

NSET Information Security Assessment Service (IT Audit)

Terms of Reference (ToR)

1. Background

The National Society for Earthquake Technology – Nepal (NSET) is a nonprofit non-government organization working for earthquake risk management sector in the last 2 decades. In the context of Technology world, Information technology (IT) security is very crucial now a days in every organization and NSET has been also using the high security technology service for the IT system. In this regard, NSET is seeking for assessment of its information security services used by NSET. Therefore, NSET is requesting to the submitting of proposal from Information Security Assessment Service provider as following TOR.

2. Objective of the IT Audit

Since operations are highly depends on IT system, IT audit are used to ensure organization assets, endure data integrity, and are associated with overall goals.

The primary objectives of an IT audit are:

- Evaluate the systems and process
- Regulate risk and help identify methods to minimize those risks
- Ensure information management process follow
- Determine inefficiencies in IT system and associated management

3. Audit Scope and Area cover

The audit to be done as per the component mentioned below:

- **Component 1: Vulnerability Assessment and Penetration Testing**
This should at least include
 - Networking and security devices
 - Security and network architecture
 - System and server
 - Web application
- **Component 2: Information System Audit**
This should at least include
 - Documentation review
 - Physical and environmental security review
 - Data center (if) and recovery
 - IT Operation controls
 - Interview with operational team
 - Business continuity
 - Employee awareness in IT
- **Component 3: Social Engineering Audit**
- **Component 4: Trainings (Cyber security, cybercrime, and Social Media)**

4. Procedure

The audit team will start the audit process through the following major phases:

- The audit team should propose the complete plan of audit with a timeline.
- Proposed audit plan can either be for all the components or as per the components.
- The audit team should orient NSET team how each component is conducted.
- If need to visit NSET, audit team must inform NSET in advance.
- Confidentiality to be maintained
- The final report at the end of each component to be submitted to NSET
- The audit report should clearly indicate the flaws and auditor's opinion to minimize the risk.
- After the completion of audit, debriefing meeting is must.

5. Access to NSET

The auditor team will have complete access to system and documents prior to the confidentially sign-up. The team must inform early for visit at NSET office.