TorchLight
Secured & Managed IT

BUILT FOR CREDIT UNIONS

CYBERSECURITY · CREDIT UNION

Cybersecurity Readiness Checklist

A C-suite playbook aligned to GLBA, FFIEC and NCUA requirements, plus the forward-looking controls examiners will be asking about next.

EDITION **6.2026** AUDIENCE **C-Suite & Board**

SCOPE **Credit Unions with $1M–$500M in Assets**

RISK ALIGNED. REWARD DEFINED. SECURED & MANAGED IT

HOW TO USE THIS DOCUMENT

An audit-ready picture, in fifteen minutes.

This checklist is built for credit union executives who want a single sit-down view of where the institution stands against current regulatory expectations and the threats that will define the next exam cycle. Every item is auditable, and every item is something a board member can ask about and a CISO can answer with evidence.

Part I covers what the rules actually require: NCUA Part 748, the FTC Safeguards Rule used as the de facto benchmark, FFIEC authentication and access guidance, the 72-hour cyber incident notification rule, and 2026 supervisory priorities. Part II covers what regulators do not require yet but examiners are increasingly asking about: phishing-resistant identity, ransomware resilience, AI-enabled fraud, instant-payments risk, and board cyber literacy.

Check the boxes you have evidence for. Anything unchecked is either a gap, an in-flight project, or a deliberate risk acceptance, and each deserves a documented owner and a date.

72-Hour
NCUA CYBER INCIDENT NOTIFICATION

30-Day
FTC SAFEGUARDS BREACH NOTICE

85
AUDITABLE CONTROLS BELOW

PART I · REGULATORY REQUIREMENTS

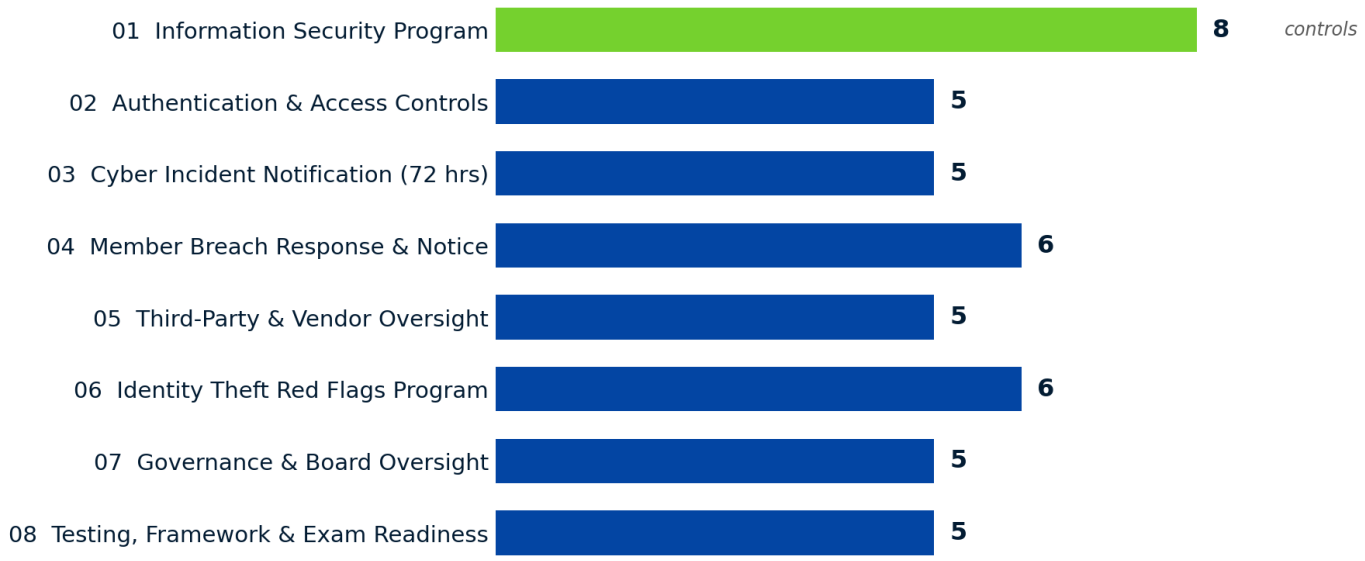
What the rules actually require.

Eight cards mapping directly to text in 12 CFR 748, 16 CFR 314, FFIEC examination guidance, and current NCUA Letters to Credit Unions.

Every item here is auditable. Every item maps to a specific paragraph in a regulation or interagency guidance document, and the AUTHORITY line at the bottom of each card tells you where. If a box is unchecked, expect a finding. If you have checked a box but cannot produce evidence, treat it the same way.

AT A GLANCE

Eight domains. 45 auditable controls, every one mapped to a regulation.



Information Security Program

The board-approved framework that anchors everything else.

- ☐ Designate a Qualified Individual (CISO or equivalent) responsible for the information security program, with documented authority in board minutes.
- ☐ Maintain a written, board-approved information security program covering administrative, technical, and physical safeguards.
- ☐ Conduct and document a written risk assessment at least annually and on material change; map findings to mitigations and owners.
- ☐ Maintain a current inventory of where member information is collected, stored, transmitted, and disposed of across all systems and vendors.
- ☐ Encrypt member information in transit and at rest; document any QI-approved compensating controls where encryption is infeasible.
- ☐ Enforce least-privilege access controls and recertify entitlements at least quarterly for systems containing member information.
- ☐ Adopt change-management procedures so security implications of system changes are evaluated and approved before deployment.
- ☐ Securely dispose of member information no later than two years after last use, with documented retention exceptions.

AUTHORITY 12 CFR 748 Appendix A · 16 CFR 314.4(a)–(f) · FTC Safeguards Rule (2023 amendments)

Authentication & Access Controls

MFA for everyone who can see member data, with layered controls behind it.

- ☐ Enforce multi-factor authentication for any individual accessing any system containing member information; no exceptions absent written QI approval of equivalent controls.
- ☐ Conduct and document an access-channel risk assessment annually for member, employee, and third-party channels.
- ☐ Apply layered security: session time-outs, system hardening, network segmentation, transaction-amount limits, and continuous monitoring.
- ☐ Maintain a current inventory of access points and authentication methods; review for stale or excessive entitlements quarterly.
- ☐ Implement and periodically test logging and monitoring of authorized user activity sufficient to detect

unauthorized access, use, or tampering.

AUTHORITY FFIEC Authentication and Access guidance (Aug 2021) · 16 CFR 314.4(c)(5)–(8)

Cyber Incident Notification (72 Hours)

The clock starts at "reasonable belief." Have the call tree tested.

- ☐ Maintain a written incident response plan that defines "reportable cyber incident" consistent with NCUA Part 748 guidance.
- ☐ Establish a 72-hour notification workflow with primary and backup contacts to NCUA via 1-833-CYBERCU or the Secure Email Message Center.
- ☐ Require all critical third-party service providers to notify the credit union of incidents within a contractual window that supports the 72-hour deadline.
- ☐ Document the basis and timestamp of the "reasonable belief" decision that triggers the clock.
- ☐ Test the notification workflow at least annually via tabletop exercise, including executive decision-makers.

AUTHORITY 12 CFR 748.1(c) · NCUA Cyber Incident Notification Final Rule (Feb 2023)

Member Breach Response & Notice

When sensitive member information is exposed, the response is regulated step-by-step.

- ☐ Maintain a documented incident response program covering assessment, containment, recovery, and post-incident review.
- ☐ Notify affected members as soon as possible when misuse of their sensitive information has occurred or is reasonably possible.
- ☐ Include in member notices: incident description, information involved, steps taken, FTC and credit bureau contacts, and fraud-alert guidance.
- ☐ Notify the NCUA Regional Director (and state supervisor for SCUs) upon suspected unauthorized access to sensitive member information.
- ☐ For affiliates or CUSOs subject to the FTC rule: notify the FTC within 30 days of any notification event involving 500+ consumers' unencrypted information.
- ☐ File a Suspicious Activity Report (SAR) when criteria are met.

AUTHORITY 12 CFR 748 Appendix B · 16 CFR 314.4(j) (effective May 13, 2024)

Third-Party & Vendor Oversight

The 72-hour clock runs against the credit union, not the vendor. Contract for it.

- ☐ Maintain a written, board-approved third-party risk management policy with risk-tiered due diligence.
- ☐ Inventory every third party that touches member data, with risk ratings and an assigned business owner.
- ☐ Require contracts to include security standards, breach-notification timelines that fit the 72-hour rule, SOC 2 deliverables, right-to-audit, and exit/transition terms.
- ☐ Reassess critical vendors at least annually with documented performance and risk reviews; escalate material changes to the board.
- ☐ Track CUSO relationships separately; ensure CUSO incidents flow into the credit union's 72-hour reporting clock.

AUTHORITY NCUA Letter to Credit Unions 07-CU-13 · Safeguards Rule 16 CFR 314.4(f)

Identity Theft Red Flags Program

Five categories of red flags. Detect, respond, report annually to the board.

- ☐ Maintain a board-approved written Identity Theft Prevention Program covering all "covered accounts."
- ☐ Identify relevant Red Flags across the five Appendix J categories: alerts, suspicious documents, suspicious PII, unusual activity, third-party notices.
- ☐ Detect Red Flags through account-opening and ongoing monitoring controls.
- ☐ Respond to detected Red Flags with documented actions: verify, contact member, close or restrict account, notify law enforcement.
- ☐ Train staff and oversee service providers performing covered activities.
- ☐ Report at least annually to the board on Program effectiveness, incidents, and recommended changes.

AUTHORITY 12 CFR 717 Subpart J · Interagency Guidelines on Identity Theft (App. J)

Governance & Board Oversight

The 2026 priority NCUA just put in writing: board members get cyber training.

- ☐ Deliver and document annual board-level cybersecurity training (newly named NCUA priority for 2026).

- ☐ Receive at least quarterly board reporting on cybersecurity metrics, incidents, and vendor posture.
- ☐ Annually review and approve the information security program, incident response plan, and risk assessment.
- ☐ Receive a written annual report from the Qualified Individual covering program status, testing, incidents, and recommendations.
- ☐ Maintain board minutes evidencing comprehension of cyber risk, including discussion of tabletop exercise results.

AUTHORITY NCUA 2026 Supervisory Priorities · FFIEC IT Examination Handbook (Management booklet)

Testing, Framework & Examination Readiness

CAT sunset closed Aug 31, 2025. Pick a successor framework and document the mapping.

- ☐ Perform annual penetration testing AND semi-annual vulnerability assessments, or implement continuous monitoring meeting 314.4(d)(2).
- ☐ Transition cybersecurity program documentation from CAT to a successor framework (CRI Profile v2.1, NIST CSF 2.0, or CISA CPGs) with mapped declarative statements.
- ☐ Complete a voluntary ACET Maturity Assessment annually and report results to the board.
- ☐ Map your information security program to ISE Core (and Core+ if applicable) examination procedures.
- ☐ Track and remediate prior IT examination findings with documented timelines and ownership.

AUTHORITY FFIEC CAT Sunset Statement (Sept 2024) · NCUA ISE/ACET · 16 CFR 314.4(d)

PART II · BEYOND COMPLIANCE

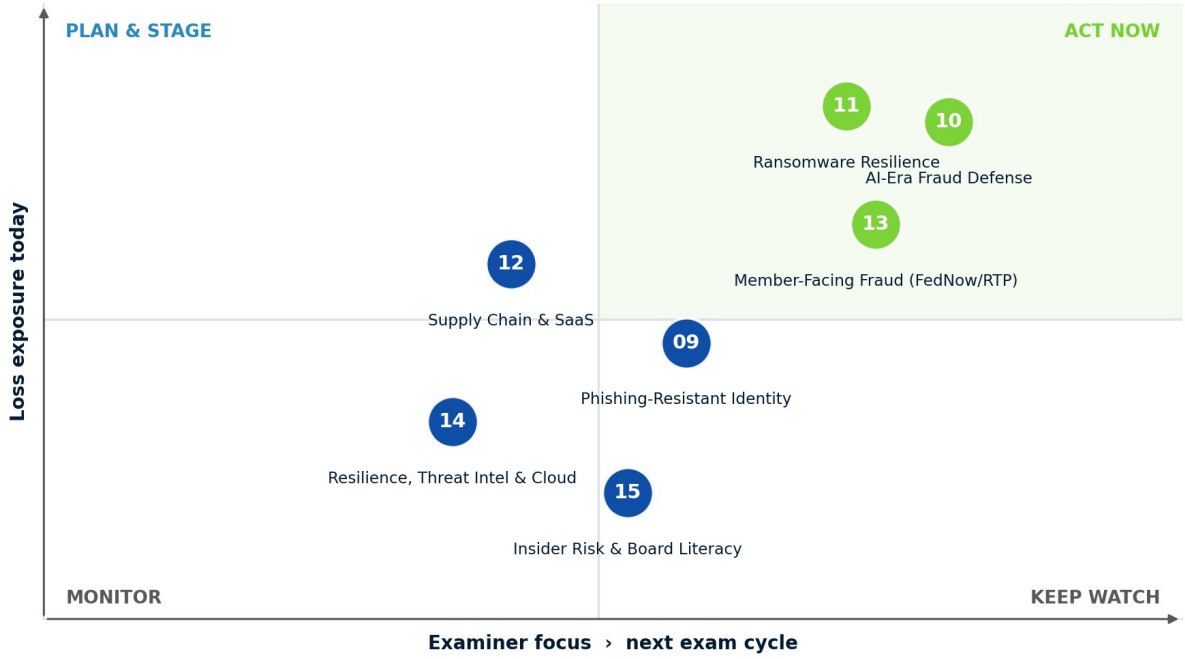
Where the next exam cycle is headed.

Seven cards on the controls regulators do not require yet, but credit unions are losing money to the threats they protect against right now.

These items map directly to the threats credit unions reported losses on in 2024 and 2025: AI-enabled fraud and deepfake authorization, ransomware and extortion, instant-payments abuse on FedNow and RTP, and supply-chain compromise. Treat unchecked items here as your strategic roadmap. The next exam cycle is increasingly going to ask about these.

STRATEGIC ROADMAP

Seven forward-looking controls, mapped to where examiners are heading next.



Phishing-Resistant Identity

Traditional MFA is no longer phishing-resistant. Move admins to FIDO2.

- ☐ Deploy phishing-resistant MFA (FIDO2 keys or device-bound passkeys) for all privileged admins; retire SMS/OTP for high-risk roles.
- ☐ Document a zero-trust architecture roadmap with explicit milestones across identity, device, network, and workload pillars.
- ☐ Enforce just-in-time and just-enough access for all privileged sessions; eliminate standing admin rights in core and AD environments.
- ☐ Implement a PAM solution with credential vaulting, session recording, and automated rotation for every privileged account.
- ☐ Require step-up authentication based on device posture, geography, and time-of-day for sensitive transactions.

AUTHORITY CISA Phishing-Resistant MFA guidance · NIST SP 800-207 (Zero Trust)

AI-Era Fraud Defense

Voice-clone attacks on call centers and wires are the fastest-growing fraud vector in the sector.

- ☐ Replace voiceprint-only call-center authentication with multi-factor callback verification or liveness-detection tools.
- ☐ Require out-of-band callback verification (to a pre-registered number, never a caller-supplied one) for all wires above a defined threshold.
- ☐ Train front-line and finance staff quarterly on deepfake, voice-clone, and synthetic-video social engineering scenarios.
- ☐ Publish an internal AI Acceptable Use Policy covering approved tools, prohibited data (member PII, MNPI), prompt logging, and human-in-the-loop requirements.
- ☐ Stand up an AI governance committee that reviews model risk, prompt-injection exposure, and vendor AI components before production deployment.

AUTHORITY America's Credit Unions (Deepfake & voice-clone briefings, 2025) · NIST AI RMF 1.0

Ransomware Resilience

Backups have to be immutable AND tested. Counsel has to be at the tabletop.

- ☐ Implement the 3-2-1-1-0 backup rule: 3 copies, 2 media, 1 offsite, 1 immutable/air-gapped, 0 errors on restore tests.
- ☐ Maintain at least one logically air-gapped, immutable backup of core banking, GL, and member data tested quarterly for full restore.
- ☐ Maintain a ransomware-specific incident response playbook covering containment, regulator notification, member communication, and ransom-payment decision authority.
- ☐ Conduct a full-scope ransomware tabletop annually including executive decision-makers and outside counsel.
- ☐ Enforce network segmentation between member-facing, corporate, branch/OT, and backup networks; verify with quarterly traffic-flow audits.

AUTHORITY CISA Stop Ransomware · FFIEC Business Continuity Management booklet

Supply Chain & SaaS Security

SOC 2 reports were never enough. SBOMs and continuous monitoring fill the gap.

- ☐ Require an SBOM from every critical software vendor (including the core processor) and re-request on each major release.
- ☐ Subscribe to a continuous vendor-monitoring service (security ratings + breach feeds), not annual questionnaires alone.
- ☐ Map fourth-party dependencies for the top 10 critical vendors and document concentration risk.
- ☐ Deploy SaaS Security Posture Management (SSPM) covering OAuth tokens, third-party app permissions, and admin-config drift for M365 and digital banking SaaS.
- ☐ Scan internally developed code with SCA tooling; remediate critical CVEs within a documented SLA.

AUTHORITY CISA SBOM guidance · NIST SP 800-161 (Supply Chain Risk Management)

Member-Facing Fraud Controls

FedNow and RTP create real-time loss potential. Score every payment.

- ☐ Deploy account-takeover controls: device fingerprinting, behavioral biometrics, step-up auth on profile and contact changes.
- ☐ Implement transaction-level fraud scoring on FedNow and RTP outbound payments using the FedNow

FraudClassifier model.

- ☐ Apply velocity, geolocation, and beneficiary-risk rules to instant payments; hold-for-review thresholds for new payees.
- ☐ Enforce DMARC at p=reject for credit-union domains; require verified callback for any vendor-payment account change.
- ☐ Coordinate with mobile carriers for SIM-swap port-out protection alerts on member numbers tied to banking credentials.
- ☐ Maintain check-fraud defenses: positive pay, payee-match, and image analysis for altered/washed checks.

AUTHORITY FedNow Fraud Classifier · FFIEC Wholesale Payment Systems · FinCEN BEC advisories

Resilience, Threat Intel & Cloud Posture

FS-ISAC + CISA alerts feeding the SOC. CSPM, secrets, and IaC scanning in CI/CD.

- ☐ Maintain active FS-ISAC membership (CNOP tier acceptable below $1B); route alerts into SOC workflow with a 24-hour triage SLA.
- ☐ Subscribe to CISA and MS-ISAC advisories; assign a named owner for review and remediation.
- ☐ Procure dark-web monitoring for member email domains, employee credentials, and brand mentions; feed hits into IR runbooks.
- ☐ Deploy CSPM/CNAPP across all cloud tenants with continuous misconfiguration scanning.
- ☐ Centralize secrets in a managed vault; rotate on schedule and on personnel changes.
- ☐ Run IaC scanning in CI/CD and scan container images for vulnerabilities and signed provenance before production.
- ☐ Define and test RTO/RPO targets for each Tier-0 service against settlement and member-service deadlines; run a live failover drill annually.

AUTHORITY FS-ISAC member guidance · CISA KEV catalog · CSA Cloud Controls Matrix

Insider Risk & Board Cyber Literacy

The board has to ask better questions. The CISO has to be able to answer them.

- ☐ Deploy User and Entity Behavior Analytics (UEBA) that baselines activity across core, teller, lending, and admin systems.

- ☐ Maintain a formal insider-risk program with HR, Legal, Security, and Compliance representation and a documented case-management workflow.
- ☐ Conduct enhanced monitoring of departing employees during notice periods (data egress, mass downloads, after-hours access).
- ☐ Provide annual cyber-risk education to every director (minimum 4 hours) covering current threats, NCUA expectations, and incident scenarios.
- ☐ Recruit or retain at least one director (or formal advisor) with documented cybersecurity expertise.
- ☐ Add a recurring CISO / cyber agenda item to every board meeting with KRI dashboards (patch latency, MFA coverage, phishing-test fail rate, third-party risk score).
- ☐ Conduct a board-level cyber tabletop annually, including ransomware payment, regulator notification, and member-communication decisions.

AUTHORITY NCUA Board Engagement Letter · Bank Policy Institute Cyber Governance

READINESS SCORE

Part I · Regulatory _____ / 45 **Part II · Beyond Compliance** _____ / 40

Next reassessment scheduled: _____

PART IV · REFERENCES

Authority & further reading.

Every requirement in Part I traces to one of the documents below. Citations are intended for use in audit workpapers.

Primary Regulations

- 12 CFR Part 748, Security Program, Cyber Incident Notification, BSA Compliance
- 12 CFR Part 748 Appendix A, Guidelines for Safeguarding Member Information
- 12 CFR Part 748 Appendix B, Response Programs & Member Notice
- 16 CFR Part 314, FTC Safeguards Rule
- 12 CFR Part 717 Subpart J, Identity Theft Red Flags (NCUA)

NCUA Guidance

- NCUA, Cyber Incident Notification Requirements
- NCUA, 2026 Supervisory Priorities
- NCUA, Information Security Examination & Cybersecurity Assessment
- NCUA, Board of Director Engagement in Cybersecurity Oversight
- NCUA, 2025 Cybersecurity & Credit Union System Resilience Report

FFIEC, FTC & CISA

- FFIEC, Authentication and Access to Financial Institution Services and Systems (Aug 2021)
- FFIEC, CAT Sunset Announcement (Sept 2024)
- FFIEC, IT Examination Handbook InfoBase
- FTC, Safeguards Rule Guidance (June 2025 update)
- CISA, Cybersecurity Performance Goals