NYDFS Cybersecurity Requirements

Part 1: The Regulation

and the ISO 27001 standard

February 2017

Protect • Comply • Thrive

Comply with the NYDFS Cybersecurity Requirements with the international standard ISO 27001

Introduction

More and more business sectors and organizations are harnessing the benefits of connectivity and ever-advancing technological solutions, but this progress comes with a downside: the increased risk of cybercrime. Various international, national, state and sectoral Regulations are therefore being introduced at various rates to support the realization that cybersecurity is relevant to every type of business in every sector, and to ensure that all of those who could be affected are appropriately protected.

The reaction from the **New York State Department of Financial Services** comes in the form of the Cybersecurity Requirements for Financial Services Companies – the Regulation applies to all companies supervised by the Department of Financial Services ('covered entities').

The primary objective of the Regulation is to protect the confidentiality, integrity and availability of a company's information systems and nonpublic information. It's important to remember that information systems include IT equipment and resources used to collect, process, maintain, use, share, disseminate or dispose of electronic information, as well as industrial/process and environmental control systems, telephone switching and private branch exchange systems, and so on.

The Regulation's requirements are in addition to what is expected as a result of the FinCEN advisory note on cyber events and cyber-enabled crime, and the related FAQs on using suspicious activity reports (SARs) for reporting cyber events, cyber-enabled crime and cyber-related information.

This green paper considers the Cybersecurity Requirements and the timescales in which they apply, and explores one of the options open to organizations that need to meet them: independently accredited certification to the international standard for information security management, ISO 27001.

Timescales and reporting

The Cybersecurity Requirements for Financial Services Companies apply to all companies conducting business in New York that are required to operate "*under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law*" of New York.

This is a broad swath of the organizations operating in New York, including large and small banks, insurance companies, New York-licensed lenders, and mortgage companies. A limited number of exemptions are in place for smaller organizations, but it would be sensible to apply many of the same conditions for the simple reason that a cyber attack is likely to be more critically damaging to a small operation. It is also reasonable to expect that many covered entities will require some of their suppliers and service providers to meet key requirements from the Regulation to provide the third-party assurances required (notably under Section 500.11 of the Regulation).

The requirements come into effect on March 1, 2017, with the reporting requirement kicking in on February 15, 2018. Reporting is through the annual submission of a certification of compliance, the first of which will cover the period up to February 15, 2018. Some of the requirements have a delayed ‘effective date’, but every company to which the requirements apply has to implement and maintain a risk-based cybersecurity program. There are further reporting obligations where cybersecurity events occur: Subject to the significance of the event, organizations may need to report events within 72 hours of identification.

The requirements apply according to the following timetable:

March 1, 2017

- The Regulation comes into effect.

August 28, 2017 (end of 180-day transition period)

Covered entities must:

- Maintain a documented, risk-based cybersecurity program designed to protect the confidentiality, integrity and availability if their information systems (Section 500.02).
- Implement and maintain a cybersecurity policy (Section 500.03) addressing:
  - Information security
  - Data governance and classification
  - Asset inventory and device management
  - Access controls and identity management
  - Business continuity and disaster recovery planning and resources
  - Systems operations and availability concerns
  - Systems and network security
  - Systems and network monitoring
  - Systems and application development and quality assurance
  - Physical security and environmental controls
  - Customer data privacy
  - Vendor and third-party service provider management
  - Risk assessment
  - Incident response
- Appoint a CISO responsible for overseeing and implementing its cybersecurity program, and enforcing its cybersecurity policy (Section 500.04, a).
- Limit access privileges to information systems that provide access to nonpublic information, and periodically review these access privileges (Section 500.07).
- Utilize qualified cybersecurity personnel to oversee core cybersecurity functions. Personnel may be employed by the covered entity, an affiliate, or a third-party service provider (Section 500.10).
- Establish a written cybersecurity incident response plan addressing internal response processes; goals; roles, responsibilities and levels of decision-making authority; communications and information

sharing; remediating weaknesses in information systems and associated controls; the documentation and reporting of cybersecurity events; the evaluation and revision of the incident response plan following a cybersecurity event (Section 500.16).

February 15, 2018

Covered entities must:

- Prepare and submit an annual written statement to the Superintendent of Financial Services, certifying their compliance with the Regulation. The first Certification of Compliance is due by February 15, 2018. (Section 500.21).

March 1, 2018

Covered entities must:

- Have their designated CISO report in writing at least annually to the board of directors or equivalent governing body (Section 500.04, b).
- Include in their cybersecurity programs continuous monitoring or annual penetration testing and biannual vulnerability assessments, as determined by risk assessments (Section 500.05).
- Conduct risk assessments to inform the design of the cybersecurity program (Section 500.09).
- Use effective controls, including multi-factor authentication, to protect nonpublic information or information systems from unauthorized access (Section 500.12).
- Introduce regular cybersecurity awareness training for all personnel that is updated to reflect the results of risk assessments (Section 500.14, b).

September 1, 2018

Covered entities must:

- Maintain systems that are designed to reconstruct material financial transactions for normal business operations and keep records for five years. Audit trails to detect and respond to cybersecurity events should be maintained for at least three years. (Section 500.06).
- Include in their cybersecurity programs written procedures, guidelines and standards that ensure the secure in-house development of applications, and procedures to evaluate, assess or test the security of externally developed applications. These documents must be periodically reviewed, assessed and updated as necessary by the covered entity’s chief information security officer (CISO) or a qualified designee (Section 500.08).
- Include in their cybersecurity programs policies and procedures for the secure disposal of nonpublic information that no longer needs to be retained, except where it must be retained by law, or where targeted disposal is not feasible (Section 500.13).

- Implement risk-based policies, procedures and controls to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with nonpublic information by unauthorized users (Section 500.14, a).
- Implement controls, including encryption, to protect nonpublic information held or transmitted by the covered entity, whether at rest or in transit. If encryption is infeasible, compensating controls may be used. These should be approved by the CISO and reviewed at least annually (Section 500.15).

March 1, 2019

- Introduce a third-party service provider policy (Section 500.11).

The most striking aspects of the timetable are that it suggests a company could delay conducting penetration testing and vulnerability scans for a year. Moreover, the inclusion of cybersecurity awareness training in the 'one-year delay' set of requirements is misleading, as the effective implementation of cybersecurity policies (section 500.03) and a cyber incident response plan (section 500.16) will require effective competence, training and awareness for the personnel involved.

ISO 27001 – the international standard for information security management

The international standard ISO/IEC 27001:2013 (ISO 27001, the Standard) sets out the specifications of a best-practice information security management system (ISMS) – "a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives" (ISO 27000:2016).

ISO 27001 takes a risk-based approach to information security that encompasses people, processes and technology, recognizing that information security is an enterprise-wide concern that therefore needs an enterprise-wide solution. It can be employed by organizations of all sizes, sectors and locations.

It is also the only international information security management standard against which organizations can achieve independently audited certification, which is globally accepted as a demonstration that the organization has adopted international best practice.

Certification to ISO 27001 has seen a steep increase in the US over the past eight years: According to the latest ISO survey, 78% more organizations were registered to ISO 27001 in 2015 than in 2014.

ISO 27001-compliant ISMS helps organizations meet their legal and regulatory compliance requirements, including state data breach notification laws, federal regulations such as FISMA, the GLBA, HIPAA, and SOX, international standards like the PCI DSS, and, of course, the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies.

ISO 27001 benefits

An ISO 27001-compliant ISMS can, when developed appropriately, provide additional benefits beyond simply addressing the Cybersecurity Requirements:

- An aligned set of processes not only meet the Regulation and your business requirements as they are today, but also ensure that they will continue to be met in the future in a cost-effective manner – the management system enables your organization to identify, monitor and maintain the optimum mix of controls for the changing environment in which you operate.

- An ISMS safeguards the integrity and availability of publicly available information as well as the appropriate protection of 'Nonpublic Information' (to the extent your organization has it beyond that described in section 500.01, g of the Regulation.)

- ISO 27001 can be directly aligned with, and encourage the adoption of, whichever control set(s) you deem appropriate – NIST, COBIT®, etc. The information security management system provides the framework by which you select good practice from a number of sources and blend them to meet multiple legal, regulatory and contractual obligations.

- The Standard is designed to ensure your organization selects adequate and proportionate security controls that help to protect information assets.

- An ISMS is a systematic approach to managing the security of sensitive information and is designed to identify, manage and reduce the range of threats to which your information is regularly subjected.

- ISO 27001 improves company culture. The Standard's holistic approach covers the whole organization, not just IT, and encompasses people, processes, and technology. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.

- ISO 27001 improves structure and focus. When a business grows rapidly, it doesn't take long before there is confusion about who is responsible for which information assets. The Standard helps businesses become more productive by clearly setting out information risk responsibilities.

As referenced earlier, organizations that want to demonstrate their compliance with the Cybersecurity Requirements can pursue accredited certification. Accredited certification of the ISMS provides a means of demonstrating to others that your organization takes its cybersecurity obligations seriously and is judged by an accredited registration body as complying with what is internationally recognized as the best-practice arrangements for the management of cybersecurity and information security. Furthermore, this third-party assurance can result in regulator and client requirements for security audits and questionnaires being reduced or even eliminated, and opens up new business opportunities.

Conclusion

An ISMS that complies with ISO 27001 is one means of ensuring your organization meets the Cybersecurity Requirements consistently over time.

While the Cybersecurity Requirements do not explicitly demand a formal management system, such as an ISMS, for compliance, it is a practical and effective approach, and the difference between an ISMS and a cybersecurity program as required by the Regulation is debatable. ISO 27001 offers such an approach and is supported by the ISO 27002 guidance on security controls: guidance that can be equally applied to the implementation of controls contained in the Regulation as to ISO 27001. Furthermore, as ISO 27001 is a popular management system standard, there is a wealth of resources available to organizations seeking to conform with or achieve accredited certification to it.

Perhaps most usefully, ISO 27001 requires a process to ensure ongoing compliance and continual improvement based on regular and consistent monitoring, measurement and review. For organizations that need to ensure that compliance with a number of changing requirements from separate sources is consistently maintained, such a structure is not just valuable; it is essential.

There are a number of other publications that support and provide guidance on the ISO 27001 specification[1]; one particularly useful one is ISO 27002, which provides guidance on the application and implementation of the 114 information security controls identified in Annex A of ISO 27001. It takes a list of controls that covers 13 sides of text and addresses them in turn over 77 pages – an additional 64 sides of valuable insight.

For an in-depth explanation of exactly how ISO 27001 can help you comply with the Cybersecurity Requirements, please download the second part of this green paper: **NYDFS Cybersecurity Requirements for Financial Services Companies Part 2: Mapped Alignment with ISO 27001.**

Useful resources

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions, and professional consultancy services.

Training

- **New York DFS Cybersecurity & ISO27001 Certified ISMS Foundation Online**

  The one-day course will provide delegates with an introduction to ISO 27001 best practice and certification, an understanding of how to identify some primary risks associated with cyber crime, and clarification on how ISO 27001 controls align with the measures needed to satisfy the Cybersecurity Requirements.

- **New York DFS Cybersecurity & ISO27001 Certified ISMS Lead Implementer Online**

  The three-day course has been designed to enable individuals to achieve the ISO27001 Certified ISMS Lead Implementer (CIS LI) qualification and ensure their ISO 27001 project aligns with the Cybersecurity Requirements. An experienced trainer and consultant will guide you through nine steps to ISO 27001 success and help you develop the skills required to achieve ISO 27001 compliance for your organization.

Tools

- **ISO 27001 Cybersecurity Documentation on Toolkit**

  Fully compliant with ISO 27001:2013, this widely applicable risk assessment tool automates and delivers an information security risk assessment quickly and easily.

- **vsRisk Standalone**

  Fully compliant with ISO 27001:2013, this widely applicable risk assessment tool automates and delivers an information security risk assessment quickly and easily. vsRisk™ has been proven to save huge amounts of time, effort and expense when tackling complex risk assessments. This standalone is intended for a single, desktop-based user.

- **vsRisk Multi-user**

  vsRisk™ Multi-user enables up to ten risk assessors to conduct a comprehensive risk assessment across the organization simultaneously. vsRisk simplifies and accelerates the risk assessment and reporting process, ensuring uniformity and consistency throughout, and makes collaborative risk assessment significantly easier, saving time, effort and expense.

Standards

- **ISO 27001 ISMS Requirements**

ISO/IEC 27001:2013, usually referred to as just as ISO 27001, is the best-practice specification that helps businesses and organizations throughout the world develop an information security management system (ISMS).

- **ISO 27002 Code of Practice for ISM**

ISO/IEC 27002:2013 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

- **ISO 27032 Guidelines for Cybersecurity**

ISO/IEC 27032: 2012 provides guidance for improving the state of cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains.

Books

- **Information Security Breaches - Avoidance and Treatment based on ISO27001**

This book uses real-life information security incidents to explain how to reduce the risks of information security breaches and what to do when they occur.

- **CyberWar, CyberTerror, CyberCrime and CyberActivism**

Understand the scale of the risk we face from criminal and other attacks mounted across the Internet, and learn about the measures that organizations and individuals can take to protect themselves.

- **IT Governance - An International Guide to Data Security and ISO27001/ISO27002**

This manual provides clear, unique guidance for both technical and non-technical managers. It details how to design, implement, and deliver an ISMS that complies with ISO 27001.

IT Governance solutions

IT Governance sources, creates and delivers products and services to meet the evolving IT governance needs of today's organizations, directors, managers, and practitioners.

IT Governance is your one-stop shop for corporate and IT governance information, books, tools, training, and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, **www.itgovernanceusa.com**, we sell the most sought-after publications covering all areas of corporate and IT governance.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT governance projects, suitable for all levels of staff knowledge, responsibility, and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium-sized organizations adapt quickly and adopt best management practice using pre-written policies, forms, and documents.

View and trial all of our available toolkits >>

Training

We offer training courses from staff awareness and foundation courses, through to advanced programs for IT practitioners and Certified Lead Implementers and Auditors.

Our training team organizes and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Through our website, you can also browse and book training courses throughout the US, which are run by a number of different suppliers.

Browse available training courses >>

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience, to help you accelerate your IT GRC (governance, risk, compliance) projects.

View our consultancy services >>

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organizations worldwide to be ISO 27001-compliant.

See all software available >>

Contact us:	1 877 317 3454
www.itgovernanceusa.com	servicecenter@itgovernanceusa.com