Cybersecurity Implementation Timeline for Class A Companies

This timeline includes key dates of the amended Cybersecurity Regulation for Class companies. Class A companies are defined in the Cybersecurity Regulation in Section 500.1(d).

This guide is provided for general planning purposes. Please consult the text of the Cybersecurity Regulation for specific requirements.

April 15, 2024
Section 500.17(b)
• Submit either Certification of Material Compliance or Acknowledgment of Noncompliance for calendar year 2023. Both annual submissions must be signed by the highest-ranking executive and the CISO.

April 29, 2024
Section 500.9
• Risk assessments, which continue to be required, must now be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to the business' cyber risk.

Section 500.3
• Cybersecurity policies must be annually reviewed and approved by senior governing body or senior officer(s) and procedures must also be documented. After assessing risks, Covered Entities must update policies and procedures to address these additional areas
if needed:
○ Data retention
○ End of life management (phasing out unsupported technical products with weaknesses)
○ Remote access controls
○ Systems and network monitoring
○ Security awareness and training
○ Systems and application security
○ Incident notification
○ Vulnerability management

... continued ➜

December 1, 2023
Section 500.17:
• Notify DFS of cybersecurity events reported to other authorities or that have a reasonable likelihood of materially harming any material part of normal operations continues to be required.

• Cybersecurity events that involve ransomware deployment and any ransom payments made must now be reported.

➜ Continued April 29, 2024 requirements

Section 500.2(c)
• Design and conduct independent audits of their cybersecurity program

Section 500.5(a)(1), (b), and (c)
• Conduct at least annual penetration testing from inside and outside information systems' boundaries.
• Have a monitoring process in place to promptly inform of new security vulnerabilities.
• Prioritize and timely remediate vulnerabilities based on risk.

Section 500.14(a)(3)
• Cybersecurity awareness training must now include social engineering and must be provided at least annually.

November 1, 2024

Section 500.4

• CISO's written report to senior governing body must be updated to include plans for remediating material inadequacies.

• CISO required to timely report to senior governing body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the cybersecurity program.

• Senior governing body must exercise oversight of its cybersecurity risk management, including:

○ Having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors;

○ Requiring executive management or its designees to develop, implement, and maintain the covered entity's cybersecurity program;

○ Regularly receiving and reviewing management reports about cybersecurity matters; and

○ Confirming that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program.

Section 500.15

• Implement a written policy requiring encryption that meets industry standards.

• Use of effective compensating controls for encryption of nonpublic information at rest that have been approved by the CISO may continue to be used, but that approval must now be in writing.

• Effective alternative compensating controls for encryption of nonpublic information in transit over external networks can no longer be used.

Section 500.16

• Incident response plans continue to be required, but they must be updated as specified.

• Ensure business continuity and disaster response plans that are reasonably designed to address a cybersecurity-related disruption as specified are in place.

• Covered Entities must also:

○ Train all employees involved in the plans' implementations, test plans with critical staff, and revise plans as necessary.

○ Test the ability to restore critical data and information systems from backups.

○ Maintain and adequately protect backups necessary to restore material operations.

May 1, 2025

Section 500.5(a)(2)

• Conduct “automated scans of information systems, and a manual review of systems not covered by such scans” to discover, analyze, and report vulnerabilities at a frequency determined by their risk assessment, and promptly after any material system changes.

Section 500.7

• Implement enhanced requirements regarding limiting user access privileges, including privileged account access.
• Review access privileges and remove or disable accounts and access that are no longer necessary.
• Disable or securely configure all protocols that permit remote control of devices.
• Promptly terminate access following personnel departures.
• Implement a reasonable written password policy to the extent passwords are used.
• Monitor privileged access activity.
• Implement a privileged access management solution.
• Implement automated method of blocking commonly used passwords.

Section 500.14(a)(2) and (b)

• Implement controls to protect against malicious code
• Implement endpoint detection and response solution to monitor anomalous activity and centralized logging and security event alert solution.
• CISO can approve reasonably equivalent or more secure compensating controls, but approval must be in writing.

November 1, 2025

Section 500.12

• Implement multi-factor authentication for all individuals accessing information systems.
• CISO may approve in writing the use of reasonably equivalent or more secure compensating controls. Such controls must be reviewed at least annually.

Section 500.13(a)

• Implement written policies and procedures designed to produce and maintain a complete, accurate and documented asset inventory of their information systems.
• Policies and procedures must include method to track specified key information for each asset, such as owner and location, and frequency required to update and validate asset inventory.