

Data Security and Compliance Risk: 2026 Forecast Report

Protecting the Most Vulnerable, With the Fewest Resources: Why Education’s AI Governance Gaps Create Unacceptable Risks for Students

Five Gap-Driven Predictions and Strategic Recommendations

Executive Summary

Education organizations enter 2026 facing a fundamental mismatch: The sector handles some of the most sensitive data imaginable—information about minors, learning disabilities, behavioral assessments, family circumstances—yet operates with governance capabilities that trail global benchmarks by double digits across critical controls. The resource constraints that define education create a governance gap with consequences that fall on society’s most vulnerable population.

The gap isn’t in awareness—it’s in capacity. Education shows strong board attention to overall cyber risk (65%, tied for highest globally) and elevated focus on data privacy (47%) and budget allocation (29%). Leaders understand the stakes. But operational capabilities tell a different story: privacy impact assessments at 6%, red-teaming at 6%, model explainability at 12%, and audit trails at 12%. The sector knows what it should do but lacks the resources to do it.

This sector analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with 17 respondents representing education organizations. The findings reveal a sector stretched thin—strong on intention, weak on implementation—deploying AI systems in contexts involving minors without the governance infrastructure other sectors apply to far less sensitive use cases. Five predictions emerge from these patterns, each representing risks that educational institutions must address despite resource constraints.

Five Predictions for Education in 2026

- 1 Privacy impact assessment gaps will create FERPA/COPPA exposure as AI adoption accelerates
- 2 Untested AI systems will produce harmful outcomes for students that red-teaming would have prevented
- 3 Weak transparency and explainability will erode parent and community trust in educational AI
- 4 Third-party EdTech AI will operate without adequate governance or oversight
- 5 Zero attention to emerging risks will leave education blindsided by evolving threats

Education vs. Global: Capability Profile

Where Education Leads or Matches

Capability	Global	Education	Advantage
Overall cyber risk posture (board)	54%	65%	+11 points (Tied Highest)
Budget allocation (board)	18%	29%	+11 points
Pre-training validation	22%	29%	+7 points
Bias/fairness audits	29%	35%	+6 points
Data breach response (board)	42%	47%	+5 points
Data privacy (board)	43%	47%	+4 points
Human oversight for high-stakes	46%	47%	+1 point

Where Education Trails (Critical Gaps)

Capability	Global	Education	Gap
PIAs/DPIAs	25%	6%	-19 points
AI red-teaming	24%	6%	-18 points
Transparency/disclosure	40%	24%	-16 points
Third-party AI policy & attestations	33%	18%	-15 points
Model explainability documentation	26%	12%	-14 points
Cyber insurance (board)	26%	12%	-14 points
Skills gap/workforce (board)	14%	0%	-14 points
Data sovereignty (board)	13%	0%	-13 points
Immutable audit trails	25%	12%	-13 points
Automatic revocation/DRM	25%	12%	-13 points
Red-teaming cadence	18%	6%	-12 points
Provenance & lineage	23%	12%	-11 points
AI governance (board)	46%	35%	-11 points
Regulatory compliance (board)	40%	29%	-11 points
Third-party/vendor risk (board)	35%	24%	-11 points

Five Gap-Driven Predictions for Education in 2026

Prediction #1: Privacy Impact Assessment Gaps Will Create FERPA/COPPA Exposure

By 2026, educational institutions will face regulatory enforcement and litigation arising from AI systems deployed without adequate privacy impact assessments—systems processing data about minors under FERPA and COPPA protections.

Privacy Assessment Capability	Global	Education	Gap
PIAs/DPIAs	25%	6%	-19 points
Compliance enforcement (training data)	34%	29%	-5 points
Data minimization & masking	41%	41%	0 points
Privacy-preserving techniques	33%	29%	-4 points

The privacy impact assessment gap is Education’s most alarming finding. At just 6%, the sector trails the global average by 19 points—the second-largest capability gap identified across all sectors and metrics. For institutions deploying AI systems that process student records, learning assessments, behavioral data, and family information, this represents fundamental non-compliance with privacy governance expectations.

FERPA requires educational institutions to protect student education records. COPPA imposes strict requirements for collecting data from children under 13. AI systems that analyze student performance, predict outcomes, or personalize learning interact directly with these protected categories. With only 6% conducting privacy impact assessments, 94% of educational institutions are deploying AI without systematic evaluation of privacy implications for the minors they serve.

Key Insight

Education handles data about children under some of the strictest privacy regulations—yet has the lowest privacy impact assessment rate of any sector measured. The 6% adoption rate represents a governance failure with direct implications for student privacy and institutional liability.

Opportunity

Implement mandatory privacy impact assessments for all AI systems processing student data. Leverage existing FERPA compliance frameworks as a foundation—extend them to address AI-specific privacy considerations. Prioritize PIAs for systems involving learning analytics, behavioral assessment, and student outcome prediction. Resource constraints are real, but privacy impact assessments for systems affecting minors cannot be optional.



Prediction #2: Untested AI Systems Will Produce Harmful Student Outcomes

By 2026, educational institutions will deploy AI systems that harm students—through biased recommendations, flawed assessments, or inappropriate interventions—because 94% never conducted adversarial testing to identify these failure modes.

Adversarial Testing Capability	Global	Education	Gap
AI red-teaming	24%	6%	-18 points
Red-teaming cadence	18%	6%	-12 points
Bias testing	26%	18%	-8 points
Bias/fairness audits	29%	35%	+6 points

Education shows a paradox: Bias/fairness audits at 35% exceed global averages (+6 pts), but red-teaming and active bias testing trail dramatically. This suggests institutions are documenting bias policies without testing whether AI systems actually produce biased outcomes. Audits review documentation; testing reveals real-world behavior.

Educational AI systems make consequential decisions: course recommendations that shape academic trajectories, early warning systems that trigger interventions, assessment tools that influence grades, and behavioral analysis that affects disciplinary outcomes. When these systems produce biased or harmful outputs, the consequences fall on students—often students from already disadvantaged backgrounds. With 94% of institutions never conducting red-team testing, these failure modes remain undiscovered until students experience harm.

The Gap

Education has policies for fairness (35% audit rate) but doesn't test whether AI systems actually behave fairly (6% testing rate). The gap between documentation and validation means institutions can't know whether their AI systems help or harm students.

Opportunity

Prioritize adversarial testing for AI systems with direct student impact. Test learning analytics for demographic bias. Evaluate early warning systems for false positive rates across student populations. Assess recommendation engines for equity of outcomes. Partner with education research institutions to develop testing protocols appropriate for educational AI contexts.

Prediction #3: Weak Transparency Will Erode Parent and Community Trust

By 2026, educational institutions will face parent backlash, community opposition, and public relations crises arising from AI systems deployed without adequate transparency—systems making decisions about children that families don’t understand.

Transparency Capability	Global	Education	Gap
Transparency/disclosure	40%	24%	-16 points
Model explainability documentation	26%	12%	-14 points
Content authenticity/disclosure	30%	29%	-1 point
Prompt/output logs	25%	24%	-1 point

Education trails on transparency by 16 points (24% vs. 40% global) and explainability by 14 points (12% vs. 26%). For a sector accountable to parents, school boards, and communities, this creates a trust vulnerability that technical security measures alone can’t address.

Parents increasingly expect to understand how technology affects their children’s education. When AI systems influence course placements, flag behavioral concerns, or personalize learning paths, families want to know how decisions are made. With only 24% of institutions implementing transparency practices and 12% maintaining explainability documentation, most educational AI operates as a black box—making consequential decisions about children that neither parents nor educators can explain.

Key Insight

Education is accountable to communities in ways commercial sectors aren’t. The 16-point transparency gap and 14-point explainability gap create trust vulnerabilities with parents, school boards, and the public that can quickly escalate into political opposition and reputational damage.

Opportunity

Develop parent-accessible explanations for educational AI systems. Document how AI influences student outcomes in terms families can understand. Create transparency reports for school boards that explain AI use cases, safeguards, and outcomes. Treat transparency as a community relations imperative, not just a compliance exercise.

Prediction #4: Third-Party EdTech AI Will Operate Without Adequate Governance

By 2026, educational institutions will discover that EdTech vendors have deployed AI systems processing student data without the governance controls, attestations, or oversight that institutions assumed were in place.

Third-Party Governance	Global	Education	Gap
Third-party AI policy & attestations	33%	18%	-15 points
Third-party/vendor risk (board)	35%	24%	-11 points
AI data gateway	35%	29%	-6 points
AI data gateway monitoring	37%	29%	-8 points

Education’s reliance on EdTech vendors creates significant third-party AI exposure—yet governance trails by 15 points (18% vs. 33% global). Only 18% of educational institutions have established AI-specific policies and attestation requirements for vendors processing student data.

The EdTech market has exploded with AI-enabled products: adaptive learning platforms, automated essay scoring, proctoring systems, student engagement monitors, and early-warning tools. Many educational institutions lack the technical expertise to evaluate these systems’ AI governance practices. Without vendor attestation requirements, institutions accept vendor assurances without verification—leaving student data protection to EdTech companies’ discretion.

The Gap

Education depends heavily on third-party EdTech AI but lacks vendor governance frameworks. The 15-point gap on third-party AI policies means student data flows through vendor AI systems without adequate oversight, attestations, or accountability mechanisms.

Opportunity

Develop EdTech AI procurement requirements that address training data practices, bias testing results, privacy protections, and transparency commitments. Join consortium purchasing programs that establish shared vendor governance standards. Require AI-specific attestations before deploying EdTech products that process student data. Leverage collective purchasing power to raise vendor accountability.



Prediction #5: Zero Attention to Emerging Risks Will Leave Education Blindsided

By 2026, educational institutions will be caught unprepared by AI risks that other sectors saw coming—skills gaps, data sovereignty challenges, and supply chain vulnerabilities—because board attention to these emerging areas registered at zero.

Emerging Risk Area	Global	Education	Gap
Skills gap/workforce	14%	0%	-14 points
Data sovereignty & cross-border	13%	0%	-13 points
Software supply chain security	8%	0%	-8 points
PQC readiness	9%	0%	-9 points
Cyber insurance & financial impact	26%	12%	-14 points

The zero-percent findings are stark. No education respondents reported board attention to skills gap/workforce issues, data sovereignty, software supply chain security, or post-quantum cryptography readiness. These aren't peripheral concerns—they're risks that other sectors are actively monitoring and addressing.

The skills gap is particularly concerning. Educational institutions face the same AI governance challenges as other sectors but with significantly fewer specialized staff. With 0% board attention to workforce issues, institutions aren't positioning to recruit, develop, or retain the expertise needed to implement the governance measures this analysis identifies as urgent priorities.

Key Insight

Education shows zero board attention to emerging risk categories that other sectors actively monitor. These blind spots—particularly skills gap and data sovereignty—will compound existing governance challenges as the AI landscape evolves.

Opportunity

Elevate emerging AI risks to board visibility before they become crises. Address the skills gap through partnerships with higher education institutions, shared services arrangements with peer institutions, or consortium approaches to AI governance expertise. Engage with data sovereignty considerations as EdTech vendors increasingly operate across borders.

Strategic Recommendations for Education Organizations

The data points to five priority investments for education organizations preparing for 2026. These recommendations recognize resource constraints while identifying actions essential for protecting students and maintaining community trust.

1. Implement Privacy Impact Assessments for All Student-Facing AI

Close the 19-point PIA gap by requiring privacy impact assessments for every AI system processing student data. Build assessment templates specific to educational contexts and FERPA/COPPA requirements. Prioritize assessments for learning analytics, behavioral monitoring, and outcome prediction systems. PIAs for systems affecting minors are non-negotiable regardless of resource constraints.

2. Establish Bias Testing Protocols for Educational AI

Bridge the gap between fairness audits (35%) and actual testing (6%) by implementing validation protocols for AI systems with direct student impact. Test learning analytics and recommendation engines for demographic bias. Evaluate early warning systems for equity of outcomes across student populations. Partner with education researchers to develop appropriate testing methodologies.

3. Build Parent-Accessible Transparency Frameworks

Address the 16-point transparency gap by creating explanations families can understand. Document how AI systems influence student outcomes. Develop transparency reports for school boards. Treat transparency as a community trust imperative—parents will accept educational AI they understand and reject AI that operates as a black box affecting their children.

4. Develop EdTech Vendor AI Governance Requirements

Close the 15-point third-party policy gap by establishing AI-specific procurement standards. Require vendor attestations covering training data practices, bias testing, privacy protections, and incident notification. Join consortium approaches that create shared vendor accountability standards. Educational institutions have collective purchasing power—use it to raise EdTech AI governance.

5. Address Emerging Risks Before They Become Crises

Elevate skills gap, data sovereignty, and supply chain risks to board visibility. Address workforce challenges through partnerships, shared services, or consortium arrangements. Engage with data sovereignty implications of EdTech vendors operating across jurisdictions. Zero attention to emerging risks guarantees future surprises—build awareness now.

From Policy to Practice

Education enters 2026 stretched between competing realities: stewardship of the most sensitive data about society’s most vulnerable population, deployed with governance capabilities that would be unacceptable in sectors handling far less consequential information. The resource constraints are real. The gaps are documented. The consequences fall on students.

The sector shows genuine strengths. Board attention to cyber risk leads all industries (65%). Budget allocation focus exceeds global averages (29%). Human oversight and bias audits show appropriate concern for student welfare. Educational leaders understand the stakes—the gap isn’t awareness; it’s implementation capacity.

But implementation gaps in Education have unique consequences. Privacy impact assessments at 6% mean AI systems process children’s data without systematic privacy evaluation. Red-teaming at 6% means systems affecting student outcomes go untested for failure modes. Transparency at 24% means families can’t understand how AI influences their children’s education. Third-party governance at 18% means EdTech vendors operate with minimal oversight.

Resource constraints explain these gaps but don’t excuse them. Students deserve protection regardless of institutional budgets. The recommendations in this analysis prioritize actions achievable within resource limitations while identifying the gaps most critical to address: privacy impact assessments for systems affecting minors, bias testing for systems influencing outcomes, transparency for maintaining community trust, and vendor governance for the EdTech systems education increasingly depends upon.

Education built its mission around student welfare. Extending that mission to AI governance isn’t optional—it’s the same commitment applied to new technology. The sector that educates the next generation must also protect them from AI systems deployed without adequate safeguards. 2026 will determine whether Education meets that obligation or becomes the cautionary example of what happens when the most vulnerable population meets the weakest governance.

Research based on survey of 225 security, IT, and risk leaders across 10 industries and 8 regions. 17 respondents represent education organizations. 97% represent organizations with 1,000+ employees. Survey fielded Q4 2025.



For the complete report with detailed methodology, industry breakdowns, and regional analysis, **download it now.**

Download the Report