

## OCIE Issues New Cybersecurity Risk

Article By:

Richard M. Cutshall

---

Two weeks ago, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued its newest guidance on the subject of cybersecurity in the form of a new [National Exam Program \(NEP\) Risk Alert](#), issued Sept. 15. In addition to the matters discussed below, the Risk Alert contains links to several earlier Commission and OCIE materials, including to the March 2014 SEC Cybersecurity roundtable, past NEP cybersecurity-related releases, and the [2015 SEC examination priorities](#).

With the purpose of "[providing] additional information on the areas of focus for OCIE's second round of cybersecurity examinations" and in addition to informing industry participants that testing and assessing the implementation of cybersecurity procedures and controls will characterize the next phase of exams, the Risk Alert identifies six key areas of focus for OCIE: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response. The Risk Alert also provides a sample document request, which regulated entities may use in assessing their cybersecurity programs.

A firm's cybersecurity program, by its nature, requires ongoing review and evaluation, and OCIE and its exam staff expects senior management and boards of directors to be involved. The release of the OCIE Risk Alert provides firms with a good opportunity to reevaluate their current cybersecurity program – the six identified areas of focus highlight crucial elements of any cybersecurity program, while the sample document request provides a roadmap to the steps, processes, and documents that a regulated firm should consider in the implementation and maintenance of its cybersecurity program.

©2025 Greenberg Traurig, LLP. All rights reserved.

---

National Law Review, Volume V, Number 278

Source URL: <https://natlawreview.com/article/ocie-issues-new-cybersecurity-risk>