Data privacy, security measures, and managing third-party service providers to meet compliance requirements

August 17, 2017

Alan Calder
IT Governance Ltd
www.itgovernanceusa.com

Please note that all attendees in the teleconference are muted on joining.
Introduction

- Alan Calder
- Founder of IT Governance Ltd
- Author of *IT Governance: An International Guide to Data Security and ISO27001/27002*
- Led the world’s first successful implementation of ISO 27001 (then BS 7799)
Trusted global provider

• The single source for cybersecurity, cyber risk management, and IT governance

• Using a proven and pragmatic approach, we provide a variety of implementation solutions to help our clients achieve accredited certification to ISO 27001 at an agreeable cost and with minimal disruption to business

• We have helped more than 400 organizations worldwide achieve ISO 27001 certification and have been privileged to work with companies from all business sectors and industries
Agenda

- How to implement multi-factor authentication with two-factor verification measures
- Data retention limits and the disposal of nonpublic information
- Encryption of nonpublic information
- Managing third-party service providers to secure non-public information
Countdown to reporting

• **August 28, 2017** - The 180-day deadline ends for the first set of requirements
  - Among the requirements organizations must follow is the need to report data breaches within 72 hours of their discovery
  - [New online portal](#) – NYDFS website now offers an online option to report events

• **February 15, 2018** - Covered entities are required to submit the first certification under 23 NYCRR 500.17
# Timelines

<table>
<thead>
<tr>
<th>180 days</th>
<th>1 year</th>
<th>18 months</th>
<th>2 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 500.02 Cybersecurity Program</td>
<td>Section 500.04 (b) Chief Information Security Officer (CISO)</td>
<td>Section 500.06 Audit Trail</td>
<td>Section 500.11 Third Party Service Provider Security Policy</td>
</tr>
<tr>
<td>Section 500.03 Cybersecurity Policy</td>
<td>Section 500.05 Penetration Testing and Vulnerability Assessments</td>
<td>Section 500.08 Application Security</td>
<td></td>
</tr>
<tr>
<td>Section 500.07 Access Privileges</td>
<td>Section 500.09 Risk Assessment</td>
<td>Section 500.13 Limitations on Data Retention</td>
<td></td>
</tr>
<tr>
<td>Section 500.10 Cybersecurity Personnel and Intelligence</td>
<td>Section 500.12 Multi-Factor Authentication</td>
<td>Section 500.14 (a) Training and Monitoring</td>
<td></td>
</tr>
<tr>
<td>Section 500.16 Incident Response Plan</td>
<td>Section 500.14 (b) Training and Monitoring</td>
<td>Section 500.15 Encryption of Nonpublic Information</td>
<td></td>
</tr>
</tbody>
</table>
Non-compliance and penalties

• Under New York’s Financial Services Law sections 102, 201, 202, 301, 302, and 408, the NYDFS Superintendent has the authority to:
  - Issue civil penalties
  - Impose fines for the non-compliance with regulations and false reporting

• Just this year, the NYDFS fined Deutsche Bank $425 million for violating anti-money laundering laws and failing to take adequate precautions to identify compliance issues, including:
  - Inaccurate and insufficient documentation
  - Weak risk assessment
  - Under-resourced staff
Multi-factor authentication (Section 500.12)

- 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

- Multi-factor authentication shall be used for any individual accessing:
  - the covered entity’s internal networks from an external network unless the covered entity’s CISO has approved in writing the use of reasonably equivalent or more secure access controls
Password-only authentication

![Bar graph showing distribution of commonly used passwords]

- 40% of all passwords appear on the top 100 list.
- 71% of all passwords appear on the top 500 list.

Copyright IT Governance Ltd 2017 – v1.0
Is two-factor authentication enough?

- An organization’s security posture is only as strong as its weakest link. The majority of attacks involve some type of human error.

- In 2015, IBM researchers identified the Dyre Wolf campaign, which had “a formidable success rate” and had been used to steal more than $1 million from corporate banking accounts using a combination of malware and social engineering.

- IBM’s report (The Dyre Wolf: Attacks on Corporate Banking Accounts) revealed that Dyre Wolf used phishing and the popular Dyre/Dyreza banking trojan to bypass two-factor authentication and transfer money out of bank accounts.
Limitations on data retention (Section 500.13)

- Policies and procedures must be included for the secure disposal on a periodic basis of:
  - Nonpublic information that is no longer necessary for business operations or for other legitimate business purposes
  - Except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained
Planning and scheduling for data retention and disposal

- Identification of what specific documents are required to be kept for each governing regulation/law
- Determine retention period and date of disposal
- Method of secure disposal to be used

<table>
<thead>
<tr>
<th>Document type</th>
<th>Regulation/law</th>
<th>Retention period</th>
<th>Disposal date</th>
<th>Method of disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Encryption of nonpublic information
(Section 500.15)

- Implement controls, including encryption, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest
  - If the encryption of nonpublic information in transit over external networks is infeasible
    - the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the CISO
  - If the encryption of nonpublic information at rest is infeasible
    - the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the CISO
- To the extent that a Covered Entity is using compensating controls, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually
NIST cryptographic standards

- **NISTIR 7977** - Cryptographic standards and guidelines development process for private sectors covers:
  - Principles
  - Publications for NIST’s cryptographic standards and guidelines
  - Stakeholders for NIST’s cryptographic standards and guidelines
  - Engaging the cryptographic community
  - Public notice and review of proposed and final standards and guidelines
  - Policies and processes for the life cycle management of cryptographic standards and guidelines

- **NIST SP 800-175B** - Cryptographic standards in the federal government covers:
  - Standards and guidelines
  - Cryptographic algorithms
  - Cryptographic services
  - Key management
  - Other issues
ISO 27001

ISO 27001:2013

Introduction
Application
Terms and definitions

Security
• Control objectives
• Controls

Bibliography

ISO 27000:2016

ISO 27002:2013

Introduction
Scope and norm. ref.
Terms and definitions
Structure and risk asmt.

Security
• Control objectives
• Controls

Control
Implementation guidance
Other info

Copyright IT Governance Ltd 2017 – v1.0
Annex A: 14 control categories

114 CONTROLS

5 Infosec policies
6 Organization of infosec
7 Human resources security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental sec.
12 Operations security
13 Comms security
14 System acq., dev. & maintenance
15 Supplier relationships
16 Infosec incident management
17 Infosec aspects of BC mgmt
18 Compliance
A.10: Cryptography

One objective, two controls

A.10.1: Cryptographic controls: ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information

- A.10.1.1: Policy on the use of cryptographic controls
  - Yes/No? If yes, corporate position

- A.10.1.2: Key management
  - Reflect jurisdiction
Importance of data protection

Since the 1995 European Data Protection Directive, organizations have been prohibited from transferring personal data from the European Union to a third country that does not ensure “an adequate level of protection.” There are several mechanisms available to US organizations that enable them to demonstrate that their privacy practices meet EU data protection requirements.

- **Privacy Shield**
  - The EU-US Privacy Shield is a binding data transfer framework that governs the transfer, handling, sharing, and use of EU residents' personal data within the United States

- **EU GDPR**
  - Applies to every organization in the world that processes the personal information of EU residents
  - Organizations that fail to comply with the Regulation could face fines of up to 4% of annual global turnover or €20 million ($21.3 million), whichever is greater
Third-party service provider
(Section 500.11)

• Is not an Affiliate of the Covered Entity
• A Person that provides services to the covered entity
• Maintains, processes or is otherwise permitted access to nonpublic information through their provision of services to the covered entity

• Nonpublic information includes all electronic information that is not publicly available information and is:
  - Business related information that could cause an adverse impact to the business operations or security
  - Information concerning an individual which because of name, number, personal mark, or identifier can be used to identify such individual, in combination with any one or more of the following data elements:
    - social security number, drivers' license number or non-driver identification card number, account number, credit or debit card number, any security code, access code or password that would permit access to an individual's financial account, or biometric records
  - Information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:
    - the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, the provision of health care to any individual, or payment for the provision of health care to any individual
Third-party service provider security policy (Section 500.11)

- 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.

- Policies and procedures shall be **based on the risk assessment** of the covered entity and shall address to the extent applicable:
  - identification and risk assessment
  - minimum cybersecurity practices required to be met
  - periodic assessment of such third-party service providers based on the risk
  - due diligence processes used to evaluate the adequacy of cybersecurity practices
Third-party service provider security policy (cont.)

• Policies and procedures must include guidelines for due diligence and/or contractual protections relating to third-party service providers including, to the extent applicable, guidelines addressing:
  
  - **multi-factor authentication** – to limit access to relevant information systems and nonpublic information
  
  - **encryption as required** – to protect nonpublic information in transit and at rest
  
  - **notice to the covered entity in the event of a cybersecurity event** – that impacts the covered entity’s information systems or nonpublic information being held by the third-party service provider
  
  - **representations and warranties addressing the third-party service provider’s cybersecurity policies and procedures** – that relate to the security of the covered entity’s information systems or nonpublic information
Protecting your organization from third-party breaches

- **Toys“R”Us**: in February 2016, the toy retailer encouraged members of its Rewards“R”Us program to reset their passwords following “unauthorized attempts to access our Rewards member accounts.”
  - According to DataBreaches.net, a Toys“R”Us spokesperson said this “appears to be related to earlier online breaches of websites not associated with Toys“R”Us, Rewards”R”Us or our [loyalty program] vendor.

- In March 2015, there were several attempts to hack Rewards“R”Us customer accounts
  - In a letter Toys“R”Us sent out to their customers, they explained it was suspected the activity was due to large breaches at other companies (not Toys“R”Us). User login names and passwords were stolen and then used for unauthorized access to other accounts, such as Rewards“R”Us accounts
Information security agreement with third parties

- Suppliers – especially those with access to confidential information or information systems – present a risk to the organization’s information assets

- It’s critical to ensure that information security is adequately addressed in agreements with third-party suppliers, including measures for redress and the distribution of culpability

- As Target discovered to its detriment, the security perimeter does not end at the limits of the organization.
Assessment, planning, and management of third-party providers

- Security posture
- Rating/ranking system
- Contingency plan in event of a cyber event
- Exit strategy with the vendor
- Contract agreement
A.15: Supplier relationships

Two objectives, five controls

A.15.1: Information security in supplier relationships: Ensure protection of the organization’s assets that are accessible by suppliers

- A.15.1.1: Information security policy for supplier relationships
- A.15.1.2: Addressing security within supplier agreements
  - Third-party contracts to include legislative requirements, responsibilities, and consequences for access to information and information technology
  - External facilities management to identify security implications and include appropriate controls
A.15: Supplier relationships

- A.15.1.3: Information and communication technology supply chain
- A.15.2: Supplier service delivery management: Maintain an agreed level of information security and service delivery in line with supplier agreements
- A.15.2.1: Monitoring and review of supplier services
  - Service performance
  - Supplier audits – conduct, review audits of suppliers
- A.15.2.2: Managing changes to supplier services
vsRisk™ (v3.0) – monitoring third-party service providers

EXTERNAL PARTIES: INFORMATION SECURITY PROCEDURE (TIER 2)

1. Scope

Organization name maintains the security of its information-processing facilities and information assets in relation to external parties. All external parties also need to ensure that the information systems they have under their control are maintained in accordance with organizational security policies.

2. Responsibilities

2.1. All relationship (external) personnel [See Control Section 8.1.2 of the Manual] responsible for working in any of the above categories are required to ensure external parties also need to ensure that the information systems they have under their control are maintained in accordance with organizational security policies.

2.2. Responsibilities are as follows:

- Information security policy
- Information processing facilities
- Any other information assets or personnel
- Risk management
- Risk assessments [See MP-DRM-ECI 6.1.2] where required by the procedure.

3. Procedure [ISO/IEC 27002 Section 19.3.2]

This procedure may vary or change depending on your current and final future circumstances. It is important to document any changes that might be made and that are in line with the requirements of ISO/IEC 27001.
MANAGING THIRD-PARTY SERVICE CONTRACTS (TIER 2)

1. Scope (ISO27001 section 1.1)
   All external party contracts that fall within the scope of Control Section 13.1.2 of the Framework are also within the scope of this procedure.

2. Responsibilities
   2.1 The [controller] of third-party relationships are responsible for
   monitoring and reviewing the service, reports, and records provided by the third party.
   2.2 The service provider (CISO) is responsible for ensuring adequate technical and other
   resources and capabilities are made available to support the relationship.
   2.3 The security manager is responsible for ensuring periodic audits and
   reviews of third-party performance.
   2.4 The Chief Information Security Officer (CISO) is responsible for
   reviewing records of service, reports, and records provided by the third party.

3. Procedure
   3.1 The external party agreement includes reporting structures, defines
   acceptable levels of security and performance and provides monitoring, inspection, and audit rights (see ISO/IEC 13335:2013).
   3.2 The controller (CISO) monitors performance against the agreement
   and reports any issues to the third party. The [controller] secures reports required under the agreement are delivered as required and reviewed.
   3.3 The security manager reviews and reports any issues identified
   by the third party. The controller is immediately informed of any issues identified.
   3.4 The controller (CISO) identifies any problems of any sort (including
   operational problems, failures, faults and changes, fraud, and disclaimers), and either
   the controller, or the controller, takes necessary action. If necessary, the
   controller and the CISO should be notified.
   3.5 The security manager is responsible for responding to issues
   identified in the third party’s internal audit reports, and actions are
   taken as necessary. The third party’s internal audit reports and
   records are monitored, and the results of those reviews are summarized.
How it can help your business

Easy to use
Your risk assessment procedure is as simple as choosing a few options and clicking a few buttons.

Aligned with ISO 27001
Meets the ISO 27001 requirements for consistent, valid and comparable results.

Can generate auditable reports
You can export reports, including the Statement of Applicability (SoA) and risk treatment plan (RTP), edit them and share them across the business and with auditors.

Geared for repeatability
It is easy for you to repeat your risk assessments in a consistent manner year after year (or whenever circumstances change).

Streamlined and accurate
Drastically reduces the chance of human error. It’s simple, fast and accurate.
Meet the requirements of the NYDFS cybersecurity regulation with confidence

IT Governance can help you gain the skills and tools to implement the ISO 27001 standard alongside the Regulation. Choose from products that are:

- Tailored to NYDFS requirements
- Developed by expert practitioners
- Cost-effective and efficient

Get training, assess risks, and make documentation easy with:

- ISO 27001 Certified ISMS online training
- ISO 27001 Cybersecurity Documentation Toolkit
- vsRisk™ risk assessment software
# Live Online training courses

<table>
<thead>
<tr>
<th>Course: ISO27001 Certified ISMS Foundation Online</th>
<th>Course: ISO27001 Certified ISMS Lead Implementer Online</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Price:</strong> $688</td>
<td>$2,244</td>
</tr>
<tr>
<td><strong>Duration:</strong> One day</td>
<td>Three days</td>
</tr>
<tr>
<td><strong>Qualification:</strong> CIS F</td>
<td>CIS LI</td>
</tr>
<tr>
<td><strong>Dates:</strong> October 24, November 13, or December 4</td>
<td>October 25, November 14, or December 5</td>
</tr>
</tbody>
</table>
ISO 27001 Cybersecurity Documentation Toolkit

• This toolkit includes:
  
  - A complete set of mandatory and supporting ISO 27001 documentation.

  - Cybersecurity control documentation aligned with NIST SP 800-53 and the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies

  - Coverage of Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth

  - Top-level instructions and guidance to help you get started

  - Project tools to guide your implementation journey, including gap analysis and mapping documents
Valuable (free) resources

• Free green papers:
  NYDFS Cybersecurity Requirements:
  • Part 1 – The Regulation and the ISO 27001 standard
  • Part 2 – Mapped alignment with ISO 27001

• Risk assessment and ISO 27001 white paper
  • 5 Critical Steps to Successful ISO 27001 Risk Assessments

• Newly released - vsRisk 3.0
  • Watch the demo >>

• EU General Data Protection Regulation
  • A Compliance Guide

• More information on ISO 27001 and the Regulation
  • https://www.itgovernanceusa.com/iso27001-nydfs-cybersecurity
Join the conversation

• Subscribe to our IT Governance LinkedIn group: NYDFS Cybersecurity Requirements
  https://www.linkedin.com/groups/8598504
Questions and answers