COMPLIANCE

REDSEAL

NYS DFS CYBERSECURITY REGULATIONS

COMPLIANCE WITH REDSEAL

THE FOUNDATION FOR RESILIENCE

The New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) officially took effect on March 1, 2017. Beginning February 2018, covered organizations must annually certify their compliance with the regulations over the previous year.

RedSeal's network modeling and risk scoring platform is a strategic solution that can greatly aid organizations in efficiently achieving and documenting compliance with the NYS DFS Cybersecurity Regulations. This data sheet will demonstrate how RedSeal can quickly help organizations design, implement, and document compliant programs and policies.

WHO IS IMPACTED?

Your organization is covered if it is an individual or non-governmental organization supervised by the New York State Department of Financial Services (NYS DFS) and relies on it for license, registration, charter, certification, permit, accreditation, or similar authorization.

Vendors and service providers for these organizations are also impacted because they will have to implement minimum cybersecurity practices to meet their client organizations' policies and be subject to regular audits and assessments.

WHAT'S IN IT?

To comply with the requirements, organizations need to establish and maintain:

1. **A cybersecurity program** designed to protect the confidentiality, integrity, and availability of the organization's information systems. The cybersecurity program needs to perform the following functions:
   a. Identify and assess internal and external cybersecurity risks
   b. Use defensive infrastructure configured according to specific policies and procedures
   c. Detect cybersecurity events
   d. Respond to cybersecurity events
   e. Recover from cybersecurity events and restore normal operations and services
   f. Fulfill obligations to report to the Board on the above

HIGHLIGHTS

- The New York State Department of Financial Services Cybersecurity Regulations went into effect on March 1, 2017.
- The regulations require organizations to enact a cybersecurity policy, design and staff a cybersecurity program to enforce the policy, and name a chief information security officer to administer and report on the program.
- RedSeal is a strategic solution that can help achieve, monitor, and demonstrate compliance with 26 subsections.

NYS DFS CYBERSECURITY REGULATIONS COMPLIANCE

2. **A cybersecurity policy -** a written policy approved by the organization's Board of Directors setting forth the policies and procedures for the protection of its information systems and nonpublic information stored on those systems. The cybersecurity policy needs to address the following areas:

   a. Information security

   b. Data governance and classification

   c. Asset inventory and device management

   d. Access controls and identity management

   e. Business continuity and disaster recovery planning and resources

   f. Systems operations and availability concerns

   g. Systems and network security

   h. Systems and network monitoring

   i. Systems and application development and quality assurance

   j. Physical security and environmental controls

   k. Customer data privacy

   l. Vendor and third-party service provider management

   m. Risk assessment

   n. Incident response

3. **A chief information security officer (CISO)** in charge of overseeing and implementing the cybersecurity program, enforcing cybersecurity policy and sustaining compliance with the NYS DFS Cybersecurity Regulations. Each year, the CISO must report the following information to the Board:

   a. Confidentiality of nonpublic information and the integrity and security of information systems

   b. Cybersecurity policies and procedures

   c. Material cybersecurity risks

   d. Overall effectiveness of the cybersecurity program

   e. Material cybersecurity events over the past year

HOW DOES REDSEAL HELP WITH NYS DFS CYBERSECURITY REGULATIONS COMPLIANCE?

The NYS DFS requirements specify a wide range of specific information security practices, processes, and goals necessary to achieve compliance. RedSeal can help achieve and demonstrate compliance with a large proportion of the regulations.

NYS DFS CYBERSECURITY REGULATIONS COMPLIANCE

REQUIREMENTS SECTION	SUB-REQUIREMENTS SUPPORTED	REDSEAL CAPABILITIES USED
500.02 Cybersecurity Program	500.02(b)(1); 500.02(b)(2); 500.02(b)(3); 500.02(b)(4)	RedSeal helps identify and assess internal and external risk by analyzing network infrastructure, configurations, and all relevant access controls. RedSeal checks secure configurations and network segmentation policies. This ensures that defensive infrastructure is in place, configured securely, and complies with network segmentation policies.
500.03 Cybersecurity Policy	500.03(a); 500.03(c); 500.03(d); 500.03(g); 500.03(h); 500.03(l); 500.03(m); 500.03(n)	RedSeal can be incorporated into cybersecurity policies and processes to address requirements in the supported sections. RedSeal can discover and identify assets and devices, ingesting their configurations to develop a comprehensive understanding of the relevant access controls. RedSeal checks secure configurations and evaluates all existing access paths. Then, it makes recommendations to ensure systems and network security, and it continuously monitors compliance. Similarly, incorporating RedSeal into vendor or third-party provider management, risk assessments, and incident response policies will allow for quick and efficient compliance with the regulations.
500.04 Chief Information Security Officer	500.04(b); 500.04(b)(1); 500.04(b)(3); 500.04(b)(4)	RedSeal provides extensive reporting to meet the CISO reporting requirements of the NYS DFS Cybersecurity Regulations. These include the RedSeal Digital Resilience Score (DRS) and reports on secure configuration violations, policy compliance, and risk-based vulnerability. The DRS is a comprehensive and reliable measure of a cybersecurity program’s overall effectiveness.
500.05 Penetration Testing and Vulnerability Assessments	500.05(a); 500.05(b)	RedSeal is used by penetration testing teams to identify risks, build a map of the network and the attack surface. As a part of vulnerability assessments and regular vulnerability management programs, RedSeal helps perform risk-based prioritization of findings, taking into account network location and access.

NYS DFS CYBERSECURITY REGULATIONS COMPLIANCE

REQUIREMENTS SECTION	SUB-REQUIREMENTS SUPPORTED	REDSEAL CAPABILITIES USED
500.09 Risk Assessment	500.09(a); 500.09(b)(1); 500.09(b)(2)	RedSeal can help evaluate internal and external risks and identify technical controls to mitigate and respond to evolving threats. RedSeal's analysis includes the organization's cybersecurity business operations, collected or stored nonpublic information, information systems and the availability and effectiveness of controls to protect nonpublic information and information systems.
500.11 Third Party Service Provider Security Policy	500.11(a); 500.11(a)(2); 500.11(a)(3); 500.11(a)(4)	RedSeal implements and monitors network segmentation policies to ensure the security and confidentiality of nonpublic information on third parties' systems. RedSeal can also perform due diligence on third party networks to ensure that there are minimum cybersecurity practices in place.
500.16 Incident Response Plan	500.16(a); 500.16(b)(1); 500.16(b)(5)	As part of a written incident response plan, RedSeal helps organizations promptly respond to and recover from cybersecurity events that affect the confidentiality, integrity or availability of their information systems. Additionally, RedSeal can help identify devices and associated controls necessary for remediation or mitigation of identified weaknesses.