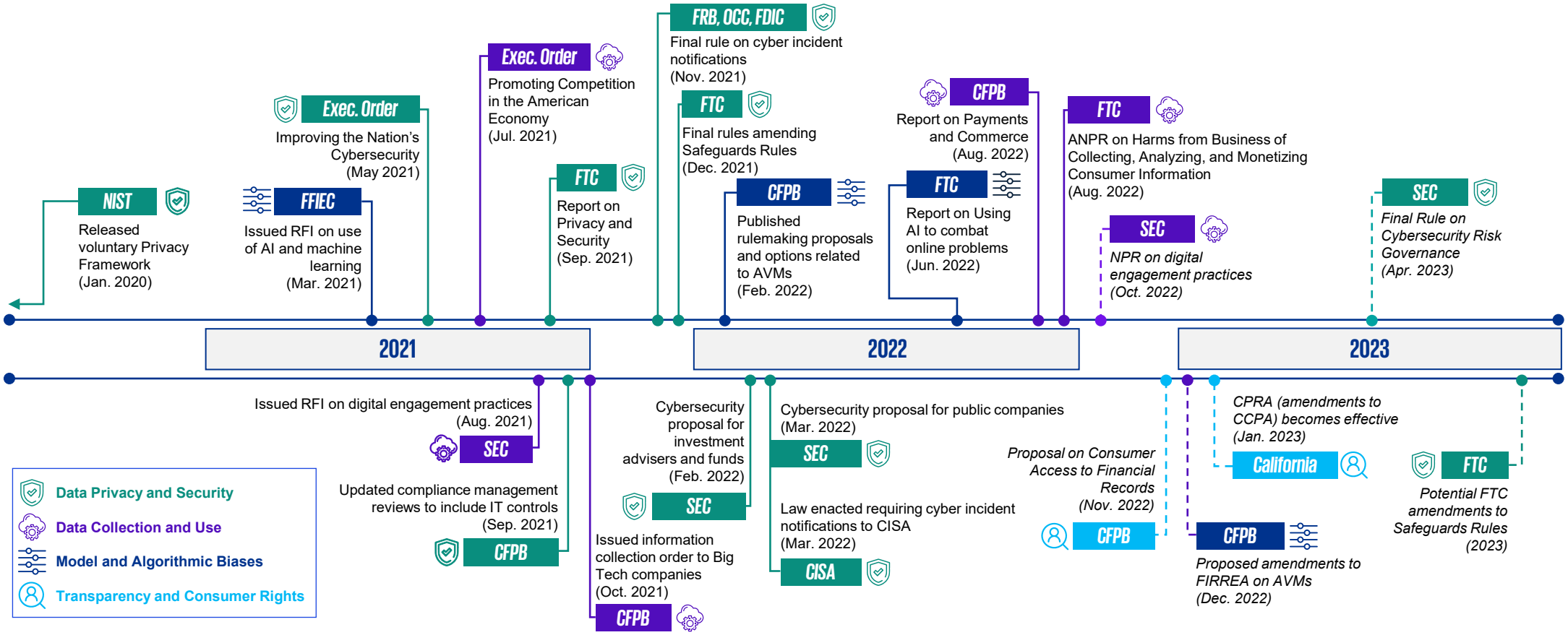
Regulators are increasing their scrutiny and enforcement of issues involving data privacy and security and the applications of new technologies. They are actively seeking information to understand and set parameters around the expanding number of ways that financial institutions are able to collect and use consumer financial data as well as to ensure controls to protect data privacy and security. Increasingly, regulators are considering rules that give consumers more control over their own financial data while also calling out and taking action where lax security protocols, such as those around access channels or records retention, put customer data at risk of misuse, including fraud, theft, or abuse. Key areas of regulatory action include these themes:



Actions to consider in each of these areas along with an analysis of relevant regulatory developments and expectations follow.

Regulatory events timeline

Companies face an assortment of requirements and standards around data privacy and security, data collection and use, potential model and/or algorithmic biases, and transparency and consumer rights. Regulators are actively seeking input on the impact of new technologies on data privacy and security.



1 Data privacy and security

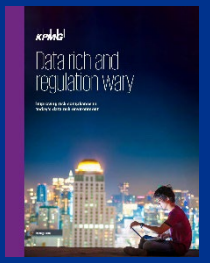
Companies should examine their approach to protecting consumer data privacy, giving consideration to "privacy-by-design" principles - embedding privacy into the design, operation, and management of new applications, including technology systems, artificial intelligence, and digital business practices - with the goal of preventing privacy vulnerabilities (e.g., malware, fraud, identity theft, insider risk, reputation risk).

Key considerations include:

- Are current privacy-related policies, practices, and procedures adequate with regard to:
  - All applicable laws and regulations?
  - The size and scope of business activities?
  - The sensitivity of data being handled?
  - The volume of data being handled?
  - The number of individuals or devices from which data is collected, processed, or transferred?
  - The number and variety of access channels available?
- Do privacy vulnerabilities or risks identified include a risk of fraud or other illicit activities associated with consumer data or the company's technology?
- Are privacy risks being integrated into enterprise-wide risk management?
- Are current cybersecurity policies, procedures, programs, and protocols:
  - Compliant with applicable regulatory requirements, such as breach notifications, records retention, disclosures?
  - Adequately managing cybersecurity risks, including fraud and consumer data theft?
  - Utilizing best practices to ensure data protection and security, such as multi-factor authentication, password management, and timely software updates?

To learn more...

Enhancing the cybersecurity risk framework



Data rich and regulation wary

Regulatory landscape: Data privacy & security (1/2)

		Highlighted Examples (privacy)
2021	***NIST*** Released voluntary Privacy Framework (Jan. 2020)	**NIST:** Provides guidance across three sections, with each section reinforcing privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities
2022	***CFPB*** Updated compliance management reviews to include IT controls (Sep. 2021)	**CFPB:** Evaluation may consist of technology controls and those of service providers, including board and management oversight, compliance program, service provider oversight, and violations of law and consumer harm. Evaluation may consider IT related to compliance with consumer protections.
	FTC Report on Privacy and Security (Sep. 2021)	**FTC:** Outlined priority areas, including examining market power or competitive advantages and expanding remedies for harmed consumers.
	FTC Final rule amending Safeguards Rules (Dec. 2021)	**FTC:** Effective January 1, 2022, including guidance, implementation, governance, and accountability for information security programs.
2023	***FTC*** *Potential FTC amendments to Safeguards Rules (2023)*	**FTC:** Released a RFI on further amendments to the Safeguards Rule to require reporting any security event where companies determine the misuse of the information. Proposal expected in 2023.

Regulatory landscape: Data privacy & security (2/2)

		Highlighted Examples (security)
2021	***Exec. Order*** Improving the Nation's Cybersecurity (May 2020)	**Exec. Order:** Directs a "whole of government" effort to enable more effective defense of federal IT assets and networks, and improve overall cybersecurity
2022	***FRB, OCC, FDIC*** Final rule on cyber incident notifications (Nov. 2021)	**Interagency:** Reporting requirements for computer-security incidents
2022	***SEC*** Cybersecurity proposal for investment advisers and funds (Feb. 2022)	**SEC:** Proposed rules promoting cyber preparedness and resilience for registered advisers and funds
2022	***SEC*** Cybersecurity proposal for public companies (Mar. 2022)	**SEC:** Proposed rules to enhance and standardize cybersecurity disclosures for public companies including risk management, strategy, governance, and incidence reporting
2022	***CISA*** Law enacted requiring cyber incident notifications to CISA *(Mar. 2022)*	**CISA:** Owners and operators of critical infrastructure, including financial services, must report cyber incidents within 72 hours, ransomware payments within 24 hours
2023	***SEC*** *Final Rule on Cybersecurity Risk Governance* (Apr. 2023)	**SEC:** Final rules on cybersecurity risk management and governance are expected in April 2023

2 Data collection and use

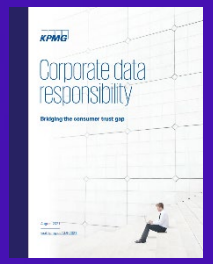
As consumer data collection, or "harvesting," proliferates, and sharing, selling, and utilizing that data become common practice, companies should examine their practices to ensure compliance with laws and regulations, as well as adequate management of data risks associated with these activities.

Key considerations include:

- Does the company have specific, explicit purpose(s) for handling consumer data *(purpose limitation)*?
- Does the company hold consumer data for only as long as is necessary for its purpose *(data minimization)*?
- Does the company have adequate oversight of third party handling of consumer data? Is a special contract with the service provider required by law or regulation?
- Does the company's utilization of data and technology result in equal treatment of consumers?
- Does the company utilize data and technology to directly interact with consumers? Does the company, or its tools, influence consumer decisions or provide "advice"?
- Does the company transfer, share, sell or otherwise monetize the data?
- Do consumers know when and how the company is collecting their data? Must they opt in or opt out of data sharing?

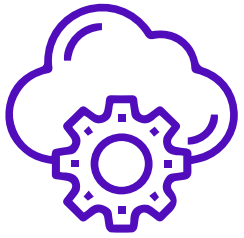
To learn more...

Platforms and conduct
Fraud and financial crimes
Fairness and inclusion



Corporate data responsibility: Bridging the consumer trust gap

Regulatory landscape: Data collection & use



		Highlighted Examples
2021	***Executive Order*** Promoting Competition in the American Economy (Jul. 2021)	**Executive Order:** Directs FTC to consider rulemaking on "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy." Directed CFPB to consider rulemaking that would facilitate the access and portability of consumer financial data ("section 1033")
	SEC Issued RFI on digital engagement practices (Aug. 2021)	**SEC:** DEPs can include behavioral prompts, differential marketing, or other elements designed to digitally engage retail investors. RFI seeks information on the extent to which firms use DEPs, types most frequently used, tools and methods used to develop and implement them, and information on retail investor engagement with DEPs
2022	***CFPB*** Issued information collection order to Big Tech companies (Oct. 2021)	**CFPB:** Information on business practices related to data harvesting, use, and monetization; business practices' alignment with consumer expectations; consumer expectations of protection from fraud and payment errors, protection of data and privacy, responsive customer service, and equal treatment
	CFPB Report on Payments & Commerce (Aug. 2022)	**CFPB:** Discusses advances in technology and payments innovations, as well as opportunities for companies to aggregate and monetize consumer financial data, and for large players to dominate consumers' financial and commercial lives. Features "super apps," "BNPL," and "embedded commerce."
	FTC ANPR on Harms from Business of Collecting, Analyzing, & Monetizing Consumer Info. (Aug. 2022)	**FTC:** Topics for comment include: lax data security, harm to children, retaliation, surveillance creep, inaccuracy, bias and discrimination, and dark patterns
2023	***SEC*** *NPR on digital engagement practices (Oct. 2022)*	**SEC:** Following the Aug. 2021 RFI, proposed rules on DEPs are expected fall 2022.

3 Model and algorithmic bias

The use of machine learning and artificial intelligence (ML/AI), as well as and complex algorithms, has led to numerous opportunities for companies in the areas of market identification, automated decision-making, customer outreach, risk mitigation, and strategic investments.

However, the risks posed by their use can lead to unfair or discriminatory outcomes, as well as perpetuating existing socioeconomic disparities. Often these risks can be hidden within data fed into the models. Regulators have indicated increasing scrutiny and enforcement based on ML/AI algorithms.

Key considerations include:

Transparency

- Do consumers know when and how the company is collecting their data?
- Do consumers know when they are interacting with automated tools?
- Do “adverse action” notices to consumers, especially if making automated decisions based on third-party data) meet regulatory requirements?

Explainability

- If using algorithms to risk-score consumers, are disclosures adequately explaining the key factors impacting their scores?
- If denying products or services to a consumer, does the notice explain what data was used and how it was used to arrive at the decision?
- Do hidden biases appear to exist in the data; are unexpected correlations with protected classes explored?

Fairness

- Is the data being used as model inputs representative of the relevant consumer population?
- Do model inputs and outcomes lead to disparate and/or adverse impacts for particular groups or protected classes?
- Do consumers have the access and/or opportunity to correct information used as model inputs?

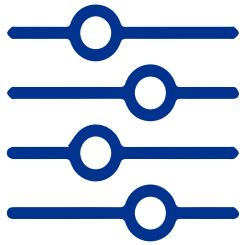
Verifiability

- How accurate are model predictions based on big data? How is accuracy determined?
- Are models validated and revalidated, with intended outcomes and no illegal discrimination?

Accountability

- Are the governance and accountability mechanisms (e.g. escalation protocols, board approvals, etc.) around models, AI, and algorithms adequate?

Regulatory landscape: Model & algorithmic bias



		Highlighted Examples
2021	***FFIEC*** Issued RFI on use of AI and machine learning (Mar. 2021)	**FFIEC:** Topics covered in the RFI included explainability, risk from broader or more intensive data processing and usage, overfitting, cybersecurity risks, dynamic updating, use of AI, oversight of third parties, and fair lending
2022	***CFPB*** Published rulemaking proposals and options related to AVMs (Feb. 2022)	**CFPB:** SBREFRA outline of potential rulemakings related to confidence in AVM (automated valuation model) estimates, protections against data manipulation, avoidance of conflicts of interest, and random testing/review
2022	***FTC*** Report on Using AI to combat online problems (Jun. 2022)	**FTC:** Outlines concerns that AI tools can be inaccurate, biased, or discriminatory by design and incentivize relying on increasingly invasive forms of commercial surveillance
2022	***CFPB*** *Proposed amendments to FIRREA on AVMs (Dec. 2022)*	**CFPB:** Proposed amendments to address quality control standards for AVMs) and are expected December 2022
2023	***New York City*** *Effective date for law governing automated employment decision tools (Jan. 2023)*	**New York City:** Local law requires companies operating within NYC that utilize “automated employment decision tools” to: 1) create a bias audit process for the tool(s) and 2) notify candidates or employees about use of the tool and job characteristics or qualifications used in the tools.

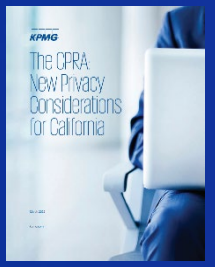
4 Transparency and consumer rights

Depending on their business type and primary regulator, companies are currently subject to numerous requirements and standards around data privacy and security from provisions of the Gramm-Leach Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), individual state privacy laws (such as California's California Consumer Privacy Act (CCPA), and international requirements (if applicable), such as the EU's General Data Protection Regulation (GDPR).

Key considerations include:

- Do current policies, procedures, or processes outline or define "standards of care" for data that facilitates transparency and consumer rights?
- Are the processes through which consumers can exercise their data rights? Can consumers access, correct, delete, or opt-out of data collection, processing, and utilization?
- Are the processes that inform consumers of their data rights?
- Do current processes obtain consumer consent prior to collecting and processing sensitive personal data, such as geolocation data, data about protected characteristics, and genetic or biometric data?

To learn more...



The CPRA: New Privacy Considerations for California

Regulatory landscape: Transparency & consumer rights

2021

2022

2023

Highlighted Examples

CFPB

Proposal on Consumer Access to Financial Records (Nov. 2022)

CFPB: Proposal is expected to cover topics including consumer rights to access financial records under the Dodd-Frank Act and data access, particularly authorized data access ecosystems, users, modes of access, competitive incentives and standard-setting, and consumer impacts

California

CPRA (amendments to CCPA) becomes effective (Jan. 2023)

California: The CPRA amends the CCPA to provide the following consumer rights: the right to correct inaccurate personal data and the right to limit use and disclosure of personal data. CCPA provided consumer rights to know what data is collected, delete personal data, opt-out of sale of personal data, access information about and opt-out of automated decision making, and non-discrimination in exercising their rights (*Note: four other states have adopted privacy rules similar to California's and a number of others are actively considering doing so.*)

Technology risk: Priority areas of focus

To date, regulators have focused on areas of risk particularly including data security.

Adequacy of risk assessments processes

- Definition of and approval for cybersecurity risk appetite statement
- Connection between risk assessments/risk monitoring to risk appetite statement and threat intelligence
- Documentation of risk acceptances and risk treatment activities
- Ongoing monitoring and adjustment of internal controls
- Board approved risk appetite/tolerances

Vulnerability management (incl. End of Life system mgmt.)

- Aged un-remediated vulnerabilities
- Tools used for vulnerability discovery and verification (coverage and visibility)
- Prioritization strategy for remediation activities
- Management of non-patchable vulnerabilities
- Control enforcement in legacy environments
- Traceability of reporting

Data and cloud governance

- Existence/adequacy of data and cloud governance programs
- Definition of data strategy and inventory across cloud and legacy environments for structured, semi-structured, and unstructured data
- Effectiveness of oversight, review, and challenge
- Program coverage for all divisions/processes (not just mission critical)

Identity and access management

- Existence/adequacy of PAM (privileged access management) program and controls (e.g., MFA, least privilege, recertifications)
- Prevention of toxic entitlement combinations
- Protection of authentication credentials (e.g., encryption)
- Use of jump servers to reduce span of access
- Management of non-person accounts (incl. control enforcement)

Secure software development life cycle

- Testing in production environments
- Obfuscation of data in development environments
- Controls over system acquisition

Third-party risk

- Identification of non-vendor third parties
- Management of third party security risk via means other than assessment
- Fourth/nth party security
- Assessment of risks emanating from suppliers and third parties
- Development of a comprehensive cooperative approach to operational resilience

Threat intelligence/ Insider threat

- Adequacy of threat detection and monitoring; maturity of SIM capabilities
- Maturity of endpoint detection and monitoring solutions
- Coverage of threat intelligence (on-prem and cloud environments)
- Existence of insider threat program/Inventory of threats and associated mitigating actions
- Relevancy of insider threat use cases and continuous use case monitoring, including relevant metrics

Operational resilience

- Effectiveness of governance practices (to help maintain operational resilience, and comply with applicable laws and regs)
- Review of operational resilience practices. Identification of critical operations, core business lines, and material entities
- Development and implementation of effective controls and resilient information systems to maintain critical operations
- Testing and ongoing updates; coordination with business continuity management and disaster recovery teams

Board reporting

- Quality and timeliness of metrics (both operational and risk)
- Depth of insights provided via reporting
- Ability of the Board to provide relevant, meaningful challenge and track required corrective actions
- Periodic review of risk appetite statements (weathering operational risk disruptions)
- Board reporting during a cyber incident (incl. notification timeframe)
- Definition and testing of Board requirements regarding a cyber incident

2nd/3rd line of defense oversight

- Existence/adequacy of 2nd and 3rd lines of defense
- 2nd line's quality of risk visibility for assessment and monitoring
- 3rd line's ability to enforce findings in the 1st line

Appendix: Abbreviations & Acronyms

AI	Artificial Intelligence	FFIEC	Federal Financial Institutions Examination Council	ML	Machine learning
CFPB	Consumer Financial Protection Bureau	FRB	Federal Deposit Insurance Corporation	NIST	National Institute for Standards and Technology
CISA	Cybersecurity and Infrastructure Security Agency	FTC	Federal Trade Commission	OCC	Office of the Comptroller of the Currency
FCRA	Fair Credit Reporting Act	GDPR	General Data Protection Regulation	SEC	Securities and Exchange Commission
FDIC	Federal Deposit Insurance Corporation	GLBA	Gramm-Leach-Bliley Act	SOX	Sarbanes-Oxley Act
		IT	Information technology		

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia