**CYBERPOOLS**  
  
Risk Assessment Evolution  
  
Executive Brief for CEO  
2026 Strategic Direction  
  
  
Prepared: October 30, 2025  
Target Launch: January 1, 2026  
  
  
  
*Framework-Aligned | Insurance-Validated | K-12 Specialized*

# Table of Contents

# CyberPools Risk Assessment Evolution

## Executive Brief for CEO - 2026 Strategic Direction

**Prepared:** October 30, 2025

**Target Launch:** January 1, 2026

**Purpose:** Strategic assessment alignment with insurance industry requirements and cybersecurity frameworks

---

## Executive Summary

CyberPools' current risk assessment model effectively serves members but does not align with the fundamental way cyber insurance underwriters evaluate risk in 2025-2026. This creates a **strategic misalignment** where organizations can score well on our assessment while facing insurance coverage denial or significant premium increases.

**Recommendation:** Evolve to a **dual-score assessment model** aligned with NIST CSF 2.0, CIS Controls v8, and insurance industry underwriting practices. Launch January 1, 2026.

**Business Impact:**

• Strengthens CyberPools' position as the K-12 cyber insurance assessment authority

• Aligns assessment methodology with how carriers make coverage decisions

• Provides members clearer prioritization for security investments

• Differentiates from new market entrants (CAI launched competing product July 2025)

---

## Current State Assessment

### What We Have Today

**CyberPools Risk Assessment (Production):**

• 51 questions across 9 security categories

• Single overall score (0-100%)

• Risk-based scoring: Control Rating × Impact Rating

• 12 questions designated as "Cyber Requirements" (from The Trust pool)

• Professional PDF reports with category breakdowns

**Framework Alignment:**

• ✅ Informed by NIST, CISA, and CIS standards

• ✅ Insurance pool partnership with The Trust (7 requirements)

• ✅ Proven delivery model with strong member relationships

### The Problem

**Insurance underwriting operates on a two-stage evaluation:**

1. **Foundation Controls** → Binary qualification decision (Approve/Decline coverage)

2. **Comprehensive Controls** → Premium tier decision (Preferred/Standard/Substandard rates)

**Our single-score model combines these distinct decisions into one number, creating critical gaps:**

#### Real-World Example: Santa Catalina School

• **CyberPools Score:** 80% (B grade) - appears acceptable

• **Missing Controls:** No EDR, no vulnerability scanning, annual (not bi-annual) backup testing

• **Insurance Reality:** Would face application denial or 30-50% premium increases

**The score suggests adequate risk, but insurance carriers would classify this as uninsurable.**

---

## Gap Analysis - Framework Perspective

### NIST Cybersecurity Framework 2.0 (February 2024)

**Six Core Functions:**

1. **Govern** - Cybersecurity governance and risk strategy

2. **Identify** - Asset and risk identification

3. **Protect** - Safeguards to ensure delivery

4. **Detect** - Identify cybersecurity events **(CRITICAL GAP)**

5. **Respond** - Incident response actions

6. **Recover** - Restoration of capabilities

**CyberPools Coverage Gap:**

• **DETECT Function: 0% coverage** - No questions on security monitoring, logging, or SIEM

• Insurance carriers now require detection capabilities (60-70% of carriers)

• NIST CSF 2.0 elevated "Detect" to equal status with "Protect"

**Impact:** Our assessment has zero visibility into whether members can detect breaches. Average dwell time without monitoring: 200+ days.

### CIS Controls v8 (Current Standard)

**CIS Critical Security Controls - 18 total controls**

**CyberPools Coverage:**

• ✅ 16 of 18 CIS Controls covered (89% after Security Monitoring addition)

• ⚠️ **CIS Control 8 (Audit Log Management)** - Not covered (CRITICAL GAP)

• ⚠️ **CIS Control 13 (Network Monitoring)** - Not covered (CRITICAL GAP)

**These are not "nice to have" - they are CIS CRITICAL controls.**

### Insurance Industry "Big Four" Requirements

**Universally mandatory controls (2025-2026):**

**The Gap:** We cover 4 of 5 mandatory controls well, but completely miss security monitoring - which is rapidly becoming table stakes.

---

## Insurance Market Context

### Market Shifts (2024-2025)

**From "Best Practices" to "Minimum Requirements":**

• 41% of insurance applications denied on first submission (Marsh McLennan 2024)

• 82% of denied claims involve organizations without MFA (Coalition 2024)

• EDR (not traditional antivirus) now universally required

• Vulnerability scanning moved from optional to required

**The Trust / Gallagher Relationship:**

Gallagher (Global insurance conglomerate)

↓

Risk Program Administrators (RPA)

↓

The Trust (Insurance pool)

↓

7 simplified requirements → 12 CyberPools questions

**Assessment:** The Trust's 7 requirements align with 2023-2024 standards. For 2026 relevance, expansion to 10-12 requirements recommended.

### Competitive Landscape

**CAI (Computer Aid Inc.) - July 2025 Launch:**

• $1B revenue, 8,700 employees, global presence

• Launched "Cyber Insurance Assessment" aligned with NIST CSF 2.0

• 15 categories, cloud dashboard, insurance-focused

• **Direct competitor** in insurance assessment space

**CyberPools Competitive Advantages:**

• K-12 specialization (FERPA, ed-tech, school-specific threats)

• Insurance pool relationships (The Trust)

• Assessment depth (51 questions vs. CAI's 15 categories)

• On-site consulting model vs. self-assessment

**Strategic Imperative:** Must differentiate on sophistication and specialization, not compete on brand size.

---

## Recommended Solution: Dual-Score Assessment Model

### The Framework-Aligned Approach

**Insurance underwriting + NIST CSF + CIS Controls all support a two-tier structure:**

1. **Foundation Controls** (Critical Safeguards)

- Core defensive capabilities

- Binary pass/fail for insurance qualification

- Maps to CIS Critical Controls and insurance mandatory requirements

2. **Comprehensive Maturity** (Defense in Depth)

- Full spectrum of security practices

- Demonstrates maturity and continuous improvement

- Maps to complete NIST CSF implementation

### How It Works

**Two separate scores reported:**

╔═══════════════════════════════════════════════════════════╗

║ FOUNDATION CONTROLS 75% C ║

║ Critical security safeguards required for insurance ║

║ (16-18 questions: MFA, EDR, backups, monitoring, IRP) ║

╠═══════════════════════════════════════════════════════════╣

║ COMPREHENSIVE MATURITY 80% B ║

║ Full cybersecurity program across all categories ║

║ (60+ questions: Complete NIST CSF & CIS Controls) ║

╚═══════════════════════════════════════════════════════════╝

INSURANCE READINESS: ⚠️ NOT READY

Foundation gaps must be addressed for optimal coverage

### Foundation Score Components (16-18 Questions)

**Based on CIS Critical Controls + Insurance Requirements:**

1. **Identity & Access Management**

- MFA (all systems, all users)

- Privileged access management

- Dormant account management

2. **Protective Technology**

- EDR deployment (not traditional antivirus)

- Endpoint encryption

- Patch management (7/30 day standard)

3. **Detection & Response**

- Security monitoring/logging **(NEW)**

- Log retention (90 days minimum) **(NEW)**

- Incident response plan with testing

4. **Resilience**

- Air-gapped backups

- Backup testing (bi-annual minimum)

5. **Vulnerability Management**

- External vulnerability scanning (quarterly)

- Network segmentation

**These 16-18 questions represent the "must-haves" that insurance carriers and security frameworks identify as critical.**

### Comprehensive Score Components (60+ Questions)

**Complete NIST CSF 2.0 and CIS Controls v8 coverage:**

Expands current 51 questions to 60+ by adding:

**Category 10: Security Monitoring & Detection (NEW)**

• 10.1: Centralized logging (SIEM)

• 10.2: Log retention and protection

• 10.3: Security event monitoring

• 10.4: Alerting and escalation procedures

**Expanded Data Protection Category**

• Data classification (FERPA alignment)

• Data retention and disposal

• Encryption in transit

• Least privilege data access

• Data loss prevention

**Enhanced Incident Response Category**

• IR team roles and responsibilities

• Annual tabletop exercise testing

• Insurance notification procedures

**Result:** Complete alignment with NIST CSF 2.0 (all 6 functions), CIS Controls v8 (18 controls), and insurance industry requirements.

---

## Business Outcomes

### For CyberPools

**Strategic Positioning:**

• ✅ Only K-12 assessment provider with insurance-aligned dual-score model

• ✅ Framework-validated methodology (NIST CSF 2.0, CIS Controls v8)

• ✅ Differentiated from CAI and other generic providers

• ✅ Strengthens The Trust partnership and opens doors to other insurance pools

**Competitive Advantages:**

• Sophisticated assessment model competitors don't have

• Framework alignment provides credibility and market validation

• Clear value proposition: "Insurance-ready assessment based on NIST & CIS standards"

### For Members (Schools)

**Clear Prioritization:**

• **Foundation Score** shows insurance qualification status

• **Comprehensive Score** shows overall security maturity

• Members know which gaps affect insurability vs. which improve maturity

**Better ROI on Security Spending:**

• Fix foundation gaps first → Achieve insurance qualification

• Improve comprehensive maturity → Reduce premium rates

• No more guessing about what matters most

**Transparency:**

• Understand exactly how close/far from insurance requirements

• See progress over time on both dimensions

• Clear roadmap for improvement

### For The Trust (Insurance Pool)

**Risk-Based Tiering:**

• Can segment members into risk tiers based on Foundation scores

• Foundation ≥90% = Preferred risk (standard rates)

• Foundation 75-89% = Acceptable risk (higher premiums)

• Foundation <75% = High risk (remediation required)

**Carrier Negotiations:**

• Demonstrate pool members meet minimum standards

• Show proactive risk management approach

• Foundation score data supports better rate negotiations

**Member Value:**

• Better assessment = better member guidance = lower loss ratios = sustainable premiums

---

## Framework Validation

### NIST Cybersecurity Framework 2.0

**Why NIST CSF 2.0:**

• 74% of organizations using security frameworks use NIST CSF (SANS 2023)

• Updated February 2024 with new "Govern" function

• Industry standard for cybersecurity program structure

• Insurance carriers recognize and respect NIST alignment

**CyberPools Dual-Score Alignment:**

• **Foundation Controls** → NIST "Protect" and "Detect" core functions

• **Comprehensive Maturity** → All 6 NIST functions (Govern, Identify, Protect, Detect, Respond, Recover)

**Validation:** Our dual-score model mirrors NIST's distinction between critical safeguards and comprehensive implementation.

### CIS Controls v8

**Why CIS Controls v8:**

• Community-driven, vendor-neutral

• Prioritized by implementation groups (IG1, IG2, IG3)

• Widely adopted in K-12 sector

• Clear, actionable controls

**CyberPools Alignment:**

• Current: 16 of 18 CIS Controls covered (89%)

• After Security Monitoring addition: 17 of 18 (94%)

• Foundation score emphasizes CIS Critical Controls

• Comprehensive score covers full CIS implementation

**Validation:** CIS Controls explicitly support tiered implementation (IG1/IG2/IG3), validating our dual-score approach.

### CISA Cybersecurity Performance Goals (CPGs)

**Why CISA CPGs:**

• Federal government guidance for critical infrastructure

• K-12 schools increasingly considered critical infrastructure

• Developed specifically for organizations with limited cybersecurity resources

• Focus on high-impact, low-cost practices

**CyberPools Foundation Score Alignment:**

All CISA Cross-Sector CPGs covered in Foundation score:

• ✅ Account security (MFA, credential management)

• ✅ Device security (EDR, encryption)

• ✅ Data security (backups, encryption)

• ✅ Vulnerability management (patching, scanning)

• ✅ Response planning (incident response)

• ✅ **Detection capabilities (security monitoring)** - after addition

**Validation:** CISA CPGs validate our selection of Foundation controls as the "minimum viable cybersecurity."

### Insurance Carrier Validation

**Coalition, Cowbell, Travelers, Chubb, AIG - Common Requirements:**

All major carriers require (2025-2026):

• MFA (universal)

• EDR (universal)

• Encrypted backups (universal)

• Bi-annual backup testing (80%+ of carriers)

• External vulnerability scanning (70%+ of carriers)

• Security monitoring/logging (60-70% of carriers)

• Incident response plan (universal for >$1M policies)

**CyberPools Foundation Score:** Directly addresses all seven universal requirements.

**Validation:** Insurance carriers' requirements align perfectly with our proposed Foundation controls.

---

## Recommended Approach

### Single-Phase Implementation - Launch January 1, 2026

**Timeline:**

**November 2025:**

• Finalize Foundation question set (16-18 questions)

• Add Security Monitoring category (4 questions)

• Expand Data Protection and Incident Response categories

• Design dual-score report template

• Complete NIST CSF 2.0 and CIS Controls v8 mapping documentation

**December 2025:**

• Update assessment database and scoring logic

• Implement dual-score report generation

• Train assessment team on new model

• Beta test with 3-5 member schools

• Prepare member communication materials

**January 1, 2026:**

• Launch dual-score model for all assessments

• Announce to The Trust and member schools

• Update marketing materials with framework alignments

• Begin outreach to insurance carriers for validation

### What Changes for Assessment Delivery

**Assessment Process:**

• Same on-site, consultative approach

• Same 51 base questions + ~9 new questions (total 60)

• Slightly longer assessment (30-45 minutes additional time)

• Enhanced report with two scores instead of one

**Report Format:**

• New executive summary page with dual scores

• Foundation controls section (16-18 questions highlighted)

• Comprehensive assessment section (all 60 questions)

• Insurance readiness indicator

• Framework alignment badges (NIST CSF 2.0, CIS Controls v8, CISA CPGs)

**Member Experience:**

• Clearer prioritization of remediation efforts

• Better understanding of insurance implications

• Framework-validated recommendations

### Communication Strategy

**To Members:**

"CyberPools is enhancing our risk assessment to align with the latest NIST CSF 2.0, CIS Controls v8, and cyber insurance industry standards. Your assessment will now provide two scores - Foundation (critical insurance controls) and Comprehensive (full security maturity) - giving you clearer guidance on prioritizing security investments."

**To The Trust:**

"The dual-score model strengthens our ability to demonstrate pool member risk profiles to carriers. Foundation scores provide clear qualification indicators, while comprehensive scores show ongoing maturity. This aligns with how carriers evaluate risk and supports better rate negotiations."

**To Insurance Carriers:**

"CyberPools K-12 risk assessment is now aligned with NIST CSF 2.0, CIS Controls v8, and insurance industry underwriting standards. Our dual-score model differentiates foundation controls (coverage qualification) from comprehensive maturity (premium rating), mirroring your underwriting process."

---

## Risk of Not Evolving

### Business Risks

**Loss of Market Relevance (High Probability, 12-18 months):**

• Insurance carriers increasingly require detection capabilities we don't assess

• Members face coverage gaps or premium increases despite good assessment scores

• The Trust may seek alternative assessment providers that align with carrier requirements

**Competitive Displacement (Moderate Probability, 12-24 months):**

• CAI and other providers marketing NIST CSF 2.0 alignment and insurance focus

• Larger competitors can outspend on marketing despite less specialized expertise

• Without differentiation, price becomes only competitive factor

**Member Dissatisfaction (Moderate Probability, 6-12 months):**

• Members discover assessment didn't identify insurance-critical gaps

• "Why didn't CyberPools tell us we needed security monitoring for insurance?"

• Erosion of trust in assessment value

### Technical Debt

**Framework Misalignment:**

• NIST CSF 2.0 released February 2024 - we're increasingly out of date

• CIS Controls v8 emphasizes detection and monitoring - we have zero coverage

• Every month without alignment widens the gap

**Single-Score Limitation:**

• Cannot accurately represent complex risk landscape

• Hides critical failures behind overall percentages

• Does not reflect how insurance industry evaluates risk

---

## Recommendation Summary

### Strategic Direction

**Evolve to dual-score assessment model aligned with NIST CSF 2.0, CIS Controls v8, CISA CPGs, and insurance industry underwriting practices.**

**Target Launch:** January 1, 2026

**Why Now:**

• Insurance market has fundamentally shifted to minimum requirements (2024-2025)

• CAI launched competing product (July 2025) - market validation and competitive pressure

• NIST CSF 2.0 and CIS Controls v8 provide framework validation for two-tier approach

• Q1 2026 aligns with insurance renewal season - maximum member value

**Why Dual-Score:**

• Mirrors insurance underwriting structure (qualification + premium rating)

• Validated by NIST, CIS, CISA framework structures

• Provides members clearer prioritization and ROI

• Competitive differentiation from generic providers

• Future-proof as requirements evolve

**Why Add Security Monitoring:**

• NIST CSF 2.0 "Detect" function - equal to "Protect"

• CIS Control 8 and 13 - CRITICAL controls

• 60-70% of insurance carriers require it

• Average breach dwell time: 200+ days without monitoring

• Zero current coverage is indefensible gap

### Success Metrics

**Q1 2026 (First 90 Days):**

• 100% of new assessments use dual-score model

• Member feedback: 90%+ understand dual-score purpose

• The Trust endorsement of dual-score approach

• Initial insurance carrier validation (2-3 carriers engaged)

**Q2-Q3 2026:**

• Framework mapping documentation complete (NIST, CIS, CISA)

• "NIST CSF 2.0 Aligned" and "CIS Controls v8 Validated" badges on reports

• Member case studies showing insurance outcomes improvement

• Partnership discussions with insurance carriers

**Q4 2026:**

• Market positioning as "The K-12 Insurance Assessment Authority"

• Thought leadership: Annual K-12 Cyber Insurance Report published

• Expansion beyond The Trust to other educational insurance pools

• Demonstrable competitive differentiation from CAI and others

---

## Conclusion

CyberPools has built a strong foundation with our current risk assessment. The opportunity is to **evolve from good to industry-leading** by aligning with how insurance underwriters actually evaluate risk and how cybersecurity frameworks structure comprehensive programs.

**The dual-score model is not just an enhancement - it's strategic alignment with:**

• ✅ How insurance carriers make coverage decisions

• ✅ How NIST CSF 2.0 structures cybersecurity programs

• ✅ How CIS Controls v8 prioritizes critical safeguards

• ✅ How CISA defines minimum viable cybersecurity

**This is the right technical approach validated by authoritative frameworks, and the right business strategy to maintain CyberPools' leadership in K-12 cyber risk assessment.**

**Recommendation: Approve dual-score model implementation with January 1, 2026 launch.**

---

## Appendix: Framework Alignment Matrix

**Validation:** Every major cybersecurity framework and the insurance industry supports a two-tier structure distinguishing critical safeguards from comprehensive maturity.

---

**Prepared for:** CyberPools CEO

**Next Step:** Leadership decision and approval for January 1, 2026 launch

**Questions:** Contact assessment team leadership

---

\*This document contains strategic planning and research. Filed in poc-research/docs/ per CyberPools production/POC separation policy.\*

# Appendix: Cybersecurity Frameworks

This appendix provides detailed information about the cybersecurity frameworks referenced in this brief. Understanding these frameworks is essential for staff to recognize how the dual-score assessment model aligns with industry standards and best practices.

## NIST Cybersecurity Framework 2.0

**Official Resource:** <https://www.nist.gov/cyberframework>

**Release Date:** February 2024

The NIST Cybersecurity Framework provides guidance for managing and reducing cybersecurity risk. Version 2.0 introduced a new "Govern" function and updated guidance across all six core functions.

### Core Functions:

**• Govern:** Cybersecurity governance, risk strategy, and accountability

**• Identify:** Asset identification and risk understanding

**• Protect:** Safeguards to ensure delivery of critical services

**• Detect:** Identify cybersecurity events and anomalies

**• Respond:** Incident response actions and procedures

**• Recover:** Restoration of capabilities after incidents

### Relevance to CyberPools:

*Industry standard recognized by insurance carriers and regulators. Version 2.0 release validates the framework remains current with evolving threats and best practices.*

## CIS Controls v8

**Official Resource:** <https://www.cisecurity.org/controls>

**Release Date:** May 2021 (Current)

The Center for Internet Security (CIS) Controls are a prioritized set of actions providing a foundation for effective cybersecurity. The 18 CIS Controls are organized into three Implementation Groups based on organizational resources and risk.

### Implementation Groups:

**• IG1:** Essential cyber hygiene for organizations with limited resources (6 controls)

**• IG2:** Enhanced security for organizations with moderate resources (16 controls)

**• IG3:** Advanced security for organizations with significant resources (18 controls)

### 18 CIS Controls:

• Control 1: Inventory and Control of Enterprise Assets

• Control 2: Inventory and Control of Software Assets

• Control 3: Data Protection

• Control 4: Secure Configuration

• Control 5: Account Management

• Control 6: Access Control Management

• Control 7: Continuous Vulnerability Management

• Control 8: Audit Log Management

• Control 9: Email and Web Browser Protections

• Control 10: Malware Defenses

• Control 11: Data Recovery

• Control 12: Network Infrastructure Management

• Control 13: Network Monitoring and Defense

• Control 14: Security Awareness and Training

• Control 15: Service Provider Management

• Control 16: Application Software Security

• Control 17: Incident Response Management

• Control 18: Penetration Testing

### Relevance to CyberPools:

*Vendor-neutral, community-driven controls widely adopted in K-12 education. Prioritization by Implementation Groups aligns with dual-score assessment model (IG1 = Foundation, IG2/IG3 = Comprehensive).*

## CISA Cybersecurity Performance Goals (CPGs)

**Official Resource:** <https://www.cisa.gov/cpg>

**Release Date:** March 2023

CISA Cybersecurity Performance Goals are a subset of IT and OT cybersecurity practices, selected through a risk-based approach, aimed at meaningfully reducing risks to critical infrastructure and the nation.

### Cross-Sector Cybersecurity Performance Goals:

• Account Security (MFA, strong passwords, phishing-resistant MFA)

• Device Security (automated patching, EDR, removal of unsupported/EOL software)

• Data Security (encryption at rest and in transit, secure backups)

• Vulnerability Management (asset inventory, patch management, scanning)

• Supply Chain Management (vendor security assessments)

• Response Planning (incident response plan, testing, coordination)

### Relevance to CyberPools:

*K-12 schools increasingly considered critical infrastructure. CPGs focus on high-impact, low-cost practices aligned with insurance minimum requirements.*

## FERPA - Family Educational Rights and Privacy Act

**Official Resource:** <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Federal law protecting the privacy of student education records. Schools must have written permission to release personally identifiable information, with certain exceptions.

### Key Security Requirements:

• Reasonable security measures to protect student records

• Vendor agreements requiring data protection (FERPA § 99.31)

• Data retention and disposal requirements

• Parent/student access rights to records

• Notification requirements for data breaches affecting student records

### Relevance to CyberPools:

*K-12 schools must align cybersecurity practices with FERPA requirements. Cyber insurance increasingly incorporates regulatory compliance into coverage decisions.*

# References & Citations

• **NIST Cybersecurity Framework 2.0:** <https://www.nist.gov/cyberframework>

• **CIS Controls v8:** <https://www.cisecurity.org/controls>

• **CISA Cybersecurity Performance Goals:** <https://www.cisa.gov/cpg>

• **FERPA Guidance - U.S. Department of Education:** <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

• **Marsh McLennan Cyber Risk Analytics (2024):** <https://www.marsh.com/us/insights/research-and-briefings/cyber-risk-analytics.html>

• **Coalition Cyber Threat Index (2024):** <https://www.coalitioninc.com/resources/cyber-threat-index>

• **SANS 2023 Security Framework Survey:** <https://www.sans.org/>

• **CAI Cyber Insurance Assessment:** <https://www.cai.io/services/cybersecurity/explore-a-cyber-insurance-assessment>

*Note: All external links and framework documents were accessed and verified as of October 2025. Framework documentation and standards are subject to periodic updates by their respective organizations.*