ISPM FIELD NOTES

for Credit Unions

Credit unions face unique cybersecurity challenges starting with safeguarding identity. Threat actors see credit unions as softer targets — with smaller security teams and budgets — than large commercial banks and financial institutions. Credit unions also must navigate complex webs of federal, industry, and state cybersecurity regulations like evolving mandates from the New York Department of Financial Services (NYDFS). Risk continues to grow as attackers exploit trust, gaps in observability, and exposure from third-party vendors and MSPs.

The net-net? Identity Security Posture Management (ISPM) is essential to protecting uptime, members' financial information, reputation, and compliance. Use this 12-point ISPM Field Notes Guide for Credit Unions to assess your company's identity security posture and make a plan to build defenses on a foundation of trust and strong identity management.

ISPM Field Notes for Credit Unions

Trust is a must . . .

The credit union culture revolves around trust — the very lever threat actors pull to launch phishing, social engineering, and supply chain attacks. According to the National Credit Union Administration Board (NCUA), credit institutions reported more than 1,000 cyber incidents from September 2023 through August 2024, with nearly 70% linked to third-party vendor vulnerabilities and digital exposure.

Other challenging trends include:

- **The rising costs of ransomware:** A single ransomware attack on Trellance disrupted some 60 credit unions in 2023[1]
- **Attacks growing in volume:** 33% of credit unions reported a 50–100% year-over-year increase in security incidents between 2022 and 2023[2]
- **Evolving compliance regulations:** New mandates from NYDFS and others go beyond requiring basic multi-factor authentication (MFA) to specify capabilities like phishing resistance (and passwordless?)

Secure access: The key to avoiding an identity crisis
Strengthening identity and access management (IAM) takes center stage for credit union IT teams as the human element — identity — remains security's weakest link.

24%
of breaches start with stolen credentials as the initial attack vector

$34M
Cost of a ransomware attack at the Patelco Credit Union which disrupted services for 700K members

The key word is "continuous"

Identity Security Posture Management (ISPM) takes a proactive approach to cybersecurity based on continuous monitoring and assessment to improve digital identity management. ISPM delivers a real-time, unified view of every identity, privilege, and risk across strategies cover every user, application, system, and supply chain connection.

An essential business enabler – versus another tool or upgrade — ISPM helps credit unions:

- Close identity gaps before attackers find and exploit them
- Streamline compliance reporting and audit readiness
- Capture and generate relible identity data
- Automate detection and drive proactive response

Unlike traditional IAM that revolves around authentication and permissions, ISPM takes the entire business into account. Use the questions that follow to assess gaps in your identity security posture — over-privileged accounts, orphaned users, vendor vulnerabilities, misconfigured access — and avoid attacks that exploit trust to attack your ecosystem.

1 https://www.cybersecuritydive.com/news/credit-unions-outages-ransomware/701442/?utm_source=chatgpt.com
2 https://www.pymnts.com/tracker_posts/scam-surge-how-credit-unions-are-tackling-rising-security-threats/?utm_source=chatgpt.com

12-Point ISPM Field Guide for Credit Unions

1. **Invest in ongoing awareness training**
   - Do you provide and require regular cybersecurity awareness training for employees?
   - Does your IT team test users' ability to recognize phishing exploits?
   - Are staff empowered to recognize and report suspicious activity or potential threats?

2. **Implement strong Identity & Access Management (IAM)**
   - Do you maintain a comprehensive inventory of all user, service, and privileged accounts—including those for staff, vendors, and third parties?
   - Are access rights reviewed regularly? Are permissions automatically updated as users' roles and employment status changes?
   - Is there a documented process for onboarding, offboarding, and role changes to minimize risk from human error?

3. **Implement strong MFA**
   - What percentage of users have enrolled in MFA?
   - Are identity verification requirements automatically stepped up for privileged and remote access?

4. **Aggregate and visualize identity data**
   - Can you see everything in one portal or dashboard?
   - Does your dashboard provide real-time visibility?
   - Does it automatically visualize relationships, permissions, and risk exposure?

5. **Monitor for threats 24/7**
   - Does your security stack or MSP continuously monitor for anomalies and suspicious activity like unusual access and privilege escalations?
   - Do you conduct regular audits of service and privileged accounts to remove unnecessary or orphaned access? Does this happen automatically?

IAM by the numbers
Assign a risk posture score to identity security to chart progress and demonstrate the value of strategic investments in IAM — multifactor authentication (MFA), single sign-on (SSO), and privilege access management (PAM).

6. **Strengthen supply chain and third-party identity controls**
   - Have you implemented 'just-in-time' access controls and automated offboarding for third-party users?
   - Do you maintain visibility into all supplier and partner identities accessing your systems?

7. **Implement Identity Threat Detection & Response (IDTR)**
   - Can you detect and respond to identity-based threats like including phishing and social engineering quickly? Automatically?
   - Do you routinely test and update your incident response and business continuity plans?
   - Are ITDR tools integrated seamlessly with existing IT workflows?

8. **Streamline audits and compliance reporting**
   - Are your identity security practices subject to and aligned with NCUA, Gramm-Leach-Bliley Act (GLBA), BSA (Bank Secrecy Act), FFEIC (Federal Financial Institutions Examination Council), GLBA, and CIP (Customer Identification Program) other relevant regulations?
   - Can you easily generate audit trails and compliance reports?
   - Are third-party vendor accesses inventoried and regularly reviewed for compliance?

9. **Manage trust programmatically**
   - Have you implemented a zero-trust framework?
   - Are you leveraging automation to streamline identity lifecycle management and reduce manual effort and human error?

10. **Implement identity security posture scoring**
    - Can you generate and regularly update a reliable identity security posture score?
    - Are you able to chart and document progress and demonstrate value to stakeholders?

11. **Build a resilient infrastructure**
    - Have you deployed modern firewalls and intrusion prevention systems (IPS)?
    - How often do you patch software and hardware?
    - Are networks segmented to restrict access to sensitive information?
    - Does data get encrypted in use and at rest?

12. **Integrate ISPM tools with IT workflows, ticketing and messaging platforms**
    - Are IT ticketing and messaging platforms integrated to streamline incident response and remediation workflows?
    - Do you have a process for escalating critical identity threats through your messaging workflows?
    - Can you ensure all relevant stakeholders stay informed about identity threats and risk resolution?

BONUS: Consider outsourcing the whole thing

Simeio | Get access right now™

info@simeio.com | www.simeio.com