ARANCIA

2026 CGI Credit Union Technology Forum

Using Cybersecurity Compliance to Combat **Fraud** and **Cyber Crime**

Breakout Session | 60 Minutes

Presenter: Farooq Wahab Naiyer

ARANCIA

Session Agenda

1. Opening Pulse Check
2. Threat Convergence: Fraud Meets Cyber Crime
3. Compliance Frameworks That Fight Fraud
   CIS · NIST · ISO 27001 · SOC 2 · FSRA
4. Mid-Session Scenario Poll
5. MITRE FiGHT Framework, IAM & Zero Trust
6. Case Studies & Maturity Model
7. Roadmap & Closing Assessment

ARANCIA

Speaker Introduction

Farooq Naiyer
Chief Strategy Officer
Arancia

- Cybersecurity leader with 20+ years of experience in security, privacy, compliance, and assurance
- Currently serving as Chief Strategy Officer at Arancia & CEO at The NKST.
- Former Global Lead, Technology & Cyber Assurance at Munich Re
- Former CISO at ORION (Canada’s largest research & education network) and virtual CISO for Ontario’s higher education sector
- Held C-suite roles in leading financial institutions across the Middle East and South Asia; experience with Big Four consulting firms
- Awarded CSO Compass Award (2010) for work at DIB Bank
- Recipient of EC-Council Presidential Award (2019) for advancing CISO standards in Canada
- Renowned speaker and educator in IT assurance, cybersecurity, and compliance
- Advisory roles with EC-Council (CTIA program), Durham College AI-Hub, and University of Guelph cybersecurity program
- Active contributor to ISACA and major cybersecurity conferences in North America
- Recognized thought leader driving innovation and advancement in cybersecurity

ARANCIA

THREAT LANDSCAPE

Where Fraud Meets Cyber Crime

25% Increase in cyber incidents at credit unions reported by NCUA in 2024

$4.88B Total losses from business email compromise (FBI IC3, 2023)

71% of financial institutions experienced account takeover attacks in 2024

3x Increase in AI-powered deepfake fraud attempts since 2023

Fraud and cyber crime are no longer separate threats — they are converging attack strategies.

ARANCIA

THREAT PROFILE

Why Credit Unions Are Prime Targets

Trust-Based Relationships

Members trust their CU implicitly — fraudsters exploit this trust through social engineering and impersonation

Constrained Security Budgets

Smaller IT teams and budgets compared to Big 5 banks, yet facing the same sophisticated threat actors

Rapid Digital Transformation

Mobile banking, open banking, and digital onboarding create new attack surfaces faster than controls can adapt

Shared Infrastructure & Third Parties

Centralized service providers and fintech partners create systemic concentration risk across the sector

Your strength — member trust and community — is exactly what attackers exploit.

ARANCIA

The Canadian Regulatory Landscape

1 **FSRA,** ONTARIO
IT Risk Management Guidance effective April 2024. Requires documented IT risk framework, incident response, third-party risk management, and board oversight.

2 **BCFSA,** BRITISH COLUMBIA
Technology risk management expectations aligned with OSFI B-13 guidelines.

3 **CUDGC,** ALBERTA / SASKATCHEWAN
Cybersecurity standards and deposit guarantee requirements.

4 **AMF,** QUEBEC
Technology risk and operational resilience guidelines for caisses populaires.

5 **OSFI,** FEDERAL | GOLD STANDARD
Guideline B-13 on Technology and Cyber Risk Management — the gold standard influencing all provincial regulators.

Compliance is not optional — it is the foundation of fraud prevention.

ARANCIA

Compliance Frameworks That Fight Fraud

Five complementary layers of defense for Canadian credit unions

FRAMEWORK	HOW IT FIGHTS FRAUD
CIS CONTROLS V8	**Prioritized security actions:** inventory, access control, audit logging, email/web defenses reduce the attack surface fraudsters exploit.
NIST CSF 2.0	**Risk-based approach:** Identify, Protect, Detect, Respond, Recover + new Govern function ensure fraud risks are managed enterprise-wide.
ISO 27001:2022	**Information security management system:** Annex A controls provide auditable controls over data integrity, access, and incident management.
SOC 2 TYPE II	**Trust Service Criteria:** independent assurance that security, availability, and confidentiality controls are operating effectively.
FSRA IT RISK MGMT	**Ontario-specific:** board accountability, IT risk framework, incident reporting, third-party oversight, and business continuity.

These are not competing frameworks — they are complementary layers of a mature defense strategy.

COMPLIANCE FRAMEWORKS

ARANCIA

CIS Controls v8 — The Practical Foundation

CIS 1 & 2: Asset Inventory

Know every device and software in your environment. You can't protect what you can't see.

CIS 3: Data Protection

Classify and protect member PII and financial data. Encryption at rest and in transit.

CIS 5: Account Management

Enforce least privilege. Disable dormant accounts. MFA for all privileged access.

CIS 13: Network Monitoring

Detect lateral movement and data exfiltration, the precursors to financial fraud.

CIS 8: Audit Log Management

Centralized logging with real-time alerting. Essential for fraud detection and forensics.

CIS 6: Access Control

Role-based access. Segregation of duties for wire transfers and high-risk transactions.

Key Insight: CIS Controls are prescriptive — they tell you exactly what to do, in priority order. Implement these six controls well to dramatically reduce your fraud risk surface.

NIST CSF 2.0 ISO 27001:2022

ARANCIA

NIST CSF 2.0 & ISO 27001 — Strategic Alignment

NIST CSF 2.0	ISO 27001 ANNEX A	FRAUD PREVENTION APPLICATION
GOVERN	A.5 Organizational Controls	Board-level accountability for cyber-fraud risk
IDENTIFY	A.8 Asset Management	Risk assessment covering fraud scenarios
PROTECT	A.9 Access Control	Identity verification, MFA, segregation of duties
DETECT	A.12 Operations Security	Transaction monitoring, anomaly detection
RESPOND	A.16 Incident Management	Fraud incident playbooks, regulatory notification
RECOVER	A.17 Business Continuity	Service restoration, member communication

Key Insight: NIST 2.0 added GOVERN as a top-level function — mapping directly to board accountability, which FSRA now requires. ISO 27001 alignment gets you 70% of the way to NIST CSF compliance.

ARANCIA

SOC 2 & FSRA — Assurance and Accountability

Two pillars of trust: independent validation meets regulatory obligation

SOC 2 Type II

1. Independent third-party audit of controls
2. Trust Service Criteria: Security, Availability, Confidentiality, Processing Integrity, Privacy
3. Demonstrates due diligence to members, partners, and regulators
4. Covers technology service providers and shared infrastructure
5. Annual assessment with ongoing monitoring

FSRA IT Risk Management

1. Board-approved IT risk management framework required
2. Documented incident response and notification procedures
3. Third-party/outsourcing risk management
4. Business continuity and disaster recovery planning
5. Regular testing and independent assessment

Together, SOC 2 + FSRA compliance creates a defensible position for your credit union, demonstrating both operational effectiveness and regulatory compliance.

ARANCIA

MITRE FRAMEWORK

MITRE Fight Fraud Framework

A behavior-based knowledge base of tactics and techniques used by financial fraud actors — extending ATT&CK into fraud prevention, detection, and response.

Threat-Informed Defense

Maps real-world adversary behaviors to your controls — moving beyond checkbox compliance to threat-based security.

Tactics & Techniques

Categorizes fraud attack patterns: account takeover, authorized push payment, synthetic identity, insider threats.

Control Mapping

Links each fraud technique to specific defensive controls from CIS, NIST, and ISO frameworks.

Maturity Benchmarking

Assess your detection and prevention capabilities against each technique — identify gaps before attackers do.

RECONNAISSANCE	DEFENSE EVASION	INITIAL ACCESS	MONETIZATION	EXECUTION	POSITIONING

F3 Fraud Lifecycle — 7 Tactics Mapping Adversary Behavior from Recon to Monetization

IDENTITY & ACCESS MANAGEMENT

ARANCIA

IAM — Your First Line of Defense

The critical control bridging cybersecurity and fraud prevention

Multi-Factor Authentication (MFA)

Mandatory for all staff, privileged accounts, and member-facing systems. Phishing-resistant MFA (FIDO2) for high-risk roles.

Privileged Access Management (PAM)

Just-in-time access for system administrators. Session recording for wire transfer authorizations. Eliminate standing privileges.

Identity Governance & Administration (IGA)

Automated joiner-mover-leaver processes. Quarterly access reviews. Segregation of duties enforcement for financial transactions.

Adaptive Authentication

Risk-based step-up authentication for unusual transactions. Device fingerprinting. Behavioral biometrics for member-facing digital channels.

Continuous Monitoring

Real-time alerting on privilege escalation, impossible travel, and concurrent sessions.

ARANCIA

Zero Trust Architecture for Credit Unions

Tying compliance frameworks to fraud prevention by design

1

Never Trust, Always Verify

Every access request is authenticated, authorized, and encrypted — regardless of network location. No implicit trust for internal users.

2

Least Privilege Access

Users get minimum permissions needed. Time-bound access for sensitive operations. Automatic de-provisioning.

3

Micro-Segmentation

Isolate core banking systems, payment processing, and member data. Contain breaches before they become fraud events.

4

Continuous Validation

Real-time risk scoring of every session. Behavioral analytics detect anomalous transactions. Automated response to suspicious activity.

5

Assume Breach

Design controls assuming attackers are already inside. Detective controls catch fraud in progress, not just after the fact.

Zero Trust + Compliance

Fraud prevention by design, not by reaction.

CIS Controls → Least Privilege

NIST CSF → Risk Approach

ISO 27001 → Management System

FSRA → Governance

CASE STUDY 1

ARANCIA

Business Email Compromise → Wire Fraud

DAY 1

Phishing email targets accounts payable staff. Credential harvested via convincing Microsoft 365 login page.

DAY 3

Attacker accesses email, creates inbox rules to hide replies. Monitors communication patterns & wire transfer procedures.

DAY 12

Spoofed email from CEO to CFO requests urgent $350K wire transfer to vendor with updated banking details.

DAY 12 — SAME DAY

Wire processed — dual authorization bypassed because one approver was on vacation and temporary exception was granted.

DAY 14 — DISCOVERY

Real vendor inquires about missing payment. **Fraud discovered. Funds unrecoverable.**

$350K TOTAL LOSS UNRECOVERABLE

CONTROLS THAT WOULD HAVE PREVENTED THIS

- Phishing-resistant MFA (CIS 6, NIST PR.AC)
- Email authentication DMARC/DKIM (CIS 9)
- Mandatory dual authorization — no exceptions ((SOC 2, FSRA)
- Out-of-band verification for wire changes (Zero Trust)
- Privileged access monitoring (CIS 8)

CASE STUDY 2

Synthetic Identity Fraud at Scale

ARANCIA

MONTH 1–3 · ACCOUNT CREATION

Fraudsters use AI to generate synthetic identities combining real SINs from data breaches with fabricated personal details. 47 accounts opened through digital onboarding.

MONTH 4–6 · TRUST BUILDING

Accounts build credit history with small deposits and on-time payments. Request credit increases and lines of credit.

MONTH 7 · BUST-OUT

$1.2M LOSS

MONTH 8 · DISCOVERY

Investigation reveals digital onboarding KYC relied solely on document verification — no behavioral analytics or device intelligence.

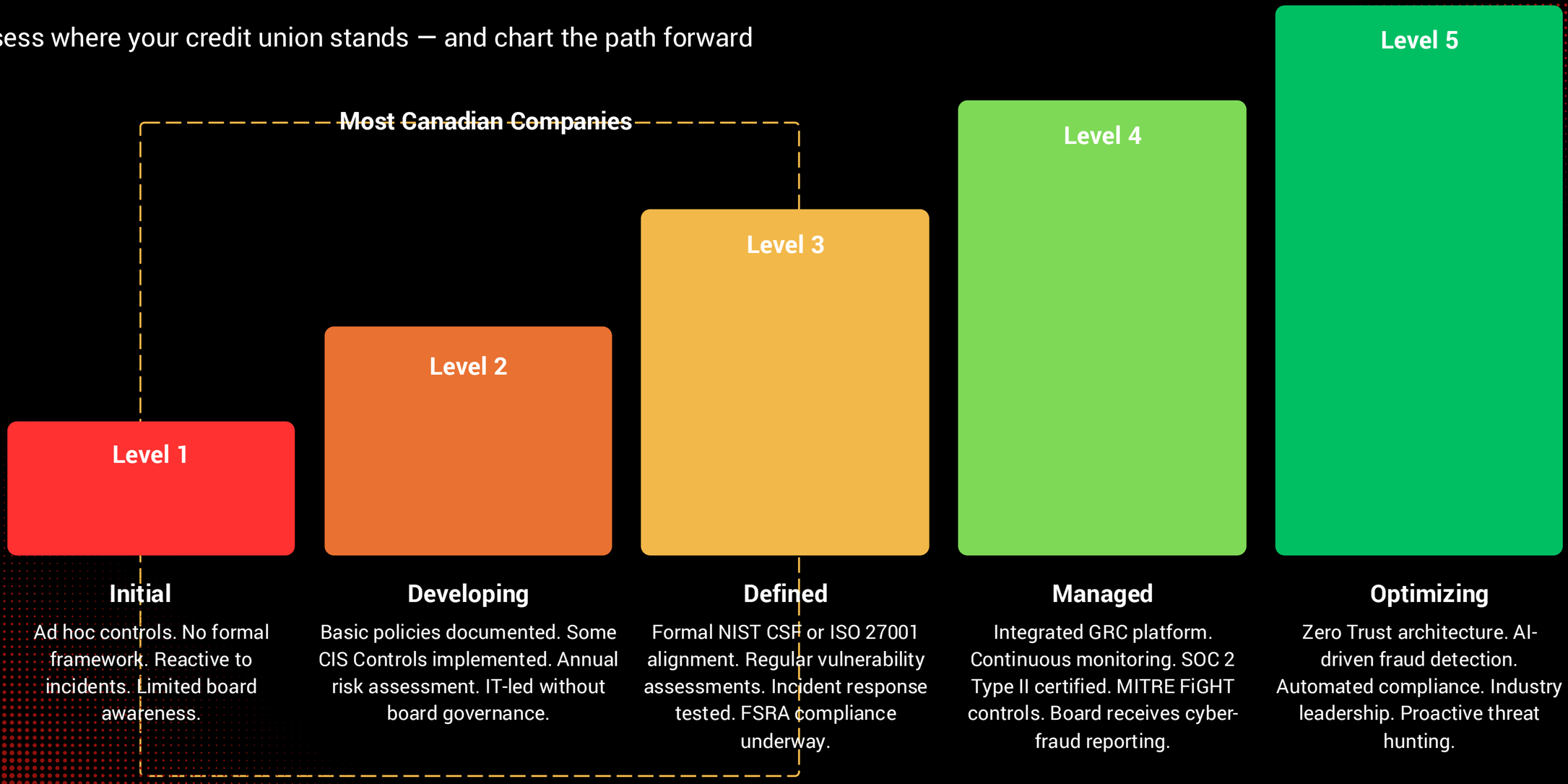
CONTROLS THAT WOULD HAVE PREVENTED THIS

- Device fingerprinting & behavioral biometrics (Zero Trust, IAM)
- AI-powered anomaly detection in onboarding ((NIST DE.CM)
- Cross-referencing SIN validation against known breach data
- Enhanced due diligence for correlated patterns (FSRA, CIS 16)
- Real-time fraud scoring integrated with account origination

Cybersecurity Compliance Maturity Model

ARANCIA

Assess where your credit union stands — and chart the path forward



Goal: Move from Level 2–3 to Level 4 (Managed) within 18–24 months with focused investment and framework alignment.

12-Month Implementation Roadmap

ARANCIA

Advancing cybersecurity compliance maturity & fraud prevention capabilities

PHASE 1

Foundation

Months 1–3

Complete gap assessment against CIS Controls & FSRA requirements

Establish board-level cyber risk governance

Deploy phishing-resistant MFA for all privileged accounts

Implement centralized log management

PHASE 2

Framework Alignment

Months 4-6

Map controls to NIST CSF 2.0

Begin ISO 27001 readiness assessment

Implement privileged access management (PAM)

Conduct tabletop exercise for BEC/wire fraud scenario

PHASE 3

Advanced Controls

Months 7-9

Deploy adaptive authentication for digital channels

Implement micro-segmentation for core banking

Begin SOC 2 Type II audit preparation

Integrate MITRE FiGHT into threat assessment process

PHASE 4

Assurance & Optimization

Months 10-12

Complete SOC 2 Type II audit

Achieve ISO 27001 certification readiness

Implement continuous compliance monitoring

Present board with maturity progression report

Key insight: Phase 1 is the critical foundation — get governance and MFA right in the first 90 days and everything else builds from there.

ACTIONABLE IN 30 DAYS

ARANCIA

Quick Wins — Start Monday Morning

Six high-impact actions your team can execute immediately with minimal budget.

1.

Enable Phishing-Resistant MFA

Deploy FIDO2/passkeys for all admin and privileged accounts. Reduce credential theft risk by 99%.

2.

Implement DMARC at Enforce

Prevent email spoofing of your credit union domain. Move from p=none to p=reject.

3.

Review Wire Transfer Procedures

Eliminate all temporary exceptions to dual authorization. Mandate out-of-band verification for banking detail changes.

4.

Conduct Access Reviews

Audit privileged access to core banking and payment systems. Remove unnecessary standing privileges immediately.

5.

Request SOC 2 Reports

Obtain and review SOC 2 Type II reports from all critical service providers. Document gaps.

6.

Brief Your Board

Present the maturity model and roadmap from today. Secure budget and mandate for cybersecurity compliance program.

Challenge: Which of these six can you complete before your next board meeting?

ARANCIA

Thank You

Let's build a more resilient credit union sector together.

Farooq Wahab Naiyer

Chief Strategy Officer, Arancia

Email

farooq@arancia.ca

LinkedIn

linkedin.com/in/farooqwahab

Website

www.arancia.ca