

Fraud and Security Risk in Schools



**Findings from Alii's 553-Leader
International Survey (AU, NZ, US, UK)**



01	Executive Summary
02	Headline Findings
07	Why Fraud and Security Risk Looks Different in Schools
08	Survey Findings (Expanded)
18	Cross-Analysis Observations
19	Governance and Strategic Implications
21	Practical Guidance: What “Operational Consistency” Looks Like in a School
23	A Risk-Focused View of “Where Fraud Lands” in Schools
24	Implementation Roadmap
29	Conclusion
30	How Alii Helps
31	Next Steps

Table of Contents

Executive Summary



Schools run on trust. Trust between staff and leadership. Trust between schools and families. Trust between finance teams and vendors. And increasingly, trust between schools and the digital systems that support learning, operations, payroll, procurement, and student administration.

This white paper shares findings from a survey of 553 school leaders across Australia, New Zealand, the United States, and the United Kingdom. Respondents included Finance leaders, Business Managers, IT leaders, and senior executives working in primary and secondary education.

Many of these respondents sit close to the workflows most frequently targeted by fraud: invoices, supplier changes, payroll, and identity-driven access to systems.

The data shows that fraud and security risk in education is not a rare event reserved for “unlucky” organisations. It is a regular operational reality.

Survey Partners



Headline Findings



02



75.4%

of schools report confirmed or suspected fraud attempts

43.8%

detected and stopped fraud activity

9.0%

experienced financial or data loss

11.4%

report paying a fraudulent invoice

37.4%

do not know when their last security audit occurred

34.2%

are unsure whether a designated fraud/data protection officer exists

Only 15%

regularly test recovery plans



Taken together, the message is consistent:

1. Threat exposure is widespread.
2. Detection is happening, but loss still occurs.
3. Governance visibility is uneven, even when controls may exist.
4. Manual processes remain common, especially in finance workflows.
5. Recovery confidence often outpaces recovery validation, because testing is limited.



There is also near-universal awareness of where risk is heading. Respondents identified the most pressing risks heading into 2026 as:

97.5%

Phishing and impersonation scams

96.2%

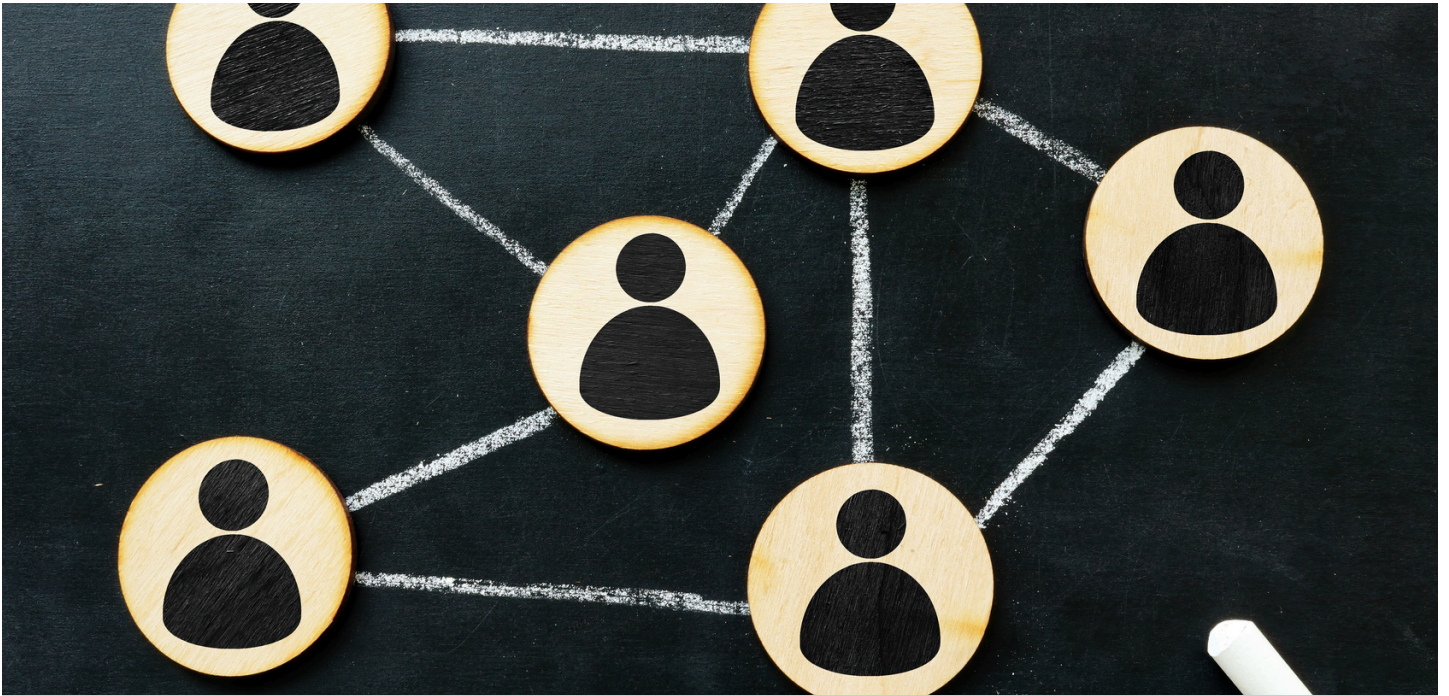
Invoice or supplier fraud

95.3%

AI-generated impersonation attempts

93%

Ransomware and extortion attacks



This is not simply an IT story. It is a governance story and an operational consistency story. In many schools, fraud and security prevention depends on a small number of people who “know what to look for,” while the organisation grows more complex: more suppliers, more systems, more devices, more credentials, more invoices, more payment approvals, and more time pressure.

The strongest theme emerging from the dataset is that fraud risk in education is not episodic—it is structural. That does not mean it is unsolvable. It means schools need controls and habits that hold up under everyday conditions: busy periods, staff changes, competing priorities, and constant interruption.

For Boards and executive teams, the priority is often not “more awareness.” Awareness is already high. The priority is:

- operational consistency (controls that happen every time),
- accountability clarity (who owns which risks),
- scalability (processes that work as the school grows), and
- validation (testing, auditing, and monitoring that proves readiness rather than assuming it).



How to Read This Paper

This report is written for school leaders who need a practical, plain-language view of fraud and cyber risk, especially those responsible for governance, finance, operations, and IT. It is not meant to alarm. It is meant to clarify what the sector is experiencing and where to focus effort.

The survey captures leaders' perspectives, incident experience, and visibility into controls. Like any survey, it reflects self-reported data. That matters because self-reported "unsure" responses are not trivial, they often signal a gap in reporting and governance clarity, even when controls exist at a technical level.

Methodology

The survey collected responses from 553 school leaders across Australia, New Zealand, the United States and the United Kingdom. Respondents were drawn from a mix of independent, Catholic/religious, and government/public schools.

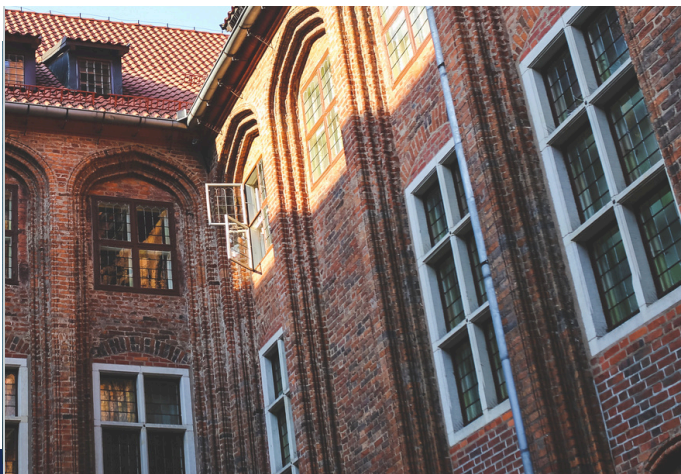
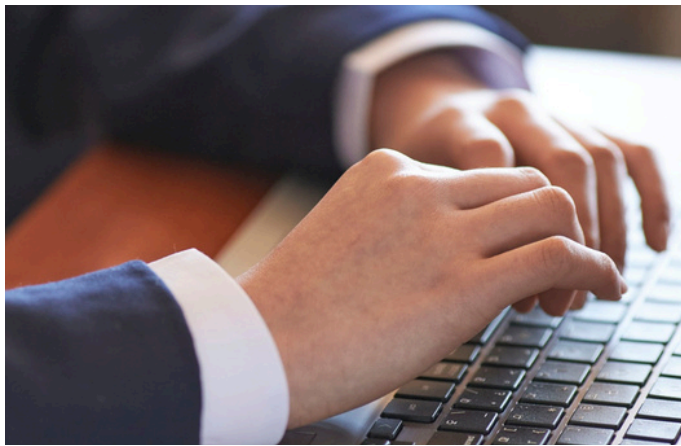
The survey focused on:

- Fraud exposure and incident history
- Perceived risk trends heading into 2026
- Root causes of security incidents
- Training frequency and effectiveness
- Monitoring and audit practices
- Fraud ownership clarity
- Recovery confidence and testing
- Financial controls and supplier verification
- AI adoption in fraud detection
- Structural barriers to improvement

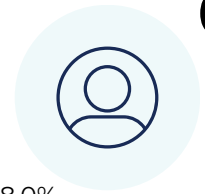
The dataset is leadership-weighted, with most responses coming from individuals responsible for financial management, operational governance, or IT oversight, roles that sit close to both operational decision-making and risk management.

Respondent Profile

06



Role Distribution



- Finance roles: 34.4%
- Business Manager / Officer: 28.0%
- IT roles: 17.3%
- Senior Operations / Executive leadership: 11.6%
- Other roles: remainder

More than 62% of respondents hold financial accountability roles. This matters because vendor payments and supplier onboarding are prime targets for modern fraud, particularly invoice fraud and impersonation attacks aimed at changing bank account details.

School Type

- Independent schools: 64.2%
- Catholic / Religious affiliation: 27.1%
- Government / Public: 7.1%

The dataset is weighted toward independent institutions. In practice, that often means internal governance and procurement frameworks are managed locally rather than through centralised system controls. That autonomy can be a strength (fast decisions, tailored process) but can also create unevenness in controls, reporting, and resourcing.

School Size

- 48.5% employ 100–200 staff
- 40.5% employ 200+ staff
- 89% employ more than 100 staff

Larger institutions carry increased operational complexity: more vendors, more devices, more credentials, higher invoice volume, and more handoffs between teams. That complexity creates more opportunity for mistakes—and more opportunity for criminals to find weak points.

Institutional Longevity

- 35.3% operating 25–50 years
- 22.6% operating 100–150 years
- 12.8% operating 75–100 years

The majority of participating institutions are mature and well established. That suggests exposure patterns reflect the evolution of fraud tactics and digital dependency—not organisational immaturity.

Why Fraud and Security Risk Looks Different in Schools



Before diving into the findings, it's worth naming a reality that many school leaders recognise intuitively: schools are not shaped like corporations. They are shaped like communities. They are open by design.

They have many stakeholders. They operate on tight cycles and tight timelines. Several conditions make schools particularly attractive targets:



1/ High trust culture.

Staff are used to helping quickly, responding to urgent requests, and assuming good intent.

2/Busy, interruption-heavy work.

Finance offices and front offices are interrupted constantly. Attackers exploit distraction.

3/Large and diverse user base.

Staff, students, contractors, casual staff, volunteers, alumni, parents, and vendors can all interact with systems.

4/Decentralised purchasing and approvals.

Many schools have departments or campuses ordering independently, creating inconsistent vendor workflows.

5/Legacy systems and competing priorities.

Schools may run a mix of modern cloud tools and older systems. Security improvement competes with educational priorities, staffing, and budget constraints. Fraud in this context is rarely a “single weakness.” It’s often a chain: an email compromise, a rushed approval, an unclear policy, a missing callback procedure, a password reused, an audit not recently reviewed, or a recovery plan that exists but hasn’t been exercised.

Survey Findings (Expanded)

08



1) Fraud Exposure Is Widespread —and Not Theoretical

Fraud attempts are common across the sector:

75.4% report confirmed or suspected fraud

43.8% detected and stopped fraud

9.0% experienced financial or data loss

14.1% report suspicious but unconfirmed activity

22.2% report no known exposure

It's also notable that **43.8%** detected and stopped fraud activity. That indicates many schools have staff who recognise red flags, controls that can prevent payment, and/or systems that help catch suspicious activity. That is good news—prevention is happening.

However, **9.0%** experienced financial or data loss. In plain terms: about one in ten schools saw the risk translate into real harm. That harm could be direct financial loss, exposure of sensitive information, disruption, or reputational damage.

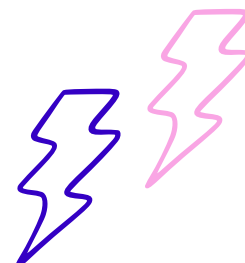
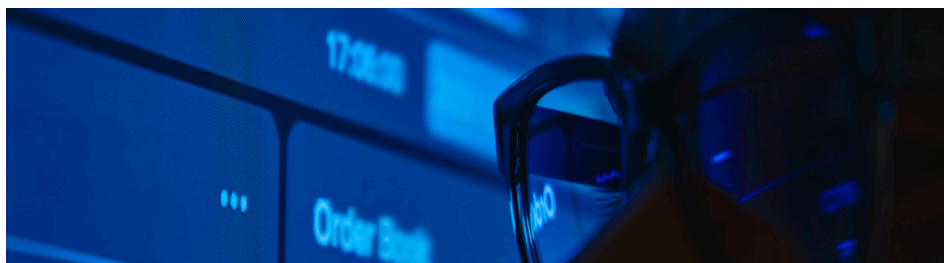
A useful way to interpret this is: detection is meaningful, but it is not sufficient on its own. Schools need prevention controls that do not rely solely on individual vigilance. Vigilance matters, but it is not scalable.

What this suggests operationally:

Fraud activity appears to be ongoing rather than isolated. Even if a school has not suffered loss, the probability of being targeted is high, and the cost of “assuming it won’t happen” is rising.

The fact that **three in four** schools have seen confirmed or suspected fraud attempts should shift how leaders frame the issue. Fraud is not a remote possibility. It is part of the operating environment.

2) Finance Teams Report Higher Exposure —Because That’s Where Attackers Focus



Among Finance respondents:



This concentration is unsurprising. Modern school fraud typically aims at money movement or credential access that enables money movement.

Common patterns in education environments include:

- **Invoice fraud:** a fake invoice is sent to accounts payable, sometimes disguised as a legitimate vendor or a “new bank details” update.
- **Supplier impersonation:** a vendor email is spoofed or compromised to request bank account changes.

- **Executive impersonation:** an attacker imitates a Principal, CFO, Business Manager, or Director to push for urgent payment.
- **Credential phishing:** staff are tricked into entering login details, giving attackers email access and the ability to monitor invoice conversations.

Finance teams face competing demands that heighten risk exposure:

- paying suppliers on time
- responding quickly to operational requests
- meeting compliance requirements
- handling peaks in invoice volume
- verifying supplier legitimacy under pressure

Attackers understand urgency. Many fraud attempts are designed to create a narrow window (“pay today,” “we changed bank accounts,” “this is time sensitive,” “please keep this confidential”). A strong process has to hold up in that moment.

What this suggests operationally:

If fraud prevention depends on one experienced staff member noticing a detail, the control is fragile. Sustainable prevention usually requires built-in steps: supplier verification, callback procedures, multi-person approvals, and system-enforced rules.

3) 2026 Outlook: Leaders Expect Impersonation to Get Smarter—Especially With AI



Respondents identified the following as major fraud risks for 2026:

97.5%	Phishing and impersonation scams
96.2%	Invoice or supplier fraud
95.3%	AI-generated impersonation attempts
93%	Ransomware and extortion attacks

The near-universal awareness of impersonation-based threats is striking. Leaders are not dismissing this as hype. They expect attacks to become more believable and more frequent.

AI changes the playing field in two practical ways:

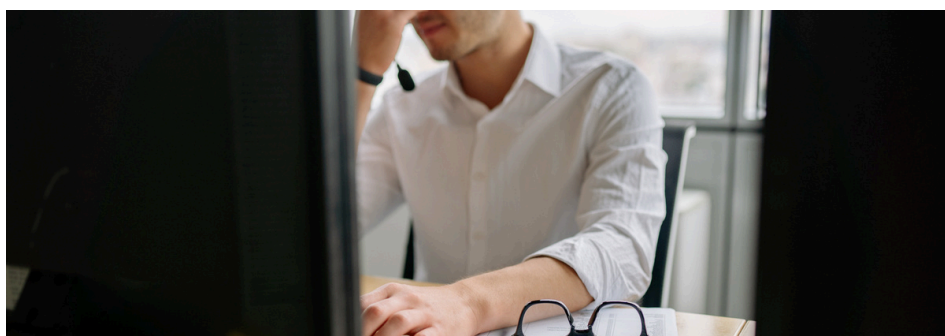
1. **Speed and scale:** attackers can generate high-quality messages quickly, tailored to a school's context, calendar, and tone.
2. **Believability:** messages can include the language patterns of leaders, accurate formatting, and plausible context.

Importantly, AI-driven fraud does not always require “deepfakes.” Even simple improvements in grammar, formatting, and plausibility can defeat the “this email looks weird” filter that staff may rely on.

What this suggests operationally:

When leaders expect risk to increase, that expectation should translate into changes in process design—particularly around payment approvals, bank detail changes, and credential security. Awareness without adaptation leaves the organisation exposed.

4) Human Error Is Seen as the Primary Root Cause—So Controls Must Account for Humans



Respondents overwhelmingly attribute incidents to human factors:



These numbers paint a consistent picture: many leaders believe the main vulnerabilities are behavioural and procedural, not purely technical. This is a critical insight because it shapes what “good security” looks like in a school.

If human error is the primary driver, then it is not enough to deploy tools and hope people behave perfectly. Schools need:

- simple, repeatable workflows
- minimum-viable friction (just enough steps to prevent mistakes)
- system guardrails that reduce the chance of a single click leading to a major incident
- training that is practical, regular, and role-specific
- accountability that is clear and visible

A helpful framing is: **people are not the problem; systems that rely on perfect people are the problem.** In a busy environment, it is unrealistic to expect constant vigilance without providing practical supports.

What this suggests operationally:

Sustainable risk reduction happens when training, process design, and system controls work together—so that a single mistake does not become a full incident.

5) Training Practices Vary Widely—and Gaps Are Material



Training frequency:

Every term:	28.4%
Twice per year:	16.1%
Once per year:	17.2%
Rarely or never:	9.0%

Effectiveness ratings:

Very effective:	32.9%
Effective but could improve:	31.5%
Somewhat effective:	20.4%
Ineffective:	8.0%
No training:	6.9%

These findings matter because the same dataset identifies human error as the most common root cause. If human factors drive exposure, then training is not optional—it is one of the core control mechanisms.

Yet nearly 15% of schools report training that is ineffective or absent. Even among schools that provide training, effectiveness is mixed.

In practice, training tends to fail when it is:

- too infrequent (once a year is easy to forget)
- too generic (“cyber safety” without real school examples)
- disconnected from workflows (finance teams need finance-specific scenarios)
- punitive in tone (people disengage when they feel blamed)
- not reinforced through simulation or follow-up

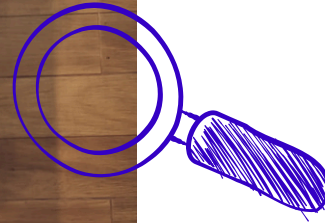
Training tends to work when it is:

- short and frequent (micro-learning)
- scenario-driven (“here is a fake bank detail change email—spot the flags”)
- role-based (finance workflows, HR workflows, IT workflows, general staff)
- supported by leadership (“we slow down payments when something feels off”)
- backed by a safe reporting culture (“reporting a mistake early is valued”)

What this suggests operationally:

Training needs to be treated like any other operational discipline—planned, scheduled, measured, improved—not as a one-time compliance activity.

6) Monitoring and Audit Visibility: Controls May Exist, But Leaders Often Can't See Them



Monitoring systems:

Dedicated monitoring:	55.3%
Manual log checks	15.9%
Outsourced monitoring:	4.7%
Unsure:	23.7%

Two “unsure” figures stand out: nearly one in four unsure about monitoring, and more than one in three unsure about audit recency.

This does not necessarily mean schools have no monitoring or no audits. In many cases, monitoring may be happening inside IT operations, through a managed service provider, or via built-in cloud platform security tools. Audits may occur as part of broader financial or compliance cycles.

However, from a governance standpoint, “unsure” is itself a risk. If leadership teams and Boards can’t confidently answer when the last security audit occurred, it becomes harder to:

- track improvement over time
- justify investment decisions
- ensure follow-through on recommendations
- demonstrate due diligence to regulators, insurers, and stakeholders
- coordinate response readiness across teams

What this suggests operationally:

Risk management depends on visibility. If visibility is weak, the organisation can’t reliably improve—even when individual controls exist.

Audit recency:

Within 6 months:	24.4%
Within 12 months:	26.4%
Over 1 year ago:	10.3%
Never:	1.1%
Unsure:	37.4%

7) Ownership Clarity Is Uneven—And That Creates Accountability Gaps



Fraud or data protection officer status:

Full-time:	27.3%
Part-time:	8.3%
Outsourced:	7.6%
None:	22.2%
Unsure:	34.2%

A third of respondents cannot identify clear ownership of fraud prevention responsibilities. That is not a minor administrative issue. Clear ownership is foundational: without it, problems are addressed inconsistently, tasks fall between teams, and improvement depends on individual initiative rather than organisational commitment.

In a school context, ownership typically spans multiple domains:

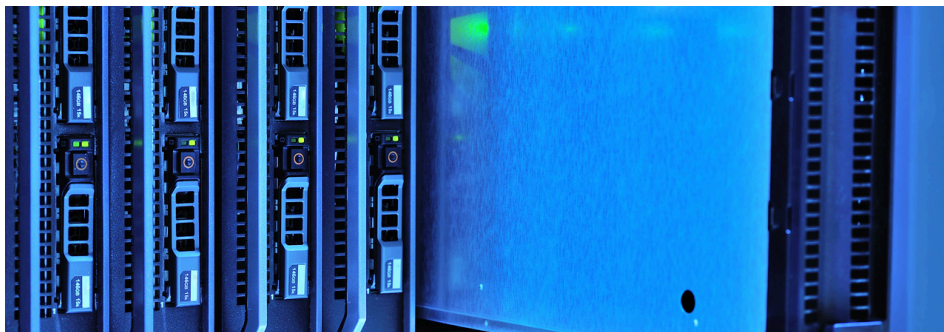
- Finance may own payment controls, supplier onboarding, and invoice verification.
- IT may own identity security, monitoring, access controls, and endpoint protections.
- Operations / leadership may own policy enforcement, training expectations, and escalation pathways.
- Governance (Board / executive) should own oversight, risk appetite, resourcing decisions, and accountability.

The key is not whether the owner is full-time or part-time. The key is whether the owner is clearly defined, empowered, and connected to leadership.

What this suggests operationally:

If the school can't name who owns fraud and data protection risk, it's difficult to build consistent practices—and difficult to respond quickly when something goes wrong.

8) Recovery Confidence Is Common—But Testing Is Rare



Recovery posture:

Very confident with regular testing:	15.0%
Confident with verified backups:	33.3%
Somewhat confident (untested):	30.0%
Unsure:	12.8%
Outdated plans:	7.6%
No plan:	0.9%

It's positive that only a small portion report having no plan at all. But the deeper story is the gap between confidence and validation:

- Most schools express confidence at some level.
- Only **15%** regularly test recovery plans.

Testing is what turns a recovery plan from a document into a capability. In real incidents, recovery often fails due to practical issues: missing credentials, untested backups, misunderstood dependencies, unclear decision rights, or underestimated recovery time.

Recovery testing does not have to be complex. It can include:

- tabletop exercises (walk through a ransomware scenario)
- restoring a small subset of systems from backup
- verifying that backups are complete and accessible
- checking who has authority to make decisions and communicate

What this suggests operationally:

A school may “feel ready” but still be exposed if the plan hasn't been exercised under realistic conditions.

9) Financial Controls and Supplier Verification: 16

Strong Intent, Mixed Consistency



Perceived financial system security:

Very secure:	51.2%
Reasonably secure:	33.8%

Partial automation: **15.9%**

Manual only: **16.6%**

Unsure: **7.8%**

Fraudulent invoice outcomes:

Paid fraudulent invoice:	11.4%
Detected before payment:	29.3%
Unsure:	3.1%

Several points stand out here.

First, perceived financial system security is high. Many schools believe their finance systems are secure, and many have verification practices in place. That's important and suggests significant work has been done across the sector.

Second, despite that, **11.4%** report paying a fraudulent invoice. That is a concrete indicator that fraud can bypass controls—especially when controls depend on manual processes, time pressure, and human interpretation.

Supplier verification practices:

Verify every payment:	51.4%
Verify when adding supplier:	39.4%
Only if suspicious:	2.0%
Unsure:	6.9%

Third, manual-only processes remain present in roughly **one in six** schools. Manual processing is not inherently bad. In some environments it can be tight and well controlled. But manual-only workflows are difficult to scale, difficult to audit consistently, and vulnerable to disruption when key staff are away.

Automation adoption:

Fully automated tools:	59.3%
------------------------	--------------

What this suggests operationally:

Financial controls need to be designed to withstand high volume and high urgency, and they need clear procedures for the most common fraud vectors: bank detail changes, new vendor onboarding, and invoice authenticity verification.

10) AI Adoption Is Early—And Schools Face Structural Barriers



AI usage:

Actively using AI detection:	13.9%
AI in specific systems:	19.2%
Exploring:	24.2%
Piloting:	2.9%
Unsure:	33.8%

AI adoption is not yet widespread. Many respondents are exploring or unsure, which is common in sectors where budgets and capacity are constrained. Even where AI is present, it may be embedded in specific systems rather than used as a dedicated fraud detection layer. The barrier list is revealing because it is not primarily about ideology or resistance. It is about capacity:

- funding constraints
- operational overload
- limited specialist expertise
- technology debt
- a threat landscape that changes faster than schools can refresh systems

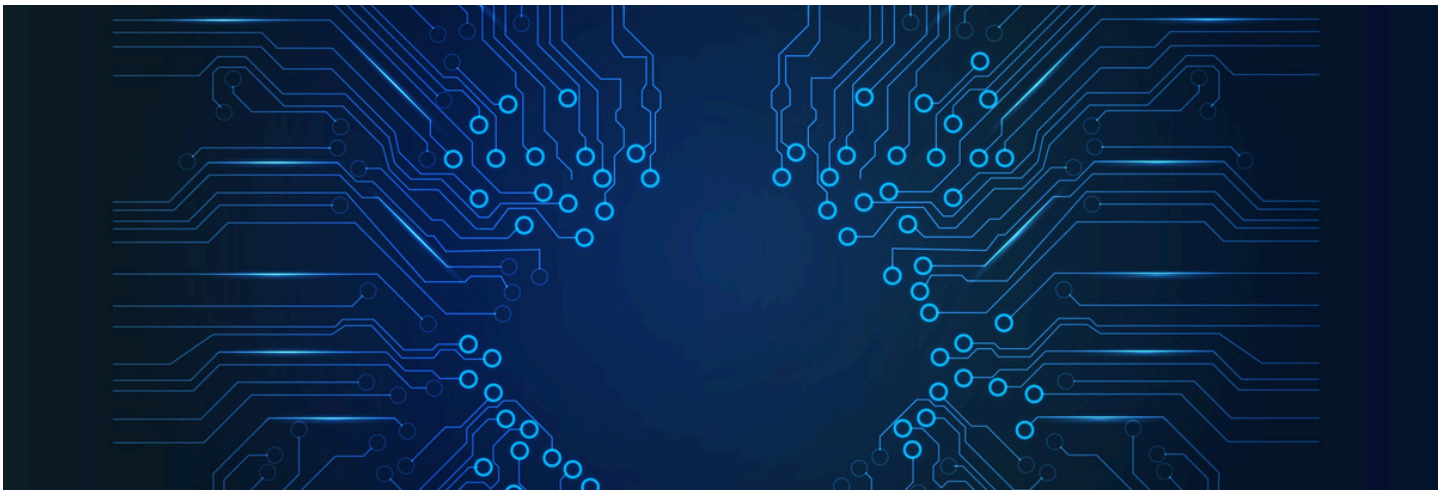
Structural barriers cited:

Lack of funding:	96%
Competing priorities:	96%
Evolving threats:	94%
Limited IT expertise:	92.8%
Outdated technology:	92.4%

What this suggests operationally:

Schools need a pathway to maturity that does not rely on “big bang” transformation. Progress is more likely through phased improvement, prioritising high-impact controls first, and leveraging external support where internal capability is limited.

Cross-Analysis Observations (What the Dataset Suggests Overall)



Across the responses, several themes appear consistently:

1. Fraud exposure is not isolated to one school type or governance model.
2. Finance roles report the highest exposure, reflecting where fraud attempts most often land.
3. Larger schools face scalability challenges, particularly where manual controls remain in place.
4. Governance visibility gaps exist even in mature institutions.
5. Awareness of threat trends outpaces implementation consistency.
6. Recovery validation often lags behind perceived confidence.

A practical way to say this is: many schools are working hard and doing many things right—but the overall system of risk management is not always consistent across the institution, and that inconsistency is where criminals find openings.



Governance and Strategic Implications (What Boards and Executives Should Take From This)

19

The survey suggests five structural imperatives for schools:



1) Treat fraud exposure as ongoing operational risk

Fraud should be managed like other persistent operational risks: staffing, compliance, safety, finance integrity. It requires ongoing attention, not a one-time “project.”



2) Strengthen Board-level visibility into audits and monitoring

When leaders are unsure about audits and monitoring, it’s difficult to demonstrate control maturity. Boards should expect regular reporting on:

- audit cadence (when, what scope, what outcomes)
- monitoring coverage (what systems, what alerts, who responds)
- incident trends (attempts, near-misses, confirmed incidents)



3) Formalise accountability and ownership 20

Someone needs responsibility for coordinating fraud and data protection efforts—whether a dedicated role or part of an existing portfolio. The key is clarity:

- who owns fraud prevention policy
- who owns financial verification steps
- who owns identity security
- who owns training schedules
- who leads incident response



4) Reduce reliance on manual controls that don't scale

Manual processes can work, but they need to be carefully designed, documented, and auditable. As schools grow, they often need automation and system-enforced rules to avoid overloading staff and increasing error rates.

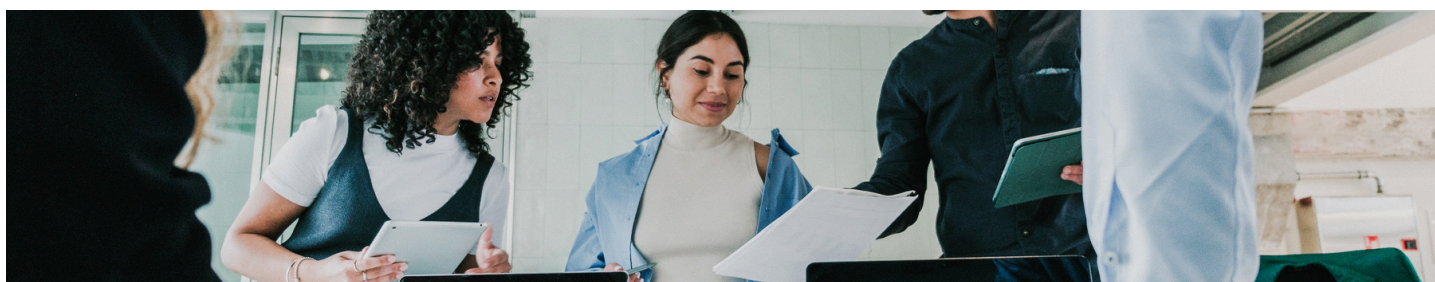


5) Validate recovery plans through regular testing

Resilience is not a document. Resilience is a practiced capability. Regular recovery testing (even simple exercises) reduces the risk of prolonged disruption after an incident.

Practical Guidance: What “Operational Consistency” Looks Like in a School

21



A. Build “Non-Negotiables” Into Payment Workflows

Fraudsters often win when a payment is processed quickly under pressure. Schools can reduce this risk by identifying a small number of non-negotiable steps that happen every time, even during busy periods.

Examples of non-negotiables (illustrative):

- Bank detail changes are verified via callback to a known number, not the number in the email.
- New vendors require a standard onboarding checklist, including verification and approval.
- Payments above a threshold require two-person approval.
- Urgent payments require an independent verification step, even if leadership requests urgency.

The goal is not to slow everything down. It’s to slow down the highest-risk moments by a few minutes—long enough to prevent a costly mistake.

B. Make Training Practical and Role-Based

Because respondents see human error as the main root cause, training should be treated as a core control.

A strong training program in a school context typically includes:

- onboarding training for new staff within the first month
- term-based refreshers for all staff
- targeted modules for finance, HR, and leadership
- short simulations (phishing simulations or scenario walkthroughs)
- clear reporting pathways: “if you think you clicked something, do this immediately”
- leadership messaging that reinforces the behaviour (it’s safe to report mistakes early)

Training should also acknowledge modern tactics: AI-generated impersonation, urgent finance requests, “new banking details,” and realistic-looking login pages.



C. Improve Visibility, Not Just Controls

A common pattern in the data is uncertainty: leaders unsure about audits, monitoring, and ownership. Schools can improve resilience simply by improving clarity.

Practical visibility tools include:

- a simple risk register with owners and review dates
- a security and fraud dashboard reported quarterly
- a written incident response plan with roles and contacts
- an annual calendar that shows: audit timing, training cadence, testing schedule

When leadership can clearly articulate “what we do, how often, and who owns it,” the school is in a better position to improve, allocate resources, and demonstrate due diligence.

D. Treat Recovery as a Practiced Capability

Testing does not have to be disruptive. Even small validation activities strengthen readiness:

- run a tabletop exercise once per term: ransomware, business email compromise, data leak
- test restoration of one critical dataset or system quarterly
- verify backup access controls and credentials
- ensure communication pathways are documented (including out-of-band communication methods if email is compromised)

Only 15% report regular recovery testing. Moving that number upward is one of the most direct ways to reduce operational disruption risk.

A Risk-Focused View ²³ of “Where Fraud Lands” in Schools

Based on the survey themes (and common school operating realities), the highest-risk areas generally include:

1) Email and identity

Email remains the most common entry point for impersonation and credential phishing. If an attacker gains access to an email account, they can watch conversations, insert themselves into invoice threads, and send believable messages from within the organisation.

2) Accounts payable and vendor changes

Vendor change requests—especially bank detail changes—are a known pressure point. If the school’s process allows bank detail changes based on email alone, risk increases sharply.

3) Leadership and authority channels

Attackers often imitate high-authority roles because staff are trained to respond quickly to leaders. Clear policies help staff feel permitted to slow down and verify, even when the request appears urgent.

4) Shared devices and password habits

Weak or reused passwords and shared access are recurring themes. Identity hygiene—unique passwords, strong authentication, minimising shared accounts—reduces the chance that a single compromise spreads.

5) Backups and recovery

Ransomware and extortion threats remain prominent in the 2026 outlook. Recovery readiness is the difference between a short disruption and a prolonged operational crisis.

Implementation Roadmap - Designed for Schools With Real Constraints

24

Because schools face funding pressure, competing priorities, and limited expertise, improvement needs to be staged. Below is a practical, phased approach consistent with the survey's themes and barriers.



Phase 1: 0–90 Days (High Impact, Low Complexity)

Governance and clarity

- Assign a named owner for fraud and data protection coordination (even if part-time).
- Publish an incident escalation pathway that everyone can find.
- Create a simple Board/executive dashboard: audit date, training cadence, recovery test status, incident counts.

Finance controls

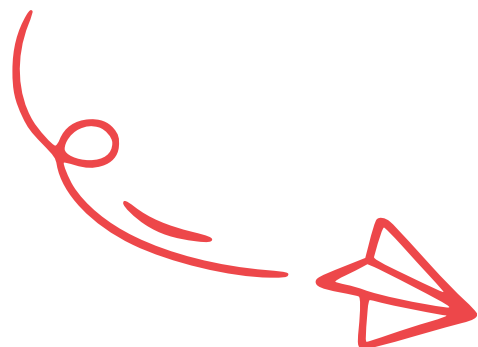
- Implement a mandatory callback verification for bank detail changes.
- Standardise vendor onboarding steps and approvals.
- Ensure payment approvals include a second reviewer for high-risk categories.

People controls

- Run short training refreshers focused on impersonation, invoice fraud, and phishing.
- Reinforce a “safe to report” culture: early reporting reduces harm.

Recovery basics

- Confirm where backups exist, who can access them, and how to restore critical systems.
- Schedule at least one recovery validation activity (tabletop or partial restore).





Phase 2: 3–12 Months (Build Repeatability and Scalability)

Monitoring and audit rhythm

- Establish a predictable audit cadence and a process for tracking recommendations to completion.
- Improve monitoring coverage and ensure leadership knows what is monitored and who responds.

Process hardening

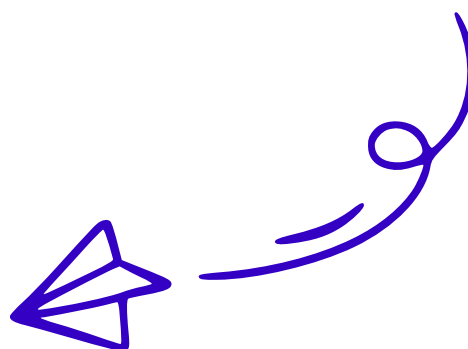
- Reduce reliance on inbox-based approvals by using structured workflows where possible.
- Document payment and vendor change procedures in plain language.

Training maturity

- Move to term-based or twice-yearly refreshers plus role-based modules.
- Add simulations and scenario-based learning to reinforce behaviour.

Recovery testing

- Conduct regular recovery tests and document outcomes and improvements.





Phase 3: 12–24 Months (Modernisation and Advanced Capability)

Automation and tooling

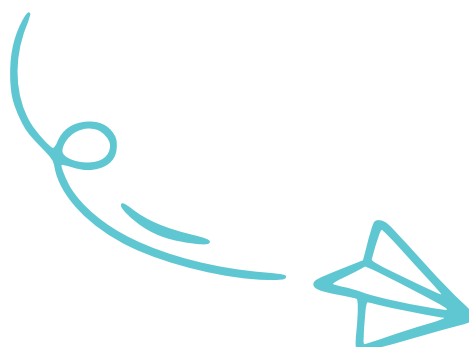
- Increase automation where it reduces manual risk in finance and identity workflows.
- Assess AI-enabled detection within existing platforms and systems.

Resourcing

- Consider shared services, managed security monitoring, or specialist external support where internal expertise is limited.

Continuous improvement

- Track metrics over time: near-misses, training completion, audit completion rates, recovery test outcomes.



What the Findings Mean for Different Leadership Groups



For Boards

Boards are not expected to manage controls day-to-day. But Boards should expect clear reporting and evidence of validation. Practical questions include:

- When was our last security audit? What did it cover?
- What monitoring do we have, and who responds to alerts?
- Who owns fraud prevention and data protection responsibilities?
- How often do we test recovery, and what did we learn?
- How many fraud attempts have we seen, and how many were stopped?

The goal is not perfect security. The goal is demonstrable, improving discipline.



For Executive Teams

Executive teams shape culture and enforce consistency. The most powerful leadership actions are:

- making verification acceptable, even when it slows a payment
- clarifying ownership and escalation pathways
- protecting time for training and testing
- resourcing the basics before pursuing advanced initiatives

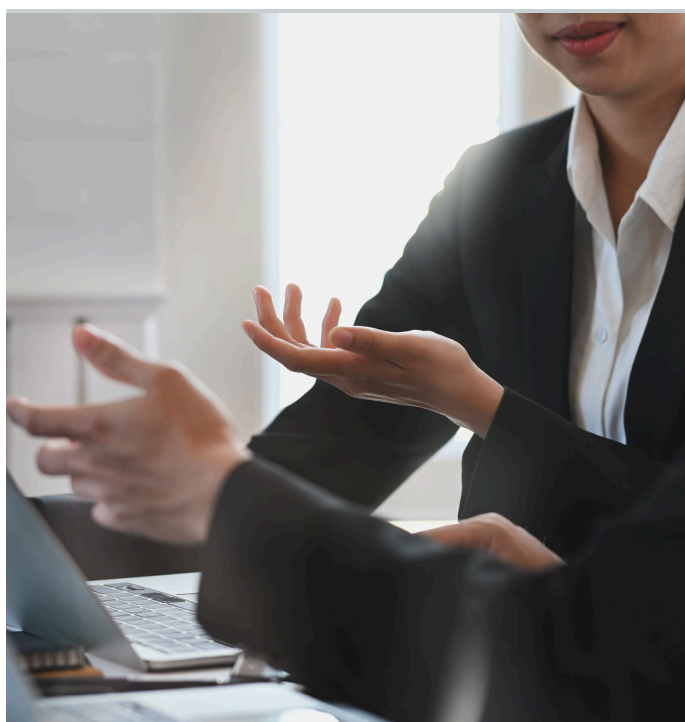




For Finance Leaders and Business Managers

The dataset shows finance teams are on the front line. Priorities that tend to reduce risk quickly include:

- stronger supplier onboarding and bank detail change controls
- documented verification steps that can be followed under pressure
- reducing single-person dependency in approvals
- using automation where it removes risky manual steps
- building a “pause and verify” culture around urgent payment requests



For IT Leaders

IT leaders often carry responsibility without the authority or resources to implement change quickly. High-impact focus areas include:

- identity and access controls
- monitoring clarity (what you monitor, who knows, who responds)
- reducing password reuse and improving authentication hygiene
- ensuring recovery plans are testable and tested
- partnering with finance to harden the workflows attackers target most

Conclusion

The 553-leader dataset presents a sector that is highly aware of modern fraud risk and often successful at detecting attempts. Detection rates are significant, and many schools are actively responding. However, exposure is widespread, manual processes remain present, and governance visibility is uneven.



Fraud in education should now be understood as a structural risk, not an isolated anomaly.

For executive teams and Boards, the priority is not simply strengthening controls. It is ensuring those controls are:

- visible (leaders know what exists and when it was tested),
- scalable (they work under volume and pressure),
- consistently applied (not dependent on one person), and
- validated (through audits, monitoring, and recovery testing).

Operational resilience requires alignment across Finance, IT, Business Operations, and leadership.

Trust remains foundational in education. Protecting it requires structural discipline.

Appendix: Key Findings (Quick Reference)

75.4%	confirmed or suspected fraud attempts
43.8%	detected and stopped fraud activity
9.0%	experienced financial or data loss
11.4%	paid a fraudulent invoice
37.4%	unsure when last security audit occurred
34.2%	unsure whether a designated fraud/data protection owner exists
15%	regularly test recovery plan

Next Steps



31



Watch the webinar

See the key findings from the Fraud and Security Risk in Schools survey and hear what stronger controls look like in practice.

[Watch the webinar](#)



Contact us

Talk to the Alii team about your current processes, priorities and where stronger controls could have the biggest impact.

[Contact us](#)