NYDFS Cybersecurity Requirements

Part 2: Mapped alignment with ISO 27001

February 2017

Protect • Comply • Thrive

ISO 27001 alignment with NY State's Cybersecurity Requirements

Introduction

The New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (Cybersecurity Requirements, the Regulation) come into effect on March 1, 2017, with mandatory reporting commencing February 15, 2018. The Regulation requires all New York financial institutions to implement security measures to protect themselves from cyber attacks.

ISO 27001 is the international standard that sets out the requirements of a best-practice information security management system (ISMS), that financial services companies can implement to help meet the Cybersecurity Requirements. The Standard's holistic approach to security encompasses people, processes, and technology, providing organizations with a strong information security posture.

Alignment of Cybersecurity Requirements with ISO/IEC 27001:2013

The Cybersecurity Requirements outline a series of arrangements and measures that covered entities should implement in order to mitigate cybersecurity risks and respond effectively to data breaches, thereby minimizing the negative consequences of an incident.

The arrangements and solutions on which you rely should operate together – the Regulation hints toward this with the use of the phrase 'cybersecurity program'. An ISMS provides such an integrated approach to cybersecurity.

The value of an effective ISMS has been recognized globally for some time, with two global standards organizations – the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) – convening a committee of leading experts to document the requirements for an effective ISMS. This requirements document, *Information technology – Security techniques – Information security management systems – Requirements*, is known as ISO/IEC 27001:2013 or, more commonly, ISO 27001.

ISO 27001 provides a set of requirements for the establishment, implementation, maintenance, and continual improvement of an ISMS. If an organization adopts ISO 27001 and ensures its information security management arrangements meet the Standard's requirements, then it can achieve accredited certification following audit by an independent registration/certification body. Accredited certification not only provides a globally recognized 'badge' that gives assurance to stakeholders, but also demonstrates that the organization is continually reviewing the changing environment in which it operates and reacting to it in a coordinated, planned, and appropriate manner. In short, ISO 27001 provides a solution that not only helps financial services companies meet the Cybersecurity Requirements, but helps them meet other requirements from other sources.

While ISO 27001 provides a best-practice approach that helps you meet the Cybersecurity Requirements (and other regulations/obligations that are relevant to your organization), it does not provide the detailed guidance you might be hoping for –

that guidance is contained in a number of supporting documents. A 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 pages of text and addresses them in turn, providing an additional 64 pages of valuable insight.

Cybersecurity Requirements summarized

The following sections provide a high-level analysis of the NYDFS Cybersecurity Requirements and explain how ISO 27001 can be used to meet each requirement.

Section 500.02 Cybersecurity Program

Having defined relevant terms, the Regulation launches into the first of the requirements: to establish a cybersecurity program. Such a program must be informed by the results of a risk assessment in order to determine the risks facing the organization, its information, and its information systems. This will enable the organization to select the relevant controls and additional measures that might be applicable.

This approach aligns with ISO 27001 – in particular clauses 4 to 6: Establishing the context and framework of an information security management system (ISMS), and using a risk assessment to determine appropriate information security measures. In ISO 27001, a set of reference controls are included in Annex A by way of a 'sense check' to ensure that no areas have been overlooked – many of these Annex A controls overlap with the measures required by the Regulation.

Of particular note, clause c of this section states: "A Covered Entity may meet the requirements of this Part by adopting a cybersecurity program maintained by an Affiliate, provided that the Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of this Part."

So, organizations can implement an ISMS to meet the compliance requirements provided that the ISMS covers its information systems and nonpublic information. An ISO 27001-compliant ISMS will also ensure that the documentary evidence referenced in clause d of this section is retained and protected appropriately.

Section 500.03 Cybersecurity Policy

The Regulation sets out a number of topics that must be covered in a top-level cybersecurity policy, as well as the stipulation that it should be based on the organization's cybersecurity risk assessment. In terms of seeking guidance in developing your cybersecurity policy, appropriate information can be gathered from the ISO 27000 series of documents, as follows:

1. **Information security**
   Information security is concerned with the protection of the confidentiality, integrity, and availability of information, just as in ISO 27001 and ISO 27002, and in particular clause

5.2 and security control category A.5. This is a broad topic more specifically addressed by the other points in this part of the Regulation, but it is worth noting that the Regulation limits its applicability to "information systems and nonpublic information". While it is possible to focus an ISO 27001-compliant ISMS on this scope, it is also possible to use ISO 27001 across a wider scope to help protect the organization's intellectual property, as well as other information assets.

2. **Data governance and classification**
   The ISO 27001 controls at A.8.2 are directly relevant here (guidance can be found in section 8.2 of ISO 27002).

3. **Asset inventory and device management**
   The ISO 27001 controls at A.8.1 are relevant (guidance can be found in section A.8.1 of ISO 27002).

4. **Access controls and identity management**
   ISO 27001 security controls at A.9.1 are relevant (guidance can be found in section A.9.1 of ISO 27002).

5. **Business continuity and disaster recovery planning and resources**
   In relation to cybersecurity, consider the guidance available in clause 17 of ISO 27002 (controls at A.17 in ISO 27001). Good-practice business continuity and disaster recovery measures can be found in the international business continuity management system standard, ISO 22301.

6. **Systems operations and availability concerns**
   The security control requirements at A.12 of ISO 27001 map to this (guidance can be found at clause 12 of ISO 27002).

7. **Systems and network security**
   ISO 27001 section A.13 are relevant (guidance can be found in section 13 of ISO 27002).

8. **Systems and network monitoring**
   Consider the guidance available in ISO 27002 that maps to ISO 27001 security controls in section A.12.4, and the individual controls at A.12.7 and A.18.2.3.

9. **Systems and application development and quality assurance**
   In relation to cybersecurity, consider the controls at A.14 of ISO 27001.

10. **Physical security and environmental controls**
    The security controls in category A.11 of ISO 27001 are relevant.

11. **Customer data privacy**
    There is a strong case that the vast majority of the ISO 27001 Annex A controls apply here, but look specifically at the controls in categories A.6 and A.8, and control A.18.1, and the supporting guidance in ISO 27002.

12. **Vendor and third-party service provider management**
    The controls in category A.15 of ISO 27001 are relevant (guidance can be found in section

15 of ISO 27002). The management system specifications at clause 8.1 of ISO 27001 are also relevant.

13. **Risk assessment**
    There is a variety of risk assessment methodologies that can be deployed, and many businesses already use one or more for managing cyber-related risks. If your organization already uses a particular risk assessment methodology, you should already have some idea of how this can be handled. If not, clauses 6 and 8 (clauses 8.2 and 8.3 in particular) of ISO 27001 set the expectations for an information security risk assessment that also meets the needs of these requirements, both here and in section 500.09 – risk assessment. Neither set of requirements specifies a particular risk methodology, however, so organizations are free to develop one that meets their needs.

14. **Incident response**
    All of the controls in A.16 of ISO 27001 relate to this requirement (guidance in section 16 of ISO 27002).

Many of these topics are further addressed in the remaining parts of the Regulation, so it's important that your cybersecurity policy is supported by a management structure. Responsibility and accountability should be asserted from a very early stage to ensure that your organization complies with the Regulation and continues to do so into the future.

Section 500.04 Chief Information Security Officer

The chief information security officer (CISO) is a mandatory role responsible for the organization's cybersecurity. They will report to the board at least annually on the organization's cybersecurity program and key cybersecurity risks.

In terms of ISO 27001, the requirements of this section of the Regulation are reflected in clauses 5.3 (Organizational roles, responsibilities and authorities) and 9.2 (Internal audit). If the CISO is an internal role then they are likely to be part of what ISO 27001 calls 'top management', which directs and controls the ISMS in accordance with clause 5, and reviews the ISMS in order to report to the board in accordance with the requirements at clause 9.3. If the CISO function is provided as a service from an external resource, then they will be reporting to top management.

Sections 500.05 – 500.17

The remaining body of the Regulation is given over to the specific operational and process measures that organizations need to put in place.

Section	ISO 27001:2013 clauses/controls	Comment
500.05 Penetration Testing and Vulnerability Assessments	Clause 9.1 A.18.2.3	Penetration testing and vulnerability assessments provide evidence of the security of information systems and applications. The feedback they provide can be used to remove weaknesses (known and emerging) and improve services.
500.06 Audit Trail	Clause 7.5 A.6.1.5 A.12 A.13 A.16 A.18.1.3	Audit trails are essential for traceability, as well as for identifying what occurred when something went wrong and identifying patterns that could lead to such errors in the future.
500.07 Access Privileges	A.9	It is a very simple concept that information should only be accessible to those who have a valid need to access it, and that the access provided is on a least-damage basis. Establishing the arrangements to ensure this and monitoring it is a stated requirement in the Regulation, and the whole of security control category A.9 in ISO 27001 can contribute to effective access management.
500.08 Application Security	A.14	Whether procuring, developing or maintaining applications, organizations need to ensure that they have established practices and processes to guarantee the appropriate security measures are, and remain, in place.
500.09 Risk Assessment	Clause 6.1 Clause 8.2 Clause 8.3	As mentioned previously, ISO 27001 includes a set of requirements for information security risk management. A wide range of information security risk assessment methods exist, the two most common being asset-based (estimating the risks to information assets) or scenario-based (estimating the range of risks posed by a given set of circumstances).

500.10 Cybersecurity Personnel and Intelligence	Clause 5.1 Clause 5.3 Clause 7.1 Clause 7.2 Clause 7.3 A.6.1.1 A.7.2	This will likely require an integrated approach to ensure the correct mix of skills are available and maintained, and that awareness is appropriate for cybersecurity issues.
500.11 Third Party Service Provider Security Policy	Clause 8.1 (and 4 & 6) A.7.2 A.10 A.15 A.16	As Target discovered to its detriment, the security perimeter does not end at the limits of the organization. Suppliers – especially those with access to confidential information or information systems – present a risk to the organization's information assets. It is critical to ensure that information security is adequately addressed in agreements with third-party suppliers, including measures for redress and the distribution of culpability.
500.12 Multi-Factor Authentication	A.9.1.1 A.9.1.2 A.9.4.2 A.11.1.2	The Regulation states that organizations must implement multi-factor authentication (a combination of factors the user knows, has, or is) for any external access to the organization's internal networks, unless the CISO has approved "reasonably equivalent or more secure access controls."
500.13 Limitations on Data Retention	A.8.3.2 A.11.2.7 A.18.1.3	The Regulation requires the organization to develop policies and procedures governing appropriate retention periods for relevant information, and ensuring these are not unnecessarily long, and support this with procedures governing the secure disposal or disposition of these information assets once the retention period expires.
500.14 Training and Monitoring	Clause 7.2 Clause 7.3 A.7.2.2 A.12.4	In concert with the requirements for awareness and competence, the organization will need to ensure that it provides relevant, effective training for appropriate employees. This will need to be supported by measures to assure

	A.12.7 A.18.2.2	the organization of the training program's effectiveness.
500.15 Encryption of Nonpublic Information	Clause 6.1.2 Clause 6.1.3 Clause 6.2 Clause 8.3 Clause 9.1 Clause 9.3 A.10	Throughout this section, the Regulation emphasizes the extent to which the organization's adoption of encryption is informed by the risk assessment. It also adopts the concept of compensating controls where cryptography is not a feasible option.
500.16 Incident Response Plan	Clause 6.2 Clause 7.4 Clause 10 A.16	The Regulation requires a written incident response plan. An effective set of information security event and incident arrangements can be established by considering the security controls in category A.16 of ISO 27001. In addition to the ISO 27002 guidance at section 16, there is more guidance available in the ISO 27035 standards (ISO 27035-1 and ISO 27035-2).
500.17 Notices to Superintendent	Clause 4 Clause 7.5 A.6.1.3 A.16.1.4	The requirement to report a cybersecurity event within 72 hours of discovery requires the incident response plan (above) to be working effectively, along with many other aspects of the cybersecurity program.
500.18 Confidentiality	A.8.2	The security controls relating to the appropriate classification, labelling, and handling of data (A.8.2 of ISO 27001) directly relate to the requirement to collectively control and share access to records as required by the listed laws (Banking Law, Insurance Law, Financial Services Law, Public Officers Law, and others as applicable).

Conclusion

While the requirements have been listed separately by section above, it is important to note that an effective cybersecurity program – and an effective ISMS – relies enormously on how the

solutions to each and every requirement depend on and interact with the others: The program, or system, has to work as a holistic solution.

Implementing an ISMS that complies with ISO 27001 will ensure that your organization meets the New York State Cybersecurity Requirements for Financial Services.

ISO 27001 provides a management system that helps you coordinate all your cybersecurity efforts (technological, people-based, and physical) consistently and cost-effectively. This framework incorporates the controls you need to meet the New York State Department of Financial Services Cybersecurity Requirements, and provides additional measures to ensure your organization is prepared for other cyber threats that you face or that might arise.

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 Toolkit**

This toolkit will help you implement ISO 27001, the international best practice for information security, quickly and cost-effectively with its customizable and editable templates.

- **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 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