netskope

WHITEPAPER

Tackle the NYDFS Cybersecurity Requirements with Netskope

The New York Department of Financial Services (DFS) 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies are a series of regulations that require banks, insurance companies, and other financial services institutions regulated by the NYDFS to establish and maintain cybersecurity programs designed to protect consumers' private data. The requirements from Department of Financial Services (DFS) go beyond what's been historically seen from regulators, requiring, among other things, organizations assess their cyber risks, implement a comprehensive written cybersecurity program, and manage the cyber risks of their third-party vendors. The cybersecurity regulation went into effect March 1, 2017 and provided organizations with transitional periods of varying length (ranging from 180 days to 2 years) to comply with the various provisions.

While some organizations scramble to make sure they meet requirements, others will already have a cybersecurity program in place to meet many of them. The unique opportunity for the latter is to use the requirements as a catalyst for taking a holistic look at enterprise risk and threats, then develop a revised strategy for cyber risk management, security, and compliance.

Here's a checklist to guide your organization's journey highlighting the requirements you can tackle with Netskope to help you get your cybersecurity framework compliant and secure.

CHECKLIST FOR NYDFS COMPLIANCE: REQUIREMENTS

		NETSKOPE OFFERS	EFFECTIVE DATE
500.02	Cybersecurity program	n/a	August 28, 2017
500.03	Cybersecurity policy covering:		August 28, 2017
	Information Security	n/a	
	Data governance and classification	✔	
	Asset inventory and device management	n/a	
	Asset controls and identify management	n/a	
	Business continuity and disaster recovery planning	n/a	
	Systems operations and availability concerns	n/a	
	Systems and network security	n/a	
	Systems and network monitoring	n/a	
	Systems and application development and quality	n/a	
	Physical security and environmental controls	✔	
	Customer data privacy	✔	
	Vendor and third party service provider	✔	
	Risk assessment	n/a	
	Incident response	n/a	
500.04	Chief Information Security Officer	n/a	August 28, 2017
500.05	Penetration testing and vulnerability testing	n/a	March 1, 2018
500.06	Audit trail	✔	September 3, 2018
500.07	Access privileges	✔	August 28, 2017
500.08	Application security	✔	September 3, 2018
500.09	Risk assessment	✔	March 1, 2018
500.10	Cybersecurity personnel and intelligence	n/a	August 28, 2017
500.11	Third party service provider security policy	✔	March 1, 2019

500.12	Multi-factor authentication	n/a	March 1, 2018
500.13	Limitations on data retention	n/a	September 3, 2018
500.14	Training and monitoring	✔	500.14(b) effective March 1, 2018,
500.15	Encryption of Nonpublic information	✔	September 3, 2018
500.16	Incident response plan	n/a	August 28, 2017
500.17	Notices to superintendent	n/a	August 28, 2017

CHECKLIST FOR NYDFS COMPLIANCE: GENERAL RECOMMENDATIONS FOR COMPLIANCE WITH THE NYDFS

Review the NYDFS regulations, then evaluate if you need to make changes and brief your executive team on their implications to your organization. Best practices include:

- Review existing cybersecurity programs and plan now for compliance
- Assess your organization's cyber risk and compliance against legal and contractual obligations
- Ensure your staff is trained, has the necessary qualifications and certifications, establish if you need to hire additional staff
- Consider assembling an internal team that will be ready to take on any added burden the regulation imposes
- Determine if you need to implement additional controls and technology to prove compliance and address gaps

CLOUD CONSIDERATIONS FOR COMPLIANCE WITH NYDFS

500.3: Cyber Security Policy

Data Classification and Data Governance

Perhaps the most interesting aspect of the NYDFS proposed rules is the incorporation of data governance and data management as fundamental components of the prescribed cybersecurity program. This requirement enforces a consistent classification of information within an organization. Data classification tools can be used to improve the handling of regulated data, enforce data governance policies, and prevent leakage in cloud services. Document classification from metadata can be consumed by data loss prevention (DLP), encryption, and other security solutions to determine which information is sensitive, and how it should be protected.

- Understand the sensitive data in your cloud apps
  - Get visual dashboards of violations and take remediation action to revoke public access of such documents
  - Protect sensitive content in real-time even before a potential violation takes place.
  - Apply out of the box DLP profiles to identify content that may fall under the regulation

- Automatically remediate classified documents that have been classified using products like Azure Information Protection (AIP), Titus, and Boldon James
- Use native encryption provided by a Cloud Access Security Broker (CASB), go even further with BYOK to protect sensitive content
- Query for and understand all access and activities by device and device classification, for example, BYOD

Physical security and environmental controls

Physical and environmental safeguards are often overlooked despite being crucial to protecting information. Ensure the physical areas holding your nonpublic information in the cloud is protected.

- Establish if your cloud app's data center been certified for SSAE-16 or SOC, and at what level and type

Customer data privacy

It's crucial to clearly communicate to customers how their data will be used and the safeguards you employ to protect the data.

- Find nonpublic information and be able to classify it separately from other data
- Apply granular policies on how you want to govern this data

Vendor and third party service provider management

Bind your service providers by contract to adequately safeguard the nonpublic information you share, to promptly notify you of cybersecurity events, and to assist in responding to cybersecurity events.

- Quickly evaluate the enterprise-readiness of the cloud services in your environment on a comprehensive set of security and privacy parameters, including data security features like encryption of data at rest, cipher type, if audit logging is enabled, and physical and logical security measures such as SOC-2 and ISO27001
- Scale your vendor risk management process to apply to thousands of cloud service providers

500.6: Audit Trail

Systems in place must able to reconstruct actions post-breach and provide audit trails.

- Ensure any app in your environment meets your auditing requirements and proactively informs you of changes
- Apps should log user and administrator actions and data access
- Track usage of services using associated classified data

500.7: Access Privileges

Limit access to systems that provide access to nonpublic information and periodically review access privileges.

- Secure app access in the same manner as the rest of your enterprise systems
- Ensure admin privileges across all services with role-based access controls
- Selectively grant access or govern activities based on context
- Use a CASB to control access from unmanaged devices. For example, provide full access to corporate resources from managed devices, but limit unmanaged devices to only view documents but not download them on to the device.

500.8: Application Security

Security practices for internally developed apps is mandatory, with the periodic evaluation, assessment, and security testing of externally-developed apps.

- Discover all the cloud services running in your environment
- Measure the apps' enterprise-readiness against an objective yardstick (CSA's Cloud Controls Matrix is a great starting point)
- Adopt a process to continuously discover and gain visibility into the cloud apps in your environment, including the unsanctioned ones, as they change frequently
- Implement a CASB to safely onboard the cloud applications

500.9: Risk Assessment

Requires documented risk assessments that consider threats and the examination of controls in relation to identifying risks.

- Assess your risk based on cloud services readiness coupled with cloud usage and user behavior
- Identify and block the riskiest cloud services, or opt to not block anything and move to applying granular controls to everything instead

500.11: Third party service provider security policy

Establish risk-based policies and procedures to ensure security of information systems and nonpublic information accessible to or held by third-party service providers.

- Specify a template of the features and options that third-party cloud service providers must have before they are considered for use

500.14: Training and monitoring

Covered entities are required to implement risk-based policies to monitor the activity of authorized users and detect unauthorized access or use of nonpublic information. Regular cybertraining of all personnel is required.

- Detect cloud activity anomalies in any cloud service
- Enforce cloud user policies wherever your users and whatever their device
- Identify and protect against users access cloud services with compromised credentials
- Identify and protect against threats and malware in or in route to cloud services

500.15: Encryption of nonpublic information

All covered entities must implement encryption controls based on the mandatory risk assessment (Section 500.09), to protect nonpublic information held or transmitted over external networks. Controls must be reviewed and approved by the CISO.

- Protect data in cloud services using strong encryption and key management technology that is FIPS 140-2 Level 3 certified
- Find personally identifiable information (PII) and encrypt it or quarantine it and pull it back on-premises, or put in legal hold for review
- Encrypt sensitive data, whether en route to or from processors or at rest in sanctioned cloud services

CONFIGURE YOUR CLOUD ACCESS SECURITY BROKER TO ENABLE NYDFS COMPLIANCE

To achieve NYDFS cloud compliance, we recommend you implement a cloud access security broker (CASB) solution such as Netskope for your organization to both mitigate risk and ensure compliance with all aspects of the DFS regulation including data governance and classification, customer privacy, and other areas.

- Assess your CASB vendor based on the guidance provided above
- Establish legal basis and business case for CASB implementation

Not sure where to start? Netskope can get you on the path to NYDFS compliance.
Contact us today to learn more.