A Security Readiness Checklist for Credit Unions & Financial Institutions

Is Your Organization Ready for Today's Security Due Diligence?

Enterprise organizations, regulators, fintech partners, and service providers are asking more detailed cybersecurity questions than ever before. Preparing before those questions arrive can accelerate partnerships, reduce business risk, and build confidence with members and stakeholders.

Use this checklist to evaluate your organization's readiness.

Governance & Leadership

1. Do we have a documented cybersecurity strategy that aligns with our business objectives?

☐ Yes
☐ No
☐ In Progress

---

2. Who is ultimately accountable for cybersecurity within our organization?

☐ Board
☐ CEO
☐ CIO
☐ CISO
☐ IT Manager
☐ Other _____

Is this responsibility formally documented?

---

3. Does executive leadership receive regular cybersecurity and risk reports?

□ Monthly
□ Quarterly
□ Annually
□ Never

---

4. Can we clearly explain our cybersecurity program to a prospective business partner in less than five minutes?

□ Yes
□ No

Identity & Access Management

5. Is Multi-Factor Authentication (MFA) required for:

□ Employees

□ Administrators

□ Remote Access

□ Vendors

□ Privileged Accounts

---

6. How quickly can user accounts be disabled after an employee leaves?

□ Immediately

□ Same Day

□ Within 24 Hours

□ Longer

---

7. Are privileged accounts reviewed regularly?

□ Quarterly

□ Annually

□ Never

Data Protection

8. Do we know exactly where member data is stored?

□ Yes

□ No

---

9. Is sensitive information encrypted:

□ At Rest

□ In Transit

□ Both

---

10. Do we have policies governing employee use of AI tools like ChatGPT, Microsoft Copilot, or Google Gemini?

□ Yes

□ No

□ Currently Developing

Third-Party Risk

11. Do we evaluate the cybersecurity posture of vendors before giving them access to our systems or member data?

□ Always

□ Sometimes

□ Rarely

---

12. Can we identify every third party with access to our environment?

□ Yes

□ No

Incident Response

13. Do we have a documented Incident Response Plan?

□ Yes

□ No

---

14. Have we tested our Incident Response Plan within the last 12 months?

□ Yes

□ No

---

15. If ransomware occurred tomorrow morning, does everyone know their role?

□ Yes

□ No

Vulnerability Management

16. How often do we perform vulnerability scanning?

□ Weekly

□ Monthly

□ Quarterly

□ Never

---

17. When was our last independent penetration test?

□ Within 12 Months

□ 1–2 Years Ago

□ More Than 2 Years

□ Never

Business Continuity

18. Have we tested restoring critical systems and data from backup within the last year?

□ Yes

□ No

Compliance & Security Readiness

19. If a strategic partner asked for evidence of our security program today, could we provide:

□ Security Policies

□ Risk Assessment

□ Incident Response Plan

□ Vulnerability Management Process

□ Security Awareness Training Records

□ Penetration Test Summary

□ Business Continuity Plan

□ Vendor Management Program

---

20. If a major enterprise, regulator, or strategic partner requested a security assessment tomorrow, how confident would we be?

□ Very Confident

□ Somewhat Confident

□ We'd Need Significant Preparation

□ We're Not Ready

Scoring Your Readiness

Score	Readiness Level	What It Means
17–20	**Security Ready**	You have a mature foundation and are well positioned for partner due

Score	Readiness Level	What It Means
Yes		diligence. Continue refining and improving your program.
13–16 Yes	**Developing**	Your program has solid fundamentals, but addressing key gaps will improve resilience and partner confidence.
8–12 Yes	**Needs Improvement**	Important controls may be missing or inconsistently applied. Prioritize foundational security practices before responding to major partner assessments.
0–7 Yes	**High Risk**	Significant work is needed to establish a security program capable of meeting today's expectations from partners and regulators.
