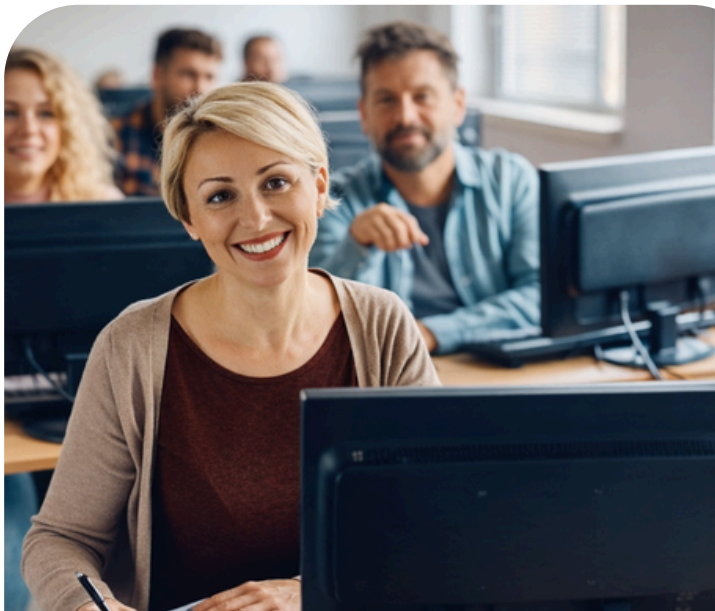
assessmentQ

Feb - Mar 2026

Spotlight Chat Series

Exam Security is a shared responsibility

What four conversations with real exam practitioners taught us about fraud, fairness, and why no single tool, rule, or stakeholder can protect an exam alone.



Reading time: 15min.

Table of contents

Over four **Spotlight Chats**, we spoke to four experts who run high-stakes exams for a living, across professional certification, language testing, regulated skills, and public safety training. Their contexts were completely different. Their conclusion was the same. Security isn't a feature you switch on. It's a **responsibility shared** across every layer of how an exam is designed, delivered, and governed.

> ***Exam security isn't so much about just catching cheats, it's about protecting the confidence in the whole programme.***
>
> - Andrew Balch

When exam integrity fails, it isn't only fraudsters who lose. **Honest candidates suffer most.** Organisations face reputational damage that takes years to repair. Certifications lose public trust. And the stakes aren't abstract. In regulated industries, a fraudulently certified worker on a construction site, handling asbestos, or working with high-voltage equipment is a safety risk for everyone around them.

The four conversations in this series explored how different organisations are responding, and what they've learned. What follows is a distillation of the most important insights: the threats, the decisions, the trade-offs, and the practical moves that actually work.

Featuring

Andrew Balch

Assessment & Platform Strategy Consultant, Certisense

Founder of Certisense and independent assessment consultant with over 20 years of experience across awarding bodies and certification providers. Specialises in exam security strategy, combining assessment design, operational procedures and technology in a practical, holistic way.

Benoît Finet

Head of Educational Unit, Campus POV

Leads police education assessment and delivery at Campus POV, the provincial training centre for emergency services in West Flanders. Oversaw the transition from paper to digital exams for police certification, navigating trade-offs around lockdown, devices and supervisor training.

Michael Nemarich

Chief Operating Officer, NAATI

Leads operations at NAATI, Australia's national certifying authority for translators and interpreters, responsible for setting and maintaining high standards for the profession. Led the organisation's transition to remote testing, now delivering over 35,000 exams a year across 98 languages.

Tom Huiskamp

Business Unit Manager, Kiwa Professional Certification

Manages exams and professional certification at Kiwa across regulated technical sectors including building sites, asbestos handling, high-voltage electrical work and gas. Focuses on ensuring professionals can demonstrate their competence in a fair, reliable and secure way.

Hosts

Leslie Cottenjé

General Manager

Aäron Claerhout

Product Manager

Pieter Pangat

Research Lead

Laurent De Laere

Head of Customer Success

01

The new fraud landscape. Exam security as a joint responsibility

In conversation with Andrew Balch, on what's changed, what's at stake, and why no single stakeholder can hold it alone.

1.1.
Cheating has always existed. What's new is the scale and the tools.

Fraud categories (collusion, corruption, memorisation, impersonation) haven't changed in decades. But the methods have. AI tools designed specifically for cheating, deepfake videos used to deceive remote proctors, and industrial-scale content harvesting services have fundamentally changed the threat profile for high-stakes exams.

> ***The biggest single risk is the reputational damage to the testing programme itself. If we lose trust in the programme and we lose trust in the results, it's the honest candidates that suffer. That's the real problem.***
>
> - Andrew Balch

Andrew Balch, who has spent over 20 years advising exam bodies on security, made this clear: when an exam's outcome can change someone's life, whether a visa, a professional licence, or a university place: candidates are sometimes willing to pay for help. And when there's a market, there will always be vendors.

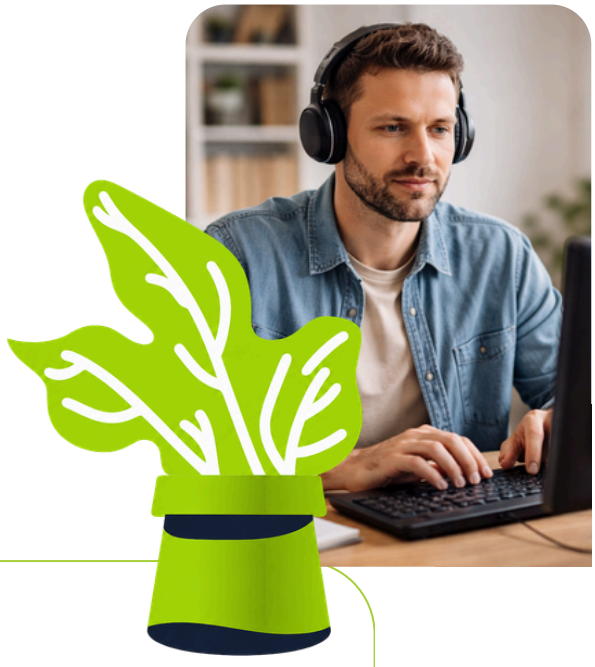
> ***For a global high-stakes exam, cheating is industrial. There are services who harvest content at scale and sell it to candidates. If passing changes your life, you might be prepared to pay a few hundred dollars for a bit more help.***
>
> - Andrew Balch

1.2. Remote vs. on-site debate misses the point

Many organisations have responded to AI-enabled fraud by reverting to test centres or even pen and paper. Andrew's view: this doesn't solve the problem, it **shifts the risks**. In test centres, corruption is real: proctors can be bribed, entire sessions compromised. In remote settings, AI tools and hidden cameras are harder to detect. The risks change. They don't disappear.

The more important question is holistic. What are your candidate population's incentives? What resources do you have? What is your risk appetite? Have you designed security into your exam from the start, or thought about it later?

> ***Security is a chain. If there's one weak link, the whole chain is weak, no matter how strong the rest is.***
>
> - Andrew Balch



1.3. Split contracts create split accountability

Andrew pointed to a live UK example: a major government immigration English language test procured through a tender. Initially the contract was split into two lots: one for test design, content, results analysis; another for running test centres, invigilation, ID checks. On paper, clean division of labour. In practice, a recipe for accountability gaps.

If content was stolen, whose fault was it? The test provider with a small item bank and no randomisation? Or the centre operator who let candidates copy? The government resolved this by merging both lots into a single contract, placing end-to-end responsibility with one organisation. Andrew's conclusion: **don't divide it up at the outset.**

> ***Fraud is evolving fast, but integrity stays defensible when responsibility is shared. No single layer wins alone. It's really about having it shared within an ecosystem.***
>
> - Leslie Cottenjé

1.4. Four moves worth making

Design security in from day one

A test with a small item bank and no randomisation puts enormous pressure on proctoring to compensate. If the test design itself has weaknesses, no amount of downstream security fully covers them.

Think digital and security first

When designing a test, digital and security considerations need to be built in from the ground up, not added on afterwards. They belong in the mindset and the decision tree from day one, not as an afterthought once the content is ready.

Don't treat every candidate as a suspect

Excessive security measures increase stress and can actually undermine the validity of results. If a candidate can't perform to their ability due to anxiety, the result is worthless anyway. The goal is a layered security approach that's mostly invisible to honest candidates, with proctoring only as the final layer.

AI has no short-term solution: start the bigger conversation now

Nobody has cracked the AI problem yet. Andrew's advice: fix your holistic weaknesses first, those are the quick wins. But in parallel, start asking the harder questions. What is this test actually for? What tools do candidates use in the real world? If you can't prevent AI use in the exam room, do you need to rethink what you're testing and how? Most providers won't redesign their tests in a year, but the conversation needs to start now.

02

To lock or not to lock? The exam security trade-off

In conversation with Benoît Finet, Campus POV, the lockdown decision and the trade-offs nobody warns you about.

2.1.
The decision to go digital was easy. Deciding to lock it down was not.

Benoît Finet oversees education at Campus POV, a Belgian police training school. He went digital not primarily for security, but for **quality**: digital exams gave him control over question analysis, faster feedback loops, and a single platform for everything. The logistics improvement was real and immediate. The transition surfaced decisions he hadn't fully anticipated, starting with the lockdown question.

In a bring-your-own-device setup in a tiered lecture theatre, candidates could still look at each other's screens even with randomised question order. Randomisation reduces the problem but doesn't eliminate it. Screen-watching replaced the old paper cheating methods. The challenge didn't disappear. It shifted.

> ***We knew cheating is tempting, so we cannot rule that out even if we go digital. If people have the chance to cheat, some will try. If we were going digital, we had to have a clear idea of what we wanted to do about fraud.***
>
> - Benoît Finet

2.2.
Safe Exam Browser is one layer, not the whole answer.

Benoît implemented Safe Exam Browser from day one. It works, but with real friction. MacBook compatibility failures mid-year forced him to split exam groups, creating two simultaneous versions and significant supervisor strain. His solution was practical: buy 32 additional school-owned devices so everyone sits on the same hardware.

He also met unexpected resistance from police officers in further training who refused to install SEB because it was flagged as malware on their devices. His response: have school laptops as a fallback, no exceptions needed.

> ***When things went wrong, people tried to convince me to go back to paper. I said no. If we had, people would have lost faith in the system entirely. We kept going and now I know it works.***
>
> - Benoît Finet

Train supervisors properly: it's easy to underestimate

Benoît built a 25-page illustrated guide, then split supervisors into two profiles: one for guiding the start, one for active monitoring. Staff who paper-invigilated for years find digital supervision more demanding, not less.

Start slow & build confidence.

Don't launch all your exams digitally at once. Start with one. Try different question formats. Build experience. When things go wrong, and they will, you need staff who can stay calm and fix it fast.

03

Fraud creativity in digital exams: How to respond?

In conversation with Michael Nemarich, NAATI: lessons from delivering 35,000 remote exams a year across 98 languages.

3.1.
Going remote didn't spike fraud. The data is surprising

NAATI is the certification body for translators and interpreters in Australia and New Zealand. Michael joined as COO in 2018. At that point NAATI was running 15 to 17,000 tests a year in about 50 languages, candidates coming in to test venues, max capacity 200 to 250 a day, tests on USB sticks with invigilators walking the room. COVID forced a move to Microsoft Teams, which accelerated conversations with assessmentQ already underway. Today they deliver over 35,000 tests a year in 98 languages.

Their most important finding: with the right controls, pass rates across decades of testing showed no material difference from in-person to remote. Cheating attempts happened, but they weren't causing a measurable systemic problem.

> ***Online is not cheap. If you think of it as a cost saving alone, that's when you come into trouble. The benefit is accessibility and scale, not cost reduction.***
>
> - Michael Nemarich

35K +
Remote exams per year

98
Languages supported

300
New test materials per month

3.2.
Fraud evolves fast. So does the response.

The range of methods NAATI has encountered is remarkable and humbling. Candidates uploaded content to WeChat. They hid recording devices under desks. They used coordinated coughing signals to get a partner in another room to kill the internet connection. They wore wigs to hide Airpods. They installed shower curtains in their living rooms to hide a second person lip-syncing. And more recently, they've attempted remote desktop connections to display different screens to the proctor than to themselves.

In each case, NAATI's response was the same: observe, identify the pattern, adapt. The money saved on test venues was reinvested into content creation (around 300 new test materials per month), so that memorising content from a previous session becomes pointless. Test windows were shortened to 45 minutes. Multiple materials are now used in the same session on the same day.

Multiple camera angles close the deepfake gap

NAATI runs webcam, secondary mobile camera, and screen share simultaneously. Live deepfakes are already being attempted, but a single deepfake covering three angles simultaneously isn't yet sophisticated enough to pass undetected.

Cognitive load on monitoring staff is real

NAATI found high burnout in their monitoring team in the early days. Their fix: monitor for half-days only. Use afternoons for content recording, a different cognitive task that gives staff genuine recovery time.

It's an arms race, and persistence wins

NAATI's overriding advice: don't be deterred. Organisations that went remote and then retreated to handwritten, on-site exams often did so because they hadn't built the specialist team or the operational rhythm to sustain it. With the right investment in people and process, next to the technology, scale is achievable.

04

How exam design choices help prevent fraud

In conversation with Tom Huiskamp, Kiwa: the most powerful security decisions are made at the drawing board.

4.1.
The drawing board is the most important security checkpoint.

Tom Huiskamp manages the certification business at Kiwa across a broad spectrum of sectors, including certification exams for building sites, asbestos handling, high-voltage electrical work and gas. As Tom put it, lives are genuinely at stake on the job.

In these sectors, the stakes of exam fraud aren't abstract: a fraudulently certified worker on a job site is a safety risk for every person around them. The moral case for exam integrity here is unambiguous.

Tom's key point: don't overlook **randomisation** as a fraud prevention measure. When 20 candidates sit in the same room and each receives a different question set, different ordering, and different answer options, looking at your neighbour's screen becomes useless. Answer A on their screen is not answer A on yours.

> ***Exam integrity is not about catching cheaters. It's about designing systems that make cheating irrelevant.***
>
> - Tom Huiskamp

4.2.
Question format variety is both a security tool and a validity tool.

Ten years ago, most exams were multiple choice with one correct answer. Today, the options are far broader: multiple correct answers, picture-based questions, audio-based prompts, hotspot interactions, scenario-based items that require combining several knowledge areas. Each additional format raises the bar for anyone trying to game the system, and more accurately reflects what real-world competence actually looks like.

The lesson from Tom's work: security and validity aren't in tension. Designing an exam that genuinely tests knowledge naturally makes it harder to cheat. The commitment to measuring real competence is, itself, an integrity measure.

Randomisation is non-negotiable

Large question banks, randomised selection, and randomised answer ordering are the foundation. Without them, proctoring carries the entire weight of security, an unsustainable position.

It's about lives, not just credentials

Tom's framing is direct: if candidates certify without having the knowledge, people can get hurt. This reframes exam security from a compliance obligation into a professional responsibility.

05

What does "Secure at Heart" actually mean?

Across all four conversations, the same architecture emerged. Security that works isn't built from a single tool. It's built from shared ownership across people, process, and technology.

Exam security lives across people, process, and technology. It works when every stakeholder, from the person writing the questions to the candidate sitting the exam to the platform running it, plays their part."

- Laurent De Laere

6 things every exam leader should take from this series

01 Design security in from day one
A small item bank with no randomisation puts all the pressure on proctoring. That's not a sustainable position.

02 Don't underestimate randomisation
Large item banks with varied ordering make collusion structurally harder, and lift pressure off every downstream layer.

03 Remote exams doesn't automatically mean more fraud
But it changes which risks are highest. Understand your specific context before choosing your approach.

04 Technology is one layer, not the whole answer
It works best paired with trained supervisors, strong content practices, and operational rhythm. The platform enables; the organisation makes it stick.

05 Don't divide and walk away
Exam organiser and platform provider must be partners, not customer and supplier, with shared visibility across the whole exam lifecycle.

06 Persistence pays
Organisations that reversed their digital transition mostly failed not because of fraud, but because they hadn't built the team and processes to sustain it.

How secure is your exam programme?

assessmentQ is the digital exam platform built for exams that can't go wrong. Exam security is a big part of that. If this topic raised questions about your own setup, let's have a chat.

Let's chat

assessmentQ

Built for digital exams
that can't go wrong.
At all.

www.assessmentq.com

sales.education@assessmentq.com

Facebook

LinkedIn

Proudly headquartered in Belgium
Leo Bekaertlaan 1
8870 Izegem