	CREATION DATE February 15, 2012	DATE REVISED July 26, 2024
	POLICY AREA / CATEGORY	DATE APPROVED / EFFECTIVE DATE March 01, 2012
POLICY TITLE AUDITS	VERSION	DATE REVIEWED July 26, 2024

### SUMMARY & PURPOSE:

This policy shall describe the purpose and processes related to random audits that are part of the routine process of business for SSH certification programs. Audits serve the process of supporting the integrity of the certification process by working through verification of submitted materials. It supports an honor-based system, thus encouraging all to submit accurate information at all parts of the certification process.

### DEFINITIONS:


**Audit:** an event that occurs based on simple count of any given event or activity that flags the need for provision of proof of the event or activity by the applicant/candidate/certificant.

### POLICY:

- Audits shall occur at a rate of 5% (one out of every 20 events) and shall be performed on a simple count basis (i.e. when every 20<sup>th</sup> event of any particular type occurs).
- Audits are assigned by the vendor's candidate management system
- Audits shall occur for the following events:
  - Verification of applicant eligibility
  - Verification of Continuing Professional Development (CPD) submissions
  - Other events/activities as determined appropriate by the Certification Council
- Those audited should submit information within 30 days of notification of being randomly audited.
- Response by SSH staff shall be within 30 days of submission of materials.
- SSH Staff shall review the information. If the provided materials are adequate, the audit shall be approved (cleared).
- If the information is inadequate, unclear, or otherwise insufficient to approve the audit:
  - The appropriate subcommittee shall be requested to review the submitted information. If they are unable to approve the audit, further information shall be requested from the candidate.
- If an audit is failed, meaning that the submitted evidence does not support the information previously submitted by the individual, the following may occur:
  - Applicants and candidates shall not be allowed to test if they have not yet tested.
  - Certificants shall not be allowed to renew their certification. They shall be allowed to reapply to become certified and take the examination to achieve certification again.
- If an applicant or candidate falsifies information or submits information that is otherwise found to be false/untrue, the Certification Council shall review the facts as known. On completion of the investigation, the Certification Council reserves the right to take disciplinary action, up to and including:
  - Prevention of testing
  - Revocation of certification
  - Other disciplinary action as determined appropriate
- If no information is submitted in response to the audit:
  - Applicants and Candidates shall not be allowed to take the examination
  - Certificants shall not be allowed to renew their certification. They are allowed to submit a new application and test to become certified.
- Applicants, candidates, and certificants shall be afforded due process for any random audit. This shall be documented and applicants, candidates, and certificants shall be afforded all reasonable opportunities to provide accurate information to resolve the audit within the timeline indicated in the audit policy.

### SCOPE/APPLICABILITY:

This shall apply to all applicants, candidates, and certificants applying for or renewing any SSH Certification examination.

	CREATION DATE February 15, 2012	DATE REVISED July 26, 2024
	POLICY AREA / CATEGORY	DATE APPROVED / EFFECTIVE DATE March 01, 2012
POLICY TITLE AUDITS	VERSION	DATE REVIEWED July 26, 2024

**PROCEDURES TO ENSURE COMPLIANCE:**

- Audits in the SMT system, if not approved, shall prevent the individual from testing and/or renewing as appropriate. Once approved, the individual shall be allowed to continue.

**SUPPORTING/REFERENCE DOCUMENTATION:**

- None

**RELATED POLICIES & PROCEDURES AND ASSOCIATED FORMS:**

- Appeals Policy
- 

**ASSOCIATED NCCA STANDARD(S):**

- 7A

**POSTED PUBLICLY: YES**