

GUIDE

Questions every director should be able to answer

Twelve questions from our director questionnaire, one set for each part of cyber oversight, with what a well-supported answer looks like.

Current as of October 13, 2026 · 3 minute read

Directors of credit unions and banks are asked to oversee cyber, fraud, BSA/AML and AI risk on the strength of what management tells them. These questions test whether that oversight rests on the record or on confidence alone. They come from the 24 questions every director answers in a BoardAlign review. Each director answers alone and says how sure they are; answers are pooled and never shown individually.

There are no trick questions here. If you can answer each one and point to where the answer is written down, your board is in a strong position. If you cannot, the question tells you what to ask for.

The program and who owns it

When did the board last approve the written information security program?

A well-supported answer: A date, recorded in the minutes, within the last year. The rules for credit unions and banks both expect the board, or a committee, to approve the written program.

Can you state where the board's responsibility for information security ends and management's begins?

A well-supported answer: The board approves, oversees and receives reports; management designs, runs and reports. A good answer names who in management is accountable.

What the board is told

Has the board approved what management must report on cybersecurity, and how often?

A well-supported answer: A written reporting schedule, approved by the board, that management works to. Without one, the board receives whatever management chooses to send.

In the reporting you receive on fraud, BSA/AML and cybersecurity, are the figures reconciled to one another?

A well-supported answer: The same event counted the same way in each report, or a note explaining why not. An account takeover can appear as a cyber incident, a fraud loss and a suspicious activity report.

Independent testing

Do you know what was excluded from the scope of the most recent penetration test?

A well-supported answer: Yes, because the summary the board saw listed the exclusions. A clean result on a narrow scope says little about the rest.

Have you been shown how long open critical or high findings have been outstanding?

A well-supported answer: An age for each, against the remediation window in your own policy, with any past due named.

Third parties

Can you name the third-party providers whose failure would materially disrupt service to your members or customers?

A well-supported answer: A short list, usually the core processor, digital banking, card processing and a few others, each with the date it was last reviewed.

Have you been shown whether independent testing includes your critical third-party providers?

A well-supported answer: Either the providers are in scope, or the board has seen their own independent reports and what they found.

Artificial intelligence

Have you been shown a written inventory of the AI systems operating in the institution?

A well-supported answer: A list that includes AI inside vendor products, not only tools the institution built or bought on purpose.

Has the board approved a policy governing the use of AI, naming an accountable executive?

A well-supported answer: A short policy and a named owner. There are no AI-specific rules for credit unions, and the main bank guidance leaves generative AI out, so this is recognized practice rather than a requirement.

Incidents

Can you state the regulatory notification clock that applies to your institution, and who starts it?

A well-supported answer: 72 hours to NCUA for a federally insured credit union; 36 hours to the primary federal regulator for a bank. A named person decides when the clock starts.

Has the board's incident escalation path been exercised, rather than only documented?

A well-supported answer: A tabletop exercise that included directors, with what it found and what changed afterwards.

If a question here has no written answer, it is a reasonable thing to ask management for before the next meeting. Asking is oversight.

Sources

12 CFR Part 748, Appendix A (credit unions).

<https://www.ecfr.gov/current/title-12/chapter-VII/subchapter-A/part-748/appendix-Appendix%20A%20to%20Part%20748>

12 CFR Part 30, Appendix B (Interagency Guidelines, OCC).

<https://www.ecfr.gov/current/title-12/chapter-I/part-30/appendix-Appendix%20B%20to%20Part%2030>

12 CFR 748.1(c), NCUA cyber incident notification. <https://www.ecfr.gov/current/title-12/chapter-VII/subchapter-A/part-748>

12 CFR Part 53, Computer-Security Incident Notification (OCC). <https://www.ecfr.gov/current/title-12/chapter-I/part-53>

NCUA, Artificial Intelligence resource page.

<https://ncua.gov/regulation-supervision/regulatory-compliance-resources/artificial-intelligence-ai>

General information for directors, not legal advice. Current as of October 13, 2026. Rules change: check the cited source before relying on it.