Compliance Brief

Data Security Compliance

With the NYDFS Cybersecurity Requirements for Financial Services

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What is the NYDFS Cybersecurity Requirements for Financial Services Companies?

The New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies, or 23 NYCRR Part 500 regulation, requires that regulated institutions implement, maintain, and annually certify that they have cybersecurity programs in place to protect the integrity of their information systems and customers' data.

The regulation promotes the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously, be responsible for the organization's cybersecurity program, and file an annual certification confirming compliance with these regulations.

Which companies are supervised by the NYDFS?

Any institution that needs a license, registration, or charter from the New York State Department of Financial Services is regulated by the NYDFS. Examples of covered entities include state-chartered banks, foreign banks licensed to operate in the state of New York, licensed lenders, private bankers, savings and loans associations, mortgage companies, insurance companies, and other financial service providers.

When did the NYDFS Cybersecurity Requirements go into effect?

The initial phase of the New York State Cybersecurity Requirements for Financial Services Companies took effect on March 1, 2017. However, the entirety of the requirements was only enforced two years later, by March 1, 2019.

What are the penalties for NYDFS Cybersecurity Requirements non-compliance?

Under NY Banking Law, the NYDFS penalties start at $2,500 a day for each day of noncompliance with NYDFS Part 500. If noncompliance is determined to be a "pattern" by the NYDFS superintendent, the fine may increase to $15,000 a day. If the superintendent decides that any violations have been committed "knowingly and willfully," the fine will jump to $75,000 daily. Recent 2022 enforcement actions imposed monetary penalties in the $4.5 million to$5million range.

How Thales Helps with NYDFS Compliance

Thales' solutions can help Financial Institutions comply with NYDFS by simplifying compliance and automating security, reducing the burden on security and compliance teams. We help address essential cybersecurity requirements under NYDFS Part 500, which require

NYCRR Part 500: Cybersecurity Requirements for Financial Services Companies

This regulation requires each company to assess its specific risk profile and design, implement, maintain, and annually certify a cybersecurity program that addresses its risks and protects customer information as well as information technology systems.

Thales helps organizations by:

- Providing a complete audit trail
- Managing and monitoring access privileges
- Securing development of applications
- Assessing risk
- Managing third party service provider risk
- Providing multi-factor authentication
- Securing disposal of information
- Monitoring access of nonpublic information
- Encrypting non-public information

companies to assess their specific risk profile and design, implement, maintain, and annually certify a cybersecurity program that addresses their risks and protects customer information and information technology systems.

We provide comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

- **Application Security:** Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).
- **Data Security:** Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.
- **Identity & Access Management:** Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

How Thales solutions help with NYDFS Compliance

NYDFS Part 500	Thales Capabilities	Thales Solutions
500.06: "...**include audit trails** designed to detect and respond to cybersecurity events."	• Detect and prevent cyber threats with web application firewall. • Monitor ICT network and protect from DDoS attacks and Bad Bots. • Monitor API activity, track usage, detect anomalies, and identify potential unauthorized access attempts. • Data activity monitoring for structured and unstructured data on Hybrid IT. • Produce audit trail and reports of all access events to all systems, stream logs to SIEM.	**Application Security** Web Application Firewall DDoS Protection Bot Protection API Security **Data Security** Data Activity Monitoring
500.07: "...**limit user access privileges** to Information Systems."	• Limit access to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Centralize access policies and enforcement to multiple hybrid environments in a single pane of glass. • Leverage smart cards for implementing physical access to sensitive facilities. • Provide customers secure access to their information in company's systems.	**Identity & Access Management** Workforce Access Management Customer Identity & Access Management Smart cards **Data Security** Transparent Encryption
500.08: "...ensure the use of **secure development practices for in-house developed applications** utilized by the Covered Entity..."	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Monitor API activity, track usage, detect anomalies. • Deploy data protection controls in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate access to secrets across DevOps tools. • Easily access data security solutions through online marketplaces.	**Application Security** Runtime Protection Web Application Firewall DDoS Protection Bot Protection API Security **Data Security** Community Edition Secrets Management DPOD Marketplace

How Thales solutions help with NYDFS Compliance

NYDFS Part 500	Thales Capabilities	Thales Solutions
500.09: "...conduct a periodic **Risk Assessment** of the Covered Entity's Information Systems."	• Discover and classify potential risk for all public, private and shadow APIs. • Identify structured and unstructured sensitive data at risk across Hybrid IT. • Identify current state of compliance and documenting gaps.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Risk Analytics Vulnerability Management
500.11: "...ensure the security of Information Systems and **Nonpublic Information that are accessible to, or held by, Third Party Service Providers."**	• Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud. • Ensure complete separation of roles between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based fine-grained authorization.	**Data Security** Cloud Key Management Transparent Encryption Data Activity Monitoring User Rights Management Discovery and Classification **Identity & Access Management** Workforce Access Management Third-party Access Control Delegated User Management Externalized Authorization
500.12: "...shall use effective controls, which may include **Multi-Factor Authentication.**"	• Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies based on the sensitivity of the data/application. • Protect against phishing and man-in-the-middle attacks.	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
500.13: "Secure disposal of any Nonpublic Information"	• Locate structured and unstructured regulated data across hybrid IT and prioritize remediation. • Remove keys from CipherTrust Manager can ensure secure deletion, digitally shredding all instances of the data.	**Data Security** Data Discovery & Classification Encryption & Key Management
500.14: "...**monitor and log the activity** of authorized users and **detect unauthorized access.**"	• Data activity monitoring for structured and unstructured data across cloud and on-prem systems. • Produce audit trail and reports of all access events to all systems, stream logs to external SIEM systems.	**Data Security** Data Activity Monitoring **Identity & Access Management** Workforce Access Management

How Thales solutions help with NYDFS Compliance

NYDFS Part 500	Thales Capabilities	Thales Solutions
500.15: "...**Implement controls, including encryption**, to protect Nonpublic Information held or transmitted by the Covered Entity both **in transit over external networks and at rest.**"	• Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Pseudonymize sensitive information in databases. • Protect data in motion with high-speed encryption. • Protect data in use by leveraging confidential computing. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. • Security products designed for post-quantum upgrade to maintain crypto-agility.	**Data Security** Transparent Encryption Tokenization Key & Secrets Management High Speed Encryption Hardware Security Modules Confidential Computing Data Governance Data Activity Monitoring

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.