NYDFS – a guide to risk assessment

July 12, 2017

Alan Calder
IT Governance Ltd
www.itgovernanceusa.com

PLEASE NOTE THAT ALL ATTENDEES ARE MUTED UPON JOINING

Agenda

www.itgoverrnanceusa.com

- Introductions
- Overview of the risk assessment policy and procedures
- The timescale to conduct a risk assessment
- The importance of the risk assessment
- vsRisk preview
- Question and answer session

Introductions

www.itgoverrnanceusa.com

- Alan Calder
- Founder of IT Governance Ltd
- CEO of Vigilant Software
- Author of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*
- Led the world's first successful implementation of ISO 27001 (then BS 7799)

Overview of the risk assessment policy and procedures

(Section 500.09)

www.itgoverrnanceusa.com

- Risk assessments of information systems should be done periodically to inform the design of the cybersecurity program.

- The risk assessment must:
  - be updated if there are any changes to information systems, non-public information, or business operations
  - allow for revision of controls to respond to threats or any technological developments; consider risks of operations that relate to cybersecurity, information systems, collected or stored non-public information; and the effectiveness of controls to protect non-public information and information systems
  - be documented and implemented in accordance with written policies and procedures

Overview of the risk assessment policy and procedures cont'd (Section 500.09)

www.itgoverrnanceusa.com

- Policies and procedures are to include:
  - measures for the evaluation and classification of identified cybersecurity threats or risks
  - conditions set for the assessment of the security, confidentiality and integrity, and availability of information systems and non-public information, including the suitability of current controls relating to identified risks
  - a plan to determine how identified risks based on the risk assessment will be mitigated or accepted, and how the cybersecurity program will address these risks

The timescale to conduct a risk assessment

- **By August 28, 2017**, organizations that are regulated by the New York State Department of Financial Services (NYDFS) must have achieved compliance with the first set of requirements, which include maintaining a cybersecurity policy and program.
- The cybersecurity program should be derived from the organization's **risk assessment.**

The importance of the risk assessment

www.itgoverrnanceusa.com

- The **risk assessment** is an essential part of complying with the Regulation and should not be delayed. Many companies might see this requirement as a grueling task, but it does not have to be.
- vsRisk is a risk assessment software tool that can help you to comply with the Regulation, saving you time and money.

Introduction to the online demonstration of vsRisk

www.itgoverrnanceusa.com

Michael Pollington

- Vigilant Software Application Specialist.
- Responsible for live one-to-one demonstrations of the software that Vigilant creates.
- Provides in-depth technical support to clients and prospective customers.

vsRisk – an introduction

www.itgoverrnanceusa.com

What is vsRisk?

- vsRisk is a desktop application for tracking and managing an asset based information security risk assessment.
- vsRisk fully aligned with ISO 27001.
- vsRisk is available in both Standalone & Multi-user versions allowing businesses of all sizes to conduct an information security risk assessment with ease.

Why is it needed?

- vsRisk ensures consistent, repeatable, and reliable risk assessments that save companies both time and money.
- Alleviates the pain points usually associated with spreadsheet based risk assessments.
- Streamlines the risk assessment process

Who is it for?

- IT managers, IT risk managers, security analysts, compliance managers, CIOs/CISOs, and heads of IT.

What it does:

www.itgoverrnanceusa.com

- Delivers the entire framework for conducting an ISO 27001 risk assessment.
- Makes storing and tracking data much easier and faster.
- Provides an audit trail for the risk assessment.
- Ensures a level of reliability and consistency that spreadsheets cannot.
- Eliminates input errors commonly found in spreadsheets.
- Generates six audit-ready reports including the Statement of Applicability (SoA) and risk treatment plan.
- Can incorporate an ISO 27001 information security management system (ISMS) toolkit, providing users with everything they need to implement the risk treatment plan that they design in vsRisk.

vsRisk Preview

www.itgoverrnanceusa.com

How it can help your business

www.itgoverrnanceusa.com

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.

Join the conversation

www.itgoverrnanceusa.com

- **Subscribe to our IT Governance LinkedIn group:**
  NYDFS Cybersecurity Requirements
  www.linkedin.com/groups/8598504

Question and answer session