A Security-Culture Oversight Checklist

Questions Your Committee Should Ask

Take these to your next meeting with management or the CISO. You don't need to be a technologist, just a good overseer.

01 LEADERSHIP COMMITMENT

- ☐ How much of our security budget goes to people and training versus tools?
- ☐ Where does the person responsible for security sit, and do they have real authority and access to us?
- ☐ Is security part of executive performance expectations, or treated as separate from "the business"?

02 PSYCHOLOGICAL SAFETY & REPORTING

- ☐ When an employee reports a mistake (a click, a lost device), what actually happens to them?
- ☐ How many security concerns did staff report last quarter? (A very low number is a warning, not a comfort.)
- ☐ Can staff report a concern easily, and do they know how?

03 MEASUREMENT: CULTURE, NOT JUST COMPLIANCE

- ☐ Beyond training completion, what do we measure: reporting rate, time-to-report, repeat clickers, violation trends?
- ☐ Do we run phishing simulations, and do we track the reporting rate, not just the click rate?
- ☐ Have we ever run a security-culture assessment (survey, walk-through, interviews)? What did it find?

04 PEOPLE VS. TOOLS, & BOARD ENGAGEMENT

- ☐ Are we buying security tools while under-resourcing the people who operate them?
- ☐ Is there a documented plan describing security objectives, training requirements, and responsibilities?
- ☐ Have all board & committee members completed cyber training this year, with proof of what, when, and who?

Remember the one metric that matters most: the reporting rate beats the click rate.

A culture where people report suspicious emails is worth more than one where people simply claim they never click. Most credit unions sit at maturity Level 1–2 (Compliance → Awareness). Level 3, Behavior Change, is a realistic target.