Client Alert | Financial Institutions Advisory

Regulators Diverge on How Best to Manage Growing Cybersecurity Risks

November 2016

Authors: Kevin Petrasic, Benjamin Saul, Matthew Bornfreund, Joshua Garcia

On October 19, the Federal Reserve Board, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency (the Agencies) issued an advance notice of proposed rulemaking (ANPR) seeking to enhance cyber risk management standards at large financial institutions via implementation of nearly 80 separate cybersecurity-related requirements.[1]

The ANPR, which solicits public comment on 39 multi-part questions,[2] was issued four weeks after the New York State Department of Financial Services (NYDFS) proposed its own rule requiring New York state-licensed entities to adopt specific cybersecurity protections (NY Proposal).[3] While the ANPR solicits comment, the NY Proposal is scheduled to become effective in January 2017.

Although both the ANPR and NY Proposal would heighten regulatory expectations and require covered institutions to enhance controls to manage cybersecurity risks, the proposals differ significantly in approach. The ANPR sets forth a more fluid, principles-based framework of cybersecurity controls, whereas the NY Proposal details specific, proscriptive cybersecurity requirements for covered institutions. The ANPR envisions a rule requiring covered financial institutions to incorporate cybersecurity controls in all aspects of their existing risk management procedures, allowing them to customize compliance approaches. In contrast, the NYDFS rule would require covered entities to implement specific technologies and actions to contain cybersecurity risks, and imposes a significantly more rigorous and aggressive compliance regime.

Financial Institutions Advisory

- Bank Advisory
- Broker-Dealer
- Consumer Financial Services
- Cybercurrency
- Cybersecurity
- Data Privacy & Protection
- EU and WTO
- FinTech
- Investment Advisory & Management
- Payments
- Sanctions, Bank Secrecy and Export Controls
- Securities
- Trust and Fiduciary

The Year of Cyber Guidance

Cybersecurity has become an overriding theme among regulators this year. Beyond the ANPR and NY Proposal, there were two other notable cybersecurity releases. In June, the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) released Guidance on cyber resilience for financial market infrastructures (CPMI-IOSCO Guidance).[4] In September, the Federal Financial Institutions Examination Council updated its Information Security booklet (IS Booklet), an integral part of the FFIEC Information Technology Examination Handbook.[5] Among other initiatives and statements, most notable was a joint statement issued by the Agencies in June reminding banks about the cybersecurity risks posed by interbank messaging and wholesale payment networks.[6]

The recent flurry of regulatory activity reflects a concerted policy response to a series of cyber-attacks that numerous companies faced between 2013 and 2015. During that period, a major retailer announced malware in its systems was used to steal millions of customers' credit card numbers; an online auction site revealed that over 200 million user records had been taken by attackers who used stolen employee credentials; a major bank suffered a breach that allowed hackers to access over 80 million customer accounts; and a federal government agency had personnel records of over 20 million US government employees stolen. And 2016 has highlighted more of the same, including the announcement by a major web portal of a 2014 data breach in which over 500 million customer accounts were compromised, representing reportedly the largest data breach to date. In an environment where the risks of large-scale cyber-attacks have become ever present, regulators are working both reactively and proactively to improve cybersecurity for the financial system.

First Steps to Formal Rules

The NYDFS was a relatively early mover on cybersecurity issues, releasing a May 2014 report on cybersecurity in the banking sector.[7] The report, based on a survey of 154 institutions conducted in 2013, focused on specific technologies and practices that NYDFS identified as important for cybersecurity. For example, the report highlights the benefits of multi-factor authentication (MFA) and notes the significant disparity in its use between large and small institutions.[8]

A few months prior to the NYDFS report, on February 12, 2014, the Obama Administration launched the Cybersecurity Framework compiled by the Department of Commerce's National Institute of Standards and Technology (NIST Framework).[9] The NIST Framework is a comprehensive guide that helps organizations in any sector design appropriate cybersecurity systems and procedures. Three key features of the NIST Framework are: (1) it was designed with significant input from the private sector to be consistent with best practices from across numerous industries; (2) it is a collection of general statements, standards and guidelines that is neither industry-specific nor country-specific; and (3) it is voluntary. Although large companies are not required to follow it, because of the private sector input used to develop the NIST Framework, many large companies trust and refer to it when implementing cybersecurity protections.

In June 2015, the FFIEC created a more targeted resource, the Cybersecurity Assessment Tool (FFIEC Tool), which is available to any federally supervised banking organization to evaluate its own cybersecurity systems.[10] The FFIEC Tool was specifically designed to be consistent with the NIST Framework, and just as adoption of the NIST Framework is voluntary, so is use of the FFIEC Tool. However, because the updated IS Booklet embeds the principles contained in the FFIEC Tool, bank examiners will consider those cybersecurity principles when evaluating the impact of information technology systems on a banking organization's safety and soundness.

Federal Versus New York Approach

With the NIST Framework and FFIEC Tool providing guiding principles, the ANPR can be viewed as a continuation of the process to incorporate cybersecurity principles into the operations of financial institutions. Notably, the Agencies coordinated their efforts to develop the ANPR through the FFIEC's Cybersecurity and Critical Infrastructure Working Group. The Agencies also follow the lead of international standards-setting bodies, such as CPMI and IOSCO, in implementing a principles-based approach for cybersecurity at large and systemically important institutions. In contrast, the NY Proposal, although clearly influenced by the NIST Framework, appears focused mostly on remedying deficiencies identified in the May 2014 NYDFS report.

This generative process may explain some of the differences between the NY Proposal and the ANPR. For instance, the NY Proposal requires adoption of MFA in certain circumstances. In contrast, both the NIST Framework and the updated IS Booklet identify MFA as an important mechanism for preventing unauthorized access to computer systems but acknowledge that other methods may provide comparable or superior protection. The ANPR also would push covered institutions to integrate robust access controls, but it would do so by requiring the institutions to adopt certain cyber risk management principles, not by identifying the specific means to resolve each cyber threat.

Further, given their different jurisdictions, the NYDFS and the Agencies have different perspectives on their approach to cybersecurity controls. The NY Proposal is centered on the need to protect non-public consumer data that is stored on individual financial institution systems. This posture led to a proposal weighted more heavily with proscriptive rules designed to ensure each covered entity will protect the data under its control. The Agencies, however, view improving cybersecurity as necessary to preserve and protect the functioning of the financial system. Understandably, this perspective caused the Agencies to consider more generally applicable, principles-based regulations focused on interconnectedness and the role covered entities play in the financial markets.[11]

By focusing on “the cyber risks of the largest, most interconnected U.S. financial entities,” the Agencies could adapt existing enhanced risk management protocols.[12] Large banks are already subject to enhanced prudential standards such as stress testing, resolution planning, and certain capital and liquidity requirements.[13] The ANPR indicates that the enhanced cyber risk management standards—particularly the independent cyber risk management function—are structured similarly to the prudential standards, *i.e.* general principles as opposed to specific requirements. In contrast, the NY Proposal is more broadly focused and considers the ability of smaller licensed entities—with little or no experience implementing prudential regulation—to comply with new cybersecurity requirements. The NYDFS approaches its wider regulatory focus by enumerating clear and specific cybersecurity requirements and protections.

The following discussion highlights a number of the more important differences and similarities of the NY Proposal and ANPR. In addition, Appendix A contains a line-by-line chart of each requirement and recommendation under consideration by the Agencies in the ANPR, identifying whether a similar or analogous provision exists in the NY Proposal, the IS Booklet, the CPMI-IOSCO Guidance or the NIST Framework.

A Proscriptive Approach: The NY Proposal

As structured, the NY Proposal would impose new requirements on nearly all entities the NYDFS regulates, including businesses and individuals “operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.”[14] This definition covers everything from large New York chartered banks to smaller community banks, and from insurance companies to BitLicensed digital currency companies.[15]

The NY Proposal is largely centered on measures necessary to protect Nonpublic Information (NPI), which is defined as all information that is not Publicly Available Information.”[16] Under the NY Proposal, NPI includes:[17]

- Business related information that, when tampered with, could hurt the Covered Entity
- Information about individuals related to a financial product or service
- Information from a health care provider (except age or gender)
- Any information that reveals or can be used to trace an identity (including medical, educational, financial, or employment)
- Information used for marketing purposes
- Passwords or any other authentication factors

All Covered Entities under the NY Proposal (including those that fit the limited exemption) would have to establish a cybersecurity program and develop written policies, including a Cybersecurity Policy and Third Party Information Security Policy.[18] Covered Entities would also have to perform annual risk assessments of information systems, destroy certain NPI no longer necessary to provide products or services, and submit a written certificate of compliance with the rules annually to the superintendent.[19] Under the NY Proposal, a compliant cybersecurity program would, at a minimum:[20]

- Establish a program to manage cybersecurity threats to information systems
- Closely manage third parties through partnership policies and contract provisions
- Limit access privileges to information systems and NPI
- Notify the NYDFS superintendent within 72 hours of certain cybersecurity events

The NY Proposal would require non-exempt Covered Entities to engage in annual penetration testing and quarterly vulnerability assessments. Such entities would also have to develop a written incident response plan to respond promptly to and recover from certain cybersecurity events. Covered Entities would be required to:[21]

- Hire a Chief Information Security Officer and specialized staff
- Train personnel regarding cybersecurity risks, detection and readiness
- Monitor access to NPI
- Implement a cybersecurity audit trail system
- Ensure the security of internal and externally-developed applications
- Require MFA and risk-based authentication for specific scenarios
- Encrypt NPI data both in transit and at rest

A Principles-Based Approach: The ANPR

In contrast to the NY Proposal, the ANPR takes a principles-driven approach to enhancing the cybersecurity regime of regulated financial institutions having $50 billion or more in total assets.[22] The standards under the ANPR would be organized into five categories:[23]

- Category 1: Cyber risk governance
- Category 2: Cyber risk management
- Category 3: Internal dependency management
- Category 4: External dependency management
- Category 5: Incident response, cyber resilience and situational awareness

These categories closely match the CPMI-IOSCO Guidance, which is also designed for systemically important financial institutions. As with the CPMI-IOSCO Guidance, the ANPR would require entities to establish a comprehensive, written cyber risk management strategy. The cyber risk strategy would be incorporated into each firm’s overall, enterprise-wide risk management strategy. As proposed, the board of directors for each covered entity would be required to approve the cyber risk management strategy and to ensure the strategy is successfully implemented.[24] In order to accomplish this goal, the ANPR stipulates that boards of directors would be required to have adequate expertise in cybersecurity, including that directors should be able to provide a credible challenge to management in connection with the handling of cybersecurity matters and risks.[25]

Importantly, the Agencies are considering a requirement that covered entities situate cyber risk management in an independent risk management function.[26] This requirement—which is not contemplated in the other recent cybersecurity issuances—is designed to function at the holding company level. The ANPR would require the independent cyber risk management function to report directly to the chief risk officer and the board of directors.[27] Through this independent function, covered entities would be required to quantitatively measure the enterprise-wide efficacy of the firm's risk management strategy in reducing aggregate residual cyber risk.

The ANPR would require covered entities to integrate both internal and external dependency management strategies into their enterprise-wide strategic risk management strategy.[28] To monitor cybersecurity compliance, the Agencies propose requiring each covered entity to include an assessment of cyber risk management as part of the enterprise's overall audit plan.[29]

The ANPR, reflecting the Agencies' desire to implement cybersecurity controls and safeguards in an attempt to reduce cyber-attack risks to the financial system writ large, also places special focus on sector-critical systems (SCSs). The Agencies are seeking public input on the methods that would be used to determine an SCS. In general, SCSs would be systems that: (a) control or host at least five percent of the value of transactions in certain markets; (b) hold at least five percent of the assets in certain markets; or (c) exceed a to-be-determined measure of interconnectedness.[30] For these SCSs, the ANPR proposes a relatively aggressive (but understandable) two-hour recovery time objective.[31]

Comparing the ANPR to the NY Proposal

Certainly, there are similarities in the efforts of the Agencies and the NYDFS in the ANPR and NY Proposal, respectively, to manage cybersecurity risks. However, based on the different philosophies that drove the ANPR and NY Proposal, there are several noteworthy differences in the two approaches:

- Independent Risk Management (IRM) Function – As discussed above, the ANPR would require covered entities to include cyber risk in an IRM function. This would be a substantial burden if not for the fact that entities subject to the ANPR are already required to have such a function. Nonetheless, the ANPR would add numerous cyber related responsibilities to each entity's IRM function, which would require significant resources. The only new corporate governance requirement under the NY Proposal is the creation of a Chief Information Security Officer.

- Multi-Factor Authentication – The NY Proposal is particularly specific in its treatment of MFA. Within their operations, covered entities must require MFA for any individual accessing internal systems from an external network and for privileged access to database servers that allow access to NPI. Further, covered entities must support MFA for any individual accessing web applications that capture, display or interface with NPI (*i.e.*, for use by their customers). In contrast, the ANPR does not discuss user authentication or access controls; instead, the Agencies note that financial institutions are already required to establish programs that ensure the security and confidentiality of customer information.

- External Dependency Management (EDM) – The Agencies identify EDM as one of five main categories of enhanced cybersecurity standards. EDM refers to how a covered entity manages its relationships with outside vendors, suppliers, customers, utilities and other external service providers. Although the NY Proposal contains detailed third party information security policy requirements, it does not envision managing these relationships as part of a unified, interconnected structure. The ANPR elevates EDM to be part of the strategic risk management plan and requires entities to prioritize and rank by criticality every external dependency across the enterprise. The ANPR expects EDM to assess not only the cyber risks that third parties pose to a covered entity, but also the risks that a covered entity's own systems pose to such third parties. Through the EDM requirements, the Agencies would force covered entities to protect the financial system by protecting themselves.

Conclusion

Next year will be critical for cybersecurity regulation. The ANPR and the NY Proposal represent different approaches to addressing cyber and information security risks. The NYDFS approach presents the obvious risks of becoming antiquated quickly and "one-size-not-fitting-all." But developing consensus around standards for a principles-based approach requires considerable time and resources, and risks additional delays in the face of the rapidly increasing need for robust cybersecurity controls and protections. For these reasons, entities potentially subject to either or both proposals should consider submitting comments to the Agencies on the ANPR and to the NYDFS on the NY Proposal, as appropriate. Regardless, potentially covered entities should continue to closely monitor and track developments regarding the ANPR and NY Proposal and, in this regard, strongly consider proactive efforts to review risk management structures to ensure exam readiness on cybersecurity issues, as well as promoting cybersecurity preparedness and prevention.

AMERICAS

New York

Ian Cuillerier
Partner
T +1 212 819 8713
E icuillerier@whitecase.com

John Donovan
Partner
T +1 212 819 8530
E jdonovan@whitecase.com

David Johansen
Partner
T +1 212 819 8509
E djohansen@whitecase.com

Ernie Patrikis
Partner
T +1 212 819 8200
E ernest.patrikis@whitecase.com

Duane Wall
Partner Of Counsel
T +1 212 819 8453
E dwall@whitecase.com

Francis Zou
Partner
T +1 212 819 8733
E fzou@whitecase.com

Glen Cuccinello
Counsel
T +1 212 819 8239
E gcuccinello@whitecase.com

Washington, DC

Kevin Petrasic
Partner
T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner
T +1 202 626 3665
E benjamin.saul@whitecase.com

Jolina Cuaresma
Counsel
T +1 202 626 3589
E jolina.cuaresma@whitecase.com

Helen Lee
Counsel
T +1 202 626 6531
E helen.lee@whitecase.com

EMEA

Frankfurt

Dennis Heuer
Partner
T +49 69 29994 0
E dheuer@whitecase.com

Matthias Kasch
Partner
T +49 69 29994 0
E mkasch@whitecase.com

Andreas Wieland
Partner
T +49 69 29994 1164
E andreas.wieland@whitecase.com

Benedikt Gillessen
Counsel
T +49 69 29994 0
E bgillessen@whitecase.com

Hamburg

Kai-Michael Hingst
Partner
T +49 40 35005 364
E kmhingst@whitecase.com

London

Francis Fitzherbert-Brockholes
Partner
T +44 20 7532 1400
E ffitzherbert-brockholes@whitecase.com

Stuart Willey
Partner
T +44 20 7532 1508
E swilley@whitecase.com

Carmen Reynolds
Counsel
T +44 20 7532 1421
E creynolds@whitecase.com

ASIA

Hong Kong

Baldwin Cheng
Partner
T +852 2822 0405
E bcheng@whitecase.com

Sharon Hartline
Partner
T +852 2822 8733
E shartline@whitecase.com

Singapore

David Barwise
Partner
T +65 6347 1345
E dbarwise@whitecase.com

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

[1] *See* https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

[2] Appendix A, attached below, lists every requirement and recommendation in the ANPR.

[3] *See* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf. The New York State Department of Financial Services is the state regulator for banks, money transmitters, lenders, and insurance companies that operate in New York.

[4] *See* http://www.bis.org/cpmi/publ/d146.pdf.

[5] *See* http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf.

[6] *See* https://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf.

[7] *See* http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

[8] MFA is often described as something you know plus something you have. The passwords that employees typically use to access company systems are a single factor: something they know. Adding a requirement such as using a key-fob or sending a code to a pre-determined mobile phone would be a second factor: something they have, *i.e.* the fob or mobile phone. MFA is using two or more of these techniques.

[9] *See* https://www.nist.gov/cyberframework. The NIST Framework is available as both a document (https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf) and a table of principles (https://www.nist.gov/document-3764).

[10] *See* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[11] ANPR pp. 10–12.

[12] ANPR p. 11.

[13] *See generally,* Enhanced Prudential Standards (Regulation YY), 12 CFR Part 252.

[14] *Covered Entity,* NY Proposal § 500.01(c).

[15] There limited exceptions from the NY Proposal for certain very small entities for which compliance would be difficult. NY Proposal § 500.18.

[16] Publicly Available Information is any information a “Covered Entity has a reasonable basis to believe is lawfully made available to the general public,” whether from government records, widely distributed media, or required general public disclosures under law. NY Proposal § 500.01(j).

[17] NY Proposal § 500.01(g).

[18] NY Proposal §§ 500.03 and .11.

[19] NY Proposal §§ 500.09, .13, and 17(b).

[20] NY Proposal §§ 500.01(d), .02(b), .07, .11, and .17.

[21] NY Proposal §§ 500.06, .08, .10, .12, .14, and .15.

[22] ANPR pp. 13–15. The full scope of the ANPR includes every type of banking organization supervised by the Agencies (including state banks, national banks, savings associations, and their holding companies) that has $50 billion or more in total assets, as well as financial market infrastructures, financial market utilities and non-bank financial companies that the Financial Stability Oversight Council has determined should be supervised by the FRB.

[23] ANPR p. 22.

[24] ANPR p. 24.

[25] ANPR p. 25.

[26] ANPR p. 27.

[27] *Id.*

[28] ANPR pp. 31–33.

[29] ANPR p. 30.

[30] ANPR pp. 18–19.

[31] ANPR p. 41.

Appendix A

[1] Most category names and requirements use the ANPR language. Other documents use different language for related or similar requirements, and as such, matches are subjective approximations for comparison purposes only. This chart is not legal advice and should not be used for legal compliance.

[2] The ANPR requirements are proposals under initial consideration, and similarly, the proposed NYDFS Rule is not yet final.

		Joint ANPR	NYDFS Rule	FFIEC Handbook	CPMI-IOSCO	NIST Framework
Scope	Applies only to financial entities (of any type) with total assets of US$50 billion or more	●			X	X
	Applies to depository institutions (banks, savings associations and thrifts)	●	●	●	X	X
	Applies to holding companies and subsidiaries (bank holding and savings and loan holding)	●		●	X	X
	Applies to money transmitters, non-bank lenders and brokers, and insurance companies		●		X	X
	Applies to designated financial market infrastructures and utilities (FMI and FMU)	●		●	X	X
	Applies *directly* to third parties that are service providers to depository institutions	●			X	X
	Applies *indirectly* to third parties that are service providers to depository institutions		●	●	X	X
	Applies *indirectly* to third parties that are service providers to FMI and FMU	●			X	X
Sector critical systems	Enhanced standards for systems that are critical to the functioning of the financial sector	●			●	
	Sector critical systems (SCS) are determined using measures of interconnectedness	●			●	
	SCS are determined using percentage of total transactions in a market that an entity controls	●				
	For any SCS, establish a two-hour recovery time objective	●			●	
	For any SCS, measure ability to reduce aggregate residual cyber risk to a minimal level	●				
Cyber risk governance	Written, enterprise-wide cyber risk management strategy	●				
	Written, entity-specific cyber risk management strategy		●	●		
	Cyber risk management strategy integrated into overall firm risk management strategy	●		●	●	
	Board approval of cyber risk management strategy	●		●	●	
	Cyber risk management strategy differentiates between inherent and residual cyber risk	●		●	●	

[1] Most category names and requirements use the ANPR language. Other documents use different language for related or similar requirements, and as such, matches are subjective approximations for comparison purposes only. This chart is not legal advice and should not be used for legal compliance.

[2] The ANPR requirements are proposals under initial consideration, and similarly, the proposed NYDFS Rule is not yet final.

		Joint ANPR	NYDFS Rule	FFIEC Handbook	CPMI-IOSCO	NIST Framework
Cyber risk governance	Written, enterprise-wide, cyber-specific risk appetite and tolerances	●			●	●
	Board approval of cyber risk appetite and tolerances	●			●	
	Residual cyber risk must be reduced to a level consistent with risk appetite and tolerances	●				
	Identify and assess activities and exposures that present cyber risk	●	●	●	●	●
	Aggregate activities and exposures to assess entity’s total residual cyber risk	●		●		
	Board responsible for ensuring implementation of cyber risk management framework	●		●	●	
	Board must have adequate expertise in cybersecurity	●			●	
	Board must have ability to provide credible challenge to management on cybersecurity	●		●		
Cyber risk management	Management responsible for cyber risk oversight is independent from business lines	●	●	●	●	
	Management responsible for cyber risk oversight has direct access to the Board	●	●	●	●	
	Establish enterprise-wide policies and reporting structures to support framework	●			●	●
	Framework delineates cyber risk management and oversight responsibilities (clear reporting lines)	●	●	●	●	●
	Establish policies to ensure sufficient resources and knowledge to implement framework	●		●		
	Establish mechanisms for identifying, reporting, and responding to cyber incidents and threats	●	●	●	●	●
	Establish procedures for testing effectiveness of cyber response protocols and updating accordingly	●		●	●	●
Business units	Cyber risk framework is divided by functions: business units, risk management and audit	●		●		
	Business units assess cyber risks associated with their activities on an ongoing basis	●	●	●		●
	Business units assess risks associated with every asset, service and connection point	●	●	●		●
	Business units ensure risk information is shared with senior management	●	●	●	●	●

		Joint ANPR	NYDFS Rule	FFIEC Handbook	CPMI-IOSCO	NIST Framework
Business units	Business units ensure resources and staff are sufficient to comply with cyber framework	●		●		
	Business units restrict data access privileges to those individuals who require such access		●	●	●	●
	Require multi-factor authentication to access internal systems that contain nonpublic data		●	●		
	Encrypt nonpublic data both in transit and at rest		●	●	●	●
	Establish policies for timely destruction of nonpublic data that is no longer necessary		●	●		●
Independent risk management function	Establish an independent risk management (IRM) function	●				
	IRM function reports to the chief risk officer and Board	●				
	IRM function measures and monitors cyber risk and adequacy of controls across the enterprise	●				
	IRM function assesses material aggregate residual risk on an ongoing basis	●				
	IRM function assesses the effectiveness and timeliness of aggregate residual risk reduction	●				
	IRM function has up-to-date understanding of structures and processes	●				
	IRM function has clear and separate reporting lines from business units	●				
Audit function	Audit function assesses compliance of entity's cyber risk management framework	●		●	●	
	Overall audit plan incorporates an assessment of cyber risk management	●		●		
	Audit function evaluates entire security lifecycle (penetration and vulnerability testing)	●	●	●	●	
	Audit function assesses the business unit and independent risk management capabilities	●		●		
	Audit function includes maintaining logs of access to and alteration of data and systems		●	●	●	●
	Establish risk-based procedures and controls to monitor activity of authorized users of data		●	●	●	●
IDM	Integrate internal dependency management (IDM) into strategic risk management plan	●			●	

[1] Most category names and requirements use the ANPR language. Other documents use different language for related or similar requirements, and as such, matches are subjective approximations for comparison purposes only. This chart is not legal advice and should not be used for legal compliance.

[2] The ANPR requirements are proposals under initial consideration, and similarly, the proposed NYDFS Rule is not yet final.

[1] Most category names and requirements use the ANPR language. Other documents use different language for related or similar requirements, and as such, matches are subjective approximations for comparison purposes only. This chart is not legal advice and should not be used for legal compliance.

[2] The ANPR requirements are proposals under initial consideration, and similarly, the proposed NYDFS Rule is not yet final.

		Joint ANPR	NYDFS Rule	FFIEC Handbook	CPMI-IOSCO	NIST Framework
Internal dependency management	IDM has well-defined roles, responsibilities, policies, standards and procedures	●	●	●		●
	IDM maintains an inventory of all business assets prioritized by criticality to the firm and the sector	●		●	●	●
	IDM maintains complete list of internal assets, business functions and information flows	●	●	●	●	●
	IDM tracks connections among assets and functions and assesses lifecycle cyber risk	●		●	●	
	IDM supports enterprise-wide data collection and analysis	●			●	
	IDM enables timely notification of internal issues and supports timely responses to cyber threats	●		●		●
	IDM applies controls to address inherent cyber risk of business assets	●	●	●	●	●
	IDM conducts resiliency tests of the back-ups to business assets	●				
	Require all personal to attend regular cybersecurity awareness training		●	●	●	●
External dependency management	Integrate external dependency management (EDM) into strategic risk management plan	●			●	
	EDM has well-defined roles, responsibilities, policies, standards and procedures	●		●		●
	EDM has awareness of all external dependencies prioritized by criticality to the firm and the sector	●			●	
	EDM identifies and manages real-time cyber risk associated with external dependencies	●		●	●	●
	EDM prioritizes monitoring and incident response and recovery for “critical systems”	●			●	
	EDM supports timely responses to cyber risks to the enterprise and the sector	●		●	●	
	EDM supports enterprise-wide data collection and analysis	●			●	
	EDM tracks connections among external dependencies and assets throughout lifecycle	●			●	
	EDM reviews external relationships and tests alternatives in case external partners fail	●		●		
	EDM applies controls to reduce cyber risk of external dependencies to entity and sector	●	●	●	●	

[1] Most category names and requirements use the ANPR language. Other documents use different language for related or similar requirements, and as such, matches are subjective approximations for comparison purposes only. This chart is not legal advice and should not be used for legal compliance.

[2] The ANPR requirements are proposals under initial consideration, and similarly, the proposed NYDFS Rule is not yet final.

		Joint ANPR	NYDFS Rule	FFIEC Handbook	CPMI-IOSCO	NIST Framework
External DM	Establish a third-party information security policy for due diligence and data access		●	●		●
	Require multi-factor or other authentication to access internal systems from external networks		●	●		
	Require risk-based authentication for any web application that inputs/outputs nonpublic data		●			
Incident response and cyber resilience	Establish and maintain effective incidence response (IR) and cyber resilience (CR)	●	●	●	●	●
	Establish plans to identify and mitigate cyber risk to interconnections (prevent contagion)	●	●	●	●	
	IR and CR programs based on enterprise-wide cyber risk management strategies	●			●	
	IR and CR programs include escalation protocols and contain set communication procedures	●	●	●	●	●
	IR and CR programs include a process to incorporate lessons learned back into program	●	●		●	●
	CR strategies consider wide-scale recovery and support sector-wide resilience	●			●	
	CR strategies consider potential for malware to replicate and propagate across connections	●		●	●	
	CR strategies designed to achieve recovery points based on criticality of data	●			●	
	CR includes performing core business during multiple or wide-spread disruptions	●			●	
	CR includes protocols for secure, immutable, off-line storage of critical records and data	●			●	
	CR includes mechanisms to transfer disrupted functions to another entity or provider	●				
	CR includes specific tests of disruptive or destructive cyber events	●		●	●	●
	CR testing addresses interdependencies and market connections (joint tests)	●			●	
	IR requires ongoing situational and operational awareness to preempt cyber events	●	●		●	
	IR includes maintaining threat profiles and establishing threat modeling capabilities	●		●	●	
	Provide to regulator notice of any cyber event and annual report of cyber compliance		●			