

Cybersecurity for Medium and Smaller Firms

I. SEC's Proposed Cybersecurity Risk Management Rules

a. Regulation

- i. SEC's Proposed Cybersecurity Risk Management Rules Recent Division of Examinations Risk Alerts and Division of Enforcement cases Reasonably Designed Cybersecurity Policies and Procedures Practical Practice Pointers

<https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

- ii. SEC's Proposed Cybersecurity Risk Management Rules Recent Division of Examinations Risk Alerts and Division of Enforcement cases Reasonably Designed Cybersecurity Policies and Procedures Practical Practice Pointers

<https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

1. Investment Adviser Cybersecurity Incident Report

b. Relevant Comment Letters

- i. IAA Comment Letter to SEC Regarding Adviser Proposals

<https://www.investmentadviser.org/resources/iaa-comment-letter-to-sec-regarding-adviser-proposals/>

- ii. ICI Comment Letter on SEC's Cybersecurity Risk Management

<https://www.ici.org/letters/23-cl-sec-cyber-proposal>

II. Recent Division of Examinations Risk Alerts and Division of Enforcement cases

a. OCIE Cybersecurity and Resiliency Observations (2019)

<https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>

b. Observations from Cybersecurity Examinations (2017)

<https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf>

- c. SEC Announces Three Actions Charging Deficient Cybersecurity Procedures

<https://www.sec.gov/news/press-release/2021-169>

- d. SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets

<https://www.sec.gov/news/press-release/2023-52>

- e. Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P - Privacy Notices and Safeguard Policies

<https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-s-p>

- f. Cybersecurity Risk Governance, SEC Agency Rule List – Spring 2023

<https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=3235-AM89>

III. Reasonably Designed Cybersecurity Policies and Procedures

- a. National Institute of Standards and Technology - Framework

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

- b. Security Information and Event Management Systems (SIEMs) – a single pane of glass to monitor the attack surface with automated alerts

- c. Security Operations Center (SOC) – a team to detect, respond and recover

- d. Data Loss Prevention Systems – detect potential exfiltration

- e. Network Traffic Analysis – detect DDoS attacks

IV. Practical Practice Pointers

- a. NIST Self Testing Tool

https://expel.com/expel-self-scoring-tool-for-nist-csf/?utm_medium=sem&utm_source=google&utm_campaign=dgt-comm-mident-ent-mofu-bofu-nist-go-mofu-dtb-nist&utm_content=marketing-content-nist-csf-tool&bt=499708119833&bk=nist%20framework&bm=b&bn=g&bg=568941875

[27&gad_source=1&gclid=CjwKCAiA_tuuBhAUEiwAvxkgTtHcs8ohrVrDs4VbUx5VxoDR8UX8afV6T3c3jOQUtaEismC6kaegFRoCZaQQAvD_BwE](https://www.acaglobal.com/our-solutions/cybersecurity-privacy-risk)

b. ACA Vantage – Cybersecurity Self Assessment

- i. <https://www.acaglobal.com/our-solutions/cybersecurity-privacy-risk>