ASCILITE 2025

Future-Focused:

Educating in an Era of Continuous Change

Secure online assessments: Strategies to mitigate generative AI risks in higher education

Joane Jonathan, Chris Walsh
Victoria University

The rapid rise of generative artificial intelligence (AI) tools has intensified universities' long-standing challenge of ensuring that student work is authentic, an issue that is particularly acute in fully online programs. In 2024, new Tertiary Education Quality and Standards Agency (TEQSA) guidelines prompted our university to revise its Assessment for Learning Policy and Procedures, requiring every unit to have a secure assessment that is explicitly mapped to learning outcomes and validates core knowledge and skills. This study reports on the first pilot of that policy in three wholly online, postgraduate units. Using the 4-A Framework for secure assessment design, we implemented remotely-invigilated final exams in two units and a live, oral presentation in the third. Semi-structured interviews are planned with academics and students, and completion data and incident reports will be analysed. Preliminary pilot findings indicate that secure tasks can credibly validate student ownership of learning outcomes in an online environment. While both formats reduced academic-integrity breaches, oral presentations garnered higher perceptions of authenticity and lower than expected administrative overheads. We argue that secure, outcome-mapped assessments are feasible, scalable, and pedagogically valuable in online postgraduate education, and we outline policy and practice implications for institutions facing similar regulatory pressures.

Keywords: Higher education, assessment, online learning, secure assessments, academic integrity, generative AI, 4-A Framework

Introduction

Higher educational institutions are charged with the critical role of instructing and certifying their students possess the requisite skills and knowledge within a field of study. Hence, it is incumbent on universities to ensure students' work is authentic and their own. Academic dishonesty, in the forms of contract cheating, plagiarism, and collusion, is a historical battle between students and educators since antiquity and condemned by early scholars unto this day (Li, 2024). The focus on compliance with academic integrity principles ebbs and flows, garnering more attention during periods of public outrage (Ellis & Murdoch, 2024). Currently, the focus of outrage is firmly centred on the perception of the prevalent use of generative AI for academic dishonesty (Denkin, 2024; TEQSA, 2024).

In contemporary history, AI usage in many forms has been widespread, yet the emergence of readily available text generative AI (e.g., ChatGPT, CoPilot, Gemini) has witnessed an explosion in uptake across all industries. Whilst the transformative impact of generative AI on productivity is undeniable, the challenges that AI creates for educators is profound. Generative AI capabilities allow for the construction of fully formed responses to assessment tasks in seconds. This capability has a negative impact on education in two key ways, student learning and academic integrity. First, the untrustworthiness and inaccuracy of the AI output may lead to novice students' potential misunderstanding of the content. AI exposes students to misinformation. Additionally, assessment for learning is lost through students undervaluing the assessment task as an opportunity to learn as they are not actively engaged in the assessment, which is required for learning to take place (Wiliam, 2011). Second, and the focus on this paper, the ease of availability to AI produced assessment

responses threatens academic integrity. Unlike cost-incurring contract cheating that required a human second party, basic AI functioning is free and readily available in the home via internet access.

In this age of rapid technological improvements, universities are tasked with the challenge of combatting academic dishonesty and enhance the design of assessments. The TEQSA (2024) guidelines place an emphasis

on secure, learning outcome-aligned assessment and push universities to upgrade their assessment practices. TEQSA proposed, "Assessment should emphasise security at meaningful points across a program to inform decisions about progression and completion" (Lodge et al., 2023, p. 6). Our study explores the trial of enhanced security methods employed in assessment tasks to ensure authenticity and students' achievement of learning outcomes. This study specifically addresses the research question:

- What happens when secure assessments are implemented in Higher Education units?

Secure Assessments Compliance

As outlined in the university's Generative AI Action Plan, a secure assessment is defined as one that ensures a verifiable link between the enrolled student and the work submitted, particularly in an environment where generative AI tools are widely accessible. Secure assessments are intended to protect academic standards while supporting fair and inclusive learning.

Units across the university's programs are required to incorporate at least one secure assessment task aligned with unit and course learning outcomes. These assessments are reviewed through the university's established Assessment Refresh process. Assessment design is guided by what we refer to as the 4-A Framework: authenticity, alignment, accessibility and assurance. These principles help ensure tasks are not easily outsourced, fabricated or automated, and encourage the use of context-specific, identity-verified responses.

Secure assessments include invigilated exams, synchronous oral defences, applied simulations and problem-solving tasks that require personalised outputs. All tasks are supported by clear marking rubrics and moderation procedures and are subject to archival and reporting requirements overseen by Academic Quality and Standards. Staff developing or marking secure assessments must complete academic integrity and Gen-AI training, reinforcing consistent and informed implementation across the university.

Methodology

This study adopted a case study methodology to trial and evaluate the implementation of secure assessments in a fully online learning environment. The focus was on three postgraduate units, which provided an ideal setting for testing how identity-verified and AI-resilient assessment formats could function at scale in remote delivery. Three postgraduate units were selected for the pilot. Two included a remotely invigilated final exam using proctoring technology, while the third required students to complete a live oral presentation via secure online video platforms. These assessment tasks were designed using backward design principles and the 4-A Framework, which underpins the institutional approach to secure assessment.

Following task delivery, qualitative data collection was undertaken through semi-structured interviews with both academic staff and students. The interviews explored perceptions of fairness, workload, confidence in academic integrity and usability of the technology platforms involved. Interviews were conducted one-on-one via Zoom and recorded with participant consent. In parallel, we collected institutional data on completion rates, academic misconduct reports and examiner observations across the three units. This data provided insight into both the effectiveness of the secure assessment tasks and the logistical or procedural challenges encountered during implementation.

Ethics approval was obtained through the university Human Research Ethics Committee. Interview data is being coded thematically to identify common challenges and areas for improvement in assessment design, student communication and academic staff support. This methodology offers a practical, grounded lens into the implementation of secure assessment strategies in the context of a rapidly changing academic integrity

landscape. By combining lived experience from participants with performance and incident data, the study contributes to a broader understanding of what effective, scalable secure assessment looks like in practice, especially in fully online learning environments.

Site Description

In addition to the university's on-campus programs, a separate branch delivers fully online courses. This branch of the university provides undergraduate and postgraduate education in a fully digital mode and served as the key site for testing new secure assessment designs in this study. Fully online delivery offers unique challenges and opportunities in implementing identity-verified, authentic assessments in a remote context.

The university response to the emergence of generative artificial intelligence has been institution wide. The release of the Generative AI Action Plan formalised the university's commitment to academic integrity while recognising the potential for AI to support student learning. The Action Plan mandates that all accredited units include at least one secure assessment task to ensure the authenticity and traceability of student work to their unit learning outcomes (ULO). This requirement aligns secure assessment with broader academic quality and assurance processes. In this context, the case study provides a live test case of how large institutions are reshaping assessment practices to meet emerging integrity risks in AI-influenced learning environments and ensuring the 4-A Framework elements of Authenticity, Alignment, Accessibility, and Assurance are met.

Preliminary findings

Invigilated exams

Our pilot found that remotely proctored exams in our Financial Planning units remain the benchmark for secure conventional or traditional assessments. Our use of this secure approach, like many online courses in HE, achieved three primary objectives. First it guaranteed identity assurance through multi-factor log-in, identity checks with identification and continuous proctor webcam monitoring. Second, the invigilated exams provided students the opportunity to provide controlled knowledge sampling via open-ended questions within a given timeframe. Third, the pilot generated video recorded audit trails of the proctored and invigilated exams that satisfy external regulators (Dawson, 2022). Our online invigilation of the two pilot Financial Planning unit exams did deter contract cheating and eliminated the use generative AI drafting.

Invigilated oral presentations

In contrast, the health-unit pilot replaced its traditional pre-recorded presentation with a live online presentation and defence with randomised questions students answered orally via the Zoom recording in the Respondus locked down browser. The design philosophy drew on Rundle et al.'s (2020) application of the Swiss-Cheese Model to assessment integrity, instead of relying on one defence to defer cheating (the Respondus LockDown browser in our LMS), the task weaves multiple, smaller but connected, layers of protection, each with small "holes" that seldom line up. These included:

- ULOs mapped to explicit presentation criteria; task counts as the designated secure assessment under the revised procedure;
- Student submits slides 24h in advance to ensure their academic work;
- Real-time ID check and session recording within the LMS using Zoom; and
- Academics assessed the presentations via recordings using rubrics where the ULOs are mapped to the explicit presentation criteria and cross-checked the students' submission of their slides and scripts with the accompanying Turnitin originality reports in the LMS.

Our pilot's multilayered approach to the secure presentation is an authentic assessment, that is preferable to exams and sessions with open-ended questions for three reasons. First, it duplicates professional practice where future graduates are routinely required to articulate and defend their thinking, actions and reflections on practice to workplace peers and stakeholders. Second, the dialogic format of the randomised questions requires students to provide explanations, clarifications, recommendations and arguments that generative AI cannot pre-write (Foley et al., 2024; Brumby et al., 2025). Third, because the randomised questions are

mapped to ULOs, student responses provide evidence of threshold concept mastery, satisfying the "alignment" arm of Biggs's (1996) framework as students demonstrate the skills of critical thinking and ownership of their ideas in relation to the ULOs.

Towards secure online authentic assessments

Building on these insights, we will scale the study to additional postgraduate disciplines over the next academic year, embedding at least one non-exam secure task (e.g., viva, simulation, role-play, or reflective interview) in each unit to satisfy our university's new policy and assessment procedures in response to generative AI. This expansion will allow us to stress-test the "swiss-cheese" layering across different courses in business, health, nursing, education and law. Crucially, it will assess whether the authenticity gain we observed generalises when generative-AI tooling becomes more sophisticated. Diversifying secure assessment formats now is therefore an anticipatory future-proofing strategy. Each new assessment type, whether a dialogic defence, situated performance or reflective interrogation, will add a barrier that student use of AI must breach synchronously, thereby preserving the evidentiary link between what students claim and what they can prove in real-time online secure assessments.

Discussion

Our pilot demonstrated that widely available tools were sufficient to deliver secure, camera-verified exams in two postgraduate business units. No bespoke code or additional institutional licenses were needed, and the set-up time for learning-design staff was in the master copy of the units, could easily be integrated into regular workload. This finding aligns with TEQSA's recent advice that "technology already in common use can be configured to meet integrity benchmarks" (TEQSA, 2024).

Our university's policy shift that now requires every secure assessment to be explicitly aligned with at least three ULO had two practical payoffs. First, it exposed several legacy tasks that were testing the same outcome in multiple units, allowing academics to retire or consolidate redundant assessments. Second, the new mapping made it straightforward to assign existing tasks as the designated secure assessment without adding assessment load for academics or students. This approach supports Biggs' (1996) constructive-alignment principles and debunks fears that integrity reform necessarily means "more exams."

While remote-invigilated exams effectively suppressed misconduct before and during our pilot, the live oral presentation emerged as a scalable, low-overhead alternative that provides students with an opportunity to demonstrate the unit's learning outcomes. The presentation or defence will likely emerge as the most authoritative indicator of learning-outcome attainment, because in the future, we will take steps to ensure that academics assessing student learning, interact with students in real time online. In the invigilated online presentation, academics can query student's claims against targeted questions mapped directly to the unit learning outcomes, thereby generating evidence of higher-order cognition. Recent systematic reviews confirm that oral assessments offer a uniquely secure, authentic, and cost-efficient mechanism for validating knowledge ownership and professional-communication competence in online settings (Nallaya et al., 2024; Stephenson et al., 2025). When a student successfully completes these types of dialogic defences, the academic team and other university stakeholders, can have high confidence that the unit's learning outcomes have been genuinely achieved.

Over the coming 12 months we will broaden the pilot to six additional postgraduate disciplines. Each course team will redesign at least one non-exam secure task (e.g., viva-voce defences, video-recorded synchronous skills demonstrations, structured reflective interviews, or role-play simulations) that can be invigilated with the university's existing proctoring tools. The goal will be to test whether these authentic, dialogue-rich formats replicate the low-breach rates and high-authenticity ratings observed in the initial business and health units, while reducing the logistical costs and equity concerns that accompany remote proctored exams.

Conclusion

This work-in-progress pilot study confirms that secure, outcome-mapped assessments are not only feasible but pedagogically advantageous in fully online postgraduate education. Universities need not undertake wholesale system overhauls; instead, they can repurpose existing tasks, including remote-proctored exams, live

presentations, viva defences, or open-ended, assessor-moderated discussions, provided each is unambiguously and explicitly tied to the unit's earning outcomes and supported by proportionate invigilation confirmed identity-verification measures.

By foregrounding diversity of assessment task type, institutions can move beyond an over-reliance on high-stakes exams, thereby increasing authenticity, reducing costs, and enhancing student engagement while still meeting stringent regulatory expectations in the generative-AI era. Our forthcoming multi-disciplinary rollout will supply the sector with deeper evidence on scalability and graduate impact, but the pilot's message is already clear: integrity, alignment, and student-centred design can coexist, even flourish, online.

References

Biggs, J. (1996). Enhancing teaching through constructive alignment. *Higher Education*, 32(3), 347–364. https://doi.org/10.1007/BF00138871

Brumby, D., Cox, A., Sarkar, A., & Gould, S. (2025, 6 March). Sampled vivas are pivotal in combating AI cheating. *Times Higher Education.* https://www.timeshighereducation.com/opinion/sampled-vivas-are-pivotal-combating-ai-cheating

Dawson, P. (2022). *Strategies for using online invigilated exams.* Tertiary Education Quality and Standards Agency. Retrieved 17 June 2025 from https://www.teqsa.gov.au/sites/default/files/2022-10/strategies-for-using-online-invigilated-exams.pdf

Denkin, R. (2024). On Perception of Prevalence of Cheating and Usage of Generative AI. *arXiv preprint arXiv:2405.18889*. https://doi.org/10.48550/arXiv.2405.18889

Foley, M., Ng, J. L., & Loh, V. (2024, 26 January). *'Tell me what you learned': Oral assessments and assurance of learning in the age of generative AI.* Teaching@Sydney. https://educational-innovation.sydney.edu.au/teaching@sydney/tell-me-what-you-learned-interactive-oral-assessments-and-assurance-of-learning-in-the-age-of-generative-ai/

Li, Y. (2024). *Perspectives on plagiarism in China: History, genres, and education*. Taylor & Francis. https://doi.org/10.4324/9781003398677

Lodge, J. M. (2024). The evolving risk to academic integrity posed by generative artificial intelligence: Options for immediate action. *Tertiary Education Quality and Standards Agency*, 2024-08. https://www.teqsa.gov.au/sites/default/files/2024-08/evolving-risk-to-academic-integrity-posed-by-generative-artificial-intelligence.pdf

Lodge, J. M., Howard, S., Bearman, M., Dawson, P, & Associates. (2023). *Assessment reform for the age of Artificial Intelligence.* Tertiary Education Quality and Standards Agency. https://www.teqsa.gov.au/sites/default/files/2023-09/assessment-reform-age-artificial-intelligence-discussion-paper.pdf

Nallaya, S., Gentili, S., Weeks, S., & Baldock, K. (2024). The validity, reliability, academic integrity and integration of oral assessments in higher education: A systematic review. *Issues in Educational Research*, *34*(2), 629-646. https://search.informit.org/doi/10.3316/informit.T2024121800014001121097284

Rundle, K., Curtis, G., & Clare, J. (2020). *Why students choose not to cheat.* In T. Bretag (Ed.), *A research agenda for academic integrity* (100–111). Edward Elgar Publishing. https://doi.org/10.4337/9781789903775.00014

Stephenson, Z., Johnson-Glauch, N., & Cruchley, S. (2025). Interventions and facilitators of oral assessment performance in higher education: a systematic review. *Assessment & Evaluation in Higher Education*, 1-14. https://doi.org/10.1080/02602938.2025.2504621

Tertiary Education Quality and Standards Agency. (2024, August 8). *The evolving risk to academic integrity posed by generative artificial intelligence: Options for immediate action*. https://www.teqsa.gov.au/sites/default/files/2024-08/evolving-risk-to-academic-integrity-posed-by-generative-artificial-intelligence.pdf

Wiliam, D. (2011). What is assessment for learning?. *Studies in educational evaluation, 37*(1), 3-14. https://doi.org/10.1016/j.stueduc.2011.03.001

ASCILITE 2025

Future-Focused:

Educating in an Era of Continuous Change

Jonathan, J. & Walsh, C. (2025). Secure online assessments: Strategies to mitigate generative AI risks in higher education. In Barker, S., Kelly, S., McInnes, R. & Dinmore S. (Eds.), *Future Focussed. Educating in an era of continuous change*. Proceedings ASCILITE 2025. Adelaide (pp. 386-391).
https://doi.org/10.65106/apubs.2025.2680