Identity Verification Readiness Checklist

A one-page gate to run before you add identity verification to an assessment: match assurance to stakes, clear consent and biometric law, test fairness, defend against deepfakes, and set retention. Engineering guidance, not legal advice.

A. Match the assurance level to the stakes

- [ ] Decided the assurance level from the cost of a successful impersonation
- [ ] Used the lightest defensible method stack (knowledge / ID / face match / liveness)
- [ ] Added continuous identity only where full-session biometrics are justified
- [ ] Set the match threshold deliberately, weighing false rejections vs false acceptances

B. Consent & biometric law

- [ ] Written, informed consent obtained before any faceprint is collected (BIPA)
- [ ] Lawful basis + GDPR Art 9 condition documented for EU/UK candidates
- [ ] FERPA 'school official' exception confirmed for any US student-record disclosure
- [ ] Vendor signs the data-processing agreement (GDPR Art 28)

C. Fairness, accessibility & human review

- [ ] Face match tested across skin tones, lighting, age, and camera quality (NIST FRVT)
- [ ] Alternative verification path for candidates the camera fails repeatedly
- [ ] Accommodations for disabled, neurodivergent, and changed-appearance candidates
- [ ] Every failed match reviewed by a human; documented appeal route; no auto-fail

D. Anti-fraud, retention & security

- [ ] Liveness / PAD tested to ISO/IEC 30107-3 against photos, replays, and masks
- [ ] Capture-source validation + multi-frame signals to stop deepfake injection
- [ ] Faceprint and images encrypted in transit and at rest; least data collected
- [ ] Retention period defined; biometric template deleted once verification completes