10 Essential Steps to NYDFS Compliance

Panorays

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation, also known as 23 NYCRR 500, is "designed to promote the protection of customer information as well as the information technology systems of regulated entities." Like GDPR, its goal is to protect sensitive nonpublic information.

NYDFS consists of rigorous cybersecurity rules for covered financial institutions like credit unions, banks, insurance firms and mortgage companies. It applies to all entities that are regulated by DFS, as well as any unregulated third-party service providers that work with them.

This guide provides a partial overview of NYDFS requirements and some of the steps you need to take to fulfill them.

01

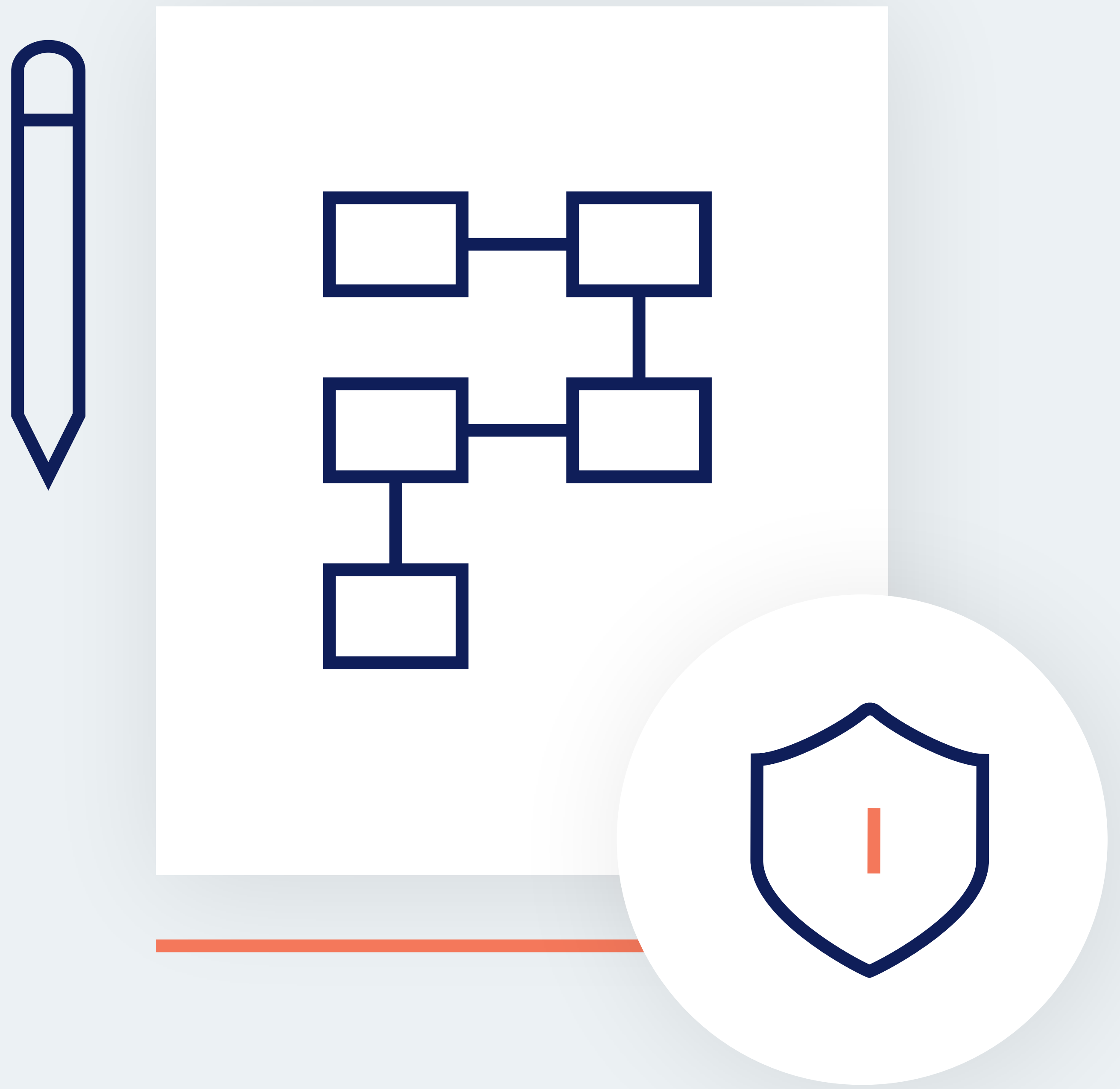
Implement a cybersecurity policy

(Section 500.03)

The requirement: "Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems."

What it includes: Your organization's cybersecurity policy should be approved by senior execs, and should address information security, data governance and classification, asset inventory and device management, access controls and identity management, business continuity and disaster recovery planning and more.

Bottom line: Your organization needs to implement and maintain a serious cybersecurity policy that specifies policies and procedures to protect information systems.



02

Maintain a cybersecurity program

(Section 500.02)

The requirement: “Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered Entity’s Information Systems.”

What it includes: Your cybersecurity program should cover the identification and addressing of internal and external cybersecurity risks, as well as detecting, responding to and recovering from cyber events. It should include the implementation of policies and procedures designed to protect the organization’s data and the fulfillment of regulatory reporting obligations.

Bottom line: Your organization needs to put in place a comprehensive cybersecurity plan that addresses how to protect information systems, as well as how to detect, respond to and recover from cyber events.

03

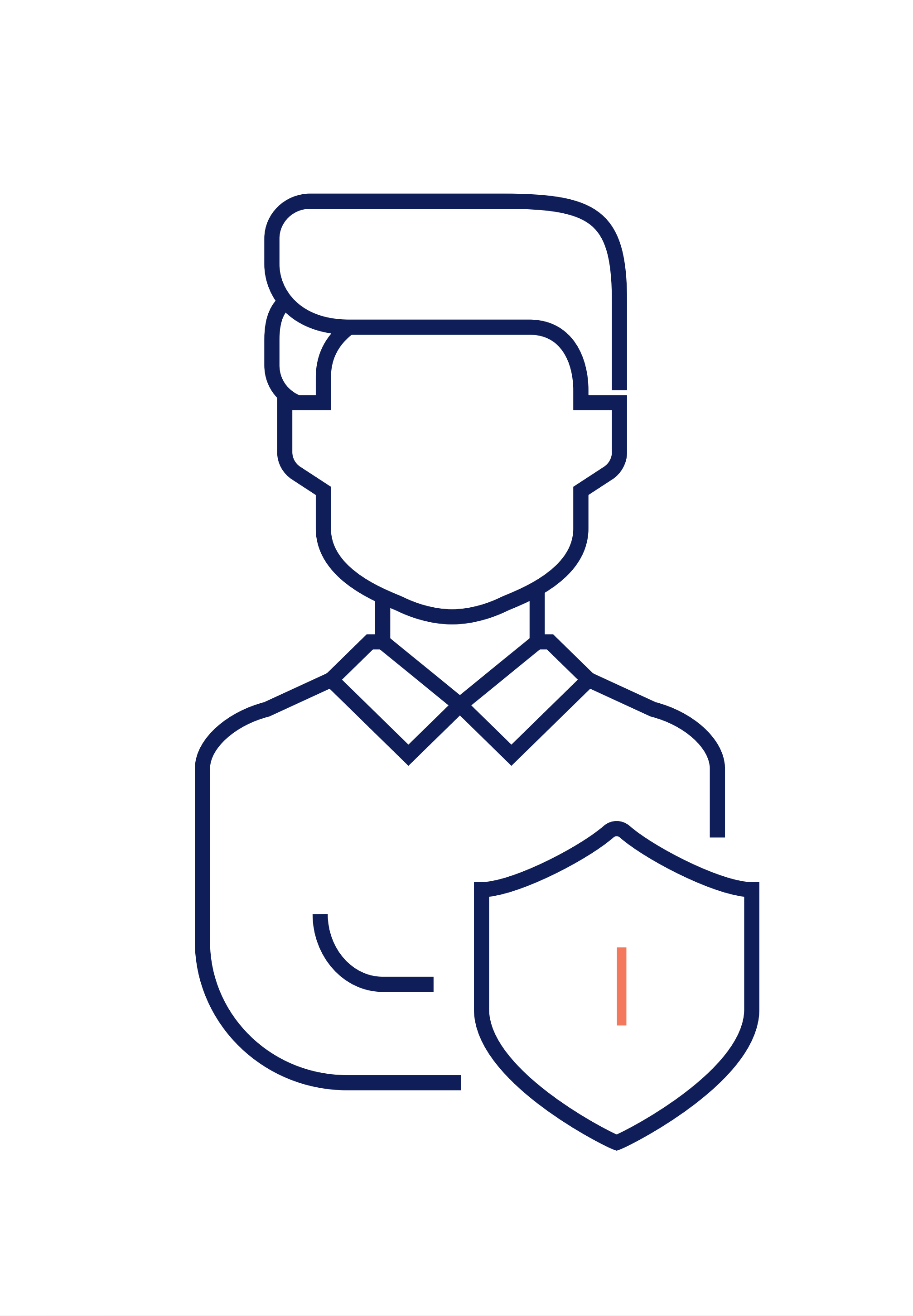
Appoint a CISO

(Section 500.04)

The requirement: “Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its cybersecurity policy.”

What it includes: The CISO must submit a report in writing at least annually to the organization’s board of directors, governing body or senior officer about the organization’s cybersecurity program and risks. The CISO should consider the integrity and security of the organization’s information systems, its cybersecurity policies and procedures, cyber risk, program effectiveness and any cyber events the organization has experienced.

Bottom line: Your organization needs someone who is responsible for implementing and enforcing your cybersecurity.



04

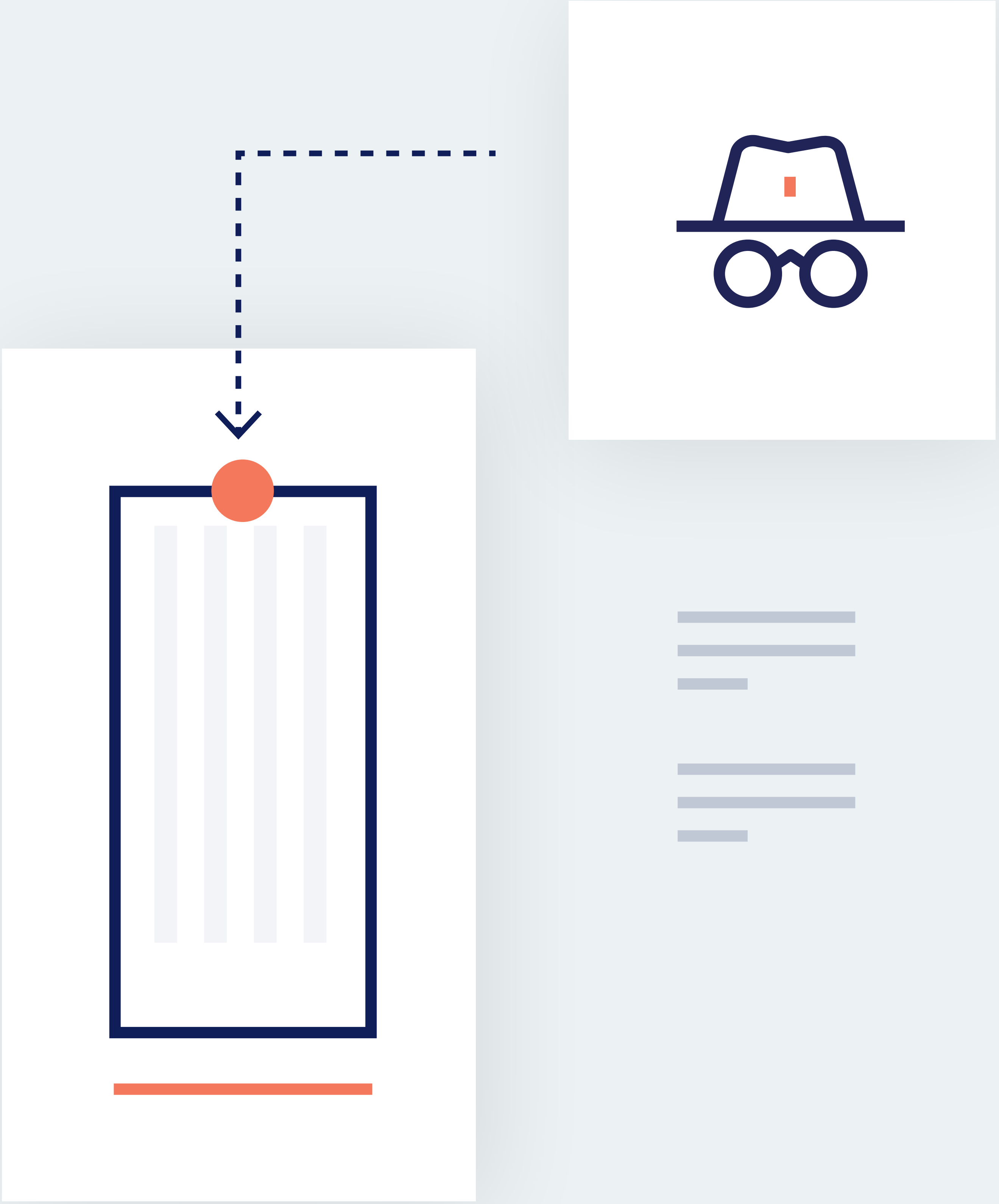
Perform pentest and vulnerability assessments

(Section 500.05)

The requirement: "The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program."

What it includes: Your organization should undergo continuous monitoring or periodic penetration testing and vulnerability assessments. Pentests should occur annually and vulnerability assessments should occur bi-annually.

Bottom line: Defending your organization requires constant vigilance, monitoring and periodic testing.



05

Limit access privileges

(Section 500.07)

The requirement: “As part of its cybersecurity program, based on the Covered Entity’s Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.”

What it includes: Your organization should be aware of which employees can access information, and those privileges should be reviewed regularly.

Bottom line: It’s important to keep access on a need-to-know basis.

06

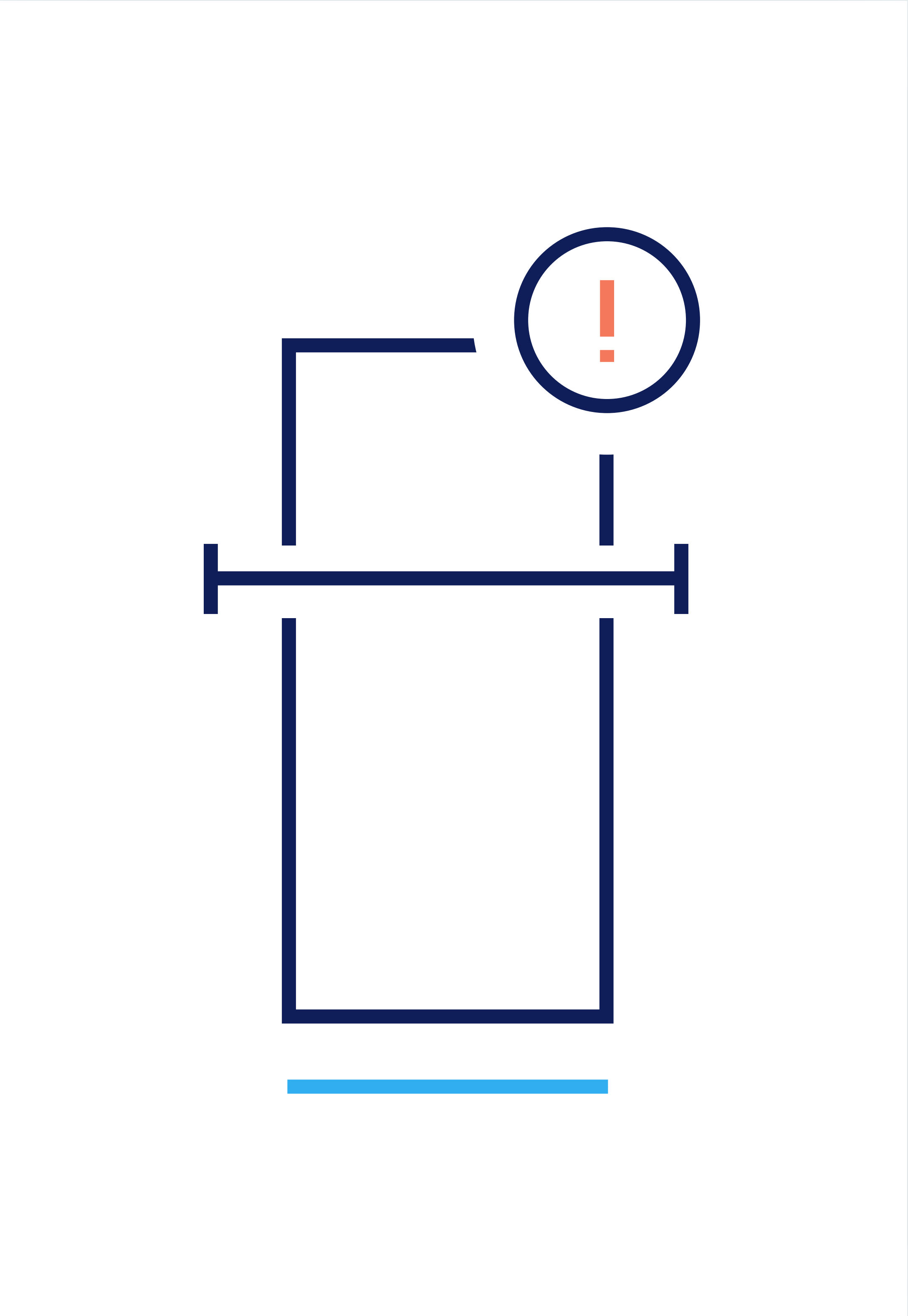
Perform a risk assessment

(Section 500.09)

The requirement: “Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity’s Information Systems sufficient to inform the design of the cybersecurity program as required by this Part.”

What it includes: Your risk assessment should consider the risks of business operations related to cybersecurity, data that’s collected or stored, systems that are used and the effectiveness of controls. It should be performed according to your written policies and procedures, which should include criteria for the evaluation of cyber risks and assessing security, as well as how to mitigate risks.

Bottom line: Your organization must periodically check for risks that may surface as business operations change.



07

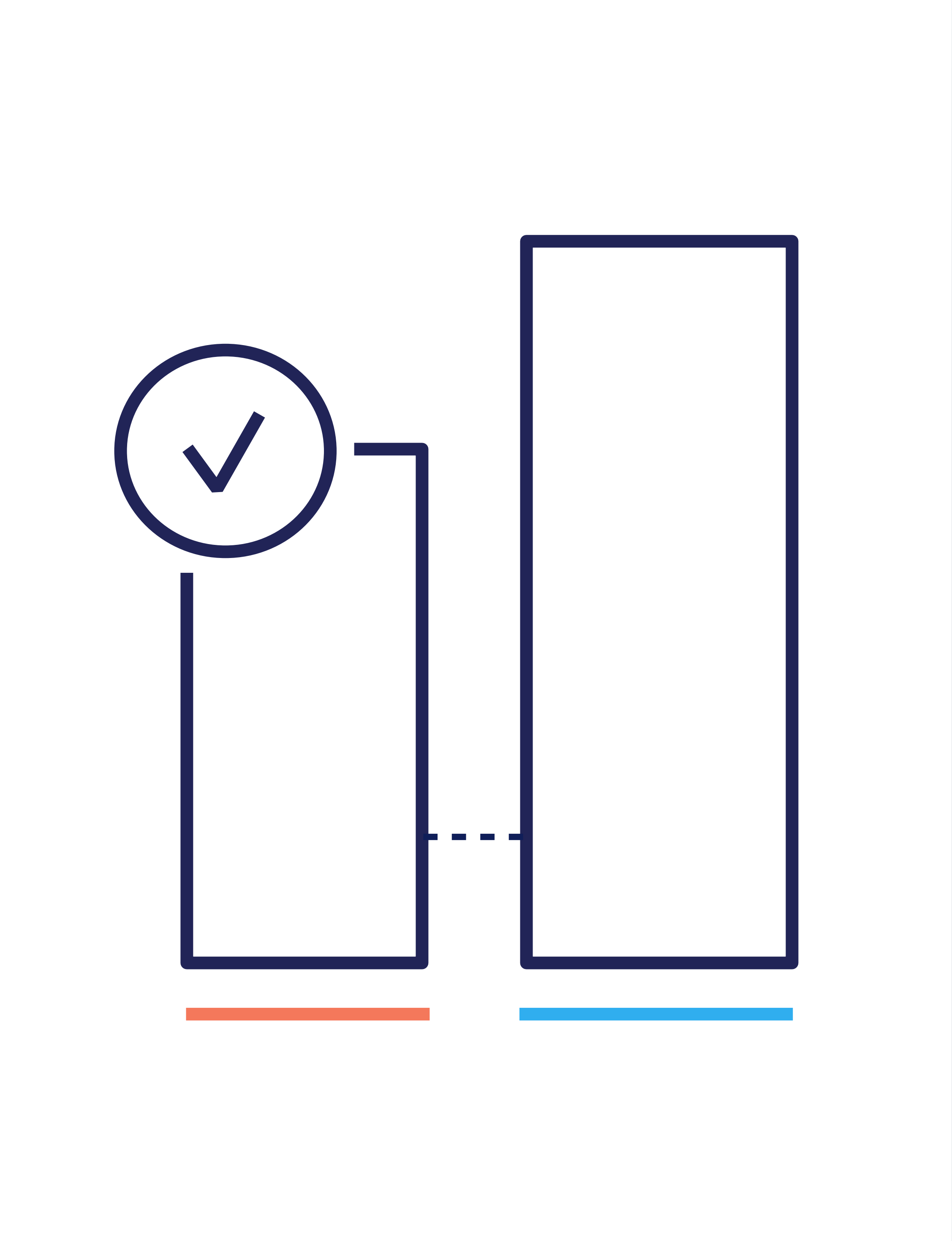
Implement a third-party service provider policy

(Section 500.11)

The requirement: “Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers.”

What it includes: Your policies and procedures should state minimum cybersecurity thresholds that must be met by third parties and due diligence processes that are used. Specifically, there should be guidelines for third parties, including the use of multi-factor authentication, encryption and cyber event notifications.

Bottom line: Financial institutions will need to evaluate all of their third parties and hold each one to a minimum security standard.



08

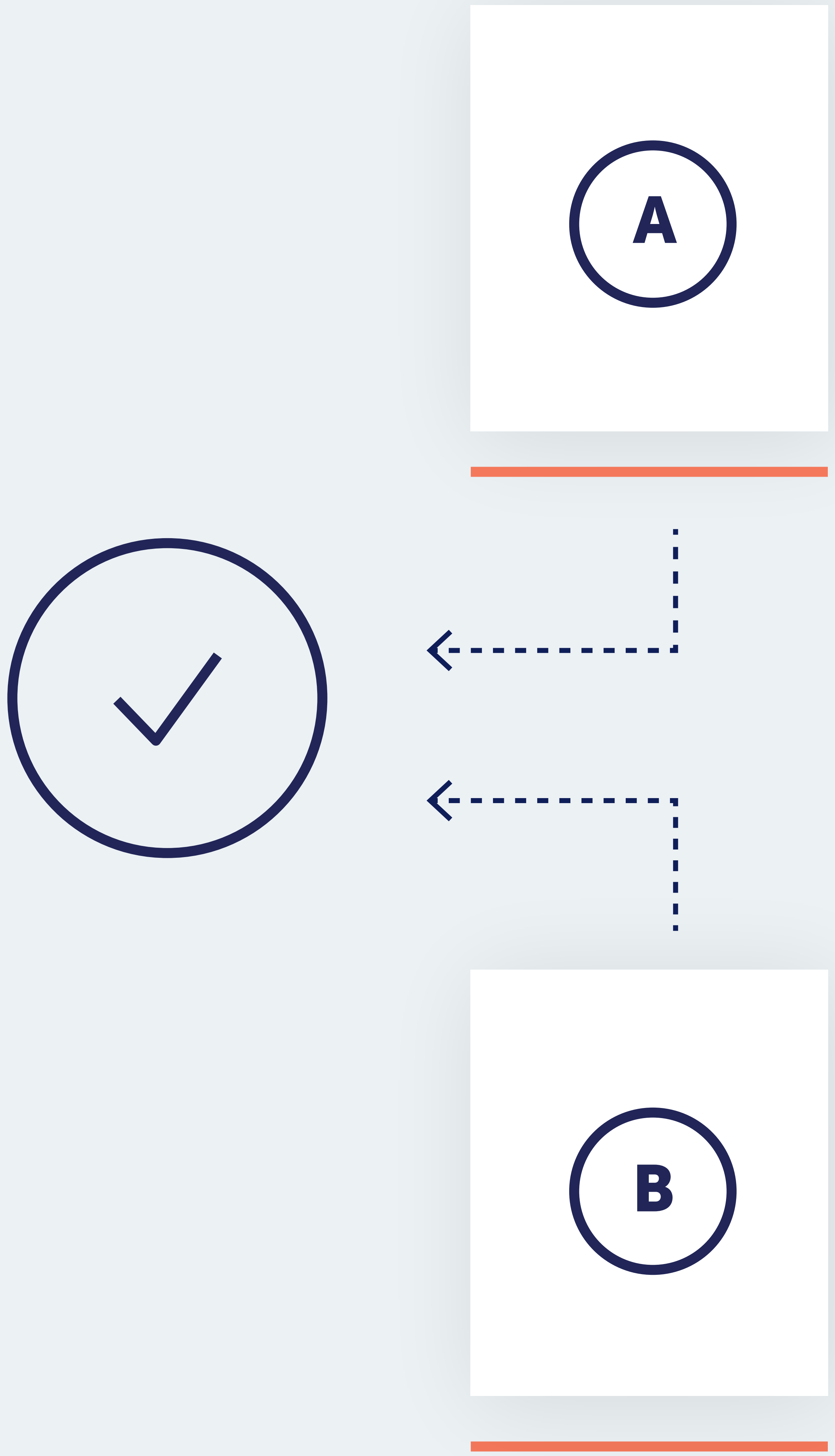
Enable multi-factor authentication

(Section 500.12)

The requirement: “Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.”

What it includes: MFA must be in place for anyone accessing your organization’s network from an external location, unless the CISO has approved more secure access controls.

Bottom line: MFA has been proven to be effective at verifying a person’s identity, which is why the regulation specifically singles it out as a control that should be present.



Limit data retention

(Section 500.13)

The requirement: “As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information. . .that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity.”

What it includes: Organizations should regularly review and delete data that is no longer necessary for business operations and is not required by law.

Bottom line: By cutting down on the amount of data that your organization holds, your attack surface is reduced, thus reducing your risk of a cyberattack.

10

Provide cybersecurity awareness training

(Section 500.14)

The requirement: “As part of its cybersecurity program, each Covered Entity shall provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.”

What it includes: Organizations should make sure their employees are trained to be aware of cyber risks and how to guard against them. For example, using strong passwords, not responding to phishing emails, avoiding suspicious links and never leaving laptops unattended.

Bottom line: It’s not enough to put policies and procedures in place; organizations must consider the human factor as well.

How Panorays Can Help

The NYDFS Cybersecurity Regulation has very specific requirements for financial institutions that do business with third parties. To properly assess risk according to NYDFS, organizations will not only need to have visibility into their third parties, but also have context around the business and technology relationship between themselves and their third parties.

Panorays provides a 360-degree view of third parties through discovery and unveiling of the attack surface along with automated questionnaires that check internal policies. This is combined with continuous monitoring and live alerts about any changes to cyber posture. Using these tools, Panorays generates rapid reports that specifically address whether your suppliers comply with NYDFS, and what can be done to rectify any issues.

In addition, Panorays allows you to easily engage with your third parties. This not only ensures that cyber gaps are mitigated; it provides important compliance documentation that can be helpful when attesting the state of your third-party security.

With these features in place, Panorays helps you comply with the rigorous cybersecurity third-party requirements of NYDFS.

About Panorays

Panorays automates third-party security lifecycle management. With the Panorays platform, companies dramatically speed up their third-party security evaluation process and gain continuous visibility while ensuring compliance to regulations such as GDPR, CCPA and NYDFS.

It is the only platform that enables companies to easily view, manage and engage on the security posture of their third parties, vendors, suppliers and business partners. Panorays is a SaaS-based platform, with no installation needed.

Panorays

Want to learn more about how Panorays can help you comply with NYDFS?
Contact your Panorays sales rep or email us at info@panorays.com