



Overview of Certification of Effective Controls

June 12, 2025

i3 Integrity will complete an independent audit of the operator's¹ internal controls related to age verification, identity verification ("KYC") and geolocation for purposes of the Company's efforts to meet the underwriting requirements of its payment and banking partners. i3 Integrity will issue an audit report at the conclusion of the engagement, which may be provided to external parties as needed.

As part of the audit, i3 Integrity will conduct interviews with appropriate staff of the Company, request and review Company documentation, test and sample key controls. Throughout the audit engagement, i3 Integrity will inform the Company of any deficiencies identified. This will provide the Company with the opportunity to either remedy the deficiency or prepare a management action plan before the conclusion of the audit. i3 Integrity will include the management action plans for any outstanding deficiencies in the final report as evidence of the Company's plans to ensure an effective control environment.

Documentation to be reviewed, **if available**, includes:

1. Legal opinion regarding games offered by the Company.
2. Internal controls documentation.
3. Vendor documentation for relevant 3rd party solutions implemented by the Company (e.g. age verification, identity verification, geolocation) including specific solution implementation settings.

In addition to the documentary review, i3 Integrity will interview Company staff and perform testing and sampling of the following **Scope** control areas:

1. Player registration
2. Age verification
3. Identity verification
4. Purchase & withdrawal
5. Geolocation

¹ i3 Integrity only offers this service to unregulated entities at the present time: social gaming, sweepstakes and DFS operators operating in states where it is not prohibited and gaming licenses/registrations are not required.

At the conclusion of the audit, i3 Integrity will issue a ***Certification of Compliance Controls*** for the Scope control areas listed above.

The ***Report*** will be organized around the 4 scope control areas listed above and include:

1. Narrative describing the audit's approach and scope.
2. A description of each control area and how these controls are managed.
3. A description of any findings/observations
4. Confirmation that any findings have been remediated during the audit
5. The Company's management action plans/responses for any outstanding findings
6. Screenshots relevant to the audit

General parameters of the audit include the following:

1. Devices to be tested
 - a. Mobile
 - b. Laptop
 - c. Desktop
2. Operating systems
 - a. iOS
 - b. Android
 - c. Windows
3. Browsers
 - a. Chrome
 - b. Firefox
 - c. Safari
 - d. Edge
4. Registration
 - a. Access to and user acceptance of Privacy Policy, Terms and Conditions
 - b. Age certification (if appropriate)
 - c. Date of birth controls
5. Purchase and withdrawals
 - a. Availability prior to verification
 - b. Availability after verification
6. Geolocation testing
 - a. Prohibited state testing
 - b. Permitted state testing
 - c. Non-US access testing (from Mexico)
 - d. VPN blocking
 - e. Chromium dev tools (browser location changes)
 - f. Windows default location changes
 - g. Modified Firefox configuration
 - h. Spoofing
 - i. Proxy testing
7. Age & identity verification

- a. Soft (non-documentary) KYC (if appropriate)
- b. Underage (according to the legal opinion and Company terms and conditions)
- c. Expired identification documents
- d. Invalid identification documents
- e. Valid, unexpired documents
- f. ID & selfie or photo mismatch (if appropriate)
- g. Documentary address verification (if appropriate)