

What's SEC OCIE really worried about?

As a member of the financial industry, you never stop worrying -- even just a little -- about the SEC Office of Compliance Inspections and Examinations (OCIE). Their cybersecurity exam sweeps are detailed, intensive, and constantly updating to keep up with changes in the industry.

That's why it's so important to keep track of what they're really looking for.

Last year, IA Watch obtained a copy of the OCIE's phase two document request letter, which reveals the considerable range of records they will be concerned with.

brainlink
YOU RUN YOUR BUSINESS, LEAVE THE IT TO US!

SERVING NEW YORK CITY FIRMS **SINCE 1994**

We INCREASE YOUR TEAM'S PRODUCTIVITY by responding quickly to critical issues, improving systems stability, reducing downtime and resolving long -standing performance issues.

www.Brainlink.com | **917.685.7731** | info@brainlink.com

Keep these core topic areas and the listed documents to be requested in mind when it comes to ensuring your compliance with OCIE standards:

• Governance and Risk Assessment

- o Policies and Procedures for the " protection of customer/client records and information" as well as to "protect against anticipated threats to customer/client information"
- o All Board minutes concerning cybersecurity, incident response planning, and actual cybersecurity incidents
- o The name of the CISO
- o The date of the last cybersecurity risk assessment
- o List of penetration testing, with descriptions and frequencies of the tests involved
- o A sample log or report

• Access Rights and Controls

- o List of the last ten employees to leave during the review period, with documentation as evidence of their last date of employees, and the date their access to the firm's data was terminated

• Data Loss Prevention

- o Data map with identified owners
- o Documentation that shows the location of personally indefinable information

• Vendor Management

- o Policies and Procedures (if none, description of processes related to vendor management)
- o List of third party vendors with access to firm's network and data
- o Sample contract
- o Written contingency plans in case of vendor bankruptcy or other issues

• Training

- o Dates, topics, and groups of participating employees for these training events
- o Any written guidance or provided training materials

• Incident Response

- o The 25 most recent system-generated alerts relating to data loss, sensitive customer information
- o Flag alerts that required further action
- o List of any successful unauthorized external incidents
- o Identification of the amount of actual customer losses associated with cyber incidents

Even with all this vital information, ensuring your next SEC OCIE exam goes smoothly is more easily said than done.

Allow Brainlink to help.

We've got the financial industry knowledge and expertise to bring your documentation up to snuff, ensuring you having everything on the OCIE's request list during your next cybersecurity exam.

To chat about the documentation best practices, and the OCIE exam, reach out to Brainlink right away at (917) 685-7731 or info@brainlink.com